AD–A229 245

MILITARY HANDBOOK

ELECTRONIC RELIABILITY

DESIGN HANDBOOK

AMSC N/A   AREA RELI

90 11 28 081

DISCLAIMER NOTICE
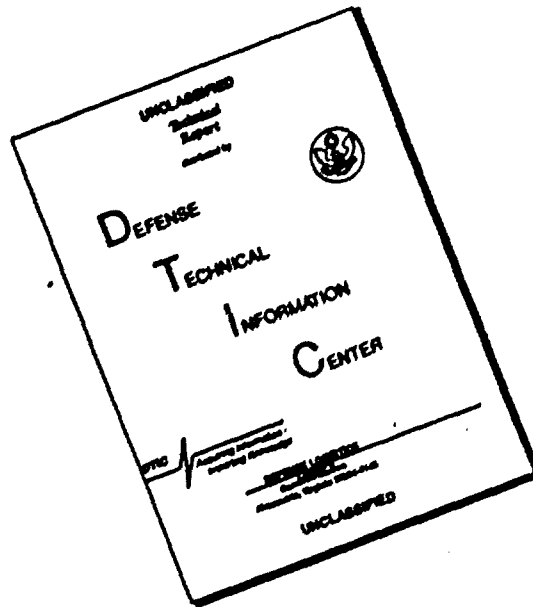
THIS DOCUMENT IS BEST
QUALITY AVAILABLE. THE COPY
FURNISHED TO DTIC CONTAINED
A SIGNIFICANT NUMBER OF
PAGES WHICH DO NOT
REPRODUCE LEGIBLY.

FOREWORD

1. This military Handbook is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: Commander, Rome Air Development Center, AFSC, ATTN: RBE-2, Griffiss Air Force Base, New York 13441-5700, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. Every effort has been made to reflect the latest information on electronic reliability design techniques. It is the intent to review this Handbook periodically to insure its completeness and currency.

4. This Electronic Reliability Design Handbook is an updating and extensive revision of the Reliability Design Handbook, published in 1976 by the Reliability Analysis Center under contract with RADC. The Handbook contains the most up-to-date, practical, pertinent guidelines for use by design engineers, reliability engineers, and managers to design, produce, and deploy reliable and maintainable military electronic equipment/systems at minimum life cycle cost.

5. The basic principles of how to design for sustained performance (reliability) and for the rapid diagnosis and removal of faults (maintainability) have not changed. However, the significant advances made in the twin disciplines of reliability and maintainability (R/M) during the past five years, coupled with the growth of digital systems, the increased usage of complex microcircuits, the looming importance of software, and increased complexity in general, have spawned a large number of new techniques which have been incorporated into the Handbook.

6. The approach taken has been to emphasize the practical aspects of R/M design and management techniques and to concentrate on real world examples which would give the reader insight into how the techniques are applied. The intent was to provide sufficient theoretical and practical information to solve those reliability problems frequently encountered. Some readers may feel that the treatment of the theoretical and mathematical aspects of the subject is inadequate; however, because of the broad coverage of the handbook, some sacrifices had to be made. Furthermore, there are many excellent standard textbooks available (and referenced) which treat the theoretical and mathematical areas in great depth. In addition, through a comprehensive list of reference material, the reader will be able to explore, for himself, aspects of the techniques required by those special problems which inevitably appear.

7. This Handbook describes a comprehensive methodology covering all aspects of electronic system reliability design engineering and cost analysis as they relate to the design, acquisition, and deployment of DOD equipment/systems. Generally, the further into the Handbook one reads, the more technical and detailed the material becomes. The fundamental

concepts are covered early in the Handbook and the details regarding imple-
menting these concepts are discussed primarily in the latter sections.
This format, together with an objective for as much completeness as possi-
ble within each Section, have resulted in some concepts being repeated or
discussed in more than one place in the Handbook. This should help facili-
tate the use of this Handbook for studying certain topics without exten-
sively referring to previous material.

8. In order to keep the Handbook as dynamic and flexible as possible, it
has been published in looseleaf form. Each section, reflecting the current
state-of-the-art for the subject matter covered, is a complete entity and
can stand by itself. Thus, as technology advances occur for each subject
or new subjects become significant, the existing sections can be removed
and revised and new sections added, as appropriate.

9. This Handbook is dedicated in memory of Mr. Joseph J. Naresky whose
untiring effort and dedication pioneered the field of reliability and made
this Handbook a reality. His vast areas of experience, contributions to
and knowledge of reliability theory and techniques have been captured
through innumerable hours Mr. Naresky spent in preparing this text. Joe's
participation and influence in the reliability community will be difficult
to replace.

10. This Handbook constitutes editorial revision of Volume I of MIL-HDBK-
338 dated 15 October 1984. Changes are as follows:

Page	Para/Table/ Figure	Title	Extent of Change
5-8	Figure 5.2.2-1	Shapes of Failure Density, Rel and Hazard Rate Functions for Commonly Used Continuous Distributions	Modified
5-22,5-23	Para 5.2.3	Failure Modeling	Last three paragraphs
7-73	Para 7.5.4	Further Redundancy Considerations	Portions
8-7,8-10	Para 8.3.1.1	Some Pointers on Graphic Methods	Portions
9-4,9-5	Table 9.1-1	Hardware & Software Reliability Difference	All
9-13	Para 9.4	Software Failure Modes	All
9-13,9-14	Para 9.4.1	Specification	All
9-14	Para 9.4.2	Software System Design	All
9-14	Para 9.4.3	Software Code Generation	All
9-16,9-17	Para 9.5.4	Specification Errors	Portions
9-18	Figure 9.5.4-1	Voltage Redundant System	All
9-38,9-39	Para 9.8.4	Program Checking and Testing	Portions
9-43	Para 9.8.5.1	Error Reporting	All
9-43,9-44	Para. 9.8.6	Software Reliability Statistics & Modeling	All
9-48,9-49,9-50	Para 9.8.8	Hardware/Software Interface	All
9-50,9-51	Para 9.8.8.1	Fault Tolerance	All
9-50	Para 9.8.8.1-1	Fault Tolerance Algorithm	All
9-51	Para 9.9	Conclusions	All
9-52	Figure 9.9-1	Software Development for Reliability	All

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF TABLES

LIST OF TABLES

LIST OF TABLES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

MIL-HDBK-338-1A

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

LIST OF FIGURES

1.0 SCOPE

1.1 PURPOSE

This handbook provides procuring activites and development contractors with an understanding of the concepts, principles, and methodologies covering all aspects of electronic systems reliability engineering and cost analysis as they relate to the design, acquisition, and deployment of DoD equipment/systems.

1.2 APPLICATION

This handbook is intended for use by both contractor and government personnel during the conceptual, validation, full scale development, production phases of an equipment/system life cycle.

1.3 ORGANIZATION

The handbook is organized as follows:

SECTION 2	Referenced Documents
SECTION 3	Definitions
SECTION 4	General Statements
SECTION 5	Reliability/Maintainability/Availability Theory
SECTION 6	Reliability Specification, Allocation and Prediction
SECTION 7	Reliability Engineering Design Guidelines
SECTION 8	Reliability Data Collection and Analysis, Demonstration and Growth
SECTION 9	Software Reliability
SECTION 10	Systems Reliability Engineering
SECTION 11	Production and Use (Deployment) R&M
SECTION 12	R&M Management Considerations

2.0 REFERENCED DOCUMENTS

The documents cited in this section are for guidance and information.

2.1 GOVERNMENT DOCUMENTS

SPECIFICATIONS

Military

MIL-E-4158	Electronic Equipment, Ground; General Specification For
MIL-E-5400	Electronic Equipment, Aerospace, General Specifications For
MIL-Q-9858	Quality Program Requirements
MIL-E-16400	Electronic, Interior Communication and Navigation Equipment, Naval Ship and Shore: General Specification For
MIL-E-17555	Electronic and Electrical Equipment, Accessories, and Provisioned Items (Repair Parts) Packaging of
MIL-S-19500	Semiconductor Devices, General Specification For
MIL-M-28787	Modules, Standard Electronic, General Specification For
MIL-M-38510	Microcircuits, General Specification For
MIL-I-45208	Inspection System Requirements
MIL-H-46855	Human Engineering Requirements For Military Systems, Equipment and Facilities
MIL-S-52779	Software Quality Assurance Program Requirements

STANDARDS

Military

MIL-STD-105	Sampling Procedures and Tables for Inspection by Attributes
MIL-STD-210	Climatic Extremes for Military Equipment

MIL-STD-414	Sampling Procedures and Tables for Inspection by Variables for Percent
MIL-STD-454	Standard General Requirements for Electronic Equipment
MIL-STD-470	Maintainability Program Requirements (for Systems and Equipment)
MIL-STD-471	Maintainability Verification/Demonstration/ Evaluation
MIL-STD-499	Engineering Management
MIL-STD-721	Definitions of Terms for Reliability and Maintainability
MIL-STD-750	Test Methods for Semiconductor Devices
MIL-STD-756	Reliability Modeling Prediction
MIL-STD-781	Reliability Testing for Engineering Development, Qualification, and Production
MIL-STD-785	Reliability Program for Systems and Equipments Development and Production
MIL-STD-810	Environmental Test Methods and Engineering Guidelines
MIL-STD-883	Test Methods and Procedures for Micro- electronics
MIL-STD-965	Parts Control Program
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-1556	Government/Industry Data Exchange Program (GIDEP) Contractor Participation Requirements
MIL-STD-1629	Procedures for Performing a Failure Mode Effects and Criticality Analysis
MIL-STD-1670	Environmental Criteria and Guidelines for Air Launched Weapons
DOD-STD-1686	Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices) METRIC

MIL-STD-45662   Calibration Systems Requirements

HANDBOOKS

MIL-HDBK-5	Aerospace Vehicle Structures, Metallic Materials and Elements For
DOD-HDBK-108	Quality Control and Reliability - Sampling Procedures and Tables for Life and Reliability Testing (Based on Exponential Distribution)
MIL-HDBK-189	Reliability Growth Management
MIL-HDBK-217	Reliability Prediction of Electronic Equipment
MIL-HDBK-251	Reliability/Design Thermal Application
DOD-HDBK-263	Electrostatic Discharge Control Handbook for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices) Metric
MIL-HDBK-472	Maintainability Prediction
MIL-HDBK-781	Reliability Testing for Engineering Development, Qualification, and Production

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Naval Publications and Forms Center, (ATTN: NPODS), 5801 Tabor Avenue, Philadelphia PA 19120-5099.)

2.2 OTHER REFERENCED DOCUMENTS

Other referenced documents, government and non-government are listed in other sections of this handbook under "REFERENCES".

3.0 DEFINITIONS

3.1 DEFINITIONS OF BASIC SYSTEM TERMS

3.1.1 SYSTEM EFFECTIVENESS

In Section 4 of this handbook mention is made of the inclusiveness of the concept of system effectiveness. It was first described rather loosely as the ability of the system to do the job for which it was purchased. This was later refined into a more precise definition in terms of availability and dependability. Still another definition might be given as follows:

(1) System effectiveness is the probability that the system can successfully meet an operational demand within a given time when operated under specified conditions.

Effectiveness is obviously influenced by the way the equipment was designed and built. However, just as critical are the way the equipment is used and the way it is maintained. To state this another way, system effectiveness can be materially influenced by the design engineer, the production engineer, the operator, and the maintenance man. It can also be influenced by the logistic system that supports the operation and by the administration through personnel policy, rules governing equipment use, fiscal control, and many other administrative policy decisions.

To apply the general definiton to a "one-shot" device such as a missile, it need only be modified as follows:

(2) System effectiveness is the probability that the system (missile) will operate successfully (kill the target) when called upon to do so under specified conditions.

The major difference between these two definitions lies in the fact that, in Definition 2 (for a one-shot device), time is relatively unimportant. In the first, more general definition, operating time is a critical element and effectiveness is a function of time. Another difference is that the first definition provides for the repair of failures, both at the beginning of the time interval (if the equipment is inoperable then) and also during the operating interval (if a failure occurs after a successful start); the second definition assumes no repair.

Both definitions imply that the system fails: (1) if it is in an inoperable condition when needed; or, (2) if it is operable when needed but fails to complete the assigned mission successfully. The expression "specified conditions" implies that system effectiveness must be stated in terms of the requirements placed upon the system, indicating that failure and use conditions are related. As the operational stresses increase, failure frequency may also be expected to increase.

If continuous operation is required, any cessation due to failure or scheduled maintenance reduces system effectiveness. If the demands on the equipment are such that an on-off use cycle provides significant free time for maintenance, system effectiveness is enhanced. Maintenance of a state of readiness on a continuous basis may (or may not) increase the percentage of equipment which reaches an inoperable condition prior to demand for use. If it does, removal from the readiness state for a portion of time each day might increase effectiveness.

It should also be mentioned that operational requirements sometimes exceed design objectives. A decrease in target vulnerability can result in a decrease in system effectiveness. Surface-to-air missiles designed to be effective against subsonic aircraft can have almost no system effectiveness when called upon to engage supersonic targets.

3.1.2 RELIABILITY

Reliability is the probability that an item will perform its intended function for a specified interval under stated conditions.

A "reliability function" is this same probability expressed as a function of the time period. Thus, reliability relates to the frequency with which failures occur. Here "failure" means "unsatisfactory performance," usually representing a judgment of an operator or a maintenance man. This does not preclude the possibility of clear-cut failure, such as complete inoperability, in which case judgment really does not enter at all.

3.1.3 MISSION RELIABILITY

Mission reliability is defined as the ability of an item to perform its required functions for the duration of a specified "mission profile."

Mission reliability thus defines the probability of non-failure of the system for the period of time required to complete a mission. The probability is a point on the reliability function corresponding to a time equal to the mission length. All possible redundant modes of operation must be considered in describing reliability, mission reliability, and system effectiveness.

3.1.4 OPERATIONAL READINESS AND AVAILABILITY

The capability of a system to perform its intended function when called upon to do so is often referred to by either of two terms: "operational readiness" and "availability." It is the emphasis on the phrase "when called upon" that differentiates this concept from the more general one of system effectiveness. This emphasis restricts attention to probability "at a point in time" rather than "over an interval of time," the latter being descriptive of system effectiveness. It should be noted that sometimes this interval can be extremely long.

There is an additional major difference. System effectiveness includes the built-in capability of the system - its accuracy, power, and so on. Operational readiness excludes these native system characteristics; that is, it excludes the ability of the system to do the intended job and includes only its readiness to do it at a particular time.

In order to differentiate between two separate and useful concepts, it is well to formalize a distinction between the terms "operational readiness" and "availability." It has been apparent in past discussions of system effectiveness that the terms are used by some to represent different concepts but are used almost synonymously by others. Both concepts relate the operating time between failures to some longer time period; they differ in what is to be included in this longer time period. "Availability" is defined in terms of operating time and down time, where down time includes active repair time, administrative time, and logistic time. On the other hand, operational readiness is defined in terms of all of these times, and, in addition, includes both free time and storage time, that is, all calendar time. Availability and operational readiness are defined as follows:

o The availability of a system or equipment is a measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time. (Includes operating time, active repair time, administrative time, and logistic time, but excludes mission time).

o The operational readiness of a system or equipment is the ability of an item (military unit) to respond to its operation plan(s) upon receipt of an operations order. (Total calendar time is the basis for computation of operational readiness.)

3.1.5 DESIGN ADEQUACY

An additional comment with respect to operational readiness and availability is required to emphasize a restriction mentioned above. These two concepts exclude from consideration the built-in capability of a system to do the job for which it is being used. Thus, misapplication of a system is entirely excluded from measurements of system effectiveness.

As an example, the differences between 75mm and 90mm tank guns in range, accuracy, and penetrating power against enemy tanks have a significant bearing on measurements of system effectiveness but are irrelevant to evaluations of their operational readiness and availability.

The characteristic discussed in the preceding paragraph can be identified by the term "system design adequacy." System design adequacy is the probability that a system will successfully accomplish its mission, given that the system is operating within design specifications.

The design may include alternative modes of operation, which are equivalent to built-in automatic repair, usually with allowable degrad-ation in performance. These alternative modes of operation are, of course,

included in the definition of system design adequacy. The probability itself is a function of such variables as system accuracy under the conditions of use, the mission to be accomplished, the design limits, system inputs, and the influence of the operator.

3.1.6 REPAIRABILITY

Repairability is defined as the probability that a failed system will be restored to operable condition in a specified active repair time.

It is useful to express this probability in two forms, the probability density function and the cumulative distribution function. These are called the active repair time density function and the repairability function, respectively. The repairability function expresses the probability that the active repair time does not exceed any given total time.

3.1.7 MAINTAINABILITY

Maintainability is defined as the measure of the ability of an item to be retained in, or restored to specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.

This is directly analogous to repairability. The difference is merely that maintainability is based on total downtime (which includes active repair time, logistic time, and administrative time), while repairability is restricted solely to active repair time.

The analogy holds with respect to the associated functions as well. The maintainability function is the cumulative probability that the failed system is restored to operable condition in not more than a specified downtime, expressed as a function of this downtime. The corresponding density function is called the maintenance time density function. These probability functions will be described in greater detail in the next chapter.

3.1.8 SERVICEABILITY

Intuitively, it would seem that some term should be used to represent the degree of ease or difficulty with which equipment can be repaired. The term "serviceability" has been selected for this concept. Serviceability has a strong influence on repairability, but the two are essentially different concepts. Serviceability is an equipment design characteristic, while repairability is a probability involving certain categories of time.

Although the definition of serviceability is stated in a manner that suggests a quantitative concept, it is often necessary to accept a qualitative evaluation of the serviceability of an equipment. The definition as given does accentuate the idea that comparison of equipments can yield a conclusion that "Equipment A is more serviceable than Equipment B."

Actually, this kind of conclusion may be entirely satisfactory, since the numerical evaluation can be made when repairability is measured. That is to say, the better the serviceability, the shorter the active repair time. Hence, repairability is a reflection of serviceability even though the two concepts are quite distinct.

Serviceability is dependent on many hardware characteristics, such as engineering design, complexity, number and accessibility of test points, and the like. These characteristics are under engineering control, and poor serviceability traceable to such items is the responsibility of design engineers. However, many other characteristics which can cause poor serviceability are not directly under the control of the design engineers. These include lack of proper tools and testing facilities, shortage of work space in the maintenance shop, poorly trained maintenance personnel, shortage of repair parts, and other factors that can increase the difficulties of maintenance.

3.1.9 INTRINSIC AVAILABILITY

It is also useful to define another term, "intrinsic availability."

The intrinsic availability of a system or equipment is the probability that it is operating satisfactorily at any point in time when used under stated conditions, where the time considered is operating time and active repair time.

Thus, intrinsic availability excludes from consideration all free time, storage time, administrative time, and logistic time. As the name indicates, intrinsic availability refers primarily to the built-in capability of the system or equipment to operate satisfactorily under stated conditions.

The effect of these definitions, is essentially to allow realistic assignment of responsibility in case an unsatisfactory situation exists. If an improvement in intrinsic availability is required, responsibility can properly be assigned to the design and production engineers - assuming, of course, that the operating conditions are compatible with design specifications. On the other hand, if availability is unsatisfactory and improvement in intrinsic availability is not indicated, the responsibility is properly placed on the commander or civilian administrator to effect the required improvement by reducing administrative and logistic delay. If neither of these steps is indicated and operational readiness is not satisfactory, improvement depends on changes in free time and storage time, implying more efficient use of the system equipment.

3.2 DEFINITIONS OF TIME CONCEPTS

Time is of fundamental importance in the quantification of the basic terms which were defined in the previous section, for it is this factor which permits the attributes to be measured rather than described in merely qualitative terms. The usual measures of time - the year, the month, the day, and the hour - form the basis for the computation of reliability. Where appropriate, the time concepts may be replaced by distance, cycles, operations or other quantities.

In general, the interval of interest is the total calendar time during which an item or system is in use. As shown in Figure 3.2-1, this interval may be divided into required time and non-required time. Let's walk down Figure 3.2-1 and define the terms. Active time is that during which an item is in an operational inventory; inactive time is that during which an item is in reserve. Active time may be further broken down into uptime (during which an item is in a condition to perform a required function) and downtime (during which an item is not in a condition to perform a required function). Downtime may be further subdivided into maintenance time (that downtime which excludes modification and delay time), modification time (that downtime necessary to introduce any specific change(s) to an item to improve its characteristics, or to add new ones), and delay time (that downtime during which no maintenance is being accomplished on the item because of either supply or adminstrative delay. Delay time may be further subdivided into supply delay time (that element of delay time during which a needed replacement item is being obtained) and adminstrative time (that element of delay time not included in supply delay time).

Maintenance time can be broken down into corrective maintenance time (during which corrective maintenance is performed on an item), and preventive maintenance time (during which preventive maintenance is performed on an item).

Uptime (left side of Figure 3.2-1) can be further subdivided into: not operating time (during which the item is not required to operate), alert time (during which an item is assumed to be in specified operating condition, and is awaiting a command to perform its intended mission), reaction time (that element of uptime needed to initiate a mission, measured from the time command is received), and mission time (during which an item is required to perform a stated mission profile).

Details as to how these time elements are combined to produce the different measures of system characteristics will be discussed in later sections of this handbook.

The system and time concepts introduced in this chapter and their definitions are summarized in Tables 3.2-1 and 3.2-2.

3.3 ADDITIONAL TERMS

The definitions of terms not called out herein shall be in accordance with MIL-STD-721 and DoD Directive 5000.40.
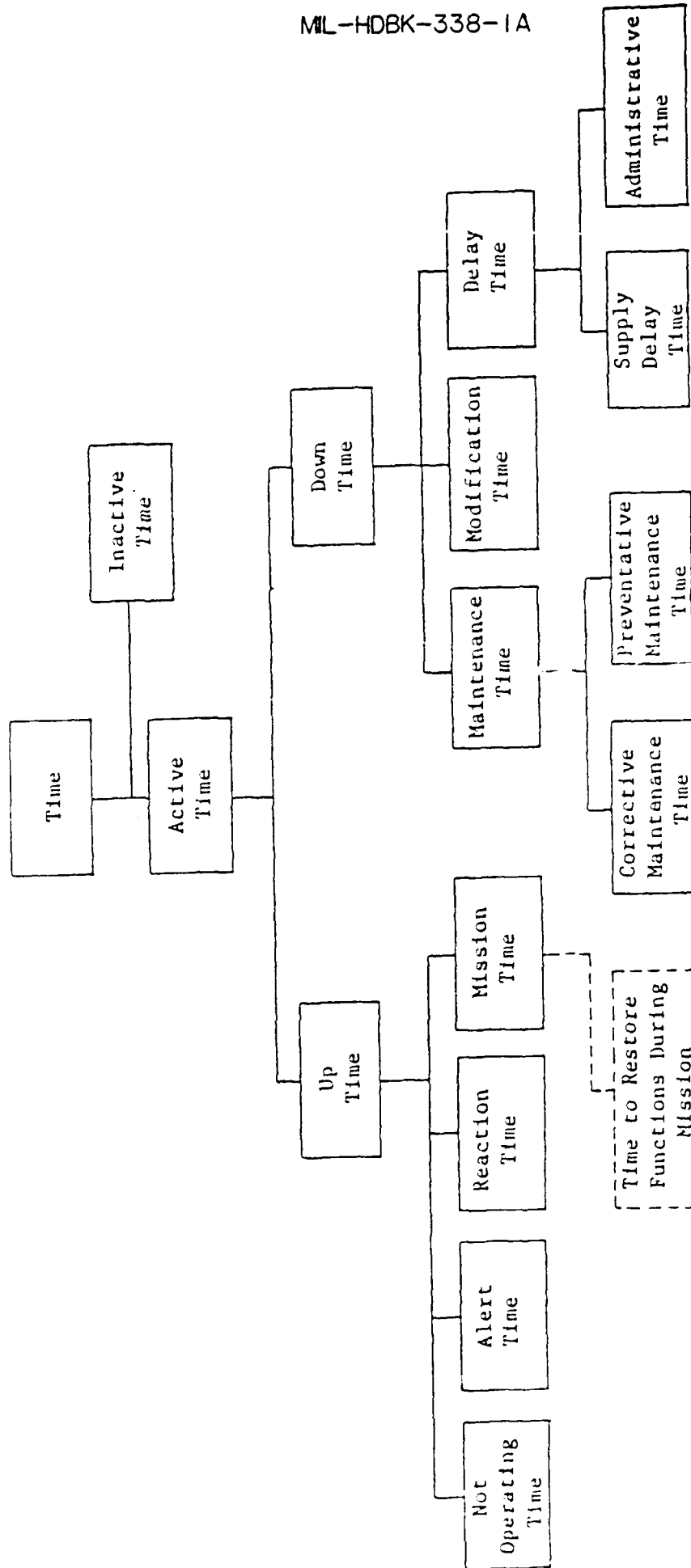
FIGURE 3.2-1: TIME RELATIONSHIPS (MIL-STD-721)

TABLE 3.2-1: DEFINITIONS OF BASIC SYSTEM TERMS

System -	A composite, at any level of complexity, of operational and support equipment, personnel, facilities and software which are used together as an entity and capable of performing and supporting an operational role.
System Effectiveness -	is the probability that the system can successfully meet an operational demand within a given time when operated under specified conditions.
System Effectiveness -	(for a one-shot device such as a missile) is the probability that the system (missile) will operate successfully (kill the target) when called upon to do so under specified conditions.
Reliability -	is the probability that an item will perform its intended function for a specified interval under stated conditions.
Mission Reliability -	is the ability of an item to perform its required functions for the duration of a specified mission profile.
Operational Readiness -	is the ability of an item (military unit) to respond to its operational plan(s) upon receipt of an operating order (total calendar time is the basis for computation of operational readiness).
Availability -	is a measure of the degree to which an item is in an operable and committable state at the start of a mission when the mission is called for at an unknown (random) time (includes operating time, active repair time, adminstrative time, and logistic time, but excludes mission time).
Intrinsic Availability -	is the probability that the system is operating satisfactorily at any point in time when used under stated conditions, where the time considered is operating time and active repair time.

TABLE 3.2-1: DEFINITIONS OF BASIC SYSTEM TERMS (Cont'd)

Design Adequacy -	is the probability that the system will successfully accomplish its mission, given that the system is operating within design specifications.
Maintainability -	is the measure of the ability of an item to be retained in, or restored to, specified condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair.
Repairability -	is the probability that a failed system will be restored to operable condition within a specified active repair time.
Serviceability -	is the degree of ease or difficulty with which a system can be repaired.

TABLE 3.2-2: DEFINITIONS OF TIME CATEGORIES

Active Time -	The period of time during which an item is in an operational inventory.
Inactive Time -	The period of time during which an item is in reserve.
Uptime -	The period of time during which an item is in a condition to perform a required function.
Downtime -	The period of time during which an item is not in a condition to perform a required function.
Maintenance Time -	That part of downtime which excludes modification and delay time.
Modification Time -	That part of downtime necessary to introduce any specific change(s) to an item to improve its characteristics, or to add new ones.
Delay Time -	That part of downtime during which no maintenance is being accomplished on the item because of either supply or administrative delay.
Supply Delay Time -	That element of delay time during which a needed replacement item is being obtained.

TABLE 3.2-2: DEFINITIONS OF TIME CATEGORIES (Cont'd)

Administrative Time -	That element of delay time not included in supply delay time.
Corrective Maintenance Time -	That part of the maintenance time during which corrective maintenance is performed on an item.
Preventive Maintenance Time -	That part of the maintenance time during which preventive maintenance is performed on an item.
Not Operating Time -	That element of uptime during which an item is not required to operate.
Alert Time -	That element of uptime during which an item is assumed to be in specified operating conditions, and is awaiting a command to perform its intended mission.
Reaction Time -	That element of uptime needed to initiate a mission, measured from the time command is received.
Mission Time -	That element of uptime during which an item is required to perform a stated mission profile.

4.0 GENERAL STATEMENTS

4.1 INTRODUCTION AND BACKGROUND

For all but the most recent years of human history, the performance expected from man's implements was quite low and the life realized was long, both because it just happened to be so in terms of man's lifetime and because he had no reason to expect otherwise. The great technological advances, beginning in the latter half of the twentieth century, have been inextricably tied to more and more complex implements or devices. In general, these have been synthesized from simpler devices having a satisfactory life. It is a well known fact that any device which requires all its parts to function will always be less stable than any of its parts. Although significant improvements have been made in increasing the lives of basic components - for example, microelectronics - these have not usually been accompanied by corresponding increases in the lives of equipment and systems. In some cases, equipment and system complexity has progressed at so rapid a pace as to negate, in part, the increased life expected from use of the longer-lived basic components. In other cases, the basic components have been misapplied or overstressed so that their potentially long lives were cut short. In still other cases, management has been reluctant to devote the time and attention necessary to ensure that the potentially long lives of the basic components were achieved.

The military services, because they had the most complex systems and hence the most acute problems, provided the impetus to the orderly development of the discipline of reliability engineering. It was they who were instrumental in developing mathematical models for reliability, as well as design techniques to permit the quantitative specification, prediction and measurement of reliability.

Reliability engineering is the doing of those things which insure that an item will perform its mission successfully. The discipline of reliability engineering consists of two fundamental aspects:

(1) paying attention to detail
(2) handling uncertainties.

The traditional, narrow definition of reliability (Ref. MIL-STD-721) is "the probability that an item can perform its intended function for a specified interval under stated conditions."

This narrow definition is applicable largely to items which have simple missions, e.g., equipment, simple vehicles, or components of systems. For large complex systems (e.g., command and control systems, aircraft weapon systems, a squadron of tanks, naval vessels), it is more appropriate to use more sophisticated concepts such as "system effectiveness" to describe the worth of a system. A more precise definition of system effectiveness and the factors contributing to it are presented in Section 3. For the present, it is sufficient to observe that system effectiveness relates to that property of a system output which was the real reason for buying the

system in the first place - namely, the carrying out of some intended function.   If the system is effective, it carries out this function well.   If it is not effective, attention must be focused on those system attributes which are deficient.

4.2 THE SYSTEM RELIABILITY PROBLEM

In the past, the military services in the acquisition of systems have tended to emphasize the achievement of the ultimate in system performance. Unless adequate funds and time were available, such as was the case of space and missile systems in the 1950's and '60's, adequate emphasis and support was not given to reliability and maintainability design.   This, coupled with the necessity to acquire increasingly complex and sophisticated weapon systems in order to meet the potential threat, resulted in the deployment of systems which exhibited low field reliability and maintainability. This was particularly true of avionic systems which were, on the average, achieving approximately 10% of the specified reliability. This, in turn, resulted in increased operation and support (0 & S) costs.   Thus, it was found that, although the reliability of the individual component parts had been improving at the rate of about 15-20% per year for two decades, the field reliability of complex systems seemed to remain constant. This was due to the fact that more components were being "crammed" into each new system to provide more capability; that is, more capability during those interludes when the system actually performed its function.

This problem became readily apparent during the late '60's and early '70's when it was found (Ref. 1) that the annual support costs for military electronics were equal to the annual procurement costs and constituted more than one-third of all annual expenditures on military electronics.   The problem was further exacerbated by the increased acquisition costs of complex weapon systems as shown in Figure 4.2-1 for combat aircraft. It shows an average cost growth rate of about 12% per year.   Though the electronics content varies for aircraft to aircraft, the average electronics fraction of total aircraft cost had increased from about 10-20 percent in the 1950's to 20-30 percent in the late 1960's and early 1970's.   Thus, the new generation avionics cost increased at a rate of, perhaps, 18 percent per year, more rapidly than the new generation aircraft cost.   Though combat aircraft were used as an example, similar trends exist in other weapon systems.

Thus, the trend for the future (if unchecked) would be for the costs of comparable weapon systems to increase, on the average, by 12% per year (or 3 to 1 per decade), the average cost of the electronics in a weapon system to increase by 18% per year (or 5 to 1 per decade), and the reliability of the electronics on a per part basis to increase, in the average by 15% per year (4 to 1 per decade) (Ref. 1).

In fact, with continuing inflation, the average cost trend for future systems may well exceed the previously mentioned figures. For example, as is shown in Figures 4.2-2 and 4.2-3, for new generation systems developed over the past several decades, the average cost of weapon systems increased by a factor of 5 to 1 per decade, and the average cost of electronic subsystems increased by a factor of 10 to 1.
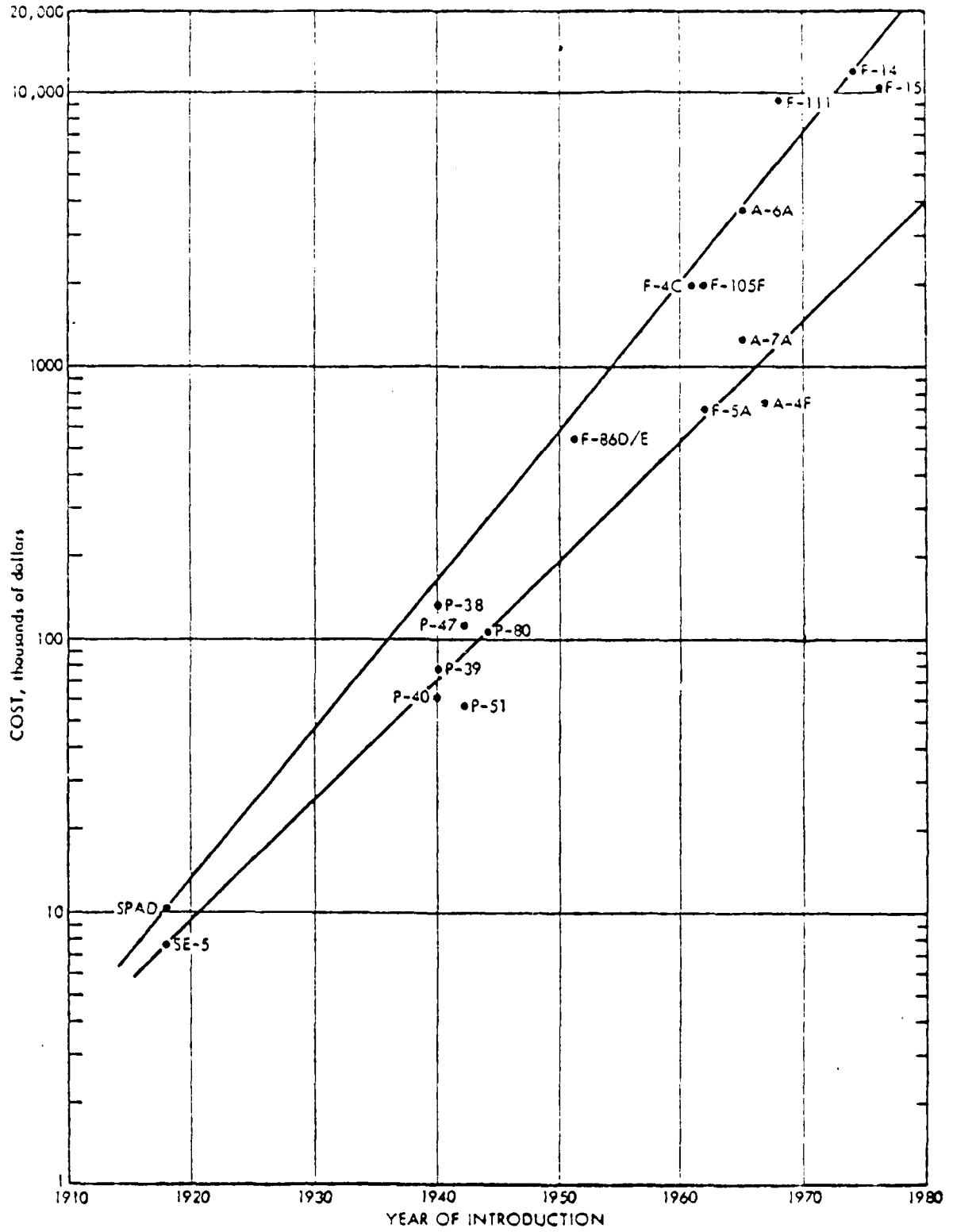
FIGURE 4.2-1: COST OF COMBAT AIRCRAFT (REF. 1)
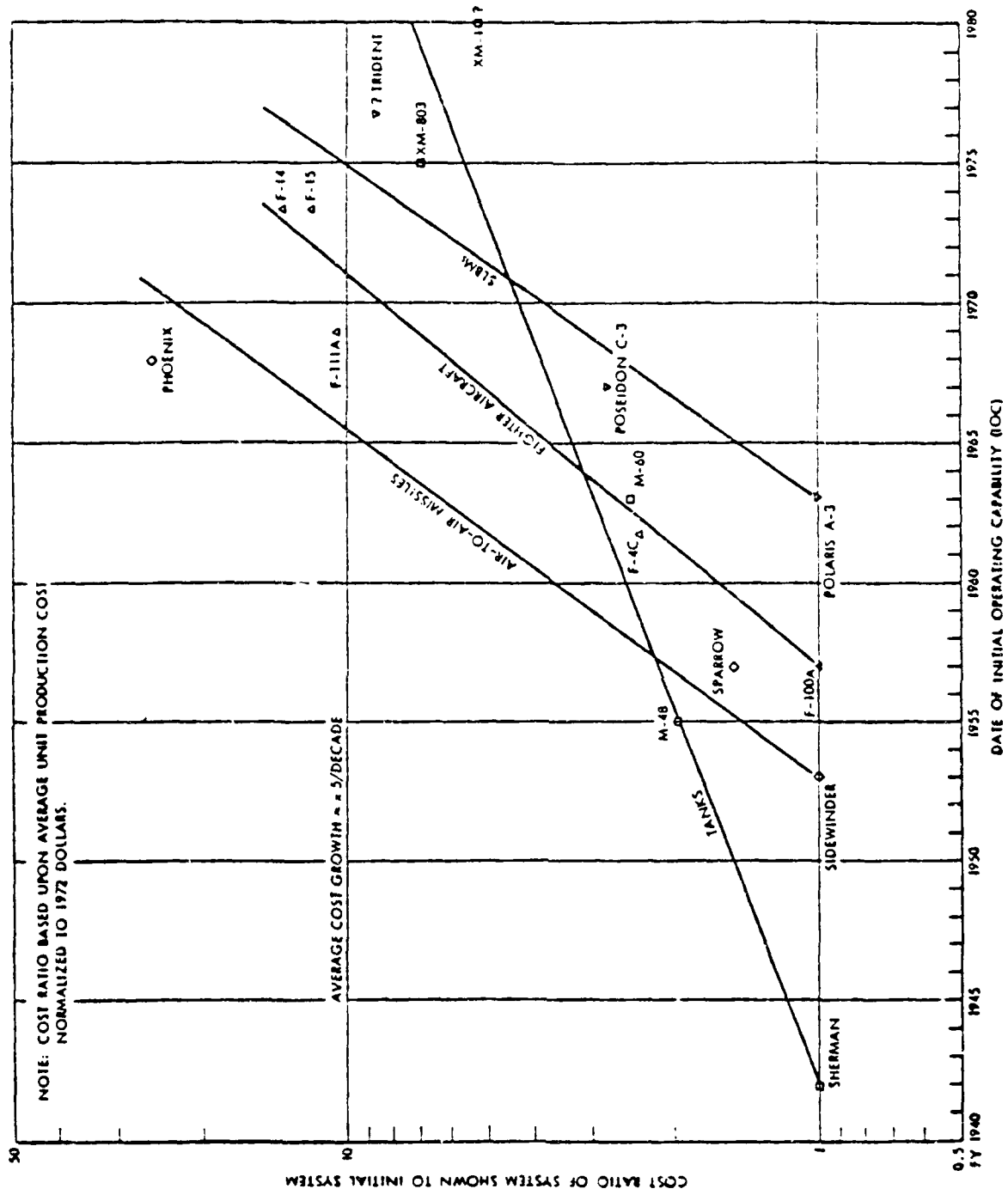
FIGURE 4.2-2: NEW-GENERATION COST PROGRESSION FOR SYSTEMS SHOWN (REF. 1)
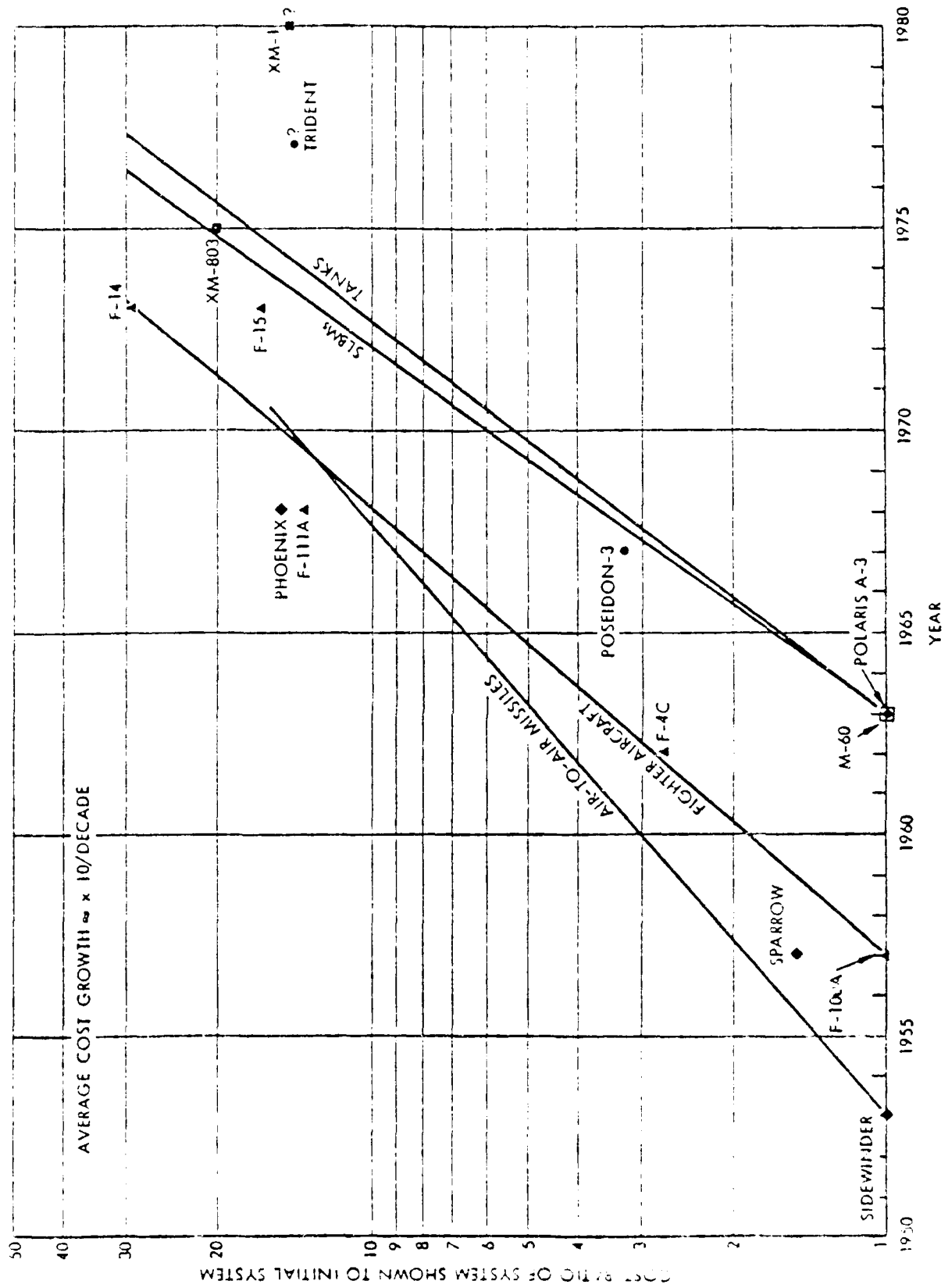
FIGURE 4.2-3: NEW-GENERATION ELECTRONIC SUBSYSTEM COST PROGRESSION
FOR SYSTEMS SHOWN (REF. 1)

The relationship between unit production cost and field reliability is illustrated for Air Force avionics equipment by Figure 4.2-4. The data includes tube, transistor, integrated circuit and hybrid equipments of various vintages. Both cost and reliability are functions of equipment complexity. As complexity increases, cost increases, and reliability, as measured by mean flight hours between failures (MFHBF), decreases. Thus, Figure 4.2-4 shows a median relationship* in which:

$$MFHBF = 1.3 \times 10^6 / cost \text{ (in dollars)}$$

*A similar relationship based on limited data is found for Army Area Communications Systems (AACOMS): Field MTBF $= 10^7$/cost (in dollars).

From this, one might reach the paradoxical conclusion that as system cost increases, reliability decreases. This is not entirely true. If one further analyzes the data in Figure 4.2-4, several potential solutions to the seeming paradox become evident. The first of these derives from the empirically observed trend (which makes intuitive sense) that reliability goes down when unit production cost (a function of complexity) goes up. An equipment of half the unit production cost (and, consequently, half the complexity) of another unit can be expected to have twice its reliability. This suggests that if the performance requirements can be reduced to those which are absolutely essential, and, perhaps, even reduced somewhat, the costs will go down and the reliability up.

The second observation to be made from Figure 4.2-4 is that there is substantial spread in the results: certain equipments were three or more times as reliable in the field than the median. Among these are three data points that deserve special attention. All three represent cost versus reliability for avionic equipments that underwent special programs for the development of reliability. (The results of the three are not directly comparable to each other because of differences in operating environment and methods of reliability measurements.) The point R represents the General Electric AN/APQ-113 radar for the F-111 aircraft. The point WL represents the Bendix RDR-1F weather radar used by commercial airlines and maintained by the supplier under contractor maintenance warranty. The point WF represents the Delco Carousel IV inertial navigator used by commercial airlines and the U.S. Air Force and also required to be maintained under warranty. For these it can be deduced that there existed design, workmanship, and parts selection criteria and development approaches that yielded very superior results, and it may be inferred that these approaches can be found for other systems and applied, if there is adequate incentive to do so.

Thus, faced with shrinking weapons purchasing power, marginal operational readiness rates, and the soaring costs of operating and maintaining modern weapons systems, the DOD (Director of Defense Research and Engineering) initiated the Electronics-X Project (Ref. 1) at the Institute for Defense Analyses (circa 1973) with the purpose of reviewing the process of acquisition and maintenance of military electronics, recommending specific policies and procedures to remedy the situation.
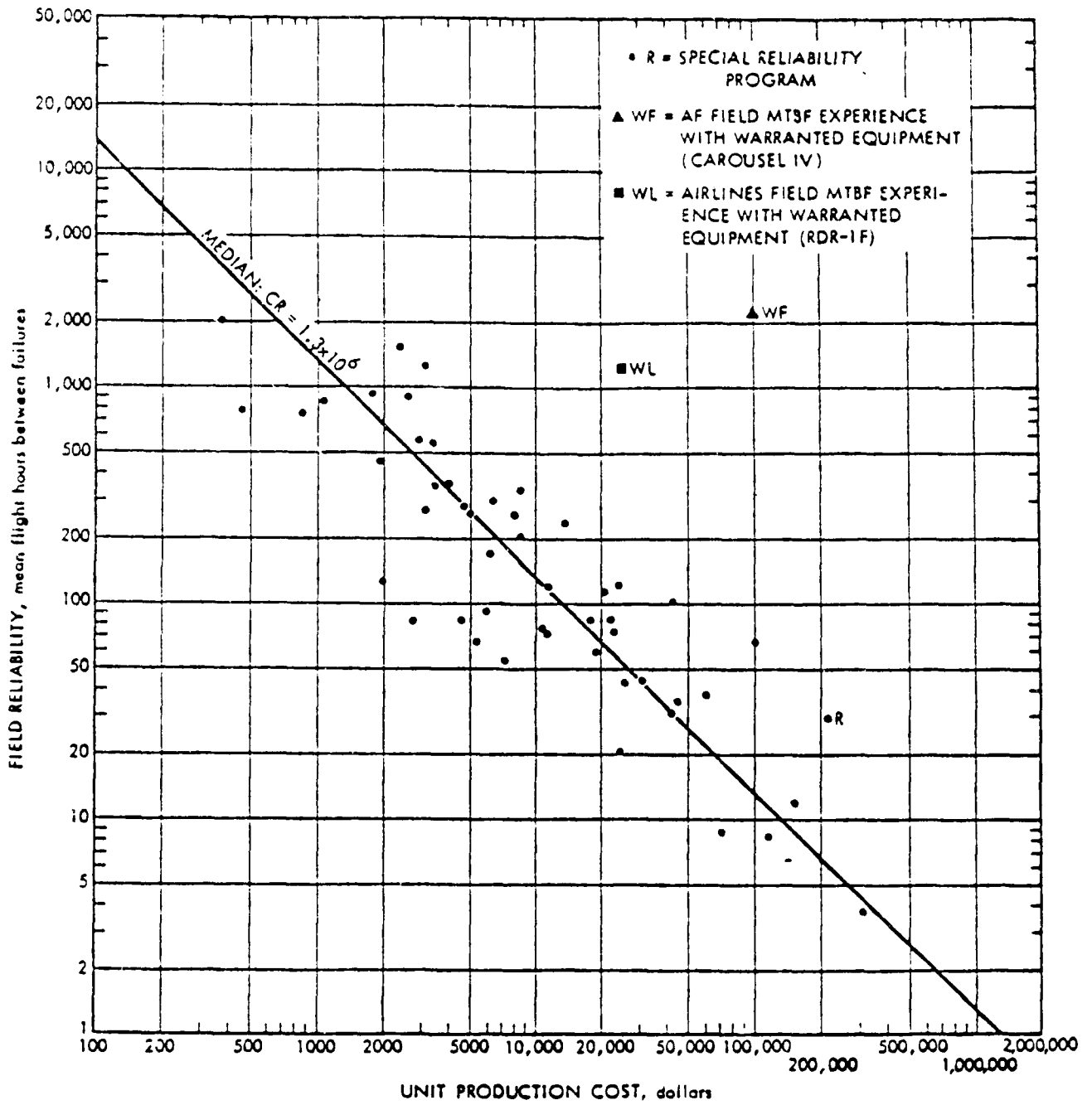
FIGURE 4.2-4: AVIONICS FIELD RELIABILITY VERSUS UNIT PRODUCTION COST (REF. 1)

The Electronics-X Final Report resulted in a number of recommendations to the DOD on procedures for improving the reliability of military electronic systems. Some of these have been implemented; other are in the process of being implemented. One example of this implementation is DOD Directive 5000.40, "Reliability and Maintainability," published in July 1980, (Ref. 7) which directs, among other things, that adequate funds and time be made available for front-end investment in reliability and maintainability design in order to minimize system life cycle costs.

With the increased emphasis, both in Congress and the military services, on reducing life cycle costs of weapons systems, the disciplines of reliability and maintainability will receive more emphasis in the 1980's than they have over the past couple of decades. The reason is simple. No matter how spectacular the performance, the system is useless to the operational commander in the field if it is not flyable or launchable. The goal of reduced life cycle costs may, for certain system developments, take priority over the achievement of maximum system performance. A recent example of this is the Navy F/A-18 aircraft in which reliability and maintainability were emphasized, and no attempt was made to match the performance of the F-14. After 2000 hours of testing, it has demonstrated a mean flight hours between failures of 3 hours, which is three times better than the fleet operating average.

Thus, the decade of the 1980's may, of necessity, be the decade of reliability; the dilemma of the decade will be that of determining optimum system performance versus reliability tradeoffs. In order to make a contribution to the determination of such tradeoffs, the reliability engineer must do more than merely collect data and perform actuarial services during the design, development, and field use of equipment. He must be sensitive to the countless decisions made during the evolution of a product, and he must assist in making these decisions. The reliability engineer has a responsibility to build specific amounts of longevity into equipment. He must be able to trade off the reliability parameters against the many other important parameters such as cost, weight, size, and scheduling. Great emphasis is placed on failures whose cause can be eliminated. Reliability mathematics must reflect the engineering search for causes of failure and the adequacy of their elimination. It must permit a reliability prediction from the planning phase through the field-use phase to assure that failure probability does not exceed a permissible bound. Reliability is a quantitative probabilistic factor, which must be predictable in design, measurable in tests, assurable in production and maintainable in the field. In short, it must be controllable throughout the life cycle of the product. Other system characteristics, such as maintainability and safety, also affect the mission performing equipment and its related subsystems, including maintenance and support equipment, checkout and servicing, repair parts provisioning and actual repair functions. Thus, reliability and other design considerations provide the basis for developing adequate systems which conform to mission objectives and requirements. This overall program is called system engineering.

4.3 THE SYSTEM ENGINEERING PROCESS

In recent years, the word system has come to include:

(1) the prime mission equipment
(2) the facilities required for operation and maintenance
(3) the selection and training of personnel
(4) operational and maintenance procedures
(5) instrumentation and data reduction for test and evaluation
(6) special activation and acceptance programs
(7) logistic support programs

System engineering (Ref. MIL-STD-499) is the application of scientific, engineering, and management effort to:

(1) Transform an operational need into a description of system performance parameters and a system configuration through the use of an iterative process of definition, synthesis, analysis, design, test, and evaluation.

(2) Integrate related technical parameters and assure compatibility of all physical, functional, and program interfaces in a manner that optimizes the total system design.

(3) Integrate reliability, maintainability, safety, survivability (including electronic warfare considerations), human factors, and other factors into the total engineering effort.

From the system management viewpoint, system engineering is but one of five major activities required to develop a system from the initial, conceptual phase through the subsequent validation, full scale development, production, and deployment phases. These five activities (procurement and production, program control, configuration management, system engineering, and test and deployment management), their general functions within each of the system evolutionary phases, and their relationships to one another are summarized in Figure 4.3-1.

System engineering consists of four steps in an interacting cycle (Figure 4.3-2). Step 1 considers threat forecast studies, doctrinal studies, probable military service tasks, and similar sources of desired materiel and system objectives; then it translates them into basic functional requirements or statements of operation. The usual result of Step 1 is a set of block diagrams showing basic functional operations and their relative sequences and relationships. Even though hardware may help shape the basic system design, it is not specifically included in Step 1. Step 1 is intended to form a first hypothesis as a start toward the eventual solution.

In Step 2, the first hypothesis is evaluated against constraints such as design, cost, and time and against specific mission objectives to create criteria for designing equipment, defining intersystem interfaces, defining facilities, and determining requirements for personnel, training, training equipment and procedures.
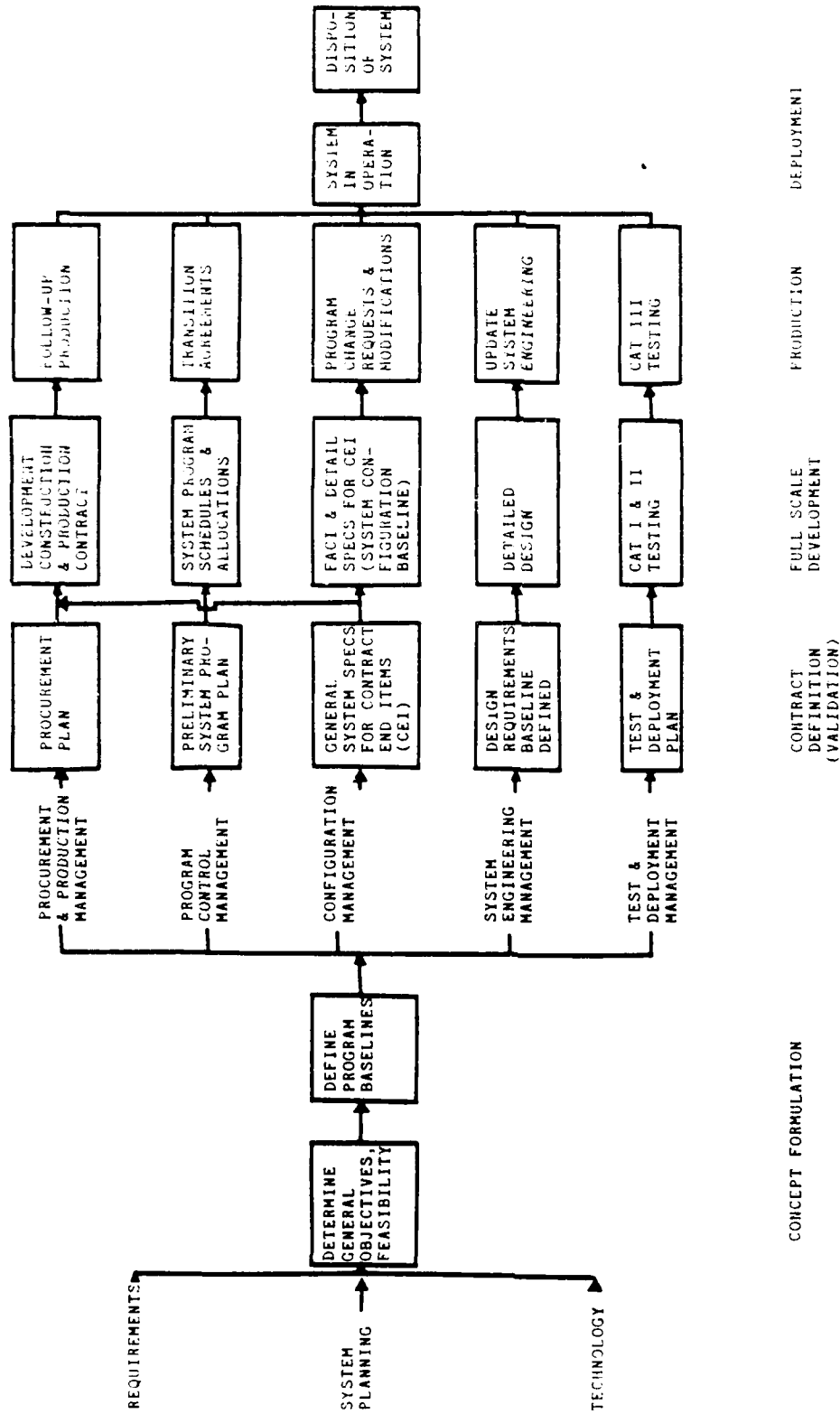
FIGURE 4.3-1: SYSTEM MANAGEMENT ACTIVITIES
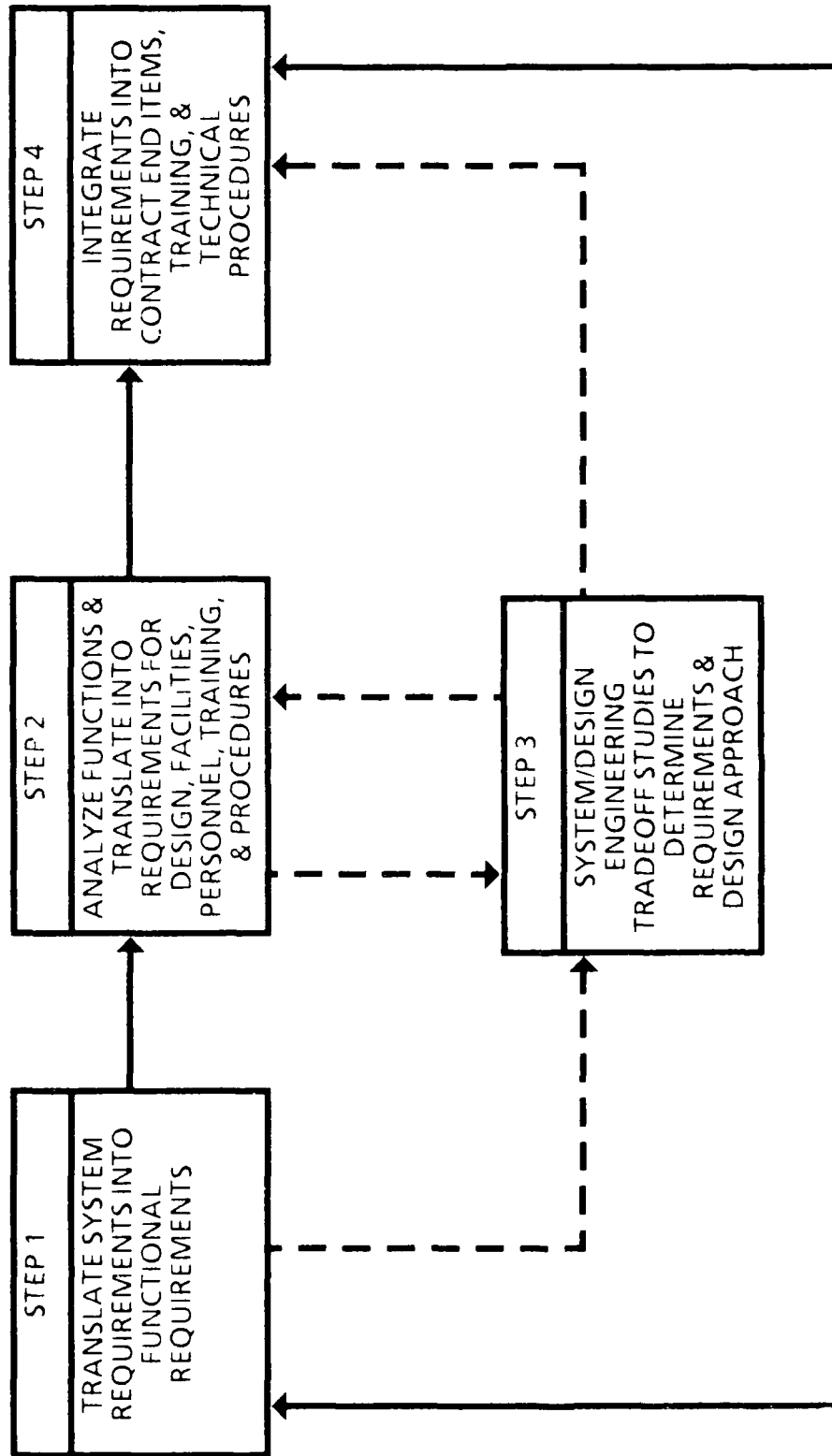
FIGURE 4.3-2: FUNDAMENTAL SYSTEM PROCESS CYCLE

STEP 4
INTEGRATE REQUIREMENTS INTO CONTRACT END ITEMS, TRAINING, & TECHNICAL PROCEDURES

STEP 2
ANALYZE FUNCTIONS & TRANSLATE INTO REQUIREMENTS FOR DESIGN, FACILITIES, PERSONNEL, TRAINING, & PROCEDURES

STEP 3
SYSTEM/DESIGN ENGINEERING TRADEOFF STUDIES TO DETERMINE REQUIREMENTS & DESIGN APPROACH

STEP 1
TRANSLATE SYSTEM REQUIREMENTS INTO FUNCTIONAL REQUIREMENTS

Step 3 consists of system design studies that are performed concurrently with Steps 2 and 4 to:

(1) Determine alternate functions and functional sequences
(2) Establish design personnel, training and procedural data requirements imposed by the functions
(3) Find the best way to satisfy the mission requirements
(4) Select the best design approach for integrating mission requirements into the actual hardware and related support activities.

Normally, the studies in Step 3 involve tradeoffs where data are in the form of schematic block diagrams, outline drawings, intersystem and intrasystem interface requirements, comparative matrices, and data supporting the selection of each approach. Some of the scientific tools used in the system design studies in Step 3 are: probability theory, statistical inference, simulation, computer analysis, information theory, queuing theory, servomechanism theory, cybernetics, mathematics, chemistry, and physics.

Step 4 uses the design approach selected in Step 3 to integrate the design requirements from Step 2 into the Contract End Items (CEI's). The result of Step 4 provides the criteria for detailed design, development, and test of the CEI based upon defined engineering information and associated tolerances. Outputs from Step 4 are used to:

(1) Determine intersystem interfaces
(2) Formulate additional requirements and functions that evolve from the selected devices or techniques
(3) Provide feedback to modify or verify the system requirements and functional flow diagrams prepared in Step 1.

When the first cycle of the system engineering process is completed, the modifications, alternatives, imposed constraints, additional requirements, and technological problems that have been identified are recycled through the process with the original hypothesis (initial design) to make the design more practical. This cycling is continued until a satisfactory design is produced, or until available resources (time, money, etc.) are expended and the existing design is accepted, or until the objectives are found to be unattainable.

Other factors that are part of the system engineering process - such as reliability, maintainability, safety, and human factors - exist as separate but interacting engineering disciplines and provide specific inputs to each other and to the overall system program. Pertinent questions at this point might be: "How do we know when the design is adequate?" or "How is the effectiveness of a system measured?" The answers to these questions lead to the concept of system effectiveness.

4.4 SYSTEM EFFECTIVENESS

System effectiveness is a measure of the ability of a system to achieve a set of specific mission requirements. It is a function of readiness (or availability), and mission success (or dependability) (Ref. MIL-STD-721).

Cost and time are also critical in the evaluation of the merits of a system or its components, and must eventually be included in making administrative decisions regarding the purchase, use, maintenance, or discard of any equipment or system.

The operational effectiveness of a system obviously is influenced by the way the equipment was designed and built. It is, however, just as influenced by the way the equipment is used and maintained; i.e., system effectiveness is influenced by the designer, production engineer, maintenance man, and user/operator. The concepts of availability and dependability illustrate these influences and their relationships to system operational effectiveness. MIL-STD-721 provides the following definitions of these concepts:

(1) Availability. A measure of the degree to which an item is in an operable and committable state at the start of a mission, when the mission is called for at an unknown (random) time.

(2) Dependability. A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission.

Dependability is related to reliability; the intention was that dependability would be a more general concept then reliability.

4.4.1 R/M CONSIDERATIONS IN SYSTEM EFFECTIVENESS

From a system effectiveness viewpoint, reliability and maintainability jointly provide system availability and dependability. Increased reliability directly contributes to system uptime, while improved maintainability reduces downtime. If reliability and maintainability are not jointly considered and continually reviewed, serious consequences may result. With military equipment, failures or excessive downtime can jeopardize a mission and possibly cause a loss of lives. Excessive repair time and failures also impose burdens on logistic support and maintenance activities, causing high costs for repair parts and personnel training, expenditure of many manhours for actual repair and service, obligation of facilities and equipment to test and service, and to movement and storage of repair parts.

From the cost viewpoint, reliability and maintainability must be evaluated over the system life cycle, rather than merely from the standpoint of initial acquisition. The overall cost of ownership has been estimated to be from three to twenty times the original acquisition cost (Ref. 5). Although these cost of ownership figures have been accepted for years, and seem intuitively reasonable, there have been very few case histories published which would tend to validate them. In fact, it was pointed out in Reference 1 that, "DOD appears to have no cost accounting system capable of providing data on full life cycle costs of any electronic subsystems." An effective design approach to reliability and maintainability can reduce this cost of upkeep.

Both reliability and maintainability are important considerations for the user of the system, although maintainability is probably more important from his point of view. Although frequent system failures may be an annoyance, if each failure can be repaired in a very short time so that the system has a high availability, then the poor reliability may be acceptable. For example, if failures occur on the average of every fifteen minutes but can be repaired in a microsecond, the user will not be too concerned. On the other hand, if repair of a failure takes hours or days, the user has a non-available weapon system which may have a significant effect on the operational commander's readiness posture.

4.5 FACTORS INFLUENCING SYSTEM EFFECTIVENESS

4.5.1 EQUIPMENT OF NEW DESIGN

A typical history of the development of a new equipment would reveal a number of interesting steps in the progression from original concept to acceptable production model. These steps are particularly marked if the equipment represents a technical innovation, i.e., if it "pushes the state of the art" by introducing entirely new functions or by performing established functions in an entirely new way. Starting with a well-defined operational need, the research scientist, designer, reliability engineer, statistician, and production engineer all combine their talents to execute a multitude of operations leading to one ultimate objective: the production of an equipment that will perform as intended, with minimum breakdowns and maximum speed of repair. All this must be done at minimum cost and usually within an accelerated time schedule.

These program requirements are severe, to say the least. In order to meet them, many compromises are required. One of the first of these compromises is often a sharp curtailment in the basic research time allotted to the job of proving the feasibility of the new design. After only brief preliminary study, a pilot model of the equipment is built. With luck, it will work; but it is likely to be somewhat crude in appearance, too big and too heavy, not well-designed for mass production, subject to frequent failure, and difficult to repair. Indeed, at this early stage in the program, it is quite possible that the first model might be incapable of working if it were taken out of the laboratory and subjected to the more severe stresses of field operation, whether this be military or civilian. By the time this situation is corrected, the development program will have included many design changes, part substitutions, reliability tests, and field trials, eventually culminating in a successful operational acceptance test.

Usually, it is not until the equipment appears to have some chance of reaching this ultimate goal of acceptance that attention is focused on reduction of the frequency of failure, thus providing the impetus for a serious reliability effort. Experience has shown that this is unfortunate. Ideally, such an effort should begin immediately after the feasibility study, because some problems can be eliminated before they arise, and others can be solved at an early development stage, when design modifications can be effected most easily and economically. Even

with this early start, reliability will continue to be a primary problem in new equipment, especially when it is of novel design. Early neglect of reliability can only be compensated for by extraordinary efforts at a later period. Since such early neglect has been common in the past, reliability has received strong emphasis in the research designed to bring equipment performance characteristics up to satisfactory levels.

The description just given is generally applicable to the development of radically new equipment. However, when attention is directed to equipment in everyday use or to new equipment built predominantly on standard design principles and from well-tested parts, it becomes evident that effectiveness is dependent not only on performance capabilities and reliability but also on a number of other factors, including operational readiness, availability, maintainability, and repairability. Definitions for these concepts are given in Section 3. From the definitions it can be seen that they are all so interrelated that they must be viewed together and discussed, not as separate concepts but within the framework of the overall system to which they contribute.

4.5.2   INTERRELATIONSHIPS AMONG VARIOUS SYSTEM PROPERTIES

The discussion above implies that it is probably not practicable to maximize all of the desirable properties of a system simultaneously. Clearly, there are "tradeoff" relationships between reliability and system cost, between maintainability and system cost, between reliability and maintainability, and between many other properties. It would be most helpful to have a numerical scale of values for each of the several properties, and to have a multi-dimensional plot or chart showing the interrelationship among those values. Before such relationships can be obtained, it is first necessary to define in a precise and quantitative manner the properties with which we are concerned. The following outline is intended to show some of the factors which must be considered:

A. SYSTEM PERFORMANCE (DESIGN ADEQUACY)
    1. Technical Capabilities
        a) Accuracy
        b) Range
        c) Invulnerability to countermeasures
        d) Operational simplicity

    2. Possible Limitations on Performance
        a) Space and weight requirements
        b) Input power requirements
        c) Input information requirements
        d) Requirements for special protection against shock, vibration, low pressure, and other environmental influences

4-15

B. OPERATIONAL READINESS
    1. Reliability
        a) Failure-free operation
        b) Redundancy or provision for alternative modes of operation

    2. Maintainability
        a) Time to restore failed system to satisfactory operating status
        b) Technical manpower requirements for maintenance
        c) Effects of use-cycle on maintenance. (Can some maintenance be performed when operational use of the system is not required?)
    3. Logistic Supportability

C. SYSTEM COST
    1. Development cost, and particularly development time, from inception to operational capability
    2. Production cost
    3. Operating and operational support costs

4.6 OPTIMIZATION OF SYSTEM EFFECTIVENESS

The optimization of system effectiveness is important throughout the system life cycle, from concept through the operation. Optimization is the balancing of available resources (time, money, personnel, etc.) against resulting effectiveness parameters (performance, operational readiness, etc.), until a combination is found that provides the most effectiveness for the desired expenditure of resources. Thus, the optimum system might be one that:

(1) Meets or exceeds a particular level of effectiveness for minimum cost, and/or
(2) Provides a maximum effectiveness for a given total cost

Optimization is illustrated by the flow diagram of Figure 4.6-1 which shows the optimization process as a feedback loop consisting of the following three steps:

(1) Designing many systems that satisfy the operational requirements and constraints
(2) Computing resultant values for effectiveness and resources used
(3) Evaluating these results and making generalizations concerning appropriate combinations of design and support factors, which are then fed back into the model through the feedback loops

Optimization also can be illustrated by the purchase of a new car or, more specifically, by putting into precise, quantifiable terms the rule, or criteria, that will be followed in the automobile selection process. Although automobiles do have quantifiable characteristics, such as horsepower, cost, and seating capacity, they are basically similar in most cars of a particular class (low-price sedans, sports models, etc.).
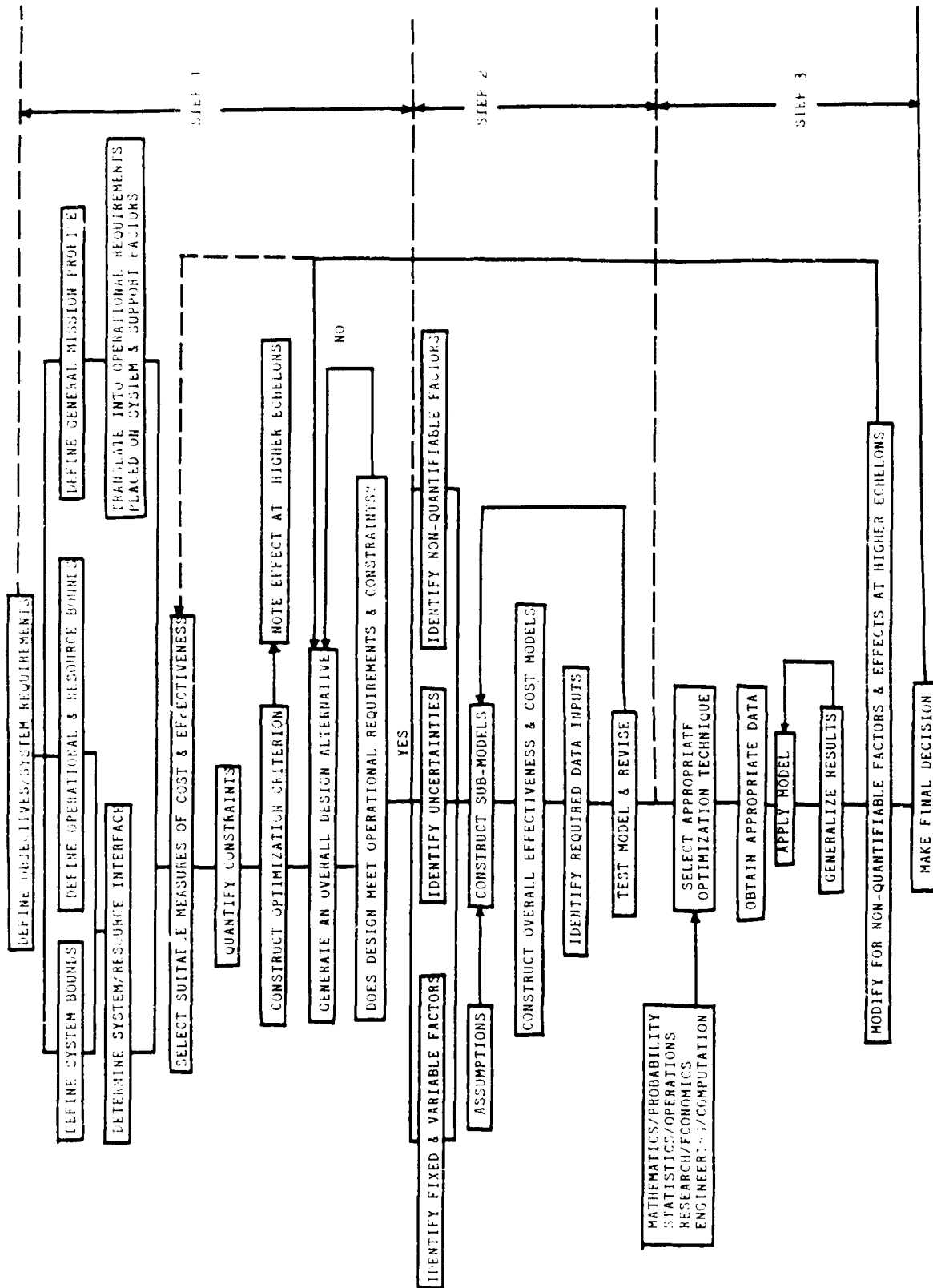
FIGURE 4.6-1: FLOW DIAGRAM FOR A GENERAL OPTIMIZATION PROCESS

Thus, the selection criteria essentially reduce to esthetic appeal, prior experience with particular models, and similar intangibles. In the same sense, the choice of best design for the weapon system is greatly influenced by experience with good engineering practices, knowledge assimilated from similar systems, and economics. Despite this fuzziness, the selection criteria must be adjusted so that:

(1) The problem size can be reduced to ease the choice of approaches
(2) All possible alternatives can be examined more readily and objectively for adaptation to mathematical representation and analysis
(3) Ideas and experiences from other disciplines can be more easily incorporated into the solution
(4) The final choice of design approaches can be based on more precise, quantifiable terms, permitting more effective review and revision, and better inputs for future optimization problems

The choice of parameters in the optimization model also is influenced by system definition. The automobile purchaser, for example, may not consider the manufacturer's and dealer's service policies. If these policies are considered, the system becomes the automobile plus the service policies. If service policies are not considered, the system consists only of the automobile.

The optimization of system effectiveness is a highly complex problem; there is a degree of interaction among the factors which enter into consideration of this problem. The actual techniques used to optimize system effectiveness will be described in greater detail in Section 10 of this handbook. Table 4.6-1 (Ref. 2), for example, lists only some of the more commonly used techniques. Ref. 2, also, contains methods and examples of basic mathematical and statistical concepts, simulation, queuing theory, sequencing and Markov processes, game theory, linear and dynamic programming, information theory, and others. These techniques are not peculiar to system effectiveness optimization, nor are they limited to system engineering.

This section is an introduction to the handbook from a top level, or system, viewpoint. The remaining sections of this handbook will expand upon the concepts introduced in this chapter. They will cover: (1) the basic reliability/maintainability/availability theory, (2) practical application of the theory in terms of the design methodology and procedures of reliability engineering at the equipment and system level, (3) procedures for insuring that inherent reliability is not degraded during production and field deployment of systems, and (4) steps that management must take to insure the acquisition and deployment of reliable systems at minimum life cycle cost.

TABLE 4.6-1: PARTIAL LIST OF OPTIMIZATION TECHNIQUES

I. Mathematical Techniques	II. Statistical Techniques
Birth and death processes Calculus of finite differences Calculus of variations Gradient theory Numerical approximation	Bayesian analysis Decision theory Experimental design Information theory Method of steepest ascent
Symbolic logic Theory of linear integrals Theory of maxima and minima	Stochastic processes
III. Programming Techniques	IV. Other
Dynamic programming Linear programming Nonlinear programming	Gaming theory Monte Carlo techniques Queuing theory Renewal theory Search theory Signal flow graphs Simulation Value theory

REFERENCES

1. Gates, H.P., et al. "Electronics X: A Study of Military Electronics With Particular Reference To Cost And Reliability." Volume 1: Executive Conspectus, Volume 2: Complete Report, Institute for Defense Analyses, January 1974, AD# 783007.

2. AMCP 706-191, Engineering Design Handbook, System Analysis And Cost Effectiveness.

3. Aeronautical Radio Inc., Reliability Engineering, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1964.

4. AFSC-TR-65-1 through 65-6, Vols. I through VI, , "Final Report of Task Groups 1 through 6, "Weapon System Effectiveness Industry Advisory Group, (WSEIAC), January 1965.

   Vol. 1 - "Requirements Methodology"
   Vol. 2 - "Prediction - Measurement"
   Vol. 3 - "Data Collection and Management"
   Vol. 4 - "Cost Effectiveness and Optimization"
   Vol. 5 - "Management Systems"
   Vol. 6 - "Chairman's Final Report"

5. AMCP 706-196, Engineering Design Handbook, Design For Reliability, AD# A027370, January 1976.

6. Sandler, G., System Reliability Engineering, Prentice-Hall Inc., Englewood Cliff, NJ, 1963.

7. DOD Directive 5000.40, Reliability and Maintainability, July 8, 1980.

5.0 RELIABILITY/MAINTAINABILITY/AVAILABILITY THEORY

5.1 INTRODUCTION

Most modern engineering disciplines are based on applied mathematics. An engineer or scientist observes a particular event and formulates a hypothesis (or conceptual model) which describes a relationship between the observed facts and the event being studied. In the physical sciences, conceptual models are, for the most part, mathematical in nature. Mathematical models represent an efficient, shorthand method of describing an event and the more significant factors which may cause, or affect, the occurrence of the event. Such models are useful to engineers since they provide the theoretical foundation for the development of an engineering discipline and a set of engineering design principles which can be applied to cause or prevent the occurrence of an event.

Mathematical models may be deterministic or probabilistic. An example of a deterministic model is Newton's second law of mechanics, $F = ma$, force equals mass times acceleration. There is nothing indefinite about this model. A probabilistic model is one in which the results cannot be determined as exactly as in the deterministic model but can only be obtained in terms of a probability or probability distribution function. An example of a probabilistic model is modern atomic theory which defines the exact future location of an electron in terms of a probability function. The use of the probabilistic as opposed to deterministic models is becoming more widespread in the modern engineering solution to problems.

The disciplines of reliability and maintainability (R/M) are based upon probabilistic or stochastic models. This is for several reasons:

(1) It would be extremely difficult, uneconomical and probably nonproductive to identify and exactly quantify all of the variables which contribute to the failure of even simple electronic components in order to develop an exact, deterministic failure model. This approach was attempted in the early days of Reliability Physics for a simple, thin film resistor and had to be abandoned because of the complexity and intractability of the final model developed (Ref. 20). Thus, we are dealing with uncertainty and the measured values which can only be stated with less than total certainty.

(2) Probabilistic models, when applied to large samples, tend to "smooth out" individual variations so that the final, average result is simple and accurate enough for engineering analysis and design.

Since R/M parameters are defined in probabilistic terms, probabilistic parameters such as random variables, density functions, and distribution functions are utilized in the development of R/M theory.

This section describes some of the basic concepts, formulas, and simple examples of application of R/M theory which are required for better understanding of the underlying principles and design techniques

presented in later sections. Practicality rather than rigorous theoretical exposition is emphasized. Many excellent texts are available (see references) for the reader who is interested in delving into the rigorous theoretical foundations of these disciplines.

5.2 RELIABILITY THEORY

Because, as was mentioned previously, reliability is defined in terms of probability, probabilistic parameters such as random variables, density functions, and distribution functions are utilized in the development of reliability theory. Reliability studies are concerned with both discrete and continuous random variables. An example of a discrete variable is the number of failures in a given interval of time. Examples of continuous random variables are the time from part installation to failure and the time between successive equipment failures.

The distinction between discrete and continuous variables (or functions) depends upon how the problem is treated and not necessarily on the basic physical or chemical processes involved. For example, in analyzing "one shot" systems such as missiles, one usually utilizes discrete functions such as the number of successes in "n" launches. However, whether or not a missile is successfully launched could be a function of its age, including time in storage, and could, therefore, be treated as a continuous function.

5.2.1 BASIC CONCEPTS

The cumulative distribution function $F(t)$ is defined as the probability in a random trial that the random variable is not greater than t (see note), or

$$F(t) = \int_{-\infty}^{t} f(t)dt \qquad (5.1)$$

where $f(t)$ is the density function of the random variable, time to failure. This is termed the "unreliability function" when speaking of failure. It can be thought of as representing the probability of failure prior to some time t. If the random variable is discrete, the integral is replaced by a summation.

The reliability function, or the probability of a device not failing prior to some time t, is given by

$$R(t) = 1 - F(t) = \int_{t}^{\infty} f(t)dt \qquad (5.2)$$

By differentiating Equation (5.2) it can be shown that

$$\frac{-d\ R(t)}{dt} = f(t) \qquad (5.3)$$

NOTE: Pure mathematicians object to the use of the same letter in the integral and also in the limits of the integral. This is done here, and in the rest of this section in spite of the objection in order to simplify the reference to time as the variable in such functions as $F(t)$, $R(t)$, $M(t)$, $f(t)$, etc.

The probability of failure in a given time interval between t_1 and t_2 can be expressed by the reliability function

$$\int_{t_1}^{\infty} f(t)dt - \int_{t_2}^{\infty} f(t)dt = R(t_1) - R(t_2) \quad t_2) \tag{5.4}$$

The rate at which failures occur in the interval t_1 to t_2, the failure rate $\lambda(t)$, is defined as the ratio of probability that failure occurs in the interval, given that it has not occurred prior to t_1, the start of the interval, divided by the interval length. Thus,

$$\lambda(t) = \frac{R(t_1) - R(t_2)}{(t_2 - t_1) R(t_1)} \tag{5.5}$$

or the alternative form

$$\lambda(t) = \frac{R(t) - R(t+\ell)}{\ell R(t)} \tag{5.6}$$

where $t = t_1$ and $t_2 = \ell + t$. The hazard rate, $h(t)$, or instantaneous failure rate is defined as the limit of the failure rate as the interval length approaches zero, or

$$h(t) = \lim_{\ell \to 0} \left[\frac{R(t) - R(t+\ell)}{\ell R(t)} \right]$$

$$= \frac{-1}{R(t)} \left[\frac{dR(t)}{dt} \right] = \frac{1}{R(t)} \left[\frac{-dR(t)}{dt} \right] \tag{5.7}$$

But it was previously shown, Eq. (5.3), that

$$f(t) = \frac{-dR(t)}{dt}$$

Substituting this into Eq. (5.7) we get:

$$\boxed{h(t) = \frac{f(t)}{R(t)}} \tag{5.8}$$

This is one of the fundamental relationships in reliability analysis. For example, if one knows the density function of the time to failure, $f(t)$, and the reliability function, $R(t)$, the hazard rate function for any time, t, can be found. The relationship is fundamental and important because it is independent of the statistical distribution under consideration.

The differential equation of Eq. (5.7) tells us, then, that the hazard rate is nothing more than a measure of the change in survivor rate per unit change in time.

Perhaps some of these concepts can be seen more clearly by use of a more concrete example. Suppose that we start a test at time, t_o, with N_o devices. After some time t, N_f of the original devices will have failed, and N_s will have survived ($N_o = N_f + N_s$). The reliability, $R(t)$, is given at any time t by

$$R(t) = \frac{N_s}{N_o} \tag{5.9}$$

$$= \frac{N_o - N_f}{N_o} = 1 - \frac{N_f}{N_o} \tag{5.10}$$

From eq. (5.3)

$$f(t) = - \frac{dR(t)}{dt} = \frac{1}{N_0} \frac{dN_f}{dt}$$

(5.11)

Thus, the failure density function represents the proportion of the original population, (N_0), which fails in the interval $(t, t+\Delta t)$.

On the other hand, from Eqs. (5.8), (5.9) and (5.11)

$$h(t) = \frac{f(t)}{R(t)} = \frac{\frac{1}{N_0} \frac{dN_f}{dt}}{N_S/N_0} = \frac{1}{N_S} \frac{dN_f}{dt}$$

(5.12)

Thus, $h(t)$ is inversely proportioned to the number of devices that survive to time t, (N_S), which fail in the interval $(t, t+\Delta t)$.

Although, as can be seen by comparing Eqs. (5.6) and (5.7) failure rate, $\lambda(t)$, and hazard rate, $h(t)$, are mathematically somewhat different, they are usually used synonymously in conventional reliability engineering practice. It is not the intent of this handbook to repeal firmly entrenched conventional practice in the interest of exact mathematical accuracy.

Perhaps the simplest explanation of hazard and failure rate is made by analogy. Suppose a family takes an automobile trip of 200 miles and completes the trip in 4 hours. Their average rate was 50 mph, although they drove faster at some times and slower at other times. The rate at any given instant could have been determined by reading the speed indicated on the speedometer at that instant. The 50 mph is analogous to the failure rate and the speed at any point is analogous to the hazard rate.

In Eq. (5.8), a general expression was derived for hazard (failure) rate. This can also be done for the reliability function, $R(t)$. From Eq. (5.7)

$$h(t) = - \frac{1}{R(t)} \left[\frac{dR(t)}{dt} \right]$$

(5.13)

$$\frac{dR(t)}{R(t)} = - h(t) \, dt$$

Integrating both sides of Eq. (5.13)

$$\int_0^t \frac{dR(t)}{R(t)} = - \int_0^t h(t) dt$$

$$\ln R(t) - \ln R(o) = - \int_0^t h(t) \, dt$$

but $R(o) = 1$, $\ln R(o) = o$, and

$$R(t) = \exp \left[- \int_0^t h(t) \, dt \right]$$

(5.14)

Eq. (5.14) is the general expression for the reliability function. If $h(t)$ can be considered a constant failure rate (λ), which is true for many cases for electronic equipment, Eq. (5.14) becomes

$$R(t) = e^{-\lambda t} \qquad (5.15)$$

Eq. (5.15) is used quite frequently in reliability analysis, particularly for electronic equipment. However, the reliability analyst should assure himself that the constant failure rate assumption is valid for the item being analyzed by performing goodness of fit tests on the data. These are discussed in Section 8.

In addition to the concepts of $f(t)$ $h(t)$, $\lambda(t)$, and $R(t)$, previously developed, several other basic, commonly used reliability concepts require development. They are: mean time to failure (MTTF), mean life (θ), and mean time between failure (MTBF).

Mean Time to Failure (MTTF)

MTTF is nothing more than the expected value of time to failure and is derived from basic statistical theory as follows:

$$MTTF = \int_{0}^{\infty} t \; f(t) \; dt$$

$$= \int_{0}^{\infty} t \left[- \frac{dR(t)}{dt} \right] dt \qquad (5.16)$$

Integrating by parts and applying l'Hopital's rule, we arrive at the expression

$$MTTF = \int_{0}^{\infty} R(t) \; dt \qquad (5.17)$$

Eq. (5.17), in many cases, permits the simplification of MTTF calculations. If one knows (or can model from the data) the reliability function, $R(t)$, the MTTF can be obtained by direct integration of $R(t)$ (if mathematically tractable), or by graphical approximation. For repairable equipment MTTF is defined as the mean time to first failure.

Mean Life (θ)

The mean life (θ) refers to the total population of items being considered. For example, given an initial population of n items, if all are operated until they fail, the mean life (θ) is merely the arithmetic mean of the total population given by

$$\theta = \frac{\sum_{i=1}^{n} t_i}{n} \qquad (5.18)$$

where
t_i = time to failure of each item in the population
n = total number of items in the population

Mean Time Between Failure (MTBF)

This concept appears quite frequently in reliability literature; it applies to repairable items in which failed elements are replaced upon failure. The expression for MTBF is

$$MTBF = \frac{T(t)}{r} \qquad (5.19)$$

where

T(t) = total operating time
r = number of failures

It is important to remember that MTBF only has meaning for repairable items, and, for that case, MTBF represents exactly the same parameter as mean life (θ). More important is the fact that a constant failure rate is assumed. Thus, given the twin assumptions of replacement upon failure and constant failure rate, the reliability function is

$$R(t) = e^{-\lambda t} = e^{-t/\theta} = e^{-t/MTBF} \qquad (5.20)$$

and (for this case)

$$\lambda = \frac{1}{MTBF} \qquad (5.21)$$

Figure 5.2.1-1 provides a convenient summary of the basic concepts developed in this section.

Failure Density Function (time to failure)	$f(t)$
Reliability Function	$R(t) = \int_0^{\infty} f(t)dt = \exp\left[-\int_0^t h(t)dt\right]$
Hazard Rate (Failure Rate)	$h(t) = f(t)/R(t)$ $[\lambda(t)] = \int_0^t h(t)dt$
Expected Value (MTTF) (no repair)	$MTTF = \int_0^{\infty} R(t)dt$
Mean Time Between Failure (constant failure rate, λ, with repair)	$MTBF = \frac{T(t)}{r}$ $= 1/\lambda$

FIGURE 5.2.1-1

SUMMARY OF BASIC RELIABILITY CONCEPTS

5.2.2 STATISTICAL DISTRIBUTIONS USED IN RELIABILITY MODELS

There are many standard statistical distributions which may be used to model the various reliability parameters. It has been found that a relatively small number of statistical distributions satisfies most needs in reliability work. The particular distribution used depends upon the nature of the data, in each case. Following is a short summary of some of the distributions most commonly used in reliability analysis, criteria for their use, and examples of application. Figures 5.2.2-1 and 5.2.2-2 are summaries of the shape of common failure density, reliability, and hazard rate functions for the distributions described. Each distribution will be described in more detail, with reliability examples, in the following sections.

5.2.2.1 CONTINUOUS DISTRIBUTIONS

5.2.2.1.1 NORMAL (OR GAUSSIAN) DISTRIBUTION

There are two principal applications of the normal distribution to reliability. One application deals with the analysis of items which exhibit failure due to wear, such as mechanical devices. Frequently the wear out failure distribution is sufficiently close to normal that the use of this distribution for predicting or assessing reliability is valid.

The other application deals with the analysis of manufactured items and their ability to meet specifications. No two parts made to the same specification are exactly alike. The variability of parts leads to a variability in systems composed of those parts. The design must take this part variability into account, otherwise the system may not meet the specification requirement due to the combined effect of part variability. Another aspect of this application is in quality control procedures.

The basis for the use of normal distribution in this application is the central limit theorem which states that the sum of a large number of identically distributed random variables, each with finite mean and variance, is normally distributed. Thus, the variations in value of electronic component parts, for example, due to manufacturing are considered normally distributed.

The failure density function for the normal distribution is

$$f(t) = \frac{1}{\sigma(2\pi)^{\frac{1}{2}}} \exp\left[-\frac{1}{2}\left(\frac{t-u}{\sigma}\right)^2\right] \tag{5.22}$$

where

    u = the population mean
    σ = the population standard deviation, which is the square root of the variance.

FIGURE 5.2.2-1: DENSITY FUNCTION, RELIABILITY FUNCTION
AND HAZARD RATE FOR THE NORMAL, EXPONENTIAL,
GAMMA, WEIBULL AND LOGNORMAL DISTRIBUTIONS.

TYPE OF DISTRIBUTION	PARAMETERS	PROBABILITY DENSITY FUNCTION f(x)	RELIABILITY FUNCTION R(x)
BINOMIAL	MEAN, $\mu = np$ Std. deviation, $\sigma = \sqrt{npq}$ $\binom{n}{x} = \dfrac{n!}{(n-x)!\,x!}$	$f(x) = C(8,x)(\frac{2}{3})^x(\frac{1}{3})^{8-x}$ 	$R(x) = \sum\limits_{\lambda=x}^{i=8} C(8,1)(\frac{2}{3})^1(\frac{1}{3})^{8-1}$
		$f(x) = \binom{n}{x}p^x q^{n-x}$ $\left\{\begin{array}{l} n = 8 \\ p = 2/3 \end{array}\right\}$	$R(x) = \sum\limits_{i=x}^{n} \binom{n}{i}p^i q^{n-i}$ $\left\{\begin{array}{l} n = 8 \\ p = 2/3 \end{array}\right\}$
Poisson	Mean, $\mu = a,$ $\quad = \lambda t$ Std. deviation, $\sigma = \sqrt{a} = \sqrt{\lambda t}$	$f(x) = \dfrac{a^x e^{-a}}{x!}$ $a = 4$	$R(x) = \sum\limits_{\lambda=x}^{\infty} \dfrac{a^{\lambda}e^{-a}}{\lambda !}$
		$f(x) = \dfrac{a^x e^{-a}}{x!}$ $= \dfrac{(\lambda t)^x e^{-\lambda t}}{x!}$ $a = \lambda t = 4$	$R(x) = \sum\limits_{i=x}^{\infty} \dfrac{a^i e^{-a}}{i!}$ $= \sum\limits_{i=x}^{\infty} \dfrac{(\lambda t)^x e^{-\lambda t}}{x!}$ $a = \lambda t = 4$
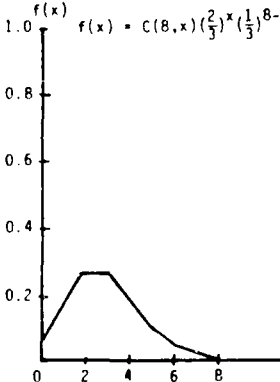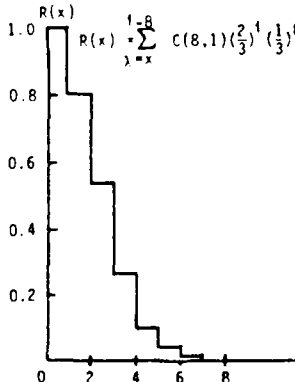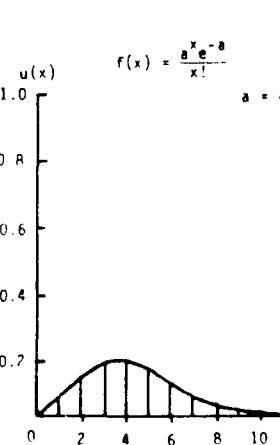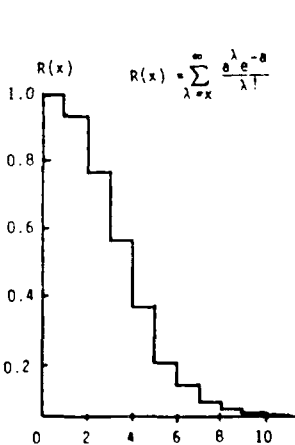
FIGURE 5.2.2-2: <u>SHAPES OF FAILURE DENSITY AND RELIABILITY FUNCTIONS OF COMMONLY USED DISCRETE DISTRIBUTIONS</u>

For most practical applications, probability tables for the standard normal distribution are used (Table A-1, Appendix A). The standard normal distribution density function is given by:

$$f(z) = \frac{1}{(2\pi)^{\frac{1}{2}}} \exp\left(\frac{-z^2}{2}\right) \tag{5.23}$$

where

$$u = 0$$
$$\sigma^2 = 1$$

One converts from the normal to standard normal distribution by using the transformations.

$$z = \frac{t-u}{\sigma} \tag{5.24}$$

$$f(t) = \frac{f(z)}{\sigma} \tag{5.25}$$

5.2.2.1.2 <u>EXAMPLES OF RELIABILITY CALCULATIONS USING THE NORMAL DISTRIBUTION</u>

5.2.2.1.2.1 <u>MICROWAVE TUBE EXAMPLE</u>

A microwave transmitting tube has been observed to follow a normal distribution with u = 5000 hours and σ = 1500 hours. Find the reliability of such a tube for a mission time of 4100 hours and the hazard rate of one of these tubes at age 4400 hours.

$$R(t) = P\left(Z > \frac{t-u}{\sigma}\right)$$

$$R(4100) = P\left(Z > \frac{4100-5000}{1500}\right)$$

$$= P(Z > -0.6) = 1 - P(Z < -0.6)$$

$$= 1 - 0.27 = 0.73$$

as found in Table A-1. Remember $P(Z > -z) = P(Z < z)$ by symmetry of the normal distribution.

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(z)/\sigma}{R(t)}$$

$$f(t = 4400) = \frac{f\left(z = \frac{4400-5000}{1500}\right)}{1500}$$

$$= \frac{1}{1500} \, f(z = -0.4)$$

$$= (0.00067)(0.37) = 0.00025$$

where $f(z = 0.4)$ was obtained from Table A-2.   Remember $f(z)=f(-z)$ because of the symmetry of the normal distribution.

$$R(4400) = P\left(Z > \frac{4400-5000}{1500}\right) = P(Z > -0.4)$$

$$= 1 - P(Z \quad -0.4) = 0.65$$

$$h(4400) = \frac{f(4400)}{R(4400)} = \frac{0.00025}{0.65} = 0.00038 \text{ failures/hour}$$

5.2.2.1.2.2 MECHANICAL EQUIPMENT EXAMPLE

A motor generator has been observed to follow a normal distribution with $u = 300$ hours and $\sigma = 40$ hours. Find the reliability of the motor generator for a mission time (or time before maintenance) of 250 hours and the hazard rate at 200 hours.

$$R(250) = P\left(Z > \frac{250-300}{40}\right) = P(Z > -1.25)$$

$$= 1 - P(Z \quad -1.25) = 1 - 0.11 = 0.89$$

$P(Z \quad -1.25)$ was found from Table A-1

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(z)/\sigma}{R(t)}$$

$$f(t = 200) = \frac{f\left(z = \frac{200-300}{40}\right)}{40} = \frac{1}{40} \; f(z = -2.5)$$

$$= (0.025)(0.0175) = 0.00044$$

where $f(z = 2.5)$ was found from Table A-2.

$$R(200) = P\left(Z > \frac{200-300}{40}\right)$$

$$= P(Z > -2.5) = 1 - P(Z < -2.5)$$

$$= 0.994$$

$$h(200) = \frac{f(200)}{R(200)} = \frac{0.00044}{0.994} = 0.00044 \text{ failures/hour}$$

5.2.2.1.3 LOGNORMAL DISTRIBUTION

The lognormal distribution is the distribution of a random variable whose natural logarithm is distributed normally; in other words, it is the normal distribution with ln t as the variate. The density function is

$$f(t) = \frac{1}{\sigma t (2\pi)^{1/2}} \exp \left[-\frac{1}{2} \left(\frac{\ln t - u}{\sigma} \right)^2 \right] \qquad (5.26)$$

for $t \geq 0$

where the mean $= \exp \left(u + \frac{\sigma^2}{2} \right)$ \qquad (5.27)

and the standard deviation $= \left[\exp (2u + 2\sigma^2) - \exp (2u + \sigma^2) \right]^{1/2}$ \quad (5.28)

where u and σ are the mean and standard deviation (SD) of ln t.

The lognormal distribution is used in reliability analysis of semiconductors and fatigue life of certain types of mechanical components. Its main application is really in maintainability analysis of time to repair data. This will be covered further in Section 5.3.

5.2.2.1.3.1 FATIGUE FAILURE EXAMPLE

Suppose it has been observed that gun tube failures occur according to lognormal distribution with u = 7 and σ = 2 (remember u and σ are the mean and SD of the ln t data). Find the reliability for a 1000 round mission and the hazard rate at 800 rounds. For this case, the variable t is the number of rounds.

$$R(t) = P \left(Z > \frac{\ln t - u}{\sigma} \right)$$

$$R(1000) = P \left(Z > \frac{\ln 1000 - 7.0}{2.0} \right)$$

$$= P (Z \quad -0.045) = 0.52$$

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(z)/\sigma t}{R(t)} \quad \longleftarrow \text{transformed variable for lognormal case}$$

$$h(800) = \frac{f(800)}{\sigma t R(800)} = \frac{f \left(z = \frac{\ln 800 - 7}{2} \right)}{(2)(800) R(800)}$$

$$= \frac{f\left(z = \frac{\ln 800 - 7}{2}\right)}{(2)(800) \, P\left(z > \frac{\ln 800 - 7}{2}\right)}$$

$$= \frac{f(z = -0.16)}{1600 \, P(Z > -0.16)} = \frac{0.3939}{(1600)(0.5636)}$$

$$h(800) = 0.0004 \text{ failures/round}$$

where $P(Z > -0.16)$ was found from Table A-1 and $f(z = -0.16)$ from Table A-2

5.2.2.1.4 EXPONENTIAL DISTRIBUTION

This is probably the most important distribution in reliability work and is used almost exclusively for reliability prediction of electronic equipment (Ref. MIL-HDBK-217). It describes the situation wherein the hazard rate is constant which can be shown to be generated by a Poisson process. This distribution is valuable if properly used. It has the advantages of:

(1) single, easily estimated parameter (λ)
(2) mathematically very tractable
(3) fairly wide applicability
(4) is additive - that is, the sum of a number of independent exponentially distributed variables is exponentially distributed.

Some particular applications of this model include:

(1) items whose failure rate does not change significantly with age.
(2) complex and repairable equipment without excessive amounts of redundancy.
(3) equipment for which the early failures or "infant mortalities" have been eliminated by "burning in" the equipment for some reasonable time period.

The failure density function is

$$f(t) = \lambda e^{-\lambda t} \tag{5.29}$$

for $t > 0$, where λ is the hazard (failure) rate, and the reliability function is

$$R(t) = e^{-\lambda t} \tag{5.30}$$

the mean life $(\theta) = 1/\lambda$, and, for repairable equipment, the MTBF $= \theta = 1/\lambda$.

5.2.2.1.4.1 AIRBORNE FIRE CONTROL SYSTEM EXAMPLE

The mean time to failure (MTTF $= \theta$, for this case) of an airborne fire control system is 10 hours. What is the probability that it will not fail during a 3 hour mission?

$$R(3) = e^{-\lambda t} = e^{-t/\theta}$$

$$= e^{-3/10} = e^{-0.3} = 0.74$$

5.2.2.1.4.2 COMPUTER EXAMPLE

A computer has a constant error rate of one error every 17 days of continuous operation. What is the reliability associated with the computer to correctly solve a problem that requires 5 hours time? Find the hazard rate after 5 hours of operation.

$$MTTF = \theta = 408 \text{ hours}$$

$$\lambda = \frac{1}{\theta} = \frac{1}{408} = 0.0024 \text{ failure/hour}$$

$$R(5) = e^{-\lambda t} = e^{-(0.0024)(5)}$$

$$= e^{-0.012} = 0.99$$

$$h(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda = 0.0024 \text{ failures/hours}$$

5.2.2.1.5 GAMMA DISTRIBUTION

The gamma distribution is used in reliability analysis for cases where partial failures can exist, i.e., when a given number of partial failures must occur before an item fails (e.g., redundant systems) or the time to second failure when the time to failure is exponentially distributed. The failure density function is

$$f(t) = \frac{\lambda}{\Gamma(a)} (\lambda t)^{a-1} e^{-\lambda t} \qquad (5.31)$$

for $t > 0$,

$$\text{where } u = \frac{a}{\lambda} \qquad (5.32)$$

$$SD = \frac{a^{\frac{1}{2}}}{\lambda} \qquad (5.33)$$

and λ is the failure rate (complete failure) and the number of partial failures for complete failure or events to generate a failure. $\lambda(a)$ is the gamma function

$$\Gamma(a) = \int_0^\infty x^{a-1} e^{-x} dx \qquad (5.34)$$

which can be evaluated by means of standard tables.

When $(a-1)$ is a positive integer, $\Gamma(a) = (a-1)!$, which is usually the case for most reliability analysis, e.g., partial failure situation. For this case the failure density function is

$$f(t) = \frac{\lambda}{(a-1)!} (\lambda t)^{a-1} e^{-\lambda t} \qquad (5.35)$$

which, for the case of $a = 1$ becomes the exponential density function, previously described.

The gamma distribution can also be used to describe an increasing or decreasing hazard (failure) rate. When $a > 1$, $h(t)$ increases; when $a < 1$, 1, $h(t)$ decreases. This is shown in Figure 5.2.2-1.

5.2.2.1.5.1 MISSILE SYSTEM EXAMPLE

An antiaircraft missile system has demonstrated a gamma failure distribution with $a = 3$ and $\lambda = 0.05$. Determine the reliability for a 24 hour mission time and the hazard rate at the end of 24 hours

$$R(t) = \frac{\lambda^a}{\Gamma(a)} \int_t^\infty t^{a-1} e^{-\lambda t} \, dt$$

Ordinarily, special tables of the Incomplete Gamma Function are required to evaluate the above integral. However, it can be shown that if is an integer

$$R(t) = \sum_{k=0}^{a-1} \frac{(\lambda t)^k e^{-\lambda t}}{k!} \tag{5.36}$$

which later in the section will be shown to be a Poisson distribution. Using Eq. (5.36)

$$R(24) = \sum_{k=0}^{2} \frac{\left[(0.05)(24)\right]^k e^{-(0.05)(24)}}{k!}$$

$$= \sum_{k=0}^{2} \frac{(1.2)^k (0.3)}{k!}$$

$$= (0.3) + (1.2)(0.3) + \frac{(1.2)^2 (0.3)}{2}$$

$$= 0.3 + 0.36 + 0.216 = 0.88$$

$$h(t) = \frac{f(t)}{R(t)}$$

$$f(t) = \frac{\lambda}{(a-1)!} (\lambda t)^{a-1} e^{-\lambda t}$$

$$f(24) = \frac{0.05}{2} (1.2)^2 e^{-1.2}$$

$$= (0.025)(0.434) = 0.011$$

$$h(24) = \frac{f(24)}{R(24)} = \frac{0.011}{0.88} = 0.012 \text{ failures/hour}$$

5.2.2.1.6 <u>WEIBULL DISTRIBUTION</u>

The Weibull distribution is particularly useful in reliability work since it is a general distribution which, by adjustment of the distribution parameters, can be made to model a wide range of life distribution characteristics of different classes of engineered items. One of the versions of the failure density function is

$$f(t) = \frac{\beta}{\eta} \left(\frac{t-\gamma}{\eta}\right)^{\beta-1} \exp\left[-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right] \qquad (5.37)$$

where β is the shape parameter
   η is the scale parameter or characteristic life
      (life at which 63.2% of the population will have failed)
   γ is the minimum life

In most practical reliability situations, γ is often zero (failure assumed to start at t = 0) and the failure density function becomes

$$f(t) = \frac{\beta}{\eta} \left(\frac{t}{\eta}\right)^{\beta-1} \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right] \qquad (5.38)$$

and the reliability and hazard functions become

$$R(t) = \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right] \qquad (5.39)$$

$$h(t) = \left(\frac{\beta}{\eta}\right)\left(\frac{t}{\eta}\right)^{\beta-1} \qquad (5.40)$$

Depending upon the value of β, the Weibull distribution function can take the form of the following distributions as follows,

   $\beta < 1$ Gamma

   $\beta = 1$ Exponential

   $\beta = 2$ Lognormal

   $\beta = 3.5$ Normal (approximately)

Thus, it may be used to help identify other distributions from life data (backed up by goodness of fit tests) as well as being a distribution in its own right. Graphical methods are used to analyze Weibull failure data and are described in Section 8.

5.2.2.1.6.1 EXAMPLE OF USE OF WEIBULL DISTRIBUTION

The failure times of a particular transmitting tube are found to be Weibull distributed with β = 2, and η = 1000 hours (consider η somewhat related to MTTF). Find the reliability of one of these tubes for a mission time of 100 hours, and the hazard rate after a tube has operated successfully for 100 hours.

$$R(t) = e^{-\left(\frac{t}{\eta}\right)^{\beta}}$$

$$R(100) = e^{-\left(\frac{100}{1000}\right)^{2}} = e^{-(0.1)^{2}} \approx 0.99$$

$$h(100) = \left(\frac{\beta}{\eta}\right)\left(\frac{t}{\eta}\right)^{\beta-1} = \left(\frac{2}{1000}\right)\left(\frac{100}{1000}\right)^{2-1}$$

$$= 0.0002 \text{ failures/hour}$$

5.2.2.2 DISCRETE DISTRIBUTIONS

5.2.2.2.1 BINOMIAL DISTRIBUTION

The binomial distribution is used for those situations in which there are only two outcomes, such as success or failure, and the probability remains the same for all trials. It is very useful in reliability and quality assurance work. *The probability density function (pdf) of the binomial distribution is*

$$f(x) = \binom{n}{x} p^{x} q^{(n-x)}$$

(5.41)

$$\text{where } \binom{n}{x} = \frac{n!}{(n-x)!x!} \text{ and } q = 1-p$$

(5.42)

$f(x)$ is the probability of obtaining exactly x good items and (n-x) bad items in a sample of n items where p is the probability of obtaining a good item (success) and q (or 1-p) is the probability of obtaining a bad item (failure).

The cumulative distribution function (CDF), i.e., the probability of obtaining r or fewer successes in n trials, is given by

$$F(x; r) = \sum_{x=0}^{r} \binom{n}{x} p^{x} q^{(n-x)}$$

(5.43)

5.2.2.2.1.1 QUALITY CONTROL EXAMPLE

In a large lot of component parts, past experience has shown that the probability of a defective part is 0.05. The acceptance sampling plan for lots of these parts is to randomly select 30 parts for inspection and accept the lot if 2 or less defective are found. What is the probability, $P(a)$, of accepting the lot?

$$P(a) = \sum_{x=0}^{2} \binom{30}{x} (0.05)^x (0.95)^{30-x}$$

$$= \frac{30!}{0! \, 30!} (0.05)^0 (0.95)^{30} + \frac{30!}{1! \, 29!} (0.05) (0.95)^{29}$$

$$+ \frac{30!}{2! \, 28!} (0.05)^2 (0.95)^{28}$$

$$= 0.812$$

Note that in this example the probability of success was the probability of obtaining a defective part.

5.2.2.2.1.2 RELIABILITY EXAMPLE

The binomial is useful for computing the probability of system success when the system employs partial redundancy. Assume a five channel VHF receiver as shown in Figure 5.2.2.2.1.2-1.
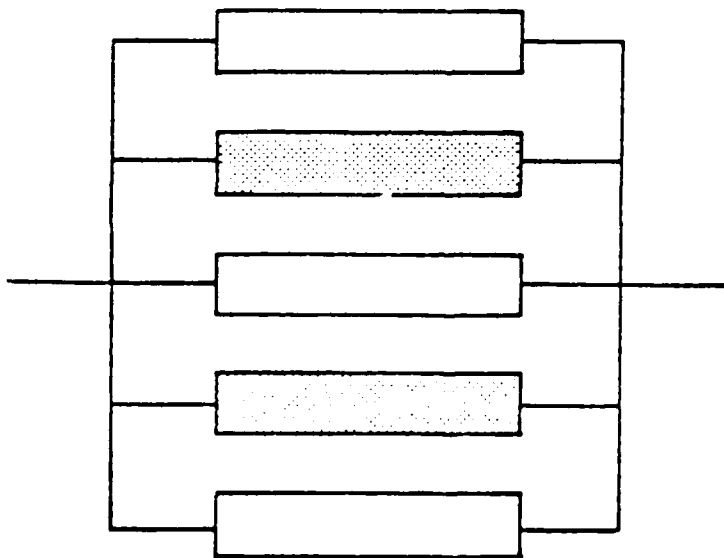
FIGURE 5.2.2.2.1.2-1: FIVE CHANNEL RECEIVER WITH TWO FAILURES ALLOWED

As long as three channels are operational, the system is classified as satisfactory. Each channel has a probability of 0.9 of surviving a 24 hour operation period without failure. Thus, two channel failures are allowed. What is the probability that the receiver will survive a 24 hour mission without loss of more than two channels?

Let n = 5 = number of channels
     r = 2 = number of allowable channel failures
     p = 0.9 = probability of individual channel success
     q = 0.1 = probability of individual channel failure
     x = number of successful channels
     P(S) = probability of system success

Then

$$P(S) = \sum_{x=3}^{n} \frac{n!}{x!(n-x)!} p^x q^{n-x}$$

$$= \frac{5!}{3!2!} (0.9)^3 (0.1)^2 + \frac{5!}{4!1!} (0.9)^4 (0.1)^1$$

$$+ \frac{5!}{5!0!} (0.9)^5 (0.1)^0$$

$$= 0.99144$$

This is the probability that three or more of the five channels will survive the 24 hour operating period.

The problem can be solved another way, by subtracting the probability of three or more failures from one, e.g.:

$$P(S) = 1 - P(F)$$

$$= 1 - \sum_{x=(r+1)}^{n} \frac{n!}{n!(n-x)!} q^x p^{n-x}$$

$$= 1 - \left[\frac{5!}{3!2!} (0.1)^3 (0.9)^2 + \frac{5!}{4!1!} (0.1)^4 (0.9)^1 \right.$$

$$\left. + \frac{5!}{5!0!} (0.1)^5 (0.9)^0 \right]$$

$$= 1 - 0.00856 = 0.99144 \text{ as before}$$

Note the change in notation (only) that x now represents the number of failures and q^x is the probability of x failures whereas before x represented the number of successes and p^x was the probability of x successes.

Computations involving the binomial distribution become rather unwieldy for even small sample sizes; however, complete tables of the binomial pdf and cdf are available in many statistics texts.

5.2.2.2.2 POISSON DISTRIBUTION

This distribution is used quite frequently in reliability analysis. It can be considered an extension of the binomial distribution when n is infinite. In fact, it is used to approximate the binomial distribution when $n \geq 20$ **and p $\leq$ 0.05.**

If events are Poisson distributed, they occur at a constant average rate and the number of events occurring in any time interval are independent of the number of events occurring in any other time interval. For example, the number of failures in a given time would be given by:

$$f(x) = \frac{a^x e^{-a}}{x!} \tag{5.44}$$

where x is the number of failures and a is the expected number of failures.

For the purpose of reliability analysis, this becomes:

$$f(x; \lambda, t) = \frac{(\lambda t)^x e^{-\lambda t}}{x!} \tag{5.45}$$

where:

λ = failure rate
t = length of time being considered
x = number of failures

The reliability function, R(t), or the probability of zero failures in time t is given by:

$$R(t) = \frac{(\lambda t)^0 e^{-\lambda t}}{0!} = e^{-\lambda t} \tag{5.46}$$

or our old friend the exponential distribution.

In the case of redundant equipments, the R(t) might be desired in terms of the probability of r or fewer failures in time t. For that case

$$R(t) = \sum_{x=0}^{r} \frac{(\lambda t)^x e^{-\lambda t}}{x!} \tag{5.47}$$

5.2.2.2.2.1 EXAMPLE WITH PERMISSIBLE NUMBER OF FAILURES

A Minuteman launch console has an average failure rate (λ) of 0.001 lamp failures per hours. What is the reliability for a 500 hour mission if the number of lamp failures cannot exceed 2?

$$\lambda = 0.001$$

$$t = 500$$

$$r \leq 2$$

$$\lambda t = 0.5$$

$$R(500) = \sum_{r=0}^{2} \frac{(0.5)^r e^{-0.5}}{r!}$$

$$= e^{-0.5} + 0.5\, e^{-0.5} + \frac{(0.5)^2 e^{-0.5}}{2}$$

$$= 0.986$$

5.2.2.2.2.2 REDUNDANT SYSTEM EXAMPLE

Assume a partially redundant system of ten elements. An average of λ failures per hour can be expected if each failure is instantly repaired or replaced. Find the probability that x failures will occur if the system is put in operation for t hours and each failure is repaired as it occurs.

If λ is the average number of failures per element for one hour, then t is the average number of element failures for t hours. Hence,

$$f(x) = \frac{e^{-\lambda t}(\lambda t)^x}{x!}$$

With n of these elements in the system, the average number of failures in t hours would be $n\lambda t$, and

$$f(x) = \frac{e^{-n\lambda t}(n\lambda t)^x}{x!}$$

If $\lambda = 0.001$ per hour, t = 50 hours, for n = 10, then

$$m = n\lambda t = 10(.001)50 = 0.5$$

$$f(x) = \frac{e^{-0.5}(0.5)^x}{x!}$$

$$f(x=0) = .607 = P(0)$$
$$f(x=1) = .303 = P(1)$$
$$f(x=2) = .076 = P(2)$$

The system then has a probability of 0.607 of surviving the 50 hour mission with no element failures; a probability of 0.91 (the sum of P(0) and P(1)) of surviving with no more than one element failure. There is a 9% chance that two or more failures will occur during the mission period. If the system will perform satisfactorily with nine elements, and, if further, we are permitted one on-line repair action during the mission (to repair a second failure), then system reliability during the mission is 0.986 (assuming instantaneous repair or replacement capability). This illustrates the advantage of on-line repairs, to permit failure occurrence without sacrificing reliability.

5.2.3   FAILURE MODELING

Failure modeling is a key to reliability engineering. Validated failure rate models are essential to the development of prediction techniques, allocation procedures, design and analysis methodologies, test and demonstration procedures/ control procedures, i.e. in other words, all of the elements needed as inputs for sound decisions to insure that an item can be designed and manufactured so that it will perform satisfactorily and economically over its useful life.

Inputs to failure rate models are operational field data, test data, engineering judgment, and physical failure information. These inputs are used by the reliability engineer to construct and validate statistical failure rate models (usually having one of the distributional forms described previously) and to estimate their parameters.

5.2.3.1 TYPICAL FAILURE RATE CURVE

Figure 5.2.3.1-1 shows a typical time versus failure rate curve for equipment. This is the well known "bathtub curve," which, over the years, has become widely accepted by the reliability community. It has proven to be particularly appropriate for electronic equipment and systems. Note that it displays the three failure rate patterns previously described (DFR, CFR, IFR).

Zone I is the infant mortality (DFR) period characterized by an initially high failure rate. This is normally the result of poor design, the use of substandard components, or lack of adequate controls in the manufacturing process. When these mistakes are not caught by quality control inspections, an early failure is likely to result. Early failures can be eliminated by a "burn in" period during which time the equipment is operated at stress levels closely approximating the intended actual operating conditions. The equipment is then released for actual use only when it has successfully passed through the "burn-in" period. For most well described complex equipment, a 48 hour "burn-in" is usually adequate to "cull out" a large proportion of the infant mortality failures.

Zone II, the useful life period, is characterized by an essentially constant failure rate (CFR). This is the period dominated by chance failures. Chance failures are those failures that result from strictly random or chance causes. They cannot be eliminated by either lengthy burn-in periods or good preventive maintenance practices. Equipment is designed to operate under certain conditions and up to certain stress levels. When these stress levels are exceeded due to random unforeseen or unknown events, a chance failure will occur. While reliability theory and practice is concerned with all three types of failures, its primary concern is with chance failures, since they occur during the useful life period of the equipment. Figure 5.2.3.1-1 is somewhat deceiving, since Zone II is usually of much greater length than Zones I or III. The time when a chance failure will occur cannot be predicted; however, the likelihood or probability that one will occur during a given period of time within the useful life can be determined by analyzing the equipment design. If the probability of chance failure is too great, either design changes must be introduced or the operating environment made less severe.

This CFR period is the basis for application of most reliability engineering design methods. Since it is constant, the exponential distribution of time to failure is applicable and is the basis for the design and prediction procedures spelled out in documents such as MIL-HDBK-217.

The simplicity of the approach utilizing the exponential distribution, as previously indicated, makes it extremely attractive. Fortunately, it is widely applicable for complex equipments and systems. If complex equipment consists of many components, each having a different mean life and variance which are randomly distributed, then the system malfunction rate becomes essentially constant as failed parts are replaced.
Thus, even though the failures might be wearout failures, the mixed population causes them to occur at random time intervals with a constant failure rate and exponential behavior. Figure 5.2.3.1-2 indicates this for a population of incandescent lamps in a factory. This has been verified for many equipments from electronic systems to bus motor overhaul rates.

Zone III, the wearout period, is characterized by an IFR as a result of equipment deterioration due to age or use. For example: mechanical components such as transmission bearings will eventually wear out and fail, regardless of how well they are made. Early failures can be postponed and the useful life of equipment extended by good design and maintenance practices. The only way to prevent failure due to wearout is to replace or repair the deteriorating component before it fails.

HAZARD RATE AS A FUNCTION OF AGE FAILURE
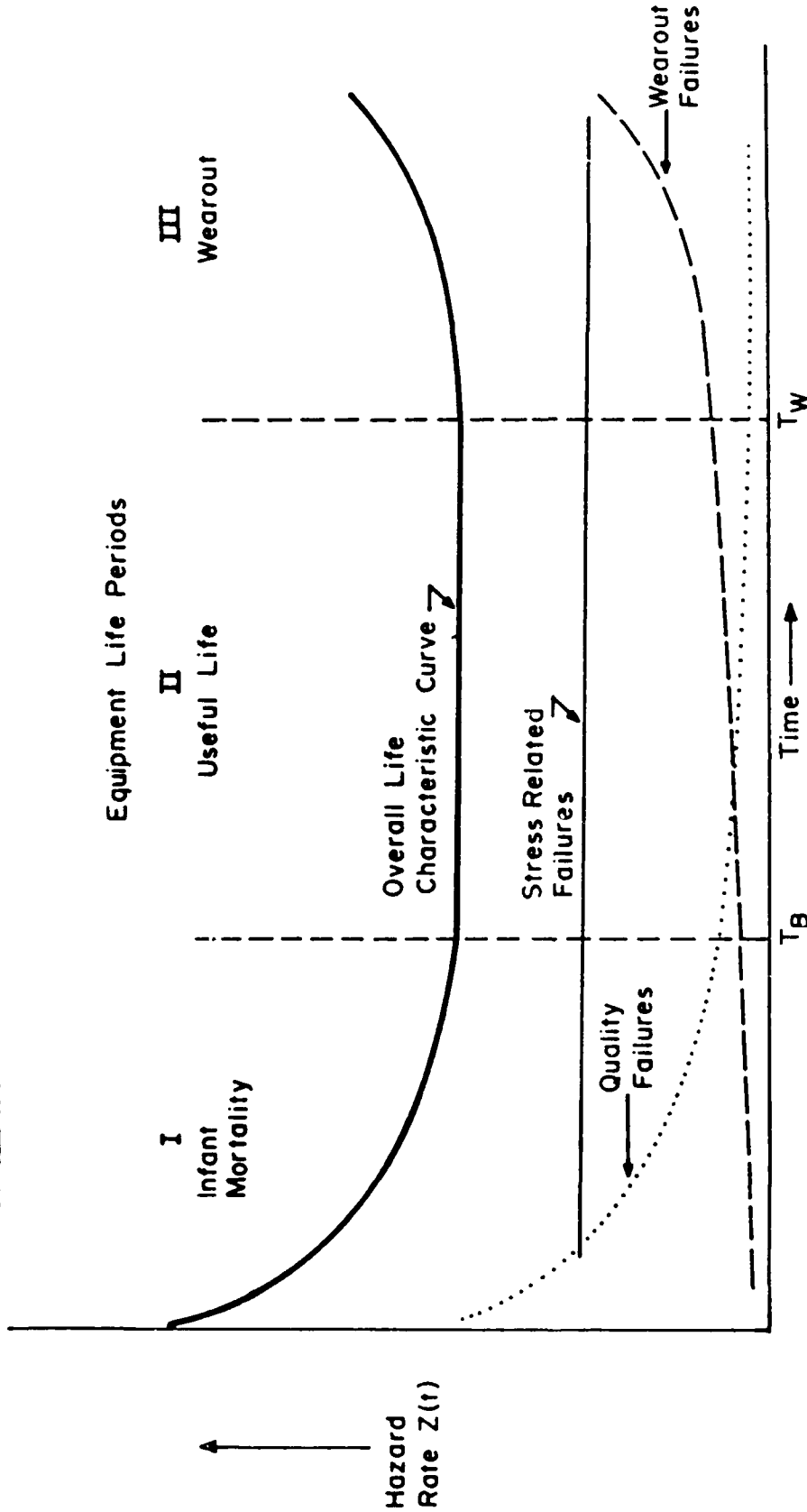
FIGURE 5.2.3.1-1: HAZARD RATE AS A FUNCTION OF AGE FAILURE
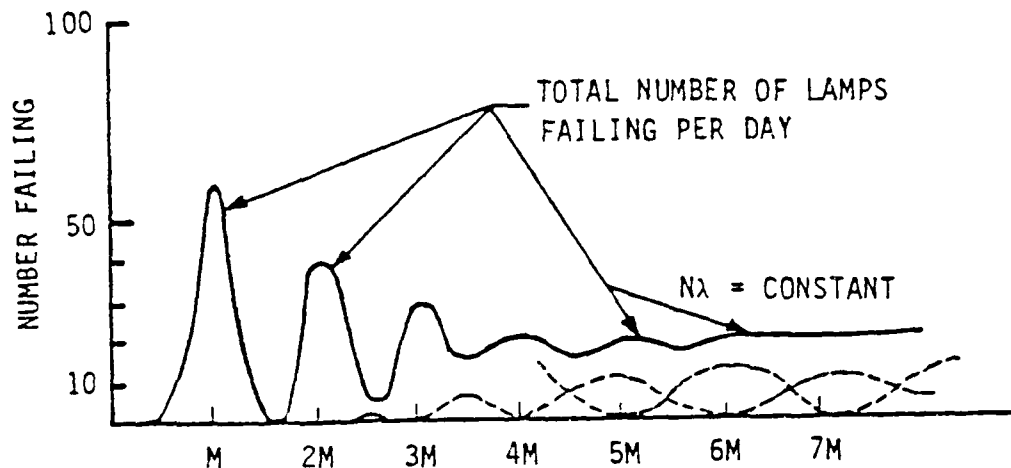
FIGURE 5.2.3.1-2: STABILIZATION OF FAILURE FREQUENCY

Since modern electronic equipment is almost completely composed of semi-conductor devices which really have no short term wearout mechanism, except for perhaps electromigration, one might question whether predominantly electronic equipment will even reach Zone III of the bathtub curve.

From Figure 5.2.3.1-1, it can be seen that different statistical distributions might be used to characterize each zone. For example, the infant mortality period might be represented by Gamma or Weibull, the useful life period by the exponential, and the wearout period by gamma or normal distributions.

The rest of this section will be devoted to models using the exponential distribution since it is applicable during the useful life period, which is the longest period of an equipment's life.

5.2.4   RELIABILITY MODELING OF SIMPLE STRUCTURES

In this section, the reliability functions of some simple, well known structures will be derived.   These functions are based upon the exponential distribution of time to failure.

5.2.4.1 SERIES CONFIGURATION

The simplest and perhaps most commonly occurring configuration in relia-
bility mathematical modeling is the series configuration. The
successful operation of the system depends on the proper functioning of
all the system components. A component failure represents total system
failure. A series reliability configuration is represented by the block
diagram as shown in Figure 5.2.4.1-1 with n components. Further, assume
that the failure of any one component is statistically independent of
the failure or success of any other. This is usually the case for most
practical purposes. If this is not the case, then conditional
probabilities must be used, which only increase the complexity of the
calculations.
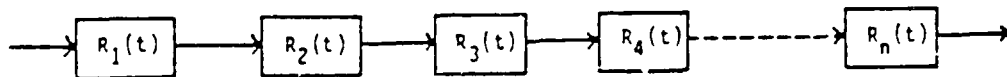
FIGURE 5.2.4.1-1: SERIES CONFIGURATION

Thus, for the configuration of Figure 5.2.4.1-1, under the assumptions
made, the series reliability is given by

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) \ldots R_n(t) \qquad (5.48)$$

$$= \prod_{i=1}^{n} R_i(t)$$

If, as we said before, a constant failure rate, λ, is assumed for each
component, which means the exponential distribution for the reliability
function, then

$$R_S(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} \ldots e^{-\lambda_n t}$$

$$= \exp \quad - \sum_{i=1}^{n} \lambda_i t \qquad (5.49)$$

where

$$\lambda = \lambda_1 + \lambda_2 + \ldots \lambda_n$$

$$= \frac{1}{\theta}$$

Thus, the system failure rate, λ, is the sum of the individual component failure rates and the system mean life, $\theta = 1/\lambda$.

Consider a system composed of 400 component parts each having an exponential time to failure density function. Let us further assume that each component part has a reliability of 0.99 for some time t. The system reliability for the same time t is

$$R(t) = 0.99^{400} = 0.018$$

Out of 1,000 component system, 982 would fail to survive to time t.

Remember for the case of component replacement upon failure,

$$MTBF = \theta = \frac{1}{\lambda}, \text{ and } R = e^{-t/MTBF}$$

The reader should keep in mind that, for the exponential distribution, the probability of surviving one MTBF without failure is

$$R = e^{-1} = 0.368 \text{ or } 37\%$$

5.2.4.2 PARALLEL CONFIGURATION

The next most commonly occurring configuration encountered in reliability mathematical modeling is the parallel configuration as shown in the reliability block diagram of Figure 5.2.4.2-1.
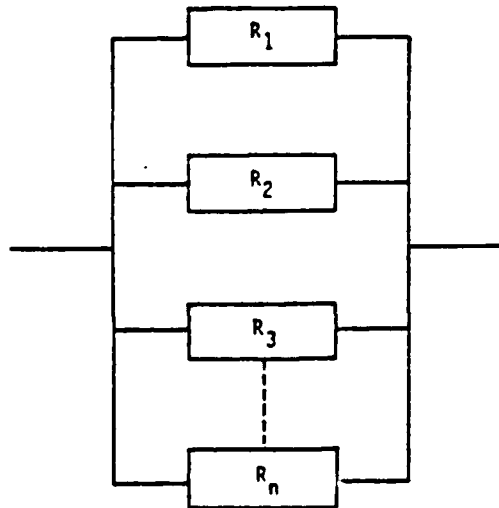
FIGURE 5.2.4.2-1: PARALLEL CONFIGURATION

For this case, for the system to fail, all of the components would have to fail. Letting $Q_i = 1-R_i = 1-e^{\lambda_i t}$, the probability of failure (or unreliability) of each component, the unreliability of the system would be given by

$$Q_S = Q_1 \cdot Q_2 \cdots Q_n = \prod_{i=1}^{n} Q_i \qquad (5.50)$$

and the reliability of the system would be

$$R_S = 1 - Q_S \qquad (5.51)$$

since $R + Q = 1$

Consider such a system composed of five parallel components, each with a reliability of 0.99. Then

$$Q_i = 1 - R_i = 1 - 0.99 = 0.01$$

$$Q_S = (0.01)^5 = 10^{-10}$$

$$= 0.0000000001$$

$$R_S = 1 - Q_S = 0.9999999999$$

Thus, parallel configurations, or the use of redundancy, is one of the design procedures used to achieve extremely high system reliability, greater than the individual component reliabilities. Of course, this is a very simple concept, which becomes more complicated in actual practice. Redundancy design techniques will be described in more detail in Section 7.

Of course most practical equipments and systems are combinations of series and parallel components as shown in Figure 5.2.4.2-2.
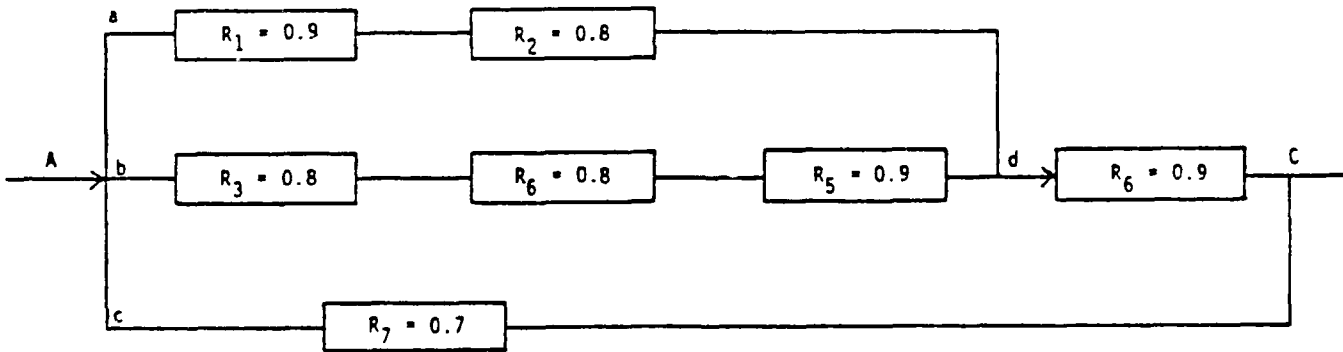
FIGURE 5.2.4.2-2: COMBINED CONFIGURATION NETWORK

To solve this network, one merely uses the previously given series and parallel relationships to decompose and recombine the network step by step. For example,

$$R_{ad} = R_1 \cdot R_2 = (0.9)(0.8) = 0.72$$

$$R_{bd} = R_3 \cdot R_4 \cdot R_5 = (0.8)(0.8)(0.9) = 0.576$$

but R_{ad} and R_{bd} are in parallel; thus, the unreliability of this parallel subsystem (S_1) is

$$Q_{S_1} = Q_{ad} \cdot Q_{bd}$$

$$= (1-R_{ad}) \cdot (1-R_{bd})$$

$$= (1-0.72)(1-0.576) = (0.28)(0.424)$$

$$= (0.119)$$

and its reliability is

$$R_{S_1} = 1-Q_{S_1} = 1 - 0.119 \quad 0.88$$

Now the network has been decomposed to
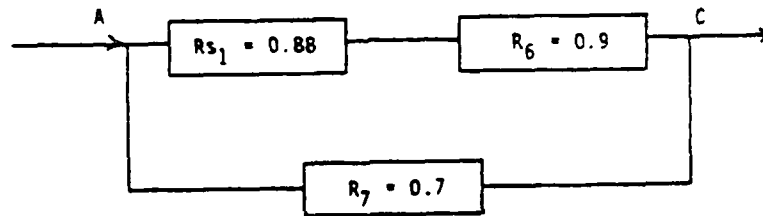
Letting R_{S_2} equal the combined reliability of R_{S_1} and R_6 in series

$$R_{S_2} = R_{S_1} \cdot R_6 = (0.88)(0.9) = 0.792$$

$$Q_{S_2} = 1 - R_{S_2} = 1 - 0.792 = 0.208$$

$$Q_7 = 1 - R_7 = 1 - 0.7 = 0.3$$

Since Q_{S_2} and Q_7 are in parallel, the total system unreliability is

$$Q_{A_C} = Q_{S_2} \cdot Q_7 = (0.208)(0.3) = 0.06$$

and the total network reliability is

$$R_{AC} = 1 - Q_{AC} = 1 - 0.06 = 0.94$$

thus, the reliability of the combined network is 0.94.

As the system network increases in complexity, the mathematics of system analysis becomes more laborious and are best handled by computerized techniques described in Section 7.

5.2.4.3 K-OUT-OF-N CONFIGURATION

A system consisting of n components or subsystems, of which only k need to be functioning for system success, is called a k-out-of-n configuration. For such a system, k is less than n. An example of such a system might be an air traffic control system with n displays of which k must operate to meet the system reliability requirement.

For the sake of simplicity, let us assume that the units are identical, they are all operating simultaneously, and failures are statistically independent.

Then,

R = reliability of one unit for a specified time period
Q = unreliability of one unit for a specified time period

and $R + Q = 1$

For n units

$$(R + Q)^n = 1$$

$$(R + Q)^n = R^n + nR^{n-1} Q + \frac{n(n-1)}{2!} R^{n-2} Q^2 + \frac{n(n-1)(n-2) R^{n-3} Q^3}{3!}$$

$$\dots\dots + Q^n = 1$$

This is nothing more than the familiar binomial expansion of $(R + Q)^n$

Thus,

$$P \left[\text{at least } (n-1) \text{ surviving}\right] = R^n + nR^{n-1} Q$$

$$P \left[\text{at least } (n-2) \text{ surviving}\right] = R^n + nR^{n-1} Q + \frac{n(n-1) R^{n-2} Q^2}{2!}$$

$$P \left[\text{at least 1 surviving}\right] = 1 - Q^n$$

Let us look at the specific case of four display equipments which meet the previously mentioned assumptions.

$$(R + Q)^4 = R^4 + 4R^3 Q + 6R^2 Q^2 + 4RQ^3 + Q^4 = 1$$

from which

$$R^4 = P \text{ (all four will survive)}$$

$$4R^3 Q = P \text{ (exactly 3 will survive)}$$

$$6R^2 Q^2 = P \text{ (exactly 2 will survive)}$$

$$4RQ^3 = P \text{ (exactly 1 will survive)}$$

$$Q^4 = P \text{ (all will fail)}$$

We are usually interested in k out of n surviving

$$R^4 + 4R^3 Q = 1 - 6R^2 Q^2 - 4RQ^3 - Q^4 = P \text{ (at least 3 survive)}$$

$$R^4 + 4R^3 Q + 6R^2 Q^2 = 1 - 4RQ^3 - Q^4 = P \text{ (at least 2 survive)}$$

$$R^4 + 4R^3 Q + 6R^2 Q^2 + 4RQ^3 = 1 - Q^4 = P \text{ (at least 1 survive)}$$

If the reliability of each display for some time t is 0.9, what is the system reliability for time t if 3 out of 4 displays must be working?

$$R_S = R^4 + 4R^3 Q = (0.9)^4 + 4(0.9)^3 (0.01)$$

$$= 0.6561 + 0.029 = 0.685$$

A similar example would be the case of launching 4 missiles, each of which had a probability of 0.9 of successfully hitting its target. What is the probability that at least 3 missiles will be on target? The procedure and result would be the same as the previous example.

For the case where all units have different reliabilities (or probabilities of success) the analysis becomes more difficult for the same assumptions. Let us look at the case of three units with reliabilities of R_1, R_2, and R_3, respectively. Then,

$$(R_1 + Q_1) (R_2 + Q_2) (R_3 + Q_3) = 1 \qquad (5.53)$$

The above equation can be expanded to permit analysis as was done for the previous case of equal reliabilities. An easy way of bookkeeping is to set up boolean truth tables where $R_i = 1$, $Q_i = 0$, as follows

1	2	3		
0	0	0	$Q_1 Q_2 Q_3$ = all three fail
0	0	1	$Q_1 Q_2 R_3$ = 1 & 2 fail, 3 survives
0	1	0	$Q_1 R_2 Q_3$ = 1 & 3 fail, 2 survives
0	1	1	$Q_1 R_2 R_3$ = 1 fails, 2 & 3 survives
1	0	0	$R_1 Q_2 Q_3$ = 2 & 3 fail, 1 survives
1	0	1	$R_1 Q_2 R_3$ = 2 fails, 1 & 3 survive
1	1	0	$R_1 R_2 Q_3$ = 3 fails, 1 & 2 survive
1	1	1	$R_1 R_2 R_3$ = all three survive

For the previous example, if we were not interested in which particular unit fails, we can set up expressions for at least 1, 2 or 3 units surviving. For example

$$P \text{ (at least 2 units surviving)} = R_1 R_2 R_3 R_1 R_2 Q_3 +$$
$$R_1 Q_2 R_3 + Q_1 R_2 R_3$$

The simple combinational reliability models developed in this section were, primarily, for illustrative purposes to demonstrate the basic theory involved. More complex examples are addressed in the references at the end of this section and in Section 7.

5.2.5 BAYESIAN STATISTICS IN RELIABILITY ANALYSIS

5.2.5.1 INTRODUCTION

During the past decade, Bayesian statistics have been increasingly used in reliability analysis. The advantage to the use of Bayesian statistics is that it allows prior information (e.g., predictions, test results, engineering judgment) to be combined with more recent information, such as test or field data, in order to arrive at a prediction/assessment of reliability based upon a combination of all available data. It also permits the reliability prediction/assessment to be continually updated as more and more test data are accumulated. The Bayesian approach is intuitively appealing to design engineers because it permits them to use engineering judgment, based upon prior experience with similar equipment designs, to arrive at an initial estimate of the reliability of a new design. It is particularly useful for assessing the reliability of new systems where only limited field data exists. For example, it can be argued that the result of a reliability test is not only information available on a product, but that information which is available prior to the start of the test, from component and subassembly tests, previous tests on the product, and even intuition based upon experience. Why should this information not be used to supplement the formal test result? Bayes' Theorem can be used to combine these results.

Thus, the basic difference between Bayesian and non Bayesian (classical) approaches is that the former uses both current and prior data, whereas the latter uses current data only.

One of the main disadvantages to the use of the Bayesian approach is that one must be extremely careful in choosing the prior probabilities based upon part experience or judgment. If these are capriciously or arbitrarily chosen for Bayesian analysis, the end results of Bayesian analysis may be inaccurate and misleading. Thus, the key to the successful use of the Bayesian method resides in the appropriate choice of prior probability distributions.

Bayes' analysis begins by assigning an initial reliability on the basis of whatever evidence is currently available. The initial prediction may be based solely on engineering judgment or it may be based on data from other similar types of items. Then, when additional test data is

subsequently obtained, the initial reliabilities are revised on the basis of this data by means of Bayes' Theorem. The initial reliabilities are known as prior reliabilities in that they are assigned before the acquisition of the additional data. The reliabilities which result from the revision process are known as posterior reliabilities.

5.2.5.2   BAYES' THEOREM

From basic probability theory, Bayes' Theorem is given by

$$Pr\left[A/B\right] = Pr\ A\ \frac{Pr\left[B/A\right]}{Pr\left[B\right]} \tag{5.54}$$

In the specific framework and context of reliability, the various terms in the equation may be motivated and defined as follows:

A   an hypothesis or statement of belief. ("The reliability of this component is 0.90.")

B   a piece of evidence, such as a reliability test result that has bearing upon the truth or credibility of the hypothesis. ("The component failed on a single mission trial.")

$Pr\left[A\right]$ the prior probability: the probability we assign to the hypothesis A before evidence B becomes available. ("We believe, based on engineering experience, that there is a 50/50 chance that the reliability of this component is about 0.90, as opposed to something drastically lower, e.g., Pr(A) = 0.5.")

$Pr\left[B/A\right]$ the likelihood: the probability of the evidence assuming the truth of the hypothesis. ("The probability of the observed failure, given that the true component reliability is indeed 0.90, is obviously 0.10.")

$Pr\left[B\right]$ the probability of the evidence B, evaluated over the entire weighted ensemble of hypotheses A_i.

$Pr\left[A/B\right]$ the posterior probability of A, given the evidence B.

The posterior probability is the end result of the application of Bayes' Equation. The following examples illustrate the use of Bayesian statistics in reliability analysis.

5.2.5.2.1 BAYES' EXAMPLE (DISCRETE DISTRIBUTION)

To demonstrate the use of Bayes' Equation within the framework of the binomial estimation of reliability, consider the following simplistic (but illustrative) example:

o   We wish to estimate the reliability of a simple pyrotechnic device which, upon being tested, either fires (success) or doesn't fire (failure).

o   We have in the warehouse two lots of this component, one of which we have been assured has a reliability of R = 0.9 (that is, in the long term, 9 of 10 randomly selected components will work). The other lot supposedly contains only 50% good items. Unfortunately, we have lost the identity of which lot is which.

o   After randomly selecting one of the lots (such that probability for each lot is 0.50), we then randomly select a single item from it (each item has equal chance of being chosen), which fails in test.

What can be said about all this in the context of Bayesian analysis?

First, terms must be defined (see Figure 5.2.5.2.1-1).

A_1 "Lot chosen has R = 0.50"

A_2 "Lot chosen has R = 0.90".

Then, from above,

$$Pr[A_1] = 0.5$$
$$Pr[A_2] = 0.5.$$
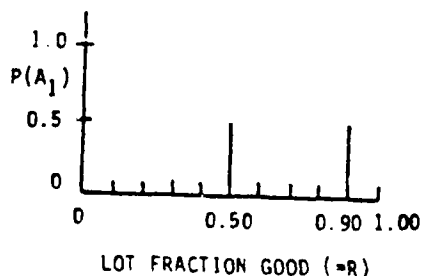
FIGURE 5.2.5.2.1-1:   SIMPLE PRIOR DISTRIBUTION

Next, the test evidence must be considered. Therefore

B   "One unit was tested and it failed."

The likelihoods required for Bayes' Equation are obviously:

$$Pr\overline{[B/A_1]} = Pr\overline{[single\ test\ failure/R = 0.5]} = (1 - 0.5) = 0.5$$

$$Pr\overline{[B/A_2]} = Pr\overline{[single\ test\ failure/R = 0.9]} = (1 - 0.9) = 0.1.$$

If A is partitioned into a set of states $\overline{[A_1...,}$ $\overline{A_n]}$ and if Pr $[A_i]$ and Pr $[B/A_i]$ are known for each i; then eq. (5.54) becomes

$$Pr[A_i/B] = Pr[A_i]\ \frac{Pr[B/A_i]}{\Sigma Pr[B/A_j]\ Pr[A_i]} = Pr[A_i]\ \frac{Pr[BIA_i]}{Pr[B]}$$

where the sum is over all n values of i. For this example, we have

$$Pr[B] = Pr[B/A_1]\ PR[A_1] + Pr[B/A_2]\ Pr[A_2]$$

$$= 0.5(0.5) + 0.1(0.5)$$

$$= 0.30.$$

Finally, all necessary inputs having been obtained, Bayes' Equation now yields:

$$Pr[A_1/B] = \frac{Pr[A_1]Pr[B/A_1]}{Pr[B]} = \frac{0.5(0.5)}{0.30} = 0.833,$$

$$Pr[A_2/B] = \frac{Pr[A_2]Pr[B/A_2]}{Pr[B]} = \frac{0.5(0.1)}{0.30} = 0.167$$

The prior distribution in Figure 5.2.5.2.1-1 has been transformed, under the impact of a single trial resulting in failure, to the posterior distribution depicted in Figure 5.2.5.2.1-2. The analyst may already be somewhat dubious that he has picked the lot with R = 0.9.

The process is usually a sequential one, i.e., as successive packets of new information $(B_1, B_2, B_3, ...)$ become available, the posterior degree of belief in proposition A_i is successively modified by each new increment of information.
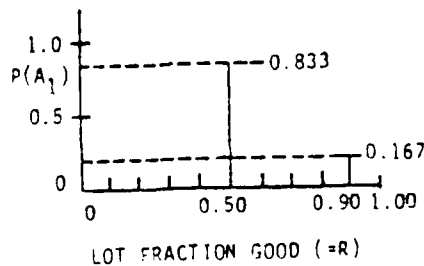
FIGURE 5.2.5.2.1-2:   SIMPLE POSTERIOR DISTRIBUTION

Another way of visualizing this situation is by constructing a tree diagram like the one shown in Figure 5.2.5.2.1-3, where the probability of the final outcome "B" is given by the products of the probabilities corresponding to each individual branch.
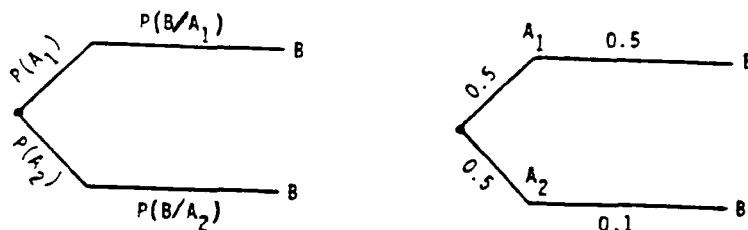
FIGURE 5.2.5.2.1-3: TREE DIAGRAM EXAMPLE

$P(B) = (0.5)(0.5) + (0.5)(0.1) = 0.3$

$$P(A_1/B) = \frac{P(A_1)P(B/A_1)}{P(B)}$$

$$= \frac{(0.5)(0.5)}{(0.3)} = 0.8333$$

$$P(A_2/B) = \frac{P(A_2)P(B/A_2)}{P(B)}$$

$$= \frac{(0.5)(0.1)}{(0.3)} = 0.167$$

5.2.5.2.2 BAYES' EXAMPLE (CONTINUOUS DISTRIBUTION)

As with the discrete example, the basic equation can be extended to cover continuous probability distributions. For example, assume that based upon prior test results, engineering judgment, etc. it has been observed that r failures occur in time t. The probability density function of t is a gamma distribution given by

$$f(\lambda) = \frac{(t)\ \lambda^{r-1}\ e^{-\lambda t}}{\Gamma(r)} \tag{5.56}$$

where t is the amount of testing time (scale parameter)
    r is the number of failures (shape parameter)

From Section 5.2.2.1.5, we know that

$$\hat{\mu}_0 \text{ (mean failure rate)} = \frac{\text{shape parameter}}{\text{scale parameter}} = \frac{r}{t} \qquad (5.57)$$

and

$$\hat{\sigma}_0^2 = r/t^2 \qquad (5.58)$$

Eqs (5.57 and 5.58) represent the prior failure rate and the prior variance. Let us assume that these are given by 0.02 and $(0.01)^2$, respectively. Assume that we then run a reliability test for 500 hours (t') and observe 14 failures (r'). What is the posterior estimate of failure rate?

The basic expression for the continuous posterior distribution is given by

$$f(\lambda/t) = \frac{f(\lambda)f(t/\lambda)}{f(t)} \qquad (5.59)$$

where $f(\lambda)$ is the prior distribution of λ, Eq. (5.56)

$f(t/\lambda)$ is the sampling distribution of t based upon the new data

$f(t)$ is $\int_0^\infty f(\lambda) \, f(t/\lambda) \, d\lambda$

$f(\lambda/t)$ is the posterior distribution of λ combining the prior distribution and the new data.

It can be shown that the posterior distribution resulting from performing the operations indicated in Eq. (5.59) is

$$f(\lambda/t) = \frac{(t+t') \quad \lambda^{r+r'-1} \exp\left[-\lambda(t+t')\right]}{\Gamma(r+r')} \qquad (5.60)$$

which is another gamma distribution with

shape parameter = $(r + r')$

scale parameter = $(t + t')$

Using Eqs. (5.57) and (5.58) to solve for r and t, we obtain

$$r = \hat{\mu}_0 t = \hat{\sigma}_0^2 t^2$$

$$\therefore \ t = \frac{\hat{\mu}_0}{\hat{\sigma}_0^2} = \frac{0.02}{(0.01)^2} = \frac{2 \times 10^{-2}}{1 \times 10^{-4}} = 200$$

$$r = \hat{\mu}_0 t = (2 \times 10^{-2})(200) = 4$$

Returning to the posterior gamma distribution, Eq. (5.60) we know that the posterior failure rate is

$$\hat{\mu}_1 = \frac{\text{shape parameter}}{\text{scale parameter}} = \frac{(r+r')}{(t+t')}$$

From the test data $r' = 14$, $t' = 500$, and we found that $r = 4$, and $t = 200$, thus

$$\hat{\mu}_1 = \frac{4+14}{200+500} = \frac{18}{700} = 0.0257$$

This compares with the traditional estimate of failure rate from the test result $14/500 = 0.028$. Thus, the use of prior information resulted in a failure rate estimate lower than that given by the test results.

5.3 MAINTAINABILITY THEORY

In reliability, one is concerned with designing an item to last as long as possible without failure; in maintainability, the emphasis is on designing an item so that a failure can be acquired as quickly as possible. The combination of high reliability and high maintainability results in high system availability; the theory of which is developed in Section 5.4.

Maintainability, then, is a measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure. It is a function of the equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed.

As with reliability, maintainability parameters are also probabilistic and are analyzed by the use of continuous and discrete random variables, probabilistic parameters, and statistical distributions. An example of a discrete maintainability parameter is the number of maintenance actions completed in some time t, whereas an example of a continuous maintainability parameter is the time to complete a maintenance action.

5.3.1 BASIC CONCEPTS

A good way to look at basic maintainability concepts is in terms of functions which are analogous to those in reliability. They may be derived in a way identical to that done for reliability in the previous section by merely substituting t (time-to-restore) for t (time-to-failure), u (repair rate) for λ (failure rate), and M (t) probability of successfully completing a repair action in time t, or $P(T \leq t)$ for F(t) probability of failing by age t, or $P(T \leq t)$. In other words, the following correspondences prevail in maintainability and reliability engineering functions.

(1) To the time-to-failure probability density function (pdf) in reliability corresponds the time-to-maintain pdf in maintainability.

(2) To the failure rate function in reliabilty corresponds the repair rate function in maintainability. Repair rate is the rate with which a repair action is performed and is expressed in terms of the number of repair actions performed and successfully completed per hour.

(3) To the probability of system failure, or system unreliability, corresponds the probability of successful system maintenance, or system maintainability. These and other analogous functions are summarized in Table 5.3.1-1.

TABLE 5.3.1-1: COMPARISON OF BASIC RELIABILITY AND MAINTAINABILITY FUNCTIONS

RELIABILITY	MAINTAINABILITY	
Time to Failure (pdf) $f(t)$	Time to Repair (pdf) $g(t)$	(5.61)
Reliability $R(t) = \int_{t}^{\infty} f(t)dt$	Maintainability $M(t) = \int_{0}^{(t)} g(t)dt$	(5.62)
Failure Rate $\lambda(t) = \dfrac{f(t)}{R(t)}$	Repair Rate $u(t) = \dfrac{g(t)}{1-M(t)}$	(5.63)
Mean Time to Failure $MTTF = \int_{-\infty}^{\infty} t\, f(t)dt$ $= \int_{0}^{\infty} R(t)dt$	Mean Time to Repair $MTTR = \int_{-\infty}^{\infty} t\, g(t)dt$	(5.64)
Pdf of Time to Failure $f(t) = \lambda(t) \cdot R(t)$ $= \lambda(t) \exp\left[-\int_{0}^{t} \lambda(t)dt \right]$	Pdf of Time to Repair $g(t) = u(t)\left(1-M(t)\right)$ $= u(t) \exp\left[-\int_{0}^{t} u(t)dt \right]$	 (5.65)

Thus as illustrated in Figure 5.3.1-1, maintainability can be expressed either as a measure of the time (T) required to repair a given percentage (P%) of all system failures, or as a probability (P) of restoring the system to operational status within a period of time (T) following a failure.

Some of the commonly used maintainability engineering terms are portrayed graphically in Figure 5.3.1-2 as a maintainability "function" derived as illustrated for the case where the pdf has a lognormal distribution. Points (1), (2), and (3) shown in the figure identify the mean, median, and maximum corrective time-to-repair, respectively.

Points (1), (2), and (3) are defined as follows:

(1) Mean Time to Repair, $\overline{M}_{ct}$ - the mean time required to complete a maintenance action, i.e., total maintenance downtime divided by total maintenance actions for a given period of time, given as:

$$M_{ct} = \frac{\Sigma(\lambda_i \overline{M}_{ct_i})}{\Sigma \lambda_i} \qquad (5.66)$$

where

λ_i = failure rate for the ith repairable element of the item for which maintainability is to be determined, adjusted for duty cycle, catastrophic failures, tolerance and interaction failures, etc., which will result in deterioration of item performance to the point that a maintenance action will be initiated

$\overline{M}_{ct_i}$ = average corrective time required to repair the ith repairable element in the event of its failure

(2) Median Time to Repair, $\widetilde{M}_{ct}$ - the downtime within which 50% of all maintenance actions can be completed

(3) Maximum Time to Repair - the maximum time required to complete a specified, e.g., 95%, percentage of all maintenance actions.

These terms will be described in more detail in the following sections, in terms of the form that they take, given the statistical distribution of time-to-repair.

5.3.2 STATISTICAL DISTRIBUTIONS USED IN MAINTAINABILITY MODELS

A smaller number of statistical distributions is used for maintainability analysis than for reliability analysis. This may be due to the fact that maintainability has traditionally lagged reliability theory in development.

The most commonly used distributions for maintainability analysis have been the normal, lognormal, and exponential. In fact, as the exponential distribution has been the one most widely used in

PROBABILITY
OF REPAIR P(t)

1.0

(P)

0

(T)
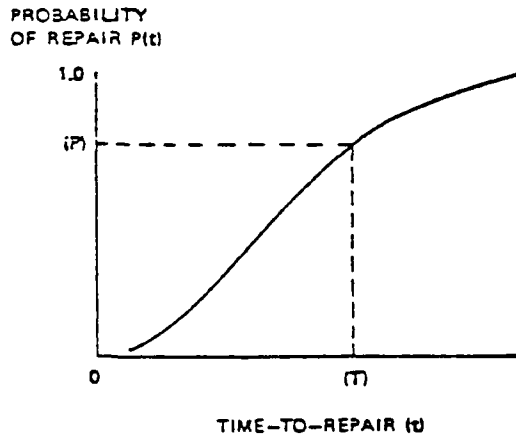
TIME-TO-REPAIR (t)

FIGURE 5.3.1-1: BASIC METHODS OF MAINTAINABILITY MEASUREMENT

RELATIVE FREQUENCY
OF REPAIRS REQUIRING
(t_r) HOURS TO COMPLETE

PROBABILITY DENSITY FUNCTION

PROBABILITY OF COMPLETING
REPAIR IN TIME (t_r)

MAINTAINABILITY FUNCTION,
CUMULATIVE

MEAN, $\bar{M}_{ct}$

MAXIMUM, $M_{max_{ct}}$

MEDIAN, $\widetilde{M}_{ct}$
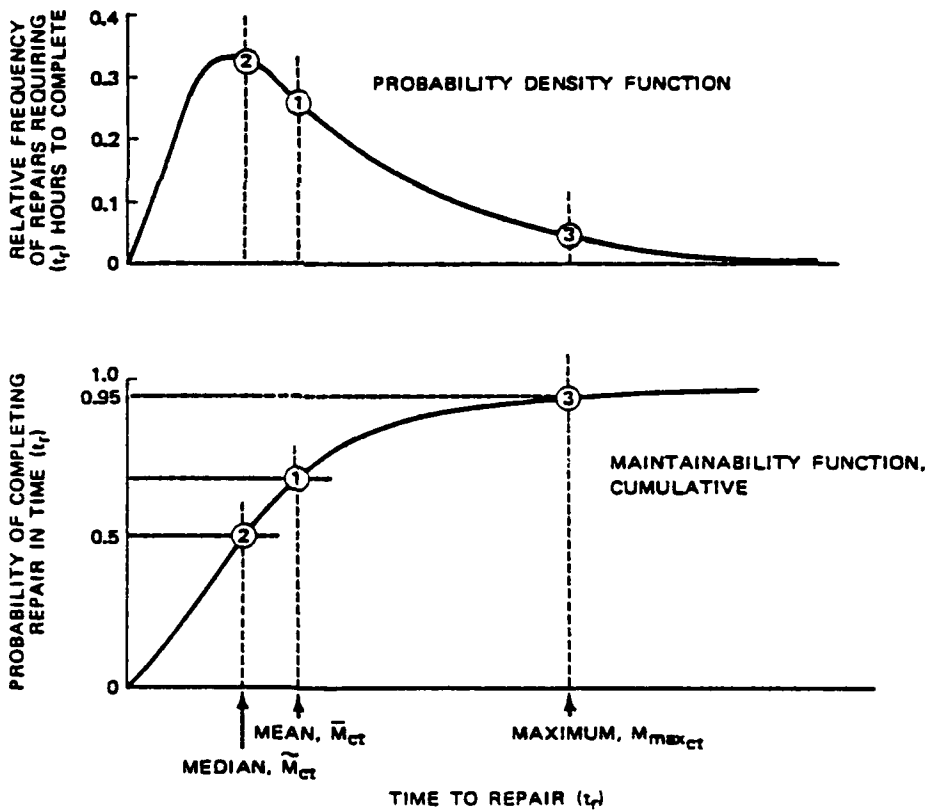
TIME TO REPAIR (t_r)

FIGURE 5.3.1-2: EXAMPLE MAINTAINABILITY FUNCTION DERIVED FROM
TIME-TO-REPAIR DISTRIBUTION

reliability analysis of equipment/systems, the lognormal distribution is the most commonly used for equipment/system maintainability analysis. A number of studies have validated the lognormal as being the most appropriate for maintainability analysis (Ref. 25).

Although the lognormal has been the most commonly used in maintainability analysis, other distributions such as the Weibull and gamma are also possible, depending upon the analysis of the data and the use of "goodness of fit" tests.

Since the form and expressions for the more commonly used distributions were previously given in Section 5.2.2, this section will concentrate on the use of the normal, exponential, and lognormal distribution, and give examples of their use in maintainability analysis.

5.3.2.1 LOGNORMAL DISTRIBUTION

As was stated previously, this is the most commonly used distribution in maintainability analysis and is the distribution called out in most DoD maintainability specifications as best representing repair times. It applies to most maintenance tasks and repair actions comprised of several subsidiary tasks of unequal frequency and time duration.

The probability density function is given by:

$$g(t = M_{ct_i}) = \frac{1}{M_{ct_i} S_{\log_e M_{ct}} \sqrt{2\pi}} \exp\left[-\frac{\left(\log_e M_{ct_i} - \overline{\log_e M_{ct}}\right)^2}{2\left(S_{\log_e M_{ct}}\right)^2}\right] \tag{5.67}$$

$$= \frac{1}{t\,\sigma_{t'}\,\sqrt{2\pi}}\; e^{-\frac{1}{2}\left(\frac{t' - \bar{t}'}{\sigma_{t'}}\right)^2} \tag{5.68}$$

where

$t = M_{ct_i}$ = repair time from each failure

$$\overline{\log_e M_{ct}} = \frac{\sum \log_e M_{ct_i}}{N}$$

$$S_{\log_e M_{ct}} = \sigma_{t'} = \sqrt{\frac{\sum(\log_e M_{ct_i})^2 - (\sum \log_e M_{ct_i})^2/N}{N-1}} \tag{5.69}$$

$$S_{log_eM_{ct}} = \sqrt{\frac{\Sigma t'_i{}^2 - (\Sigma t'_i)^2/N}{N-1}}$$

= standard deviation of log_e of repair times

$$t' = log_eM_{ct_i} = log_e t$$

$$\bar{t}' = \overline{log_eM_{ct}} = \frac{\Sigma t'_i}{N}$$

N = number of repair actions   (5.70)

the mean time to repair is given by

$$MTTR = \overline{M_{ct}} = \bar{t} = \int_0^\infty t \; g(t = M_{ct_i})dt \qquad (5.71)$$

(also see Eq. (5.66))

$$= exp \left[\overline{log_eM_{ct}} + \frac{1}{2}(S_{log_eM_{ct}})^2\right] \qquad (5.72)$$

$$= exp \left[\overline{t'} + \frac{1}{2}(\sigma_{t'})^2\right] \qquad (5.73)$$

the median time to repair is given by

$$\widetilde{M_{ct}} = \overset{u}{t} = antilog_e \frac{\Sigma \lambda_i \overline{log_e M_{ct}}}{\Sigma \lambda_i} \qquad (5.74)$$

$$= exp \; (\overline{log_eM_{ct}}) \qquad (5.75)$$

$$= exp \; (\overline{t'}) \qquad (5.76)$$

the maximum time to repair is given by

$$M_{max_{ct}} = t_{max} = antilog_e \; (\overline{log_eM_{ct}} + \phi S_{log_eM_{ct}}) \qquad (5.77)$$

$$= antilog_e \left[\overline{t'} + Z \; (t'_{1-a}) \; \overline{\sigma_{t'}}\right] \qquad (5.78)$$

where $\phi = z(t'_{1-a})$ = value from normal distribtuion function corresponding to the percentage point $(1-a)$ on the maintainability function for which $M_{max_{ct}}$ is defined

Most commonly used values of ϕ or $z(t_{1-a})$ are shown in Table 5.3.2.1-1.

TABLE 5.3.2.1-1: VALUES OF ϕ OR z $(t'_{1-\alpha})$ MOST COMMONLY USED IN
MAINTAINABILITY ANALYSIS

$1-\alpha$	ϕ or z $(t_{1-\alpha})$
0.80	0.8416
0.85	1.036
0.90	1.282
0.95	1.645
0.99	2.326

Following is an example of maintainability analysis of a system which has a lognormal distribution of repair times.

5.3.2.1.1 GROUND ELECTRONIC SYSTEM MAINTAINABILITY ANALYSIS EXAMPLE

Given the active repair times data of Table 5.3.2.1.1-1 on a ground electronic system find the following:

1. The probability density function, g(t)
2. The MTTR of the system
3. The median time to repair the system
4. The maintainability function
5. The maintainability for a 20 hour mission
6. The time within which 90% and 95% of the maintenance actions are completed.
7. The repair rate, u(t), at 20 hours.

TABLE 5.3.2.1.1-1: <u>TIME TO REPAIR DATA ON A GROUND ELECTRONIC SYSTEM</u>

Group No.	Times to repair t, hr	Frequency of observation n
1	0.2	1
2	0.3	1
3	0.5	4
4	0.6	2
5	0.7	3
6	0.8	2
7	1.0	4
8	1.1	1
9	1.3	1
10	1.5	4
11	2.0	2
12	2.2	1
13	2.5	1
14	2.7	1
15	3.0	2
16	3.3	2
17	4.0	2
18	4.5	1
19	4.7	1
20	5.0	1
21	5.4	1
22	5.5	1
23	7.0	1
24	7.5	1
25	8.8	1
26	9.0	1
27	10.3	1
28	22.0	1
$N' = 29$	24.5	1

1. Probability Density Function of $g(t)$

To determine the lognormal pdf of the times-to-repair given in Table 5.3.2.1.1-1, the values of $\bar{t}'$ and $\sigma_{t'}$, should be calculated from

$$\bar{t}' = \frac{\sum\limits_{j=1}^{N'} n_j\, t'_j}{\sum\limits_{j=1}^{N'} n_j} \tag{5.79}$$

where n_j is the number of identical observations given in the third column of Table 5.3.2.1.1-1, N' is the number of different-in-value observed times-to-repair, or number of data groups, which for this problem is N = 29, given in the second column of Table 5.3.2.1.1-1, and N is the total number of observed times-to-repair,

$$N = \sum\limits_{i=1}^{N'} n_j$$

which, for this example, is 46.

And

$$\sigma_{t'} = \left[\frac{\sum\limits_{i=1}^{N} (t'_i)^2 - N(\bar{t}')^2}{N-1} \right]^{\frac{1}{2}} = \left[\frac{\sum\limits_{j=1}^{N'} n_j(t'_j)^2 - N(\bar{t}')^2}{N-1} \right]^{\frac{1}{2}} \tag{5.80}$$

To facilitate the calculations, Table 5.3.2.1.1-2 was prepared. From Table 5.3.2.1.1-2, $\bar{t}'$ and $\sigma_{t'}$, are obtained as follows:

$$\overline{t'} = \frac{\sum\limits_{j=1}^{N'} n_j t'_j}{\sum\limits_{j=1}^{N'} n_j} = \frac{30.30439}{46}$$

or

$$\overline{t'} = 0.65879$$

TABLE 5.3.2.1.1-2: CALCULATIONS TO DETERMINE $\bar{t}'$ and σ_t
FOR THE DATA IN TABLE 5.3.2.1.1-1

t	$\log_e t = t'$	$(t')^2$	n	nt'	$n(t')^2$
0.2	-1.60944	2.59029	1	-1.60944	2.59029
0.3	-1.20397	1.44955	1	-1.20397	1.44955
0.5	-0.69315	0.48045	4	-2.77260	1.92180
0.6	-0.51083	0.26094	2	-1.02166	0.52188
0.7	-0.35667	0.12721	3	-1.07001	0.38163
0.8	-0.22314	0.04979	2	-0.44628	0.09958
1.0	0.00000	0.00000	4	0.00000	0.00000
1.1	0.09531	0.00908	1	0.09531	0.00908
1.3	0.26236	0.06884	1	0.26236	0.06884
1.5	0.40547	0.16440	4	1.62188	0.65760
2.0	0.69315	0.48045	2	1.38630	0.96090
2.2	0.78846	0.62167	1	0.78846	0.62167
2.5	0.91629	0.83959	1	0.91629	0.83959
2.7	0.99325	0.98655	1	0.99325	0.98655
3.0	1.09861	1.20695	2	2.19722	2.41390
3.3	1.19392	1.42545	2	2.38784	2.85090
4.0	1.38629	1.92181	2	2.77258	3.84362
4.5	1.50408	2.26225	1	1.50408	2.26225
4.7	1.54756	2.39495	1	1.54756	2.39495
5.0	1.60994	2.59029	1	1.60994	2.59029
5.4	1.68640	2.84394	1	1.68640	2.84394
5.5	1.70475	2.90617	1	1.70475	2.90617
7.0	1.94591	3.78657	1	1.94591	3.78657
7.5	2.01490	4.05983	1	2.01490	4.05983
8.8	2.17475	4.72955	1	2.17475	4.72955
9.0	2.19722	4.82780	1	2.19722	4.82780
10.3	2.33214	5.43890	1	2.33214	5.43890
22.0	3.09104	9.55454	1	3.09104	9.55454
24.5	3.19867	10.23151	1	3.19867	10.23151

$$N' = 29$$
$$\sum_{j=1}^{N'} n_j = 46 = N$$
$$\sum_{j=1}^{N'} n_j (t'_j)^2 = 75.84371$$
$$\sum_{j=1}^{N'} n_j t'_j = 30.30439$$

and from Eq. (5.80)

$$\sigma_{t'} = \left[\frac{75.84371 - 46 \, (0.65879)^2}{46-1} \right]^{\frac{1}{2}}$$

or

$$\sigma_{t'} = 1.11435$$

Consequently, the lognormal pdf representing the data in Table 5.3.2.1.1-1 is

$$g(t) = \frac{1}{t \, \sigma_{t'} \, \sqrt{2\pi}} \, e^{-\frac{1}{2} \left(\frac{t' - \overline{t'}}{\sigma_{t'}} \right)^2}$$

or

$$g(t) = \frac{1}{t(1.11435) \, \sqrt{2\pi}} \, e^{-\frac{1}{2} \left(\frac{t' - 0.65879}{1.11435} \right)^2}$$

where $t' = \log_e t$. The plot of this pdf is given in Figure 5.3.2.1.1-1 in terms of the straight times in hours. See Table 5.3.2.1.1-3 for the g(t) values used.

The pdf of the $\log_e t$ or of the t's is

$$g(t') = \frac{t}{t\sigma_{t'} \, \sqrt{2\pi}} \, e^{-\frac{1}{2} \left(\frac{t' - \overline{t'}}{\sigma_{t'}} \right)^2} = t \, g(t)$$

or

$$g(t') = \frac{1}{(1.11435)\sqrt{2\pi}} \, e^{-\frac{1}{2} \left(\frac{t' - 0.65879}{1.11435} \right)^2}$$

This pdf is that of a normal distribution which is what one should expect since if t follows a lognormal distribution, $\log_e t$ should be normally distributed. This is shown plotted in Figure 5.3.2.1.1-2, the values of g(t') were obtained from Table 5.3.2.1.1-3.

TABLE 5.3.2.1.1-3: The probability density of Time to Repair Data (From Table 5.3.2.1.1-1 based on the straight times to repair and the natural logarithm of the times to repair used to plot Figures 5.3.2.1.1-1 and 5.3.2.1.1-2, respectively.*)

Time to restore, t hours	Probability density, g(t)	Probability density $g(t') = g(\log_e t)$
0.02	0.00398	7.95×10^{-5}
0.1	0.10480	0.01048
0.2	0.22552	0.04510
0.3	0.29510	0.08853
0.5	0.34300	0.17150
0.7	0.33770	0.23636
1.0	0.30060	0.30060
1.4	0.24524	0.34334
1.8	0.19849	0.35728
2.0	0.17892	0.35784
2.4	0.14638	0.35130
3.0	0.11039	0.33118
3.4	0.09260	0.31483
4.0	0.07232	0.28929
4.4	0.06195	0.27258
5.0	0.04976	0.24880
6.0	0.03559	0.21351
7.0	0.02625	0.18373
8.0	0.01985	0.15884
9.0	0.01534	0.13804
10.0	0.01206	0.12061
20.0	0.00199	0.03971
30.0	0.00058	0.01733
40.0	---	0.00888
80.0	---	0.00135

*At the mode, $\hat{t}$ = 0.5584, $g(\hat{t})$ = 0.34470 and $g(\hat{t}')$ = 0.19247.
 At the median, $\check{t}$ = 1.932, $g(\check{t})$ = 0.18530 and $g(\check{t}')$ = 0.35800.
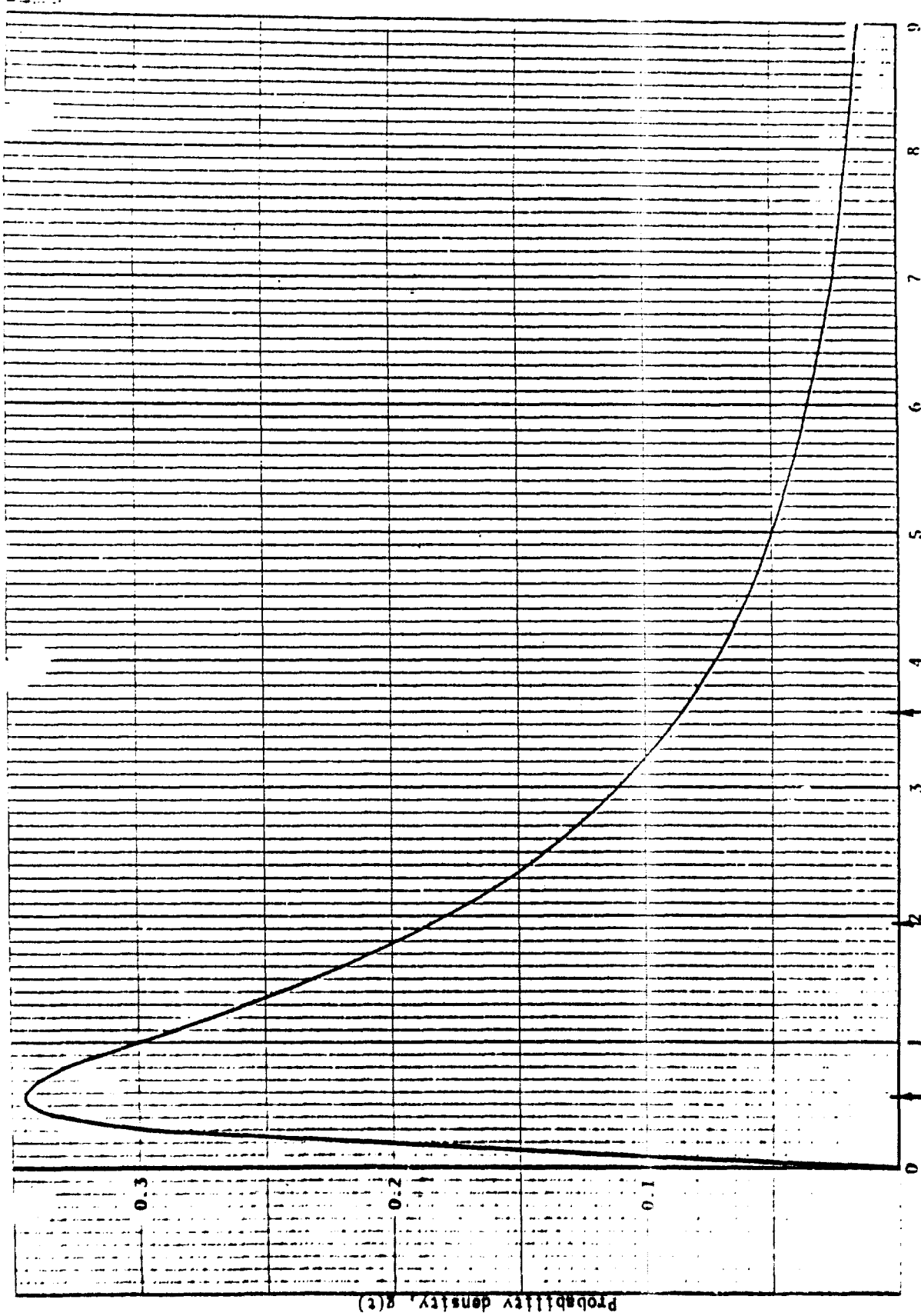
Mode = $\hat{t}$ =0.5584   Median = $\check{t}$ = 1.932   Mean = $\bar{t}$ = 3.595 hrs.

Time to restore, t, hours

FIGURE 5.3.2.1.1-1:   PLOT OF THE LOGNORMAL PDF OF THE TIMES-TO-RESTORE DATA GIVEN IN TABLE 5.3.2.1.1-3 IN TERMS OF THE STRAIGHT t's

Time to restore, t, hours
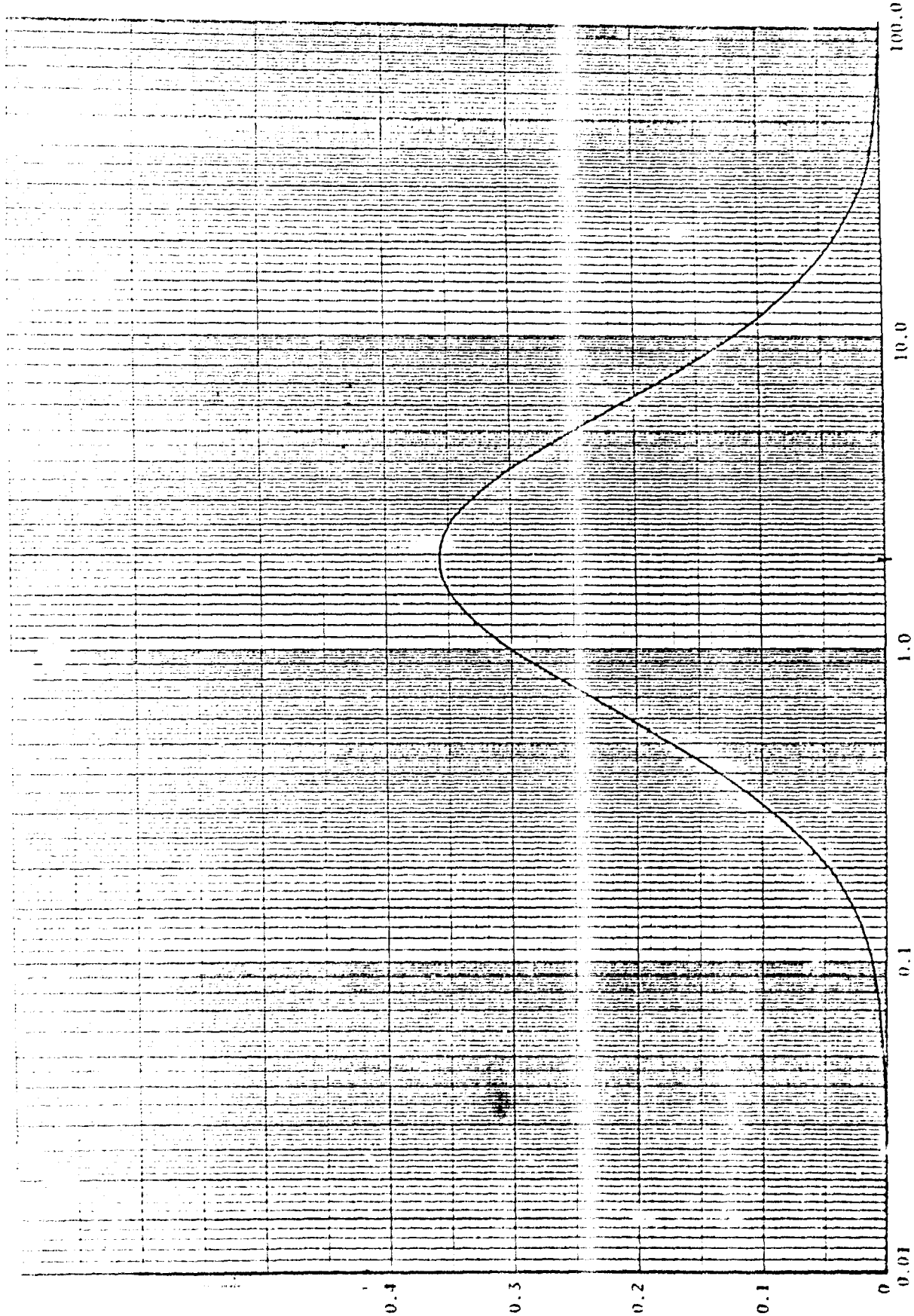
FIGURE 5.3.2.1.1-2: PLOT OF THE LOGNORMAL PDF OF THE TIMES-TO-RESTORE DATA GIVEN IN TABLE 5.3.2.1.1-3 IN TERMS OF THE LOGARITHMS OF t, OR $LOG_e t = t'$

2. <u>MTTR (Mean Time to Repair) of the System</u>

The mean time to repair of the system, $\bar{t}$, is obtained from Eq. (5.73).

$$t = e^{(t' + 1/2\,(\sigma_{t'})^2)}$$

$$t = e^{(0.65879 + 1/2\,(1.11435)^2)}$$

or

$$\bar{t} = 3.595 \text{ hr.}$$

3. <u>Median Time to Repair</u>

The median of the times-to-repair the system, $\overset{\smile}{t}$, is obtained from Eq. (5.76)

$$\overset{\smile}{t} = e^{\bar{t}'}$$

$$\overset{\smile}{t} = e^{0.65879}$$

or

$$\overset{\smile}{t} = 1.932 \text{ hr.}$$

This means that in a large sample of t's half of the t's will have values smaller than $\overset{\smile}{t}$, and the other half will have values greater than $\overset{\smile}{t}$. In other words, 50% of the repair times will be $\leq \overset{\smile}{t}$.

4. <u>Maintainability Function M(t)</u>

The maintainability of a unit can be evaluated as follows, using Eq. (5.62):

$$M(t_1) = \int_0^{t_1} g(t)\,dt = \int_{-\infty}^{t'_1} g(t')\,dt' = \int_{-\infty}^{z(t'_1)} \phi(z)\,dz \quad (5.81)$$

where $t' = \log_e t,$ (5.81a)

$$z(t'_1) = \frac{t'_1 - \bar{t}'}{\sigma_{t'}} \tag{5.81b}$$

and $\bar{t}'$ and $\sigma_{t'}$ are given by Eq. (5.79) and (5.80), respectively.

By means of the transformations shown in Eqs. (5.81a) and (5.81b), the lognormal distribution of the pdf of repair times, $g(t)$, is transformed to the standard normal distribution $\phi\,(z)$ which enables the use of standard normal distribution tables (Table A-1, Appendix A).

The maintainability function for the system, $M(t)$, from (5.81) is:

$$M(t) = \int_{-\infty}^{z(t')} \phi(z)\, dz$$

where

$$z(t') = \frac{t' - \overline{t'}}{\sigma_{t'}}$$

$$t' = \log_e t$$

From the data in Table 5.3.2.1.1-1 we previously calculated

$$\overline{t'} = 0.65879$$

$$\sigma_{t'} = 1.11435$$

The quantified $M(t)$ is shown in Figure 5.3.2.1.1-3. The values were obtained by inserting values for, $t' = \log_e t$, into the expression,

$$z(t') = \frac{t' - 0.65879}{1.11435}$$

solving for $z(t')$, and reading the value of $M(t)$ directly from the standard normal tables in Appendix A (Table A-1).

5. **Maintainability for a 20 Hour Mission**

$$M(20) = \int_{-\infty}^{z(\log_e 20)} \phi(z)\, dz$$

where $\log_e 20 = 2.9957$
and

$$Z(\log_e 20) = \frac{2.9957 - 0.65879}{1.11435} = 2.0972$$

From Appendix A we find that for $z = 2.0972$

$$M(20) = \int_{-\infty}^{2.0972} \phi(Z)\,(dZ) = 1-0.018 = 0.982 \text{ or } 98.2\%$$

6. **The time within which 90% and 95% of the Maintenance Actions are Completed ($M_{max_{ct}}$)**

This is the time $t_{1-\alpha}$ for which the maintainability is $1-\alpha$, or

$$M(t_{1-\alpha}) = P(t \le t_{1-\alpha}) = \int_0^{t_{1-\alpha}} g(t)\, dt = \int_{-\infty}^{t'_{1-\alpha}} g(t')\, dt' = \int_{-\infty}^{z(t'_{1-\alpha})} \phi(z)\, dz, \quad (5.82)$$
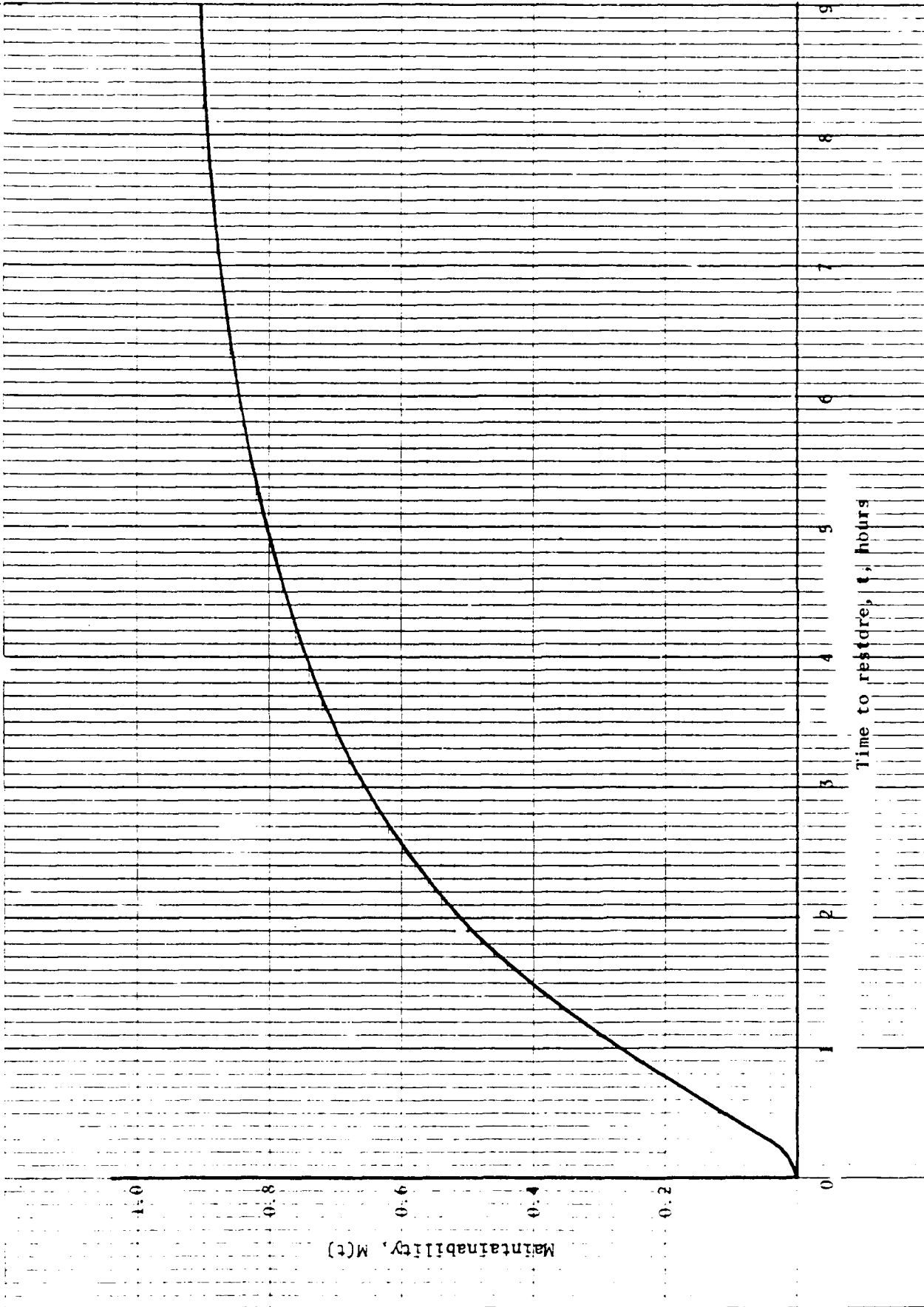
FIGURE 5.3.2.1.1-3: PLOT OF THE MAINTAINABILITY FUNCTION FOR THE TIMES-TO-REPAIR DATA OF EXAMPLE 2

and

$$z(t'_{1-a}) = \frac{t'_{1-a} - \overline{t'}}{\sigma t'} \qquad (5.83)$$

The commonly used maintainability, or $(1-a)$, values are 0.80, 0.85, 0.90, 0.95, and 0.99. Consequently, the $z(t'_{1-a})$ values which would be used most commonly would be those previously given in Table 5.3.2.1-1. Using Eq. (5.83) the time t'_{1-a} would then be calculated from

$$t'_{1-a} = \overline{t'} + z(t'_{1-a}) \cdot \sigma_{t'}$$

or

$$t_{1-a} = \text{antilog}_e(t'_{1-a}) = \text{antilog}_e\left[\overline{t'} + z(t'_{1-a}) \cdot \sigma_{t'}\right] \qquad (5.84)$$

Thus, for 90% $M_{max_{ct}}$, from the previously obtained value of $\overline{t'}$ and σ_t

$$t_{0.90} = \text{antilog}_e\left[\overline{t'} + z(t'_{0.90})\sigma_{t'}\right]$$

$$= \text{antilog}_e\left[0.65879 + 1.282(1.11435)\right]$$

$$= \text{antilog}_e(2.08737)$$

$$= 8.06 \text{ hrs.}$$

For 95% $M_{max_{ct}}$

$$t_{0.95} = \text{antilog}_e\left[0.65879 + 1.645(1.11435)\right]$$

$$= \text{antilog}_e(2.491896) = 12.08 \text{ hrs.}$$

7. <u>Repair Rate at t = 20 hours</u>

Using Eq. (5.63) and substituting the values for g(20) from Table 5.3.2.1.1-3 and the previously calculated value for M(20)

$$u(20) = \frac{g(20)}{1-M(20)} = \frac{0.00199}{1-0.982} = \frac{0.00199}{0.018}$$

$$= 0.11 \text{ repairs/hr.}$$

5.3.2.2 NORMAL DISTRIBUTION

The normal distribution has been adequately treated in Section 5.2.2.1.1 in the discussion on reliability theory. The same procedures and methodology apply for maintainability if one merely uses repair time for t, mean repair time for u, and standard deviation of repair times for σ.

In maintainability, the normal distribution applies to relatively straightforward maintenance tasks and repair actions (e.g., simple removal and replacement tasks) which consistently require a fixed amount of time to complete. Maintenance task times of this nature are usually normally distributed, producing a probability density function given by:

$$g(t = M_{ct}) = \frac{1}{S_{M_{ct}} \sqrt{2\pi}} \exp\left[\frac{-(M_{ct_i} - \overline{M}_{ct})^2}{2(S_{M_{ct}})^2}\right] \tag{5.85}$$

where

M_{ct_i} = repair time for an individual maintenance action

$$\overline{M}_{ct} = \frac{\Sigma(M_{ct_i})}{N}$$

= average repair time for N observations

$$S_{M_{ct}} = \sqrt{\frac{\Sigma(M_{ct_i} - \overline{M}_{ct})^2}{N-1}}$$

= standard deviation of the distribution of repair times, based on N observations

N = number of observations

The mean time to repair ($\overline{M}_{ct}$) is given by

$$\overline{M}_{ct} = \frac{\Sigma M_{ct_i}}{N} \tag{5.86}$$

The median time to repair ($\widetilde{M}_{ct}$) is given by

$$\widetilde{M}_{ct} = \frac{\Sigma M_{ct_i}}{N} \tag{5.87}$$

which is equal to the mean time to repair because of the symmetry of the normal distribution (see Fig. 5.3.2.1.1-2).

The maximum time to repair is given by

$$M_{max_{ct}} = \bar{M}_{ct} + \varphi S_{M_{ct}}$$

(5.88)

where

$\varphi = z(t_{1-a})$

= value from normal distribution function corresponding to the percentage point $(1-a)$ on the maintainability function for which $M_{max_{ct}}$ is defined. Values of φ as a function of $(1-a)$ are shown in Table 5.3.2.2-1. Note that this is the same as Table 5.3.2.1-1 with rounded off values.

TABLE 5.3.2.2-1: VALUES OF φ FOR SPECIFIED a

$1-a$	φ or $z(t_{1-a})$
95%	1.65
90%	1.28
85%	1.04
80%	0.84

5.3.2.2.1 EQUIPMENT EXAMPLE

An equipment whose repair times are assumed to be normally distributed was monitored and the following repair times observed (in minutes):

6.5, 13.25, 17.25, 17.25, 19.75, 23, 23, 24.75, 27.5, 27.5, 27.5, 32, 34.75, 34.75, 37.5, 37.5, 40.25, 42.5, 44.75, 52

Find the following parameters.

1. The pdf of g(t) and its value at 30 minutes
2. The MTTR and median times to repair
3. The maintainability for 30 minutes
4. The time within which 90% of the maintenance actions are completed
5. The repair rate, u(t), at 30 minutes

1. **Pdf of g(t)**

$$\overline{M}_{ct} = \frac{\Sigma M_{ct_i}}{N} = \frac{583.25}{20} = 29.16 \text{ minutes}$$

$$S_{M_{ct}} = \sqrt{\frac{\Sigma (M_{ct_i} - \overline{M}_{ct})^2}{N-1}}$$

$$= \sqrt{\frac{\Sigma (M_{ct_i})^2 - N(\overline{M}_{ct})^2}{N-1}}$$

$$= \sqrt{\frac{19527 - 17006}{19}} = 11.5 \text{ minutes}$$

$$g(t) = \frac{1}{11.5 \sqrt{2\pi}} \exp\left[-\frac{(M_{ct_i} - 29.16)^2}{2(11.5)^2}\right]$$

$$g(30) = \frac{1}{28.82} \exp\left[-\frac{(30 - 29.16)^2}{2(11.5)^2}\right]$$

$$= \frac{1}{28.82} e^{-0.0032}$$

$$= (0.035)(0.9973) = 0.035$$

2. **MTTR and Median Time to Repair**

These are the same for the normal distribution because of its symmetry, and given by:

$$\overline{M}_{ct} = \frac{\Sigma M_{ct_i}}{N} = \frac{583}{20} = 29.16 \text{ minutes}$$

3. **Maintainability for 30 Minutes**

$$M(30) = \int_{-\infty}^{30} g(t)\, dt = \int_{-\infty}^{z(30)} \phi(z)\, dz$$

$$z(30) = \frac{M_{ct_i} - \overline{M}_{ct}}{S_{M_{ct}}} = \frac{30 - 29.16}{11.5} = \frac{0.84}{11.5} = 0.07$$

From the standard normal table (Table A-1 of Appendix A)

$$\phi(0.07) = 1-.4721=0.5279 = 0.53$$

$$\therefore M(30) = 0.53 \text{ or } 53\% \text{ probability of making a repair in 30 minutes}$$

4. **Time within which 90% of the Maintenance Actions are Completed**

$$M_{0.9} = \overline{M}_{ct} + \phi S_{M_{ct}} \quad \phi = 1.28 \text{ from Table } 5.3.2.2-1$$

$$= 29.16 + (1.28)(11.5) = 43.88 \text{ minutes}$$

5. **Repair Rate at 30 Minutes**

$$u(30) = \frac{g(30)}{1-M(30)} = \frac{0.035}{1-0.53} = \frac{0.035}{0.47} = 0.074 \text{ repairs/minute}$$

5.2.2.3   EXPONENTIAL DISTRIBUTION

In maintainability analysis, the exponential distribution applies to maintenance tasks and maintenance actions whose completion times are independent of previous maintenance experience (e.g., substitution methods of failure isolation where several equally likely alternatives are available and each alternative is exercised, one at a time, until the one which caused the failure is isolated), producing a probability density function given by:

$$g(t = M_{ct}) = \frac{1}{\overline{M}_{ct}} \exp\left(-\frac{M_{ct_i}}{\overline{M}_{ct}}\right) \tag{5.89}$$

The method used in evaluating the maintainability parameters is similar to that previously shown in Section 5.2.2.1.4 for analyzing reliability with exponential times-to-failure. The fundamental maintainability parameter is repair rate, $u(t)$, which is the reciprocal of $\overline{M}_{ct}$, the mean-time-to-repair (MTTR). Thus, another expression for $g(t)$ in terms of $u(t)$, the repair rate is

$$g(t) = u\,e^{-ut} \tag{5.90}$$

where u is the repair rate (which is constant for the exponential case)

The maintainability function is given by:

$$M(t) = \int_0^t g(t)\,dt = \int_0^t ue^{-ut}dt = 1 - e^{-ut} \tag{5.91}$$

The MTTR is given by

$$\overline{M}_{ct} = \frac{1}{\mu} = \frac{\Sigma M_{ct_i}}{N} \tag{5.92}$$

If the maintainability function, M(t), is known, the MTTR can also be obtained from

$$\text{MTTR} = \overline{M}_{ct} = \frac{-t}{\left[\ln(1-M(t))\right]} \qquad (5.93)$$

The median time to repair $\widetilde{M}_{ct}$ is given by:

$$\widetilde{M}_{ct} = 0.69 \, \overline{M}_{ct} \qquad (5.94)$$

The maximum time to repair is given by:

$$M_{max_{ct}} = k_e \overline{M}_{ct} \qquad (5.95)$$

where

k_e = value of $M_{ct_i}/\overline{M}_{ct}$ at the specified percentage point a on the exponential function at which $M_{max_{ct}}$ is defined. Values of k_e are shown in Table 5.3.2.3-1.

TABLE 5.3.2.3-1: VALUES OF k_e FOR SPECIFIED a

a	k_e
95%	3.00
90%	2.31
85%	1.90
80%	1.61

5.3.2.3.1 COMPUTER EXAMPLE

For a large computer installation, the maintenance crew logbook shows that over a period of a month there were 15 unscheduled maintenance actions or downtimes, and 1200 minutes in emergency maintenance status. Based upon prior data on this equipment, the maintainability analyst knew that the repair times were exponentially distributed. A warranty contract between the computer company and the government calls for a penalty payment of any downtime exceeding 100 minutes.

Find the following:

1. The MTTR and repair rate
2. The maintainability function M(t) for 100 minutes, or the probability that the warranty requirement is being met
3. The median time to repair
4. The time within which 95% of the maintenance actions can be completed

1. **MTTR and Repair Rate**

$$MTTR = \bar{M}_{ct} = \frac{1200}{15} = 80 \text{ minutes}$$

$$u \text{ (repair rate)} = \frac{1}{\bar{M}_{ct}} = 1/80 = 0.0125 \text{ repairs/minute}$$

2. **Maintainability Function for 100 Minutes**

$$M(100) = 1 - e^{-ut} = 1 - e^{-(0.0125)(100)}$$

$$= 1 - e^{-1.25} = 1 - 0.286 = 0.714$$

or a 71% probability of meeting the warranty requirement

3. **Median Time to Repair**

$$\tilde{M}_{ct} = 0.69 \ \bar{M}_{ct} = (0.69)(80) = 55.2 \text{ minutes}$$

4. **Time within which 95% of the Maintenance Actions can be Completed**

$$M_{max_{ct}} = M_{0.95} = 3 \ \bar{M}_{ct} = 3(80) = 240 \text{ minutes}$$

5.3.2.4 EXPONENTIAL APPROXIMATION

In general, the repair time density function is lognormally distributed. In practice, however, the standard deviation of the logarithms of repair times ($\sigma_{log_e M_{ct}}$) is not usually known and must be estimated in order to compute the probability of repair for any value of repair time. A value of $\sigma = 0.55$ has been suggested by some prediction procedures, based on maintenance experience data accumulated on equipment. In the absence of justifiable estimates of σ, it is practicable to use the exponential distribution as an approximation of the lognormal.

Figure 5.3.2.4-1 compares the exponential function with several lognormal functions of different standard deviations. All functions in the figure are normalized to a common $\bar{M}_{ct}$ at $M_{ct_i}/\bar{M}_{ct} = 1.0$. The exponential approximation is, in general, conservative over the region shown. Probability of repair in time t in the exponential case is given by:

$$M(t) \approx 1 - e^{-t/\bar{M}_{ct}} = 1 - e^{-ut}$$

where

$M(t)$ = probability of repair in a specified time t

M_{ct} = known mean corrective maintenance time

This approximation will be used in the next section on availabilty theory because it allows for a relatively simple description of the basic concepts without becoming overwhelmed by the mathematics involved.

PROBABILITY
OF REPAIR

NORMALIZED TIME, $t_r/\overline{M}_{ct}$
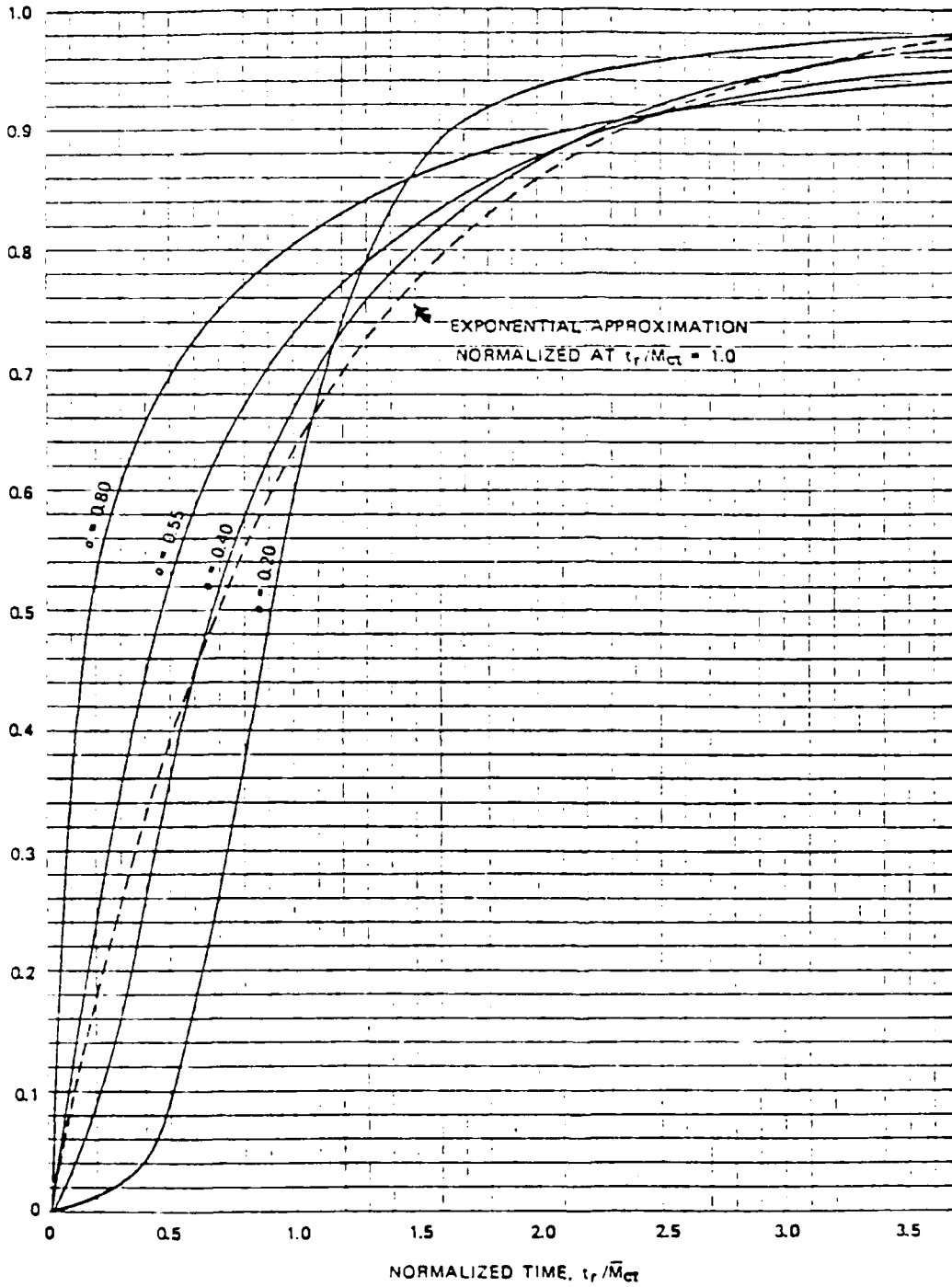
FIGURE 5.3.2.4-1: EXPONENTIAL APPROXIMATION OF LOGNORMAL MAINTAINABILITY
FUNCTIONS

5.4 AVAILABILITY THEORY

The concept of availability was originally developed for repairable systems that are required to operate continuously, i.e., round the clock, and are at any random point in time either operating or are "down" because of failure and are being worked upon so as to restore their operation in minimum time. In this original concept a system is considered to be in only two possible states - operating or in repair - and availability is defined as the probability that a system is operating satisfactorily at any random point in time t, when subject to a sequence of "up" and "down" cycles which constitute an alternating renewal process (Ref. 38). In other words, availability is a combination of reliability and maintainability parameters.

For simplicity, consider a single equipment which is to be operated continuously. If a record is kept on when the equipment is operating or down over a period of time, it is possible to describe its availability as a random variable defined by a distribution function H(A) as illustrated.
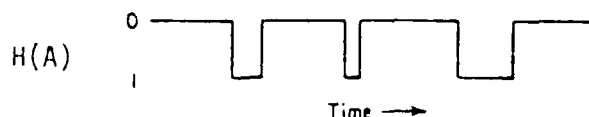
The expected value availability is simply the average value of the function over all possible values of the variable. When we discuss a system's steady state availability, we are referring, on the other hand, to the behavior of an ensemble of equipments. If we had a large number of equipments that have been operating for some time, then at any particular time we would expect the number of equipments that are in state 0 (available) to be NP_0. Thus, the ratio of the number of equipments available to the total number of equipments is simply $NP_0/N = P_0$.

5.4.1 BASIC CONCEPTS

System availability can be defined in the following ways:

1. **Instantaneous Availability - A(t)** - Probability that a system will be available for use at any random time t after the start of operation.

2. **Mission Availability - $A_m(t_2-t_1)$** - The proportion of time in an interval (t_2-t_1), during a mission, a system is available for use, or

$$A_m(t_2-t_1) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t) \, dt \qquad (5.96)$$

this is also called average availability (A_{AV})

3. <u>Steady State of Availability</u> - A$_S$ - Probability a system will be available for use at a point in time t after the start of system operation as t becomes very large, or as t → ∞, or

$$A_S = \underset{t \to \infty}{Limit} \ A(t)$$

These three availabilities are illustrated in Figure 5.4.1-1.
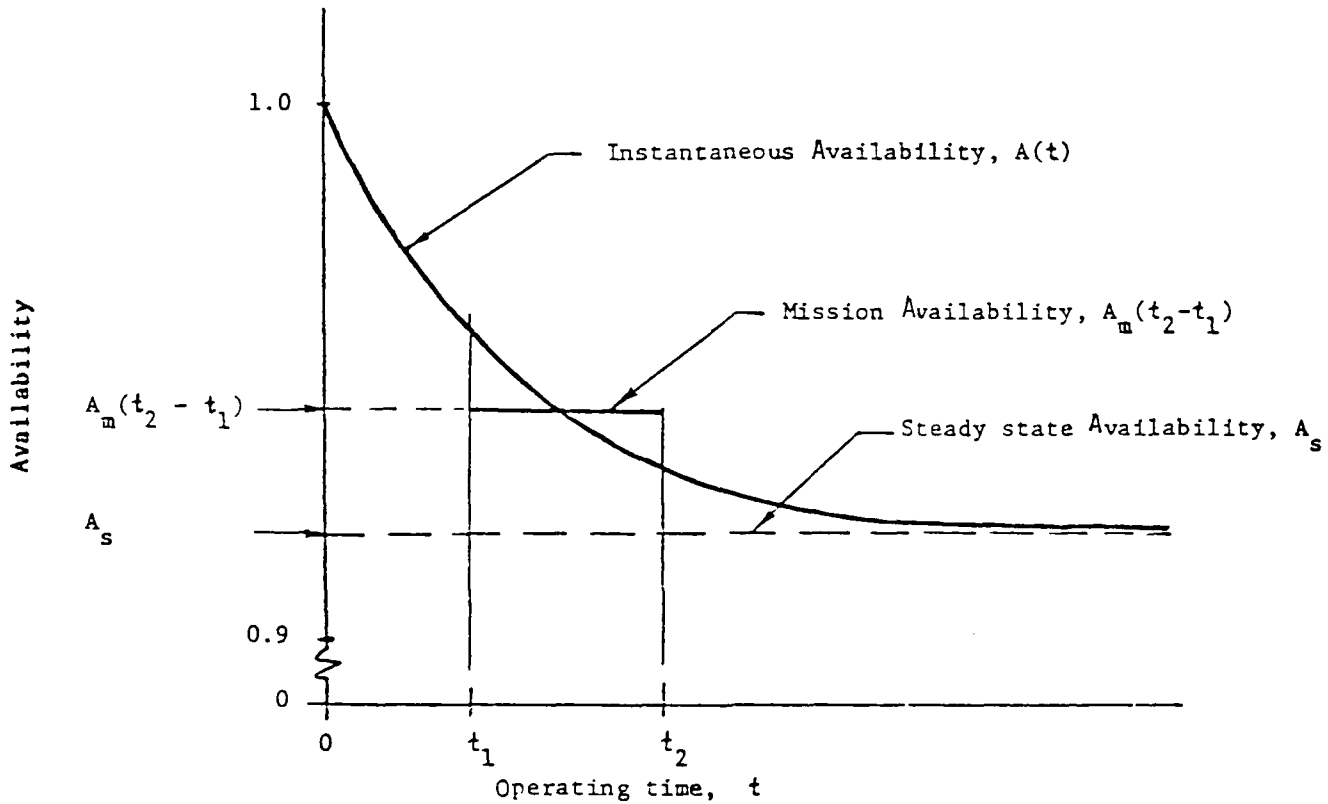
FIGURE 5.4.1-1: <u>THE RELATIONSHIP BETWEEN INSTANTANEOUS, MISSION, AND STEADY STATE AVAILABILITIES AS A FUNCTION OF OPERATING TIME</u>

4. Achieved Availability (A_A)

$$A_A = 1 - \frac{Downtime}{Total\ time} = \frac{up\ time}{Total\ time} \qquad (5.97)$$

Downtime includes all repair time (corrective and preventive maintenance time), adminstrative time and logistic time.

5. Intrinsic Availability (A_i)

$$A_i = \frac{MTBF}{MTBF + MTTR} \qquad (5.98)$$

This does not include administrative time and logistic time; in fact, it usually does not include preventive maintenance time. A_i is primarily a function of the basic equipment/system design.

5.4.2 AVAILABILITY MODELING (MARKOV PROCESS APPROACH)

5.4.2.1 INTRODUCTION

A Markov process (Ref. 5) is a mathematical model that is useful in the study of the availability of complex systems. The basic concepts of the Markov process are those of "state" of the system (e.g., operating, nonoperating) and state "transition" (from operating to nonoperating due to failure, or from nonoperating to operating due to repair).

A graphic example of a Markov process is presented by a frog in a lily pond. As time goes by, the frog jumps from one lily pad to another according to his whim of the moment. The state of the system is the number of the pad currently occupied by the frog; the state transition is, of course, his leap.

Any Markov process is defined by a set of probabilities p_{ij} which define the probability of transition from any state i to and state j. One of the most important features of any Markov model is that the transition probability p_{ij} depends only on states i and j and is completely independent of all past states except the last one, state i; also p_{ij} does not change with time.

In system availability modeling utilizing the Markov process approach, the following additional assumptions are made:

1. The conditional probability of a failure occurring in time (t, t + dt) is λ dt

2. The conditional probability of a repair occurring in time (t, t + dt) is u dt

3. The probability of two or more failures or repairs occurring simultaneously is zero

4. Each failure or repair occurrence is independent of all other occurrences.

5. λ (failure rate) and u (repair rate) are constant (e.g., exponentially distributed)

Let us now apply the Markov process approach to the availability analysis of a single unit with failure rate λ and repair rate u.

5.4.2.2 SINGLE UNIT AVAILABILITY ANALYSIS (Markov Process Approach)

The Markov graph for a single unit is shown in Figure 5.4.2.2-1.
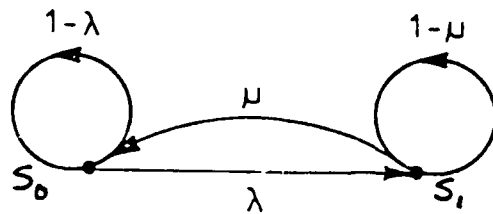
FIGURE 5.4.2.2-1: MARKOV GRAPH FOR SINGLE UNIT

where

S_0 = State 0 = the unit is operating and available for use

S_1 = State 1 = the unit has failed and is being repaired

λ = failure rate

u = repair rate

Now since the conditional probability of failure in (t, t + dt) is λ dt, and the conditional probability of completing a repair in (t, t + dt) is u dt, we have the following transition matrix:

$$P = \begin{matrix} & \begin{matrix} 0 & 1 \end{matrix} \\ \begin{matrix} 0 \\ 1 \end{matrix} & \begin{pmatrix} 1-\lambda & \lambda \\ \mu & 1-\mu \end{pmatrix} \end{matrix}$$

For example, the probability that the unit was in state 0 (operating) at time t and remained in state 0 at time t + dt is the probability that it did not fail in time dt, or $(1 - \lambda)$dt. On the other hand, the probability that the unit transitioned from state 0 (operating) to state 1 (failed) in time t + dt is the probability of systems failure in time dt, or λ dt. Similarly, the probability that it was in state 1 (failed) at time t and transitioned to state 0 (operating) in time dt is the probability that is was repaired in dt, or u dt. Also, the probability that it was in state 1 (failed) at time t and remained in state 1 at time t + dt is the probability that it was not repaired in dt, or (1 -u) dt.

The single unit's availability is

$$A(t) = P_0(t) \text{ (probability that it is operating at time t)}$$

and

$$P_0(t) + P_1(t) = 1 \text{ (it is either operating or failed at time t)}$$

The differential equations describing the stochastic behavior of this system can be formed by considering the following: the probability that the system is in state 0 and time $t + dt$ is derived from the probability that it was in state 0 at time t and did not fail in $(t, t + dt)$, or that it was in state 1 at the time t and (was repaired) returned to state 0 in $(t, t + dt)$. Thus, we have

$$P_0(t + dt) = P_0(t) (1 - \lambda \, dt) + P_1(t) \, u \, dt$$

Similarly the probability of being in state 1 at time $t + dt$ is derived from the probability that the system was in state 0 at time t and failed in $(t, t + dt)$; or it was in state 1 at time t, and the repair was not completed in $(t, t + dt)$. Therefore

$$P_1(t + dt) = P_0(t) \lambda dt + P_1(t) (1 - u \, dt)$$

It should be noted that the coeffficients of these equations represent the columns of the transition matrix. We find the differential equations by defining the limit of the ratio:

$$\frac{P_i(t + dt) - P_i(t)}{dt}$$

which yields

$$P_0'(t) = -\lambda P_0(t) + u P_1(t)$$

$$P_1'(t) = \lambda P_0(t) - u P_1(t)$$

(5.99)

The above equations are called differential - difference equations.

If we say that at time $t = 0$ the system was in operation, the initial conditions are $P_0(0) = 1$, $P_1(0) = 0$. It is also of interest to consider the case where we begin when the system is down and under repair. In this case, the initial conditions are $P_0(0) = 0$, $P_1(0) = 1$.

Transforming equations (5.99) into Laplace transforms under the initial conditions that $P_0(0) = 1$, $P_1(0) = 0$ we have

$$sP_0(s) - 1 + \lambda P_0(s) - u P_1(s) = 0$$

$$sP_1(s) - \lambda P_0(s) + u P_1(s) = 0$$

and simplifying

$$(s + \lambda)P_0(s) - u P_1(s) = 1$$

$$-\lambda P_0(s) + (s + u)P_1(s) = 0$$

(5.100)

Solving these simultaneously for $P_0(s)$ yields

$$P_0(s) = \frac{\begin{vmatrix} 1 & -\mu \\ 0 & s+\mu \end{vmatrix}}{\begin{vmatrix} s+\lambda & -\mu \\ -\lambda & s+\mu \end{vmatrix}}$$

or

$$P_0(s) = \frac{s + \mu}{s(s + \lambda + \mu)}$$

and

$$P_0(s) = \frac{s}{s(s + \lambda + \mu)} + \frac{\mu}{s(s + \lambda + \mu)}$$

or

$$P_0(s) = \frac{1}{s + \lambda + \mu} + \frac{\mu}{S_1 - S_2}\left(\frac{1}{S - S_1} - \frac{1}{S - S_2}\right)$$

where

$$S_1 = 0 \text{ and } S_2 = -(\lambda + \mu).$$

Therefore,

$$P_0(s) = \frac{1}{s + \lambda + \mu} + \frac{\mu}{\lambda + \mu}\left\{\frac{1}{s} - \frac{1}{s - (-(\lambda + \mu))}\right\}$$

or taking the inverse Laplace transform

$$P_0(t) = L^{-1}\left[\boxed{P_0(s)}\right]$$

The use of Laplace transforms, $L\,f(t)$ and inverse Laplace transforms $L^{-1}\,f(t)$ for availabilty analysis is described in a number of texts (see Refs. 38, 39)

therefore

$$P_0(t) = e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda + \mu}\boxed{1 - e^{-(\lambda + \mu)t}}$$

and

$$A(t) = P_0(t) = \underbrace{\frac{\mu}{\lambda + \mu}}_{\substack{\text{steady state} \\ \text{component}}} + \underbrace{\frac{\lambda}{\lambda + \mu}\,e^{-(\lambda + \mu)t}}_{\text{transient componet}} \tag{5.101}$$

$$1 - A(t) = P_1(t) = \underbrace{\frac{\lambda}{\lambda + \mu}}_{\substack{\text{steady state} \\ \text{component}}} - \underbrace{\frac{\lambda}{\lambda + \mu}\,e^{-(\lambda + \mu)t}}_{\text{transient componet}} \tag{5.101a}$$

If the system was intially failed, the initial conditions are $P_0(0) = 0$, $P_1(0) = 1$, and the solutions are

$$A(t) = P_0(t) = P_0(t) = \frac{\mu}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \qquad (5.102)$$

and

$$1 - A(t) = P_1(t) = \frac{\lambda}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} \qquad (5.102a)$$

We note that as t becomes very large, Eqs. (5.101) and (5.102) become equivalent. This indicates that after the system has been operating for some time its behavior becomes independent of its starting state.

We will show later that the transient term becomes negligible when

$$t = \frac{4}{\lambda + \mu} \qquad (5.103)$$

For a mission of $(t_1 - t_2)$ duration, the mission availability is

$$A_m(t_2 - t_1) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t) \, dt = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} P_0(t) \, dt$$

$$= \frac{\mu}{\lambda + \mu} - \frac{\lambda}{(\lambda + \mu)^2 T} \exp\left[-(\lambda + \mu)T\right] \qquad (5.104)$$

The steady state availability, A_S, is

$$A_S - \text{Limit } A(t) = A(\infty),$$
$$t \to \infty$$

therefore Eq. (5.101)

$$A_S = \frac{\mu}{\lambda + \mu} = \frac{1}{1 + \frac{\lambda}{\mu}}$$

As $\lambda = \frac{1}{MTBF}$ and $\mu = \frac{1}{MTTR}$ the steady state availability becomes

$$A_S = \frac{MTBF}{MTBF + MTTR}$$

Usually μ is much larger in value than λ, and A_S may be written as

$$A_S = \frac{1}{1 + \frac{\lambda}{\mu}} = 1 - \frac{\lambda}{\mu} + \frac{\lambda^2}{\mu^2} - \cdots = 1 - \frac{\lambda}{\mu}$$

As was previously stated, the transient part decays relatively fast and becomes negligible before

$$t = \frac{4}{\lambda + \mu}$$

If u is substantially greater than λ, then the transient part becomes negligible before

$$t = \frac{4}{\mu}$$

Figure 5.4.2.2-2 gives the availability of a single unit with repairs, showing how it approaches the steady state availability, as a function of

$$\frac{i}{\lambda + \mu} \quad \text{where } i = 1, 2, \ldots$$

The instantaneous and steady state availabilities for a single exponential unit are tabulated as a function of operating time in Table 5.4.2.2-1.

The same technique described for a single unit can be applied to different equipment/system reliability configurations, e.g., combinations of series and parallel units. As the systems become more complex, the mathematical manipulations can be quite laborious. The important trick is to set up the Markov graph and the transition matrix properly; the rest is just mechanical. Reference 8 contains an extensive list of solutions for different system configurations. Reference 9 contains general formulas for (m, n) systems as well as other advanced considerations such as the fact that the time to repair may not be exponential.

For example, for the most general case of n equipments and r repairmen where r = n, the steady state availability, A_s, is:

$$A_s = \left[\sum_{k=0}^{n-1} \frac{n!}{(n-k)! \, k!} \, \rho^k + \sum_{k=r}^{n} \frac{n!}{(n-k)! \, r!} \, \rho_r \left(\frac{\rho}{r} \right)^{k-1} \right] \tag{5.105}$$

where $\rho = \frac{\lambda}{\mu}$

More details on availability modeling and applications are presented in Section 10.
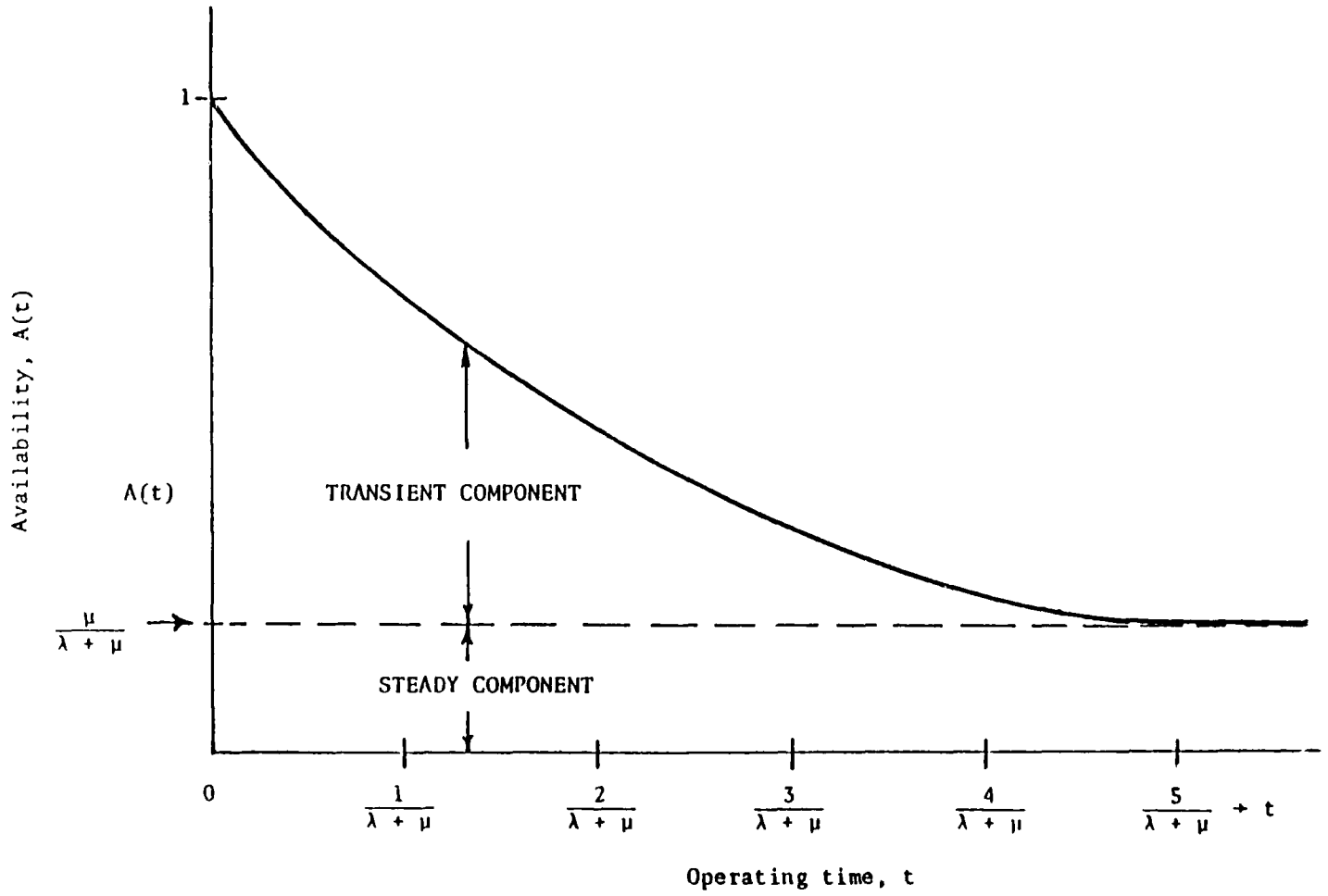
FIGURE 5.4.2.2-2:   <u>SINGLE UNIT AVAILABILITY WITH REPAIR</u>

TABLE 5.4.2.2-1: THE AVAILABILITY OF A SINGLE SYSTEM OR UNIT (a) instantaneous or point availability (b) steady state availability or inherent uptime ratio. $\lambda = 0.01$ failures/hr (fr/hr); u = 1.0 repairs/hr (rp/hr).

Operating Time (Hrs)	(a) Point Availability A(t)	(b) Steady State Availability
0	1.000000	$A_S = \dfrac{\mu}{\lambda + \mu}$
0.25	0.997791	
0.50	0.996074	
0.75	0.994741	$= \dfrac{1}{0.01 + 1}$
1.00	0.993705	
1.50	0.992275	
2.00	0.991412	$= \dfrac{1}{1.01}$
2.50	0.990892	
3.00	0.990577	
3.50	0.990388	$= 0.990099$
4.00	0.990273	
5.00	0.990162	
6.00	0.990122	
7.00	0.990107	
8.00	0.990102	
9.00	0.990100	
10.00	0.990099	
∞	0.990099	

5.5 R&M TRADE-OFF TECHNIQUES

5.5.1 GENERAL

System effectiveness and cost/effectiveness models provide the best tools for performing trade-off studies on the system level. Because of the complexities involved, most of these models are computerized. Through the computerized models any changes in any of the multitude of reliability, maintainability, performance, mission profile, logistic support, and other parameters can be immediately evaluated as to their effect on the effectiveness and total cost of a system. Thus cost effectiveness modeling and evaluation, besides being used for selecting a specific system design approach from among several competing alternatives, is a very powerful tool for performing parametric sensitivity studies and tradeoffs down to component level when optimizing designs to provide the most effective system for a given budgetary and life cycle cost constraint or the least costly system for a desired effectiveness level.

At times, however, especially in the case of the more simple systems, tradeoffs may be limited to achieving a required system availability while meeting the specified reliability and maintainability requirements. Comparatively simple trade-off techniques can then be used as shown in the paragraph. The maintainability design trade-off aspects and the cost oriented trade-offs are discussed further in Sections 10 and 12.

5.5.2 RELIABILITY VS MAINTAINABILITY

As stated earlier in this section, reliability and maintainability jointly determine the inherent availability of a system. Thus, when an availability requirement is specified, there is a distinct possibility of trading off between reliability and maintainability since, in the steady state, availability depends only on the ratio or ratios of MTTR/MTBF that is referred to as maintenance time ratio (MTR) and uses the symbol α, i.e.,

$$\alpha = MTTR/MTBF \qquad (5.106)$$

so that the inherent availability equation assumes the form

$$A_i = 1/(1+\alpha) \qquad (5.107)$$

Now, obviously innumerable combinations of MTTR and MTBF will yield the same α and, therefore, the same availability A_i. However, there is usually also a mission reliability requirement specified and also a maintainability requirement. Both of these requirements must also be met in addition to the availability requirement. Following is a tradeoff example. Figure 5.5.2-1 represents a system consisting of five major subsystems in a series arrangement. The MTBF of this system is

$$MTBF = (\Sigma \lambda_i)^{-1} = (0.0775)^{-1} = 12.9 \text{ hour}$$
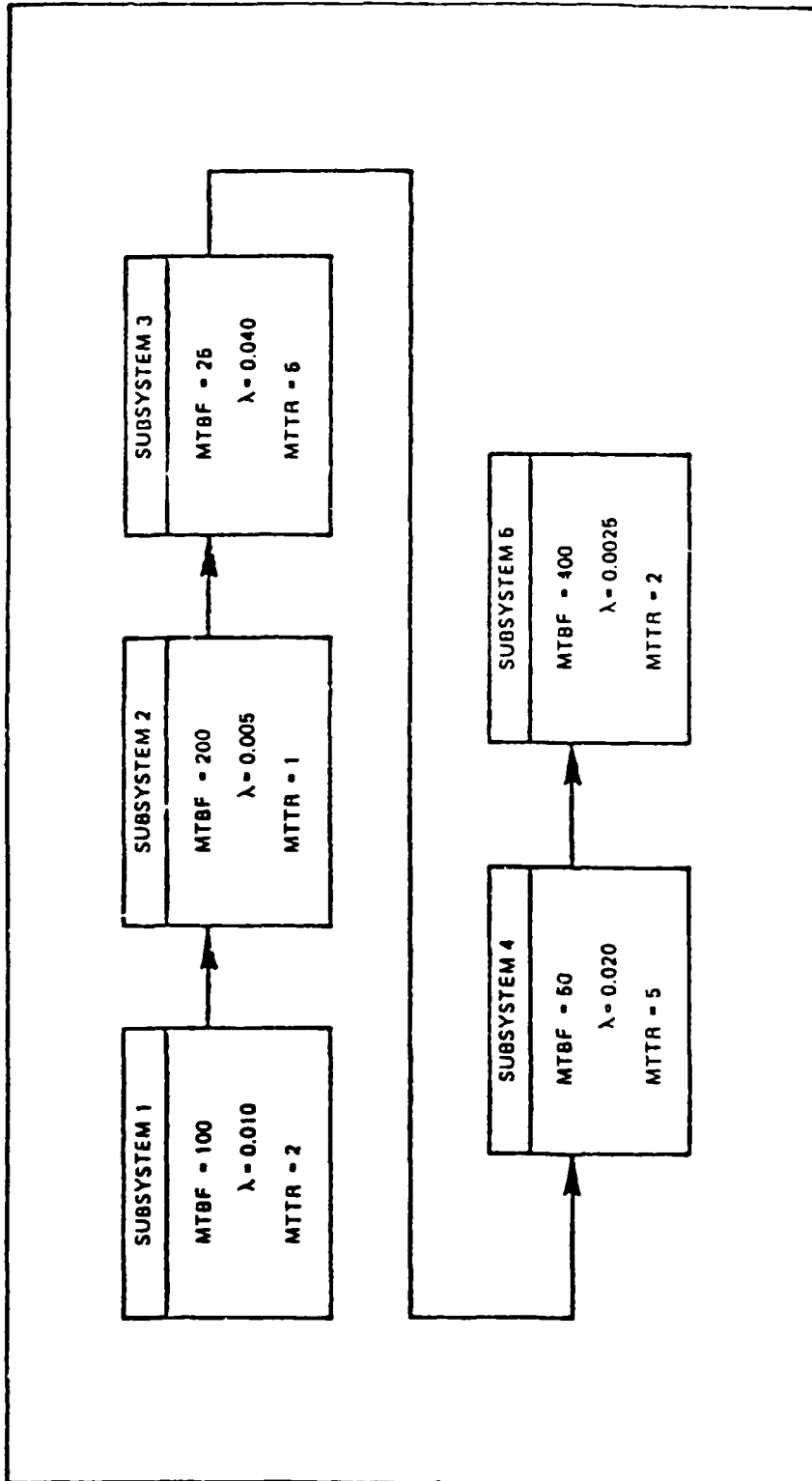
FIGURE 5.5.2-1: BLOCK DIAGRAM OF A SERIES SYSTEM

and its MTTR is

$$MTTR = \Sigma \lambda_i (MTTR)_i / \Sigma \lambda_i = 0.33(0.0775)^{-1}$$

$$= 4.26 \text{ hr}$$

Since the maintenance time ratio equals

$$\alpha = 4.26(12.9)^{-1} = 0.33 \qquad (5.108)$$

which is the sum of the maintenance ratios of the five serial subsystems

$$\alpha = \Sigma \alpha_i = 2/100 + 1/200 + 5/25 + 5/50 + 2/400 \qquad (5.109)$$

$$= 0.33$$

then

$$A = (1+4.26/12.9)^{-1} = .752$$

By inspection of Eq. (5.109) we see that Subsystems 3 and 4 have the highest maintenance time ratios, i.e., 0.2 and 0.1, and therefore are the "culprits" in limiting system availability to 0.752 which may be completely unacceptable.

If, because of state-of-the-art limitations it is not possible to increase the MTBFs of these two subsystems and their MTTRs cannot be reduced by repackaging, the first recourse could be the adding of a parallel redundant subsystem to Subsystem 3. Now two cases may have to be considered: (a) the case where no repair of a failed redundant unit is possible until both fail and the system stops operating, or (b) repair is possible while the system is operating.

In the first case the MTBF of Subsystem 3, which now consists of two parallel units, becomes 1.5 times that of a single unit, i.e., 1.5 x 25 = 37.5 hr. With both units failed, both must be repaired. If a single crew repairs both in sequence, the new MTTR becomes 2 hr and availability actually drops. If two repair crews simultaneously repair both failed units, and repair time is assumed exponentially distributed, the MTTR of both units is again 1.5 times that of a single unit, or 1.5 hr., and system availability remains the same as before, with nothing gained. But if repair of a failed redundant unit is possible while the system operates, the steady-state availability of Subsystem 3 becomes:

$$A_3 = (u^2 + 2 \lambda u)/(u^2 + 2 \lambda u + 2 \lambda^2)$$

for a single repair crew. Since, for a single unit in this subsystem the failure rate $\lambda = 0.04$ and the repair rate $u = 1/5 = 0.2$, we get

$$A_3 = (0.04 + 2 \times 0.04 \times 0.2)(0.04 + 2 \times 0.04 \times 0.02 + 2 \times 0.0016)^{-1}$$

$$= 0.056(0.0592)^{-1} = 0.946$$

as compared to 0.883 (e.g., 25/30) when no redundancy was used. The value of $A_1 = 0.946$ of the redundant configuration corresponds to a maintenance time ratio of

$$a_S = (1 - A_3)A_3^{-1} = 0.054(0.946)^{-1} = 0.057$$

The whole system maintenance time ratio now becomes

$$a = \Sigma a_i = 0.02 + 0.005 + 0.057 + 0.1 + 0.005 = 0.187$$

and system availability A is

$$A = (1 + 0.187)^{-1} = (1.187)^{-1} = 0.842$$

as compared with 0.752 without redundancy in Subsystem 3. If this new value of availability is still not acceptable, redundancy would also have to be applied to Subsystem 4. But to achieve these gains in availability, repair of failed redundant units must be possible while the system is operating. This is called availability with repair. Otherwise, redundancy will not increase availability and may even reduce it, even though it increases system reliability.

A different method of straightforward trade-off between reliability and maintainability is shown in Figure 5.5.2-2. The specific trade-off example shown in this figure is based on a requirement that the inherent availability of the system must be at least $A = 0.99$, the MTBF must not fall below 200 hr, and the MTTR must not exceed 4 hr. The trade-off limits are within the shaded area of the graph, resulting from the equation for inherent availability

$$A_i = MTBF/(MTBF + MTTR)$$

The straight line $A = 0.99$ goes through the points (200,2) and (400,4), the first number being the MTBF and the second number being the MTTR. Any system with an MTBF larger than 200 hr and an MTTR smaller than 4 hr will meet or exceed the minimum availability requirement of $A = 0.99$. If there are several system design alternatives that comply with the specification requirements, the design decision is made by computing the life cycle costs of each alternative and usually selecting the least expensive system, unless substantial gains in system effectiveness are achieved which would warrant increasing the expenditures.

More examples of R&M tradeoffs are given in Section 10.
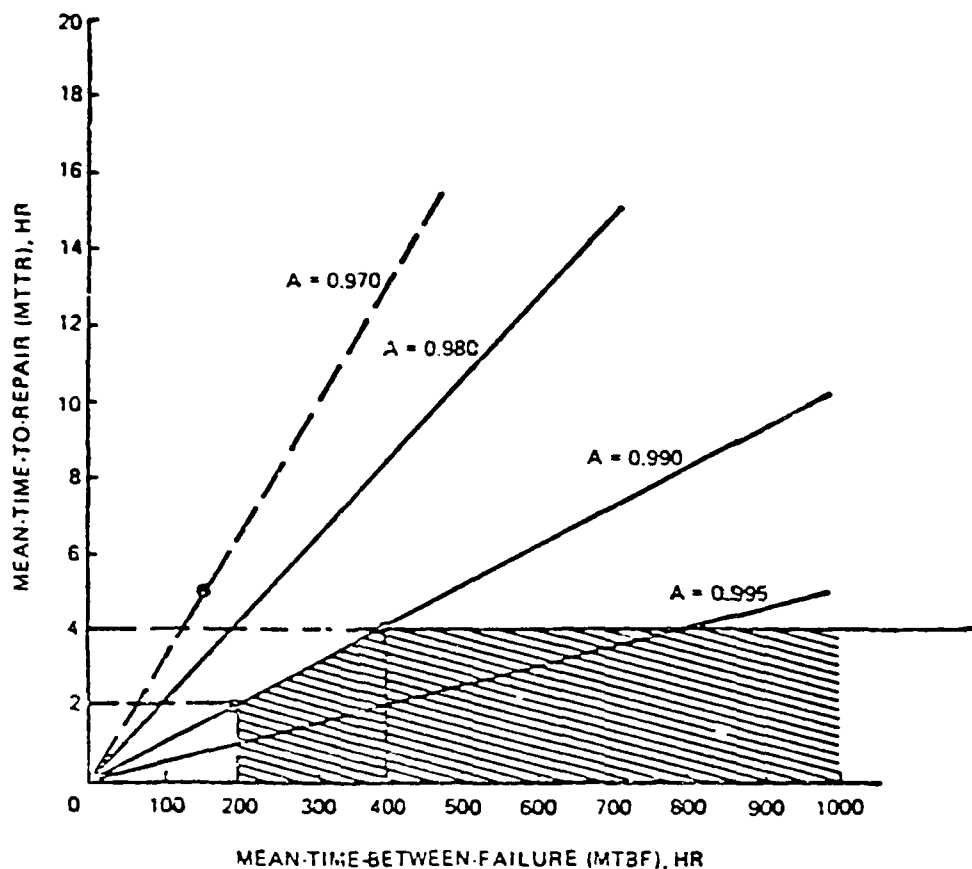
FIGURE 5.5.2-2: RELIABILITY-MAINTAINABILITY TRADEOFFS

REFERENCES

1. AFSC Design Handbook DH1-9, <u>Maintainability for Ground Electronic Systems</u>, December 1973.

2. AMCP 702-3, <u>Quality Assurance Reliability Handbook</u>, AD #702936, October 1968.

3. AMCP 706-133, Engineering Design Handbook, <u>Maintainability Engineering Theory and Practice</u>, AD #A026006, January 1976.

4. Amstader, B., <u>Reliability Mathematics</u>, McGraw-Hill, New York, 1971.

5. ARINC Research Corporation, <u>Reliability Engineering</u>, Prentice-Hall, Englewood Cliffs, NJ, 1963.

6. Arsenault, J.E. and J.A. Roberts, <u>Reliability and Maintainability of Electronic Systems</u>, Computer Science Press, Potomac, Maryland, 1980.

7. Barlow, R.E. and E.M. Scheuer, <u>An Introduction to Reliability Theory</u>, CEIR, Inc., 1969.

8. Barlow, R.E. and F. Proschan, <u>Mathematical Theory of Reliability</u>, John Wiley & Sons, Inc., NY, 1965.

9. Barlow, R.E. and L.C. Hunter, "Mathematical Theory for System Reliability," <u>The Sylvania Technologist</u>, 13, Nos. 1 and 2, 1960.

10. Bazovsky, I., <u>Reliability Theory and Practice</u>, Prentice-Hall, Englewood Cliffs, NY, 1961.

11. Bazovsky, I. et al., <u>Study of Maintenance Cost Optimization and Reliability of Shipboard Machinery</u>, AD #283428, United Control Corp., Seattle, WA, June 1962.

12. Blanchard, B.S., Jr., and E. Lowery, <u>Maintainability, Principles and Practice</u>, McGraw-Hill, NY, 1969.

13. Bourne, A.J. and A.E. Greene, <u>Reliability Technology</u>, Wiley, London, 1972.

14. Calabro, S.R., <u>Reliability Principles and Practice</u>, McGraw-Hill, NY, 1962.

15. Cox, D.R., <u>Renewal Theory</u>, John Wiley & Sons, Somerset, NY, 1962.

16. Cunningham, C.E. and W. Cox, <u>Applied Maintainability Engineering</u>, Wiley, NY, 1972.

17. Dummer, G.W., and N.B. Griffin, <u>Electronic Reliability: Calculation and Design</u>, Pergamon, Elmsford, NY, 1966.

18. Enrick, N.L., <u>Quality Control and Reliability</u>, Industrial Press, NY, 1972.

19. Gnedenko, B, J. Belyayev and A.D. Solovyev, <u>Mathematical Methods of Reliabilty</u>, translation edited by Richard E. Barlow, Wiley, NY, 1969.

20. Goldberg, M., et al., "Comprehensive Failure Mechanism Theory - Metal Film Resistor Behavior," <u>Proceedings of Second Annual Symposium on the Physics of Failure in Electronics</u>, RADC, 1963.

21. Goldman, A.S. and T.B. Slattery, <u>Maintainability: A Major Element of System Effectiveness</u>, Wiley, NY, 1964.

22. Ireson, W.G., <u>Reliability Handbook</u>, McGraw-Hill, NY, 1966.

23. Hosford, J.E., "Measures of Dependability," Operations Research, 8, No. 4, 1960.

24. Kececioglu, D., <u>Maintainability Engineering</u>, Lecture Notes, University of Arizona, 1981.

25. Kline, M.B. and R. Abmoz, "Application of the Lognormal Distribution to Corrective Maintenance Downtimes," <u>AGARD Conference Proceedings on Avionics Reliability, Its Techniques and Related Disciplines</u>, April 1979.

26. Kozlov, B.A. and I.A. Ushakov, <u>Reliability Handbook</u>, Holt, Rinehart, and Winston, NY, 1970.

27. Landers, R.R., <u>Reliability and Product Assurance</u>, Prentice-Hall, Englewood Cliffs, NJ, 1963.

28. Lloyd, D.K. and M. Lipow, <u>Reliability Management, Methods, and Mathematics</u>, second edition: published by the authors, TRW, Inc., Redondo Beach, CA, 1977.

29. Locks, M.O., <u>Reliability, Maintainability, and Availability Assessment</u>, Hayden Book Co., Rochelle Park, NJ, 1973.

30. Mann, N.R., R.E. Schafer and N.D. Singpurwallar, <u>Methods for Statistical Analysis of Reliability and Life Data</u>, Wiley, NY, 1974.

31. Myers, R.H. (ed.), <u>Reliability Engineering for Electronic Systems</u>, Wiley, NY, 1964.

32. Naval Ordnance Systems Command, NAVORD OD 39223, <u>Maintainability Engineering handbook</u>, February 1970.

33. O'Connor and P.D.T. <u>Practical Reliability Engineering</u>, Heyden & Son, Philadelphia, PA, 1981.

34. Pieruschka, E., <u>Principles of Reliability</u>, Prentice-Hall, Englewood Cliffs, NJ, 1963.

35. Polovko, A.M., <u>Fundamentals of Reliability Theory</u>, translation edited by William H. Pierce, Academic Press, NY, 1968.

36. Rau, J.G., <u>Optimization and Probability in Systems Engineering</u>, Van Nostrand-Reinhold, NY, NY, 1970.

37. Roberts, N.H., <u>Mathematical Methods in Reliability Engineering</u>, McGraw-Hill, NY, 1964.

38. Sandler, G.W., <u>System Reliability Engineering</u>, Prentice-Hall, Englewood Cliffs, NJ, 1963.

39. Shooman, M., <u>Probabilistic Reliability: An Engineering Approach</u>, McGraw-Hill, NY, 1968.

40. Smith, D.J., <u>Reliability Engineering</u>, Barnes and Noble, 1972.

APPENDIX A

STATISTICAL TABLES

-

TABLE A-1: <u>VALUES OF THE STANDARD NORMAL DISTRIBUTION FUNCTION</u>

$$\Phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} e^{-u^2/2} du = P(Z \le z)$$
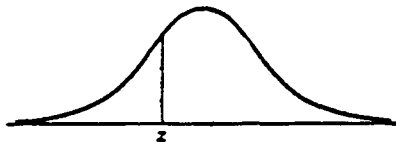
z	0	1	2	3	4	5	6	7	8	9
−3.	.0013	.0010	.0007	.0005	.0003	.0002	.0002	.0001	.0001	.0000
−2.9	.0019	.0018	.0017	.0017	.0016	.0016	.0015	.0015	.0014	.0014
−2.8	.0026	.0025	.0024	.0023	.0023	.0022	.0021	.0021	.0020	.0019
−2.7	.0035	.0034	.0033	.0032	.0031	.0030	.0029	.0028	.0027	.0026
−2.6	.0047	.0045	.0044	.0043	.0041	.0040	.0039	.0038	.0037	.0036
−2.5	.0062	.0060	.0059	.0057	.0055	.0054	.0052	.0051	.0049	.0048
−2.4	.0082	.0080	.0078	.0075	.0073	.0071	.0069	.0068	.0066	.0064
−2.3	.0107	.0104	.0102	.0099	.0096	.0094	.0091	.0089	.0087	.0084
−2.2	.0139	.0136	.0132	.0129	.0125	.0122	.0119	.0116	.0113	.0110
−2.1	.0179	.0174	.0170	.0166	.0162	.0158	.0154	.0150	.0146	.0143
−2.0	.0228	.0222	.0217	.0212	.0207	.0202	.0197	.0192	.0188	.0183
−1.9	.0287	.0281	.0274	.0268	.0262	.0256	.0250	.0244	.0238	.0233
−1.8	.0359	.0352	.0344	.0336	.0329	.0322	.0314	.0307	.0300	.0294
−1.7	.0446	.0436	.0427	.0418	.0409	.0401	.0392	.0384	.0375	.0367
−1.6	.0548	.0537	.0526	.0516	.0505	.0495	.0485	.0475	.0465	.0455
−1.5	.0668	.0655	.0643	.0630	.0618	.0606	.0594	.0582	.0570	.0559
−1.4	.0808	.0793	.0778	.0764	.0749	.0735	.0722	.0708	.0694	.0681
−1.3	.0968	.0951	.0934	.0918	.0901	.0885	.0869	.0853	.0838	.0823
−1.2	.1151	.1131	.1112	.1093	.1075	.1056	.1038	.1020	.1003	.0985
−1.1	.1357	.1335	.1314	.1292	.1271	.1251	.1230	.1210	.1190	.1170
−1.0	.1587	.1562	.1539	.1515	.1492	.1469	.1446	.1423	.1401	.1379
−.9	.1841	.1814	.1788	.1762	.1736	.1711	.1685	.1660	.1635	.1611
−.8	.2119	.2090	.2061	.2033	.2005	.1977	.1949	.1922	.1894	.1867
−.7	.2420	.2389	.2358	.2327	.2297	.2266	.2236	.2206	.2177	.2148
−.6	.2743	.2709	.2676	.2643	.2611	.2578	.2546	.2514	.2483	.2451
−.5	.3085	.3050	.3015	.2981	.2946	.2912	.2877	.2843	.2810	.2776
−.4	.3446	.3409	.3372	.3336	.3300	.3264	.3228	.3192	.3156	.3121
−.3	.3821	.3783	.3745	.3707	.3669	.3632	.3594	.3557	.3520	.3483
−.2	.4207	.4168	.4129	.4090	.4052	.4013	.3974	.3936	.3897	.3859
−.1	.4602	.4562	.4522	.4483	.4443	.4404	.4364	.4325	.4286	.4247
−.0	.5000	.4960	.4920	.4880	.4840	.4801	.4761	.4721	.4681	.4641

TABLE A-2
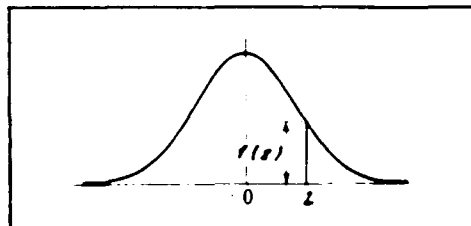
ORDINATES f(z) OF THE STANDARD NORMAL CURVE AT z

Z	0	1	2	3	4	5	6	7	8	9
0.0	.3989	.3989	.3989	.3988	.3986	.3984	.3982	.3980	.3977	.3973
0.1	.3970	.3965	.3961	.3956	.3951	.3945	.3939	.3932	.3925	.3918
0.2	.3910	.3902	.3894	.3885	.3876	.3867	.3857	.3847	.3836	.3825
0.3	.3814	.3802	.3790	.3778	.3765	.3752	.3739	.3725	.3712	.3697
0.4	.3683	.3668	.3653	.3637	.3621	.3605	.3589	.3572	.3555	.3538
0.5	.3521	.3503	.3485	.3467	.3448	.3429	.3410	.3391	.3372	.3352
0.6	.3332	.3312	.3292	.3271	.3251	.3230	.3209	.3187	.3166	.3144
0.7	.3123	.3101	.3079	.3056	.3034	.3011	.2989	.2966	.2943	.2920
0.8	.2897	.2874	.2850	.2827	.2803	.2780	.2756	.2732	.2709	.2685
0.9	.2661	.2637	.2613	.2589	.2565	.2541	.2516	.2492	.2468	.2444
1.0	.2420	.2396	.2371	.2347	.2323	.2299	.2275	.2251	.2227	.2203
1.1	.2179	.2155	.2131	.2107	.2083	.2059	.2036	.2012	.1989	.1965
1.2	.1942	.1919	.1895	.1872	.1849	.1826	.1804	.1781	.1758	.1736
1.3	.1714	.1691	.1669	.1647	.1626	.1604	.1582	.1561	.1539	.1518
1.4	.1497	.1476	.1456	.1435	.1415	.1394	.1374	.1354	.1334	.1315
1.5	.1295	.1276	.1257	.1238	.1219	.1200	.1182	.1163	.1145	.1127
1.6	.1109	.1092	.1074	.1057	.1040	.1023	.1006	.0989	.0973	.0957
1.7	.0940	.0925	.0909	.0893	.0878	.0863	.0848	.0833	.0818	.0804
1.8	.0790	.0775	.0761	.0748	.0734	.0721	.0707	.0694	.0681	.0669
1.9	.0656	.0644	.0632	.0620	.0608	.0596	.0584	.0573	.0562	.0551
2.0	.0540	.0529	.0519	.0508	.0498	.0488	.0478	.0468	.0459	.0449
2.1	.0440	.0431	.0422	.0413	.0404	.0396	.0387	.0379	.0371	.0363
2.2	.0355	.0347	.0339	.0332	.0325	.0317	.0310	.0303	.0297	.0290
2.3	.0283	.0277	.0270	.0264	.0258	.0252	.0246	.0241	.0235	.0229
2.4	.0224	.0219	.0213	.0208	.0203	.0198	.0194	.0189	.0184	.0180
2.5	.0175	.0171	.0167	.0163	.0158	.0154	.0151	.0147	.0143	.0139
2.6	.0136	.0132	.0129	.0126	.0122	.0119	.0116	.0113	.0110	.0107
2.7	.0104	.0101	.0099	.0096	.0093	.0091	.0088	.0086	.0084	.0081
2.8	.0079	.0077	.0075	.0073	.0071	.0069	.0067	.0065	.0063	.0061
2.9	.0060	.0058	.0056	.0055	.0053	.0051	.0050	.0048	.0047	.0046
3.0	.0044	.0043	.0042	.0040	.0039	.0038	.0037	.0036	.0035	.0034
3.1	.0033	.0032	.0031	.0030	.0029	.0028	.0027	.0026	.0025	.0025
3.2	.0024	.0023	.0022	.0022	.0021	.0020	.0020	.0019	.0018	.0018
3.3	.0017	.0017	.0016	.0016	.0015	.0015	.0014	.0014	.0013	.0013
3.4	.0012	.0012	.0012	.0011	.0011	.0010	.0010	.0010	.0009	.0009
3.5	.0009	.0008	.0008	.0008	.0008	.0007	.0007	.0007	.0007	.0006
3.6	.0006	.0006	.0006	.0005	.0005	.0005	.0005	.0005	.0005	.0004
3.7	.0004	.0004	.0004	.0004	.0004	.0004	.0003	.0003	.0003	.0003
3.8	.0003	.0003	.0003	.0003	.0003	.0002	.0002	.0002	.0002	.0002
3.9	.0002	.0002	.0002	.0002	.0002	.0002	.0002	.0002	.0001	.0001

6.0 RELIABILITY SPECIFICATION, ALLOCATION AND PREDICTION

6.1 INTRODUCTION

Section 5 of this handbook laid the theoretical, mathematical foundation for the reliability engineering discipline; this section emphasizes the practical approaches to specifying, allocating and predicting equipment/system reliability.

Section 6.2 discusses methods for specifying reliability, quantitatively; Section 6.3 describes procedures for allocating reliability to each of the elements of an equipment or system so as to meet the overall equipment/system reliability requirement; Section 6.4 provides details on methods for predicting equipment/system reliability; and Section 6.5 ties it all together in a step-by-step procedure for performing reliability allocation and prediction.

6.2 RELIABILITY SPECIFICATION

The first step in the reliability engineering process is to specify the required reliability that the equipment/system must be designed to achieve. The essential elements of a reliability specification are:

(1) a quantitative statement of the reliability requirement
(2) a full description of the environment in which the equipment/system will be stored, transported, operated and maintained.
(3) the time measure or mission profile
(4) a clear definition of what constitutes failure
(5) a description of the test procedure with accept/reject criteria that will be used to demonstrate the specified reliability.

6.2.1 METHODS OF SPECIFYING THE RELIABILITY REQUIREMENT

To be meaningful, a reliability requirement must be specified quantitatively. Figure 6.2.1-1 illustrates four basic ways in which a reliability requirement may be defined:

(1) As a "mean life" or mean-time-between-failure, MTBF (see (1) in Figure 6.2.1-1). This definition is useful for long life systems in which the form of the reliability distribution is not too critical or where the planned mission lengths are always short relative to the specified mean life. Although this definition is adequate for specifying life, it gives no positive assurance of a specified level of reliability in early life, except as the assumption of an exponential distribution can be proven to be valid.

(2) As a probability of survival for a specified period of time, t, (see (2) in Figure 6.2.1-1). This definition is useful for defining reliability when a high reliability is required during the mission period but mean-time-to-failure beyond the mission period is of little tactical consequence except as it influences availability.
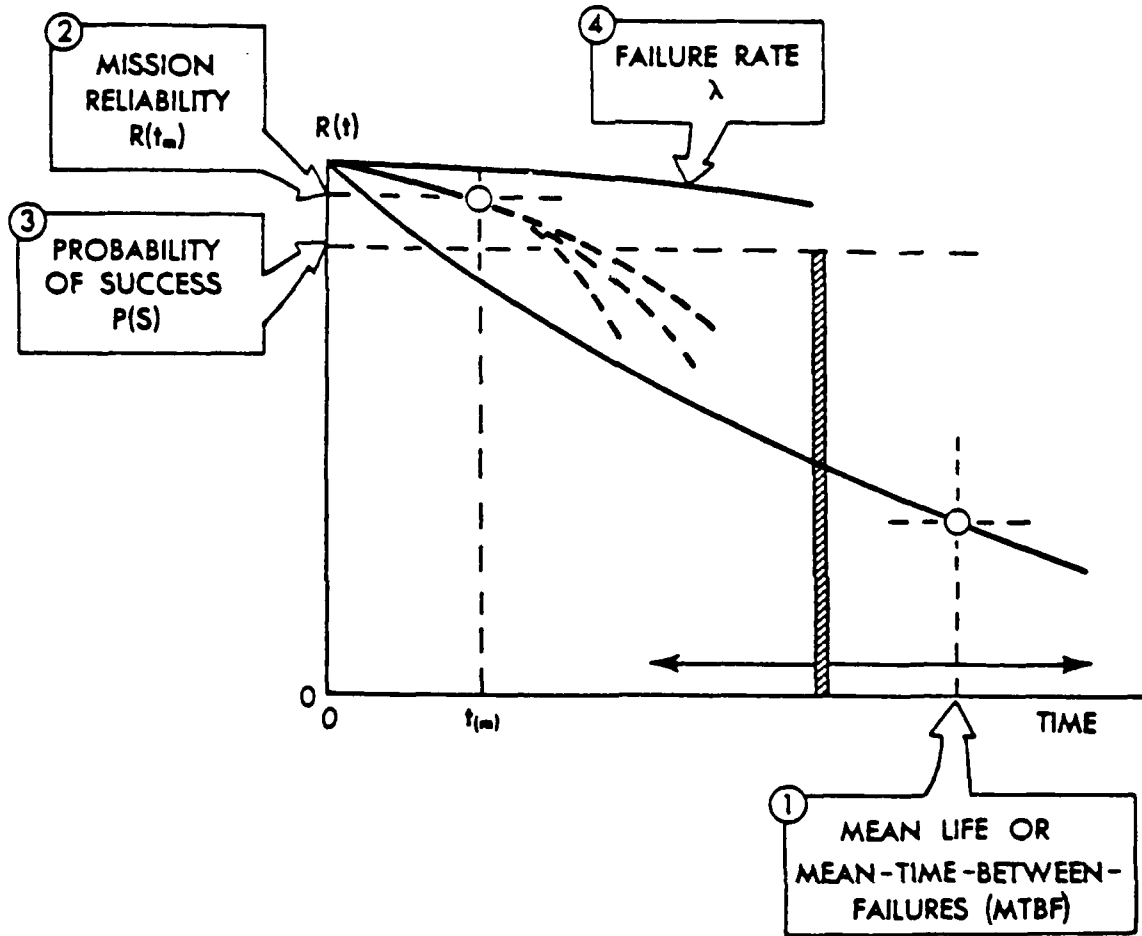
FIGURE 6.2.1-1: FOUR DEFINITIONS OF RELIABILITY

(3) As a probability of success, independent of time (see (3) in Figure 6.2.1-1). This definition is useful for specifying the reliability of one-shot devices such as the flight reliability of missiles, the detonation reliability of warheads, etc. It is also specified for these items which are cyclic such as the launch reliability of launches.

(4) As a "failure rate" over a specified period of time (see (4) in Figure 6.2.1-1). This definition is useful for specifying the reliability of parts, units, and assemblies whose mean lives are too long to be meaningful or whose reliability for the time period of interest approaches unity.

The reliability requirement may be specified in either of two ways:

(1) As a NOMINAL or design value with which the customer would be satisfied, on the average; or

(2) As a MINIMUM acceptable value below which the customer would find the system totally unacceptable and could not be tolerated in the operational environment -- a value based upon the operational requirements.

Whichever value is chosen as the specified requirement, there are two rules that should be applied; (a) when a nominal value is specified as a requirement, always specify a minimum acceptable value which the system must exceed, (b) when a minimum value alone is used to specify the requirement, always insure that it is clearly defined as minimum. In MIL-STD-781 the nominal value is termed the "upper test MTBF" and the minimum acceptable value is the "lower test MTBF."

Of the two methods, the first is by far the best, since it automatically establishes the design goal at or above a known minimum.

Figure 6.2.1-2 summarizes appropriate methods of stating the reliability requirements for various functions, usage, and maintenance conditions.

Example: A complex radar has both search and track functions. It is also possible to operate the search function in both a low and high power mode. The reliability requirement for this system could be expressed as:

"The reliability of the system shall be at least:

Case I -   High power search - 28 hours MTBF

Case II -   Low power search - 40 hours MTBF

Case III - Track - 0.98 probability of satisfactory performance for 1/2 hour"

CONDITIONS OF USE — LEVEL OF COMPLEXITY	CONTINUOUS DUTY LONG LIFE (REPAIRABLE)	INTERMITTENT DUTY SHORT MISSIONS (REPAIRABLE)	CONTINUOUS OR INTERMITTENT (NON-REPAIRABLE)	ONE-SHOT (TIME-INDEPENDENT)
COMPLEX SYSTEMS	R(t) OR MTBF	R(t) OR MTBF	R(t) OR MTBF	P(S) OR P(F)
SYSTEMS SUBSYSTEMS SETS GROUPS	R(t) OR MTBF	R(t) OR MTBF	R(t) OR λ	P(S) OR P(F)
UNITS ASSEMBLIES SUBASSEMBLIES PARTS	λ	λ	λ	P(F)

Code:

R(t) = Reliability for specified mission, or period of time, t.
MTBF = Mean-time-between-failures, or mean life.
P(S) = Probability of success.
P(F) = Probability of failure.
λ = Failure rate.

FIGURE 6.2.1-2: METHODS OF SPECIFYING RELIABILITY ACCORDING TO LEVELS OF COMPLEXITY AND CONDITIONS OF USE.

The definition of satisfactory performance must include limits for each case. These are necessary since if the radar falls below the specified limits for each case, it is considered to have failed the reliability requirement. A portion of the Satisfactory Performance Table for the radar is shown in Figure 6.2.1-3.

An important consideration in developing the reliability requirement is that it be realistic in terms of real need, yet consistent with current design state-of-the-art. Otherwise, the requirement may be unattainable or attainable only at a significant expenditure of time and money.

6.2.2 DESCRIPTION OF ENVIRONMENT AND/OR USE CONDITIONS

The reliability specification must cover all aspects of the use environment to which the item will be exposed and which can influence the probability of failure. The specification should establish in standard terminology the "use" conditions under which the item must provide the required performances. "Use" conditions refer to all known use conditions under which the specified reliability is to be obtained, including the following:

Temperature	Penetration/Abrasion
Humidity	Ambient Light
Shock	Mounting Position
Vibration	Weather (wind, rain, snow)
Pressure	Operator Skills

and other conditions covered in MIL-STD-210.

The "Use" conditions are presented in two ways:

(1) Narrative. Brief description of the anticipated operational conditions under which the system will be used.

Example:

(a) The MK 000 Computer will be installed in temperature controlled spaces aboard the aircraft.

(b) The TOY missile must be capable of withstanding exposed airborne environments encountered while suspended from the launcher for periods up to three hours. This includes possible ice-loading conditions, in subzero weather, etc.

(2) Specific. Itemized list of known or anticipated ranges of environments and conditions. When changes of environment are expected throughout an operating period, as in an aircraft flight, an environmental profile should be included.

System Characteristic	Units	Performance Limits		
		Case 1	Case 2	Case 3
Range	Yards	300,000	120,000	120,000
Resolution — Range	Yards	± 50	± 50	± 10
— Velocity	Ft./Sec.	±100	±100	± 25
Bandwidth	M			

FIGURE 6.2.1-3: <u>SATISFACTORY PERFORMANCE LIMITS</u>

Example:

(a) MK 000 Computer shall operate as specified under the following environments, either singly or combined:

Vibration: Vehicle Motion	10-25 Hz at 2.5g
Roll:	47^{0}
Pitch:	10^{0}
Yaw:	20^{0}
Temperature:	65^{0}F. to 80^{0}F
Humidity:	to 95%
Input Power:	Nominal 440 Hz 110 v $\pm$ 20%

(b) The AN/ARC-000 shall meet its performance requirements when subjected to the mission temperature profile, as illustrated in Figure 6.2.2-1.

MIL-STD-210 provides comprehensive, worldwide environmental coverage. Many individual specifications for specific categories of systems provide environmental classifications which may be referenced, providing the standard environments adequately cover the specified system's planned use. The practice of stating extreme environmental ranges for systems which will be used under controlled or limited conditions leads to undue costs.

6.2.3 TIME MEASURE OR MISSION PROFILE

Time is vital to the quantitative description of reliability. It is the independent variable in the reliability function. The system usage from a time standpoint in large measure determines the form of the reliability expression of which time is an integral part. The types of mission times commonly encountered are given in Figure 6.2.3-1. For those cases where a system is not designed for continuous operation, total anticipated time profile or time sequences of operation should be defined either in terms of duty cycles or profile charts.

Example:

The mission reliability for the "x" missile fire control system shall be at least 0.9 for a six hour mission having the typical operational sequence illustrated in Figure 6.2.3-1.

From the example it can be seen that a large portion of time is standby time rather than full power-on-time.

6.2.4 CLEAR DEFINITION OF FAILURE

A clear, unequivocal definition of "failure" must be established for the equipment or system in relation to its important performance parameters. Successful system (or equipment) performance must be defined. It must also be expressed in terms which will be measurable during the demonstration test.
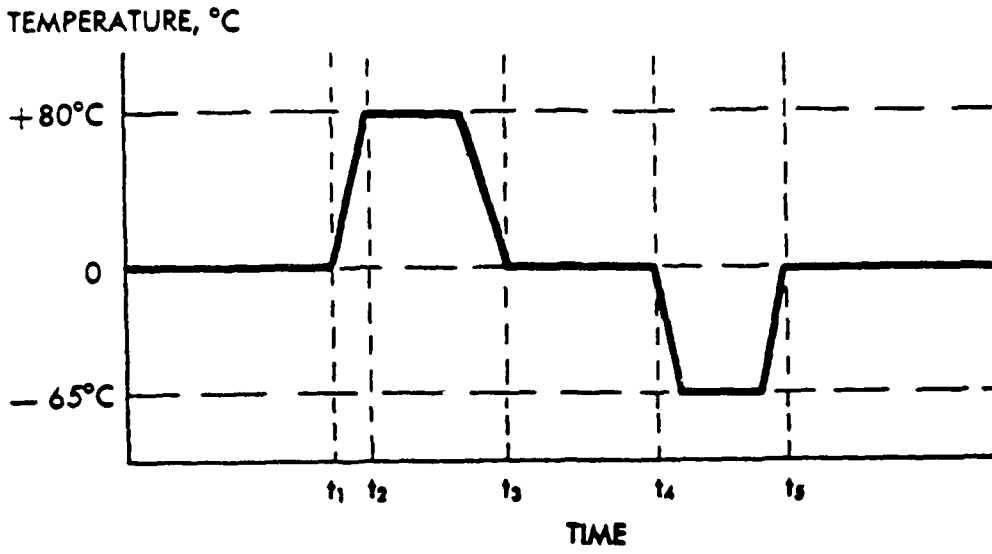
TEMPERATURE, °C

FIGURE 6.2.2-1: <u>TEMPERATURE PROFILE</u>

TOTAL TIME IN HOURS
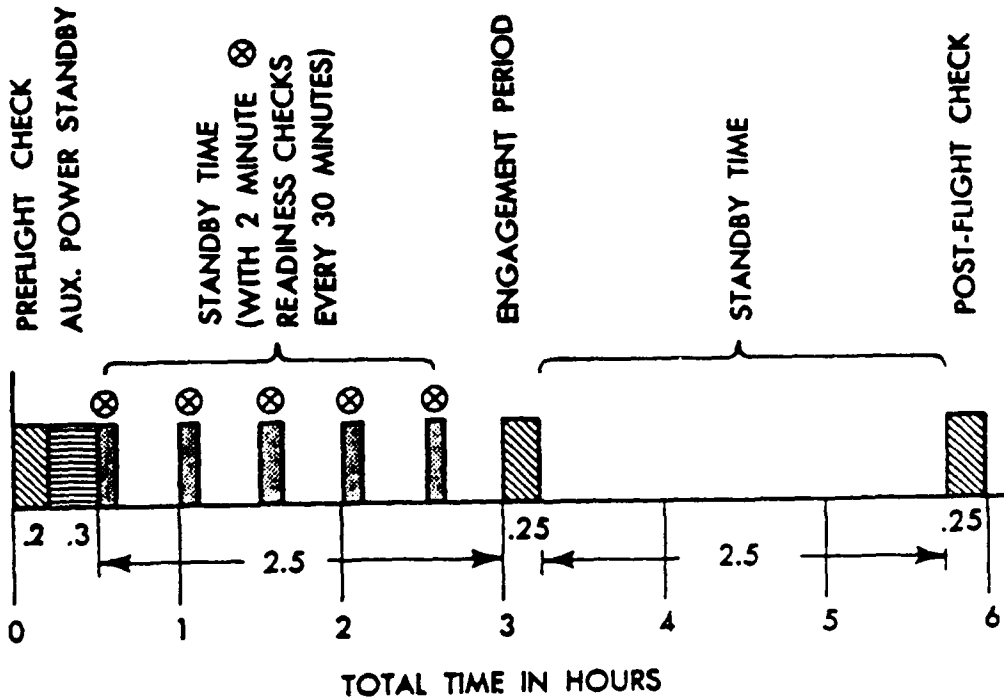
FIGURE 6.2.3-1: <u>TYPICAL OPERATIONAL SEQUENCE FOR AIRBORNE</u>
<u>FIRE CONTROL SYSTEM</u>

Parameter measurements will usually include both go/no-go performance attributes and variable performance characteristics. Failure of go/no-go performance attributes such as channel switching, target acquisition, motor ignition, warhead detonation, etc., are relatively easy to define and measure to provide a yes/no decision boundary. Failure of a variable performance characteristic, on the other hand, is more difficult to define in relation to the specific limits outside of which system performance is considered unsatisfactory. The limits of acceptable performance are those beyond which a mission may be degraded to an unacceptable level.

Figure 6.2.4-1 illustrates the two types of performance characteristics and corresponding success/failure (yes/no) decision boundaries that might be applied to a track radar or to a missile active seeker (guidance) system. In both cases, the success/failure boundary must be determined for each essential system performance characteristic to be measured in the demonstration test. They must be defined in clear, unequivocal terms. This will minimize the chance for subjective interpretation of failure definition, and post test rationalization (other than legitimate diagnosis) of observed failures.

6.2.5 DESCRIPTION OF METHOD(S) FOR RELIABILITY DEMONSTRATION

It is not enough to merely specify the reliability requirement. One must also delineate the test(s) that will be performed to verify whether the specified requirement has been met. In essence, the element of reliability specification should answer the following questions:

(1) How the equipment/system will be tested

o   the specified test conditions, e.g., environmental conditions, test measures, length of test, equipment operating conditions, accept/reject criteria, test reporting requirements, etc.

(2) Who will perform the tests

o   contractor, Government, independent organization

(3) When the tests will be performed

o   development, production, field operation

(4) Where the tests will be performed

o   contractor's plant, Government organization

Examples of several forms of reliability specifications are given in Figure 6.2.5-1.
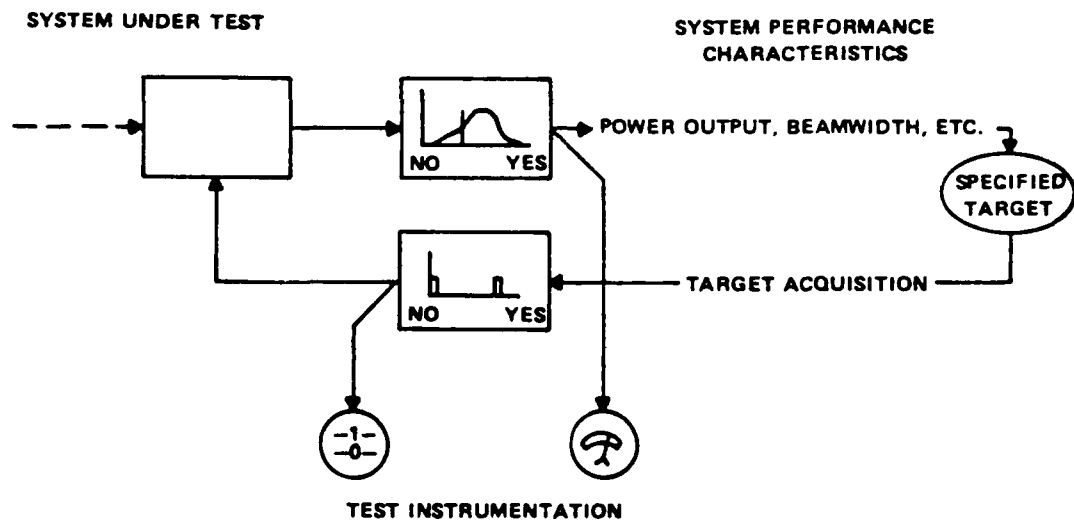
FIGURE 6.2.4-1: <u>ILLUSTRATION OF YES/NO BOUNDARIES IN SYSTEM</u>
<u>PERFORMANCE VARIABLES AND ATTRIBUTES</u>

3.2.3   Reliability

(1)   Avionics

3.2.3.1   Operational Stability — The equipment shall operate with satisfactory performance; continuously or intermittently for a period of at least _____ hours or _____ (_____) year whichever occurs first without the necessity for readjustment of any controls which are inaccessible to the operator during normal use.

3.2.3.2   Operating Life — The equipment shall have a minimum total operating life of _____ hours with reasonable servicing and replacement of subassemblies. Complete information on parts requiring scheduled replacement due to wear during the life of the equipment, and the wearout life of such subassemblies shall be determined by the contractor and submitted to the procuring agency for approval.

3.2.3.3   Reliability in Mean Time Between Failures (MTBF) — The AN/APQXXX shall be designed to meet a _____ hour specified mean (operating) time between failure demonstration as outlined under the requirements of 4.3.1.3.3.

- -

(2)   Missile System

3.2.3.1   System reliability. The system (excluding PGSE) shall have a mission reliability of 0._____ as a design objective and a minimum acceptable value of 0._____ . A mission is defined as one catapult launch and recovery cycle consisting of captive flight and missile free flight with total system performance within specifications, excluding $P_{(K)}$ (see 6.3).

3.2.3.2   Aircraft equipment subsystem reliability. The avionics equipment/aircraft installation shall have a design objective mean time between failures (MTBF) of _____ hours and a minimum acceptable MTBF of _____ hours. The launcher minimum acceptable reliability shall be 0._____ .

3.2.3.3   Missile free flight reliability. The missile shall have a free flight reliability of 0._____ as a design objective and 0._____ as a minimum acceptable value. Free flight is defined as the mission profile from launch to target including motor action, guidance to target with terminal fuze and warhead actions within specifications, but excludes $P_{(K)}$.

3.2.3.4   Missile captive flight reliability. The missile shall have a captive flight MTBF of _____ hours as a design objective and _____ hours as a minimum acceptable value. Captive flight includes catapult launch or take off and recovery, accrued flight time, and missile component operation within specifications up to missile launch. The missile shall have a _____ per cent probability of surviving 20 successive captive-flight cycles of 2.5 hours each without checkout or maintenance as a design objective and a _____ per cent probability of survival without checkout or maintenance as the minimum acceptable value.

- -

(3)   Aircraft

3.2.3.1   Mission reliability. The mission reliability expressed as the probability that the Airplane Weapon System can perform all the mission functions successfully, shall equal or exceed 0._____ based on a 2-hour mission duration with 0._____ as a goal.

3.2.3.2   Refly reliability. The refly reliability, expressed as the probability that the Airplane Weapon System can be returned to full operating capability without corrective maintenance between missions, shall equal or exceed 0._____ based on a 2-hour mission duration with 0._____ as a goal.

FIGURE 6.2.5-1: <u>EXAMPLE DEFINITION OF RELIABILITY DESIGN REQUIREMENTS IN A SYSTEM SPECIFICATION FOR (1) AVIONICS, (2) MISSILE SYSTEM AND (3) AIRCRAFT</u>

6.3 RELIABILITY APPORTIONMENT/ALLOCATION

6.3.1 INTRODUCTION

The first step in the design process is to translate the overall system reliability requirement into reliability requirements for each of the subsystems. This process is known as reliability apportionment (or allocation).

The allocation of system reliability involves solving the basic inequality:

$$f(\hat{R}_1, \hat{R}_2, \ldots \hat{R}_n) \geq R* \tag{6.1}$$

where

$\hat{R}_i$ is the allocation reliability parameter for the ith subsystem
$R*$ is the system reliability requirement parameter
f is the functional relationship between subsystem and system reliability

For a simple series system in which the R's represent probability of survival for t hours, Eq. (6.1) becomes:

$$\hat{R}_1 (t) \cdot \hat{R}_2 (t) \ldots \hat{R}_n (t) \geq R* (t) \tag{6.2}$$

Theoretically, Eq. (6.2) has an infinite number of solutions, assuming no restrictions on the allocation. The problem is to establish a procedure that yields a unique or limited number of solutions by which consistent and reasonable reliabilities may be allocated. For example, the allocated reliability for a simple subsystem of demonstrated high reliability should be greater than that of a complex subsystem whose observed reliability has always been low.

The allocation process is approximate. The reliability parameters apportioned to the subsystems are used as guidelines to determine design feasibility. If the allocated reliability for a specific subsystem cannot be achieved at the current state of technology, then the system design must be modified and the allocations reassigned. This procedure is repeated until an allocation is achieved that satisfies the system level requirement and all constraints and results in subsystems that can be designed within the state of the art.

In the event that it is found that even with reallocation some of the individual subsystem requirements cannot be met within the current state of the art, then the designer must use one or any number of the following approaches (assuming that they are not mutually exclusive) in order to achieve the desired reliability:

(1) Find more reliable component parts to use
(2) Simplify the design by using fewer component parts, if this is possible without degrading performance
(3) Apply component derating techniques to reduce the failure rates below the averages
(4) Use redundancy for those cases where (1), (2) and (3) do not apply

It should be noted that the allocation process can, in turn, be performed at each of the lower levels of the system hierarchy, e.g., equipment, module, component.

This section will discuss six different approaches to reliability allocation. These approaches differ in complexity, depending upon the amount of subsystem definition available and the degree of rigor desired to be employed. Reference 10 contains a more detailed treatment of allocation methods, as well as a number of more complex examples.

6.3.2 EQUAL APPORTIONMENT TECHNIQUE

In the absence of definitive information on the system, other than the fact that n subsystems are to be used in series, equal apportionment to each subsystem would seem reasonable. In this case, the nth root of the system reliability requirement would be apportioned to each of the n subsystems.

The equal apportionment technique assumes a series of n subsystems, each of which is to be assigned the same reliability goal. A prime weakness of the method is that the subsystem goals are not assigned in accordance with the degree of difficulty associated with achievement of these goals. For this technique, the model is:

$$R^* = \prod_{i=1}^{n} R^*_i \qquad (6.3)$$

or

$$R^*_i = (R^*)^{1/n} \text{ for } i = 1, 2, \ldots, n \qquad (6.4)$$

where

R^* is the required system reliability

R^*_i is the reliability requirement apportioned to subsystem i

Example

Consider a proposed communication system which consists of three subsystems (transmitter, receiver, and coder), each of which must function if the system is to function. Each of these subsystems is to be developed independently. Assuming each to be equally expensive to develop, what reliability requirement should be assigned to each subsystem in order to meet a system requirement of 0.729?

The apportioned subsystem requirements are found as:

$$R^*_T = R^*_R = R^*_C = (R^*)^{1/n} = (0.729)^{1/3} = 0.90$$

Then a reliability requirement of 0.90 should be assigned to each subsystem.

6.3.3 AGREE APPORTIONMENT TECHNIQUE

A method of apportionment for electronics systems is outlined in the AGREE report (Ref. 2). This technique takes into consideration both the complexity and importance of each subsystem. It assumes a series of k subsystems, each with exponential failure distributions. The apportioned reliability goal is expressed in terms of MTBF. Then the minimum acceptable mean life of the ith subsystem is defined as:

$$\theta_i = \frac{N w_i t_i}{n_i [-\ln R^*(t)]} \tag{6.5}$$

and the corresponding i^{th} subsystem reliability requirement becomes:

$$R_i^*(t_i) = \exp\left(\frac{-t_i}{\theta_i}\right) \tag{6.6}$$

where

$$
\begin{array}{ll}
i & = 1, 2, 3, \ldots, k \\[1.2em]
t & = \text{required mission time of the system} \\[1.2em]
t_i & = \text{required mission time of the } i^{th} \text{ subsystem} \\[1.2em]
w_i & = \text{importance factor expressed as the probability that} \\
& \quad \text{failure of the } i^{th} \text{ subsystem will result in system} \\
& \quad \text{failure} \\[1.2em]
n_i & = \text{number of modules in the } i^{th} \text{ subsystem} \\[1.2em]
N & = \sum\limits_{i=1}^{k} n_i = \text{total number of modules in the system} \\[1.2em]
R^*(t) & = \text{the required system reliability for system mission time} \\[1.2em]
R_i^*(t_i) & = \text{the reliability apportioned to the } i^{th} \text{ subsystem for its} \\
& \quad \text{mission time} \\[1.2em]
\theta_i & = \text{apportioned mean time to failure for the } i^{th} \text{ subsystem}
\end{array}
$$

A concept of module is used in this technique for three purposes: (1) so that the relative complexity inherently required can be taken into account; (2) so that the minimum acceptable reliability figures will not be grossly inconsistent; and (3) so that reliability requirements will be dynamic and state-of-art changes can be incorporated as they occur. A module is designated as the basic electronic building block and is considered to be a group of electronic parts. This is a fictitious way of partitioning an electronic system for reliability purposes. For systems involving electron tubes, it was found that for one tube there were approximately 15 additional electronic parts; this was considered to be a module. Thus, in the past, the number of modules for an equipment was defined as the number of electron tubes. For present day systems, this concept must be modified to expand the definition of module to include solid state devices.

Example

To illustrate the AGREE apportionment method, consider a fictitious system composed of four subsystems. The system has a mission time of four hours and required reliability of 0.9. Figure 6.3.3-1 shows the number of modules, importance factor and mission time for each subsystem.

The apportionment to each subsystem is found as follows:

$$\theta_i = \frac{N w_i t_i}{n_i [-\ln R^*(t)]}$$

and

$$R^*_i(t_i) = \exp\left(\frac{-t_i}{\theta_i}\right)$$

where

$R^*(4) = 0.90$

$$\theta_1 = \frac{(300)\ (0.7)\ (4)}{(20)\ (0.1054)} = \frac{840}{2.108} = 398 \text{ hours}$$

$R^*_1(4) = \exp(-4/398) = \exp(-0.01) = 0.990$

$$\theta_2 = \frac{(300)\ (0.5)\ (4)}{30\ (0.1054)} = \frac{600}{3.162} = 189 \text{ hours}$$

$R^*_2(4) = \exp(-4/398) = \exp(-0.021) = 0.979$

$$\theta_3 = \frac{(300)\ (0.8)\ (4)}{(200)\ (0.1054)} = \frac{960}{21.08} = 45 \text{ hours}$$

$R^*_3(4) = \exp(-4/45) = \exp(-0.089) = 0.915$

$$\theta_4 = \frac{(300)\ (0.2)\ (4)}{(50)\ (0.1054)} = \frac{240}{5.27} = 45 \text{ hours}$$

$R^*_4(4) = \exp(-4/45) = \exp(-0.089) = 0.915$

Subsystem (i)	No. Modules (n_i)	Importance Factor (w_i)	Mission Time (t_i)
1	20	0.7	4
2	30	0.5	4
3	200	0.8	4
4	50	0.2	4
	N = 300		

FIGURE 6.3.3-1: <u>SYSTEM APPORTIONMENT FACTORS</u>

6.3.4 ARINC APPORTIONMENT TECHNIQUE (Ref. 3)

This method assumes series subsystems with constant failure rates, such that any subsystem failure causes system failure and that subsystem mission time is equal to system mission time. This apportionment technique requires expression of reliability requirements in terms of failure rate.

The following steps apply:

(1) The objective is to choose λ^*_i such that:

$$\sum_{i=1}^{n} \lambda^*_i \leq \lambda^* \tag{6.7}$$

where

λ^*_i is the failure rate allocated to subsystem i
λ^* is the required system failure rate

(2) Determine the subsystem failure rates (λ_i) from past observation or estimation

(3) Assign a weighting factor (w_i) to each subsystem according to the failure rates determined in (2) above

$$w_i = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} \tag{6.8}$$

(4) Allocate subsystem failure rate requirements

$$\lambda^*_i = w_i \lambda^* \tag{6.9}$$

Example

To illustrate this method, consider a system composed of three subsystems with predicted failure rates of $\lambda_1 = 0.003$, $\lambda_2 = 0.001$, and $\lambda_3 = 0.004$ failures per hour, respectively. The system has a mission time of 20 hours and 0.90 reliability is required. Find the subsystem requirements.

The apportioned failure rates and reliability goals are found as follows:

(1) $R^*(20) = \exp[-\lambda^* (20)] = 0.90$

Then

$\lambda^* = 0.005$ failures per hour

(2) $\lambda_1 = 0.003$, $\lambda_2 = 0.001$, $\lambda_3 = 0.004$

(3) $\quad w_1 \quad = \quad \dfrac{0.003}{0.003 + 0.001 + 0.004} = 0.375$

$\quad w_2 \quad = \quad \dfrac{0.001}{0.003 + 0.001 + 0.004} = 0.125$

$\quad w_3 \quad = \quad \dfrac{0.004}{0.003 + 0.001 + 0.004} = 0.5$

(4) $\quad \lambda^*_1 = 0.375(0.005) = 0.001875$

$\quad \lambda^*_2 = 0.125(0.005) = 0.000625$

$\quad \lambda^*_3 = 0.5\ (0.005) = 0.0025$

(5) the corresponding allocated subsystem reliability requirements are

$R_1^*(20) = \exp [-20\ (0.001875)] = 0.96$
$R_2^*(20) = \exp [-20\ (0.000625)] = 0.99$
$R_3^*(20) = \exp [-20\ (0.0025)] = 0.95$

6.3.5 FEASIBILITY-OF-OBJECTIVES TECHNIQUE (Ref. 1)

This technique was developed primarily as a method of allocating reliability without repair for mechanical-electrical systems. In this method, subsystem allocation factors are computed as a function of numerical ratings of system intricacy, state of the art, performance time, and environmental conditions. These ratings are estimated by the engineer on the basis of his experience. Each rating is on a scale from 1 to 10, with values assigned as discussed:

(1) System Intricacy. Intricacy is evaluated by considering the probable number of parts or components making up the system and also is judged by the assembled intricacy of these parts or components. The least intricate system is rated at 1, and a highly intricate system is rated at 10.

(2) State of the Art. The state of present engineering progress in all fields is considered. The least developed design or method is a value of 10, and the most highly developed is assigned a value of 1.

(3) Performance Time. The element that operates for the entire mission time is rated 10, and the element that operates the least time during the mission is rated at 1.

(4) Environment. Environmental conditions are also rated from 10 through 1. Elements expected to experience harsh and very severe environments during their operation are rated as 10, and those expected to encounter the least severe environments are rated as 1.

The ratings are assigned by the design engineer based upon his engineering know how and experience. They may also be determined by a group of engineers using a voting method such as the Delphi technique.

An estimate is made of the types of parts and components likely to be used in the new system and what effect their expected use has on their reliability. If particular components had proven to be unreliable in a particular environment, the environmental rating is raised.

The four ratings for each subsystem are multiplied together to give a rating for the subsystem. Each subsystem rating will be between 1 and 10^4. The subsystem ratings are then normalized so that their sum is 1.

The basic equations are:

$$\lambda_s T = \sum \bar{\lambda}_k T \tag{6.10}$$

$$\bar{\lambda}_k = C'_k \lambda_s \tag{6.11}$$

where

C'_k = complexity of subsystem k

$$C'_k = w'_k / W' \tag{6.12}$$

$$w'_k = r'_{1k} \, r'_{2k} \, r'_{3k} \, r'_{4k} \tag{6.13}$$

$$W' = \sum_{k=1}^{N} w'_k \tag{6.14}$$

where

λ_s = system failure rate

T = mission duration

$\bar{\lambda}_k$ = failure rate allocated to each subsystem

N = number of subsystems

w'_k = rating for subsystem k

r'_{ik} = rating for each of the four factors for each subsystem

Example

A mechanical-electrical system consists of the following subsystems: propulsion, ordnance, guidance, flight control, structures, and auxiliary power. A system reliability of 0.90 in 120 hr is required. Engineering estimates of intricacy, state of the art, performance time, and environments can be made. The subsystems and their ratings are described in Table 6.3.5-1, columns 1-5. Compute the allocated failure rate for each subsystem.

Procedure	Example

(1) Compute the product of the rating r'_j for each subsystem and their sums, i.e., fill in column 6, Table 6.3.5-1 by Eq. (6.13) and (6.14)

$w'_1 = 5 \times 6 \times 5 \times 5$
$= 750$

.   .
.   .
.   .

$w'_6 = 6 \times 5 \times 5 \times 5$
$= 750$

$W' = 750 + 840 + 2500 + 2240$
$+ 640 + 750$
$= 7720$

(2) Compute the complexity factors C'_k for each subsystem, i.e., fill in column 7, Table 6.3.5-1 by Eq. (6.12)

$C'_1 = 750/7720$
$= 0.097$

.   .
.   .
.   .

$C'_6 = 750/7720$
$= 0.097$

(3) Compute system failure rate λ_s from system specifications; $R_s = 0.90$ and $T = 120$ hr

$\lambda_s = -\ln 0.90/120$ hr
$= 878.0$ per 10^6 hr

(4) Compute the allocated subsystem failure rate λ_k, i.e., fill in column 8, Table 6.3.5-1 by Eq. (6.11)

$\lambda_1 = 0.097 \times (878.0$ per 10^6 hr$)$
$= 85.17$ per 10^6 hr
$\lambda_2 = 0.109 \times (878.0$ per 10^6 hr$)$
.
.
.
$\lambda_6 = 0.097 \times (878.0$ per 10^6 hr$)$
$= 85.17$ per 10^6 hr

(5) Round off failure rates λ_k to 2 significant figures, so that too much accuracy will not be implied; sum and compare with λ_s, Step (3)

$= 85 + 96 + 284 + 255 + 73 + 85$
$= 878 \leq 878$

6.3.6 MINIMIZATION OF EFFORT ALGORITHM

This algorithm considers minimization of total effort expended to meet system reliability requirements. It assumes a system comprised of n subsystems in series. Certain assumptions are made concerning the effort function. It assumes that the reliability of each subsystem is measured at the present stage of development, or is estimated, and apportions reliability such that greater reliability improvement is demanded of the lower reliability subsystems.

TABLE 6.3.5-1: MECHANICAL-ELECTRICAL SYSTEM

(1) Subsystem	(2) Intricacy r'_1	(3) State-of-the-art r'_2	(4) Performance time r'_3	(5) Environment r'_4	(6) Overall rating w'_k	(7) Complexity C'_k	(8) Allocated failure rate (per 10^6 hours)
1. Propulsion	5	6	5	5	750	.097	85
2. Ordnance	7	6	10	2	840	.109	96
3. Guidance	10	10	5	5	2500	.324	284
4. Flight Control	8	8	5	7	2240	.290	255
5. Structure	4	2	10	8	640	.083	73
6. Auxiliary Power	6	5	5	5	750	.097	85
Total					7720	1.000	878

System s-reliability = 0.90

Mission Time = 120 hours

λ_s = 878 per 10^6 hours

Let R_1, R_2, ..., R_n denote subsystem reliabilities, and the system reliability R would be given by:

$$R = \prod_{i=1}^{n} R_i \tag{6.15}$$

Let R^* be the required reliability of the system, where $R^* > R$. It is then required to increase at least one of the values of the R_i to the point that the required reliability R^* will be met. To accomplish such an increase takes a certain effort, which is to be allotted in some way among the subsystems. The amount of effort would be some function of number of tests, amount of engineering manpower applied to the task, etc.

The algorithm assumes that each subsystem has associated with it the same effort function $G(R_i, R^*_i)$ which measures the amount of effort needed to increase the reliability of the ith subsystem from R_i to R^*_i.

The problem then is to determine R^*_i such that

$$\sum_{i=1}^{n} G(R_i, R^*_i) \tag{6.16}$$

is minimized subject to the condition

$$\prod_{i=1}^{n} R^*_i = R^* \tag{6.17}$$

With the preceding assumptions, it can be shown that the unique solution is

$$R^*_i = \begin{cases} R^*_0 & \text{if } i \leq K_0 \\ R_i & \text{if } i > K_0 \end{cases}$$

where the subsystem reliabilities R_1, R_2, ..., R_n are ordered in nondecreasing fashion (assuming such an ordering is implicit in the notation).

$$R_1 \leq R_2 \ldots \leq R_n$$

and the number K_0 is determined is

K_0 = maximum value of j such that

$$R_j < \left[\frac{R^*}{\displaystyle\prod_{i=j+1}^{n+1} R_i} \right]^{1/j} = r_j \tag{6.18}$$

where $R_{n+1} = 1$ by definition.

The number R^*_j is determined as

$$R^*_o = \left[\frac{R^*}{\prod\limits_{j=K_o+1}^{n+1} R_j} \right]^{1/K_o}$$

It is evident that the system reliability will then be R^*, since new reliability

$$(R^*_o)^{K_o} R_{K_o+1} \cdots R_n = (R^*_o)^{K_o} \left[\prod\limits_{j=K_o+1}^{n+1} R_j \right] = R^* \tag{6.20}$$

when the relationship for R^*_o is substituted.

Example

As an example, consider a system that consists of three subsystems (A, B, and C), all of which must function without failure in order to achieve system success. The system reliability requirement has been set at 0.70. We have predicted subsystem reliabilities as $R_A = 0.90$, $R_B = 0.80$, and $R_C = 0.85$. How should we apportion reliability to the subsystem in order that the total effort be minimized and that the system reliability requirement be satisfied? Assume identical effort functions for the three subsystems.

The resulting minimum effort apportionment goals are found as follows:

    (1) Arrange subsystem reliability values in ascending order:

$R_1 = R_B = 0.80$, $R_2 = R_C = 0.85$, $R_3 = R_A = 0.90$

    (2) Determine K_o, the maximum value of j, such that

$$R_j < \left[\frac{R^*}{\prod\limits_{i=j+1}^{n+1} R_j} \right]^{1/j} = r_j$$

    (3) When $j = 1$,

$$R_1 = 0.80 < r_1 = \frac{0.7}{R_2 R_3 (1.0)} = \frac{0.7}{(0.85)(0.9)(1.0)} = \frac{0.7}{0.765} = 0.915$$

Note that R_{n+1} was previously defined, Eq. (6.13), as 1.

(4) When j = 2,

$$R_2 = 0.85 < r_2 = \left(\frac{0.7}{(0.9)\ (1.0)}\right)^{1/2} = \left(\frac{7}{9}\right)^{1/2} = \frac{\sqrt{7}}{3} = 0.882$$

(5) When j = 3,

$$R_3 = 0.90 > r_3 = \left(\frac{0.7}{1.0}\right)^{1/3} = 0.888$$

(6) Since $R_1 < r_1$, $R_2 < r_2$, but $R_3 > r_3$, v = 2 because 2 is the largest subscript j such that $R_j < r_j$. Thus,

$$R*_0 = \left(\frac{0.7}{0.9}\right)^{1/2} = 0.882$$

which means that the effort is to be allotted so that subsystem B increases in reliability from 0.80 to 0.882, and subsystem C increases in reliability from 0.85 to 0.882; whereas subsystem A is left alone with a reliability of 0.90. The resulting reliability of the entire system is, as required, $0.70 = (0.882)^2$ (0.90). This means that effort should be expended on subsystems C and B to raise their respective reliabilities to 0.882 with no developmental effort spent on subsystem A. This policy would minimize the total expended effort required to meet system reliability requirements. The minimization, however, is dependent upon the effort function meeting the initial assumptions, which may not be possible.

6.3.7 DYNAMIC PROGRAMMING APPROACH

If all subsystems are not equally difficult to develop, dynamic programming provides an approach to reliability apportionment with minimum effort expenditure when the subsytems are subject to different, but identifiable effort functions. The preceding minimization of effort algorithm requires that all subsystems be subject to the same effort function.

The dynamic programming approach can be most useful because it can be implemented with a simple algorithm that consists of only arithmetic operations. Some advantages of the dynamic programming approach are:

(1) Large problems can be solved with a minimum number of calculations (this "minimum" may be very large for a complex system).

(2) There is always a finite number of steps required in computing an optimum solution.

(3) There are no restrictions of any kind on the form of the functional expression for computing reliability or the form of the cost estimating equations. Nonlinear functions can be used if required.

The dynamic programming algorithms provide a guide through the maze of possible alternate calculations that may arise when big systems are being analyzed. The dynamic programming approach also can be applied to the problem of reliability optimization of redundant systems with repair. The use of the dynamic programming algorithm does not in any way remove the requirement for computing the reliability and cost for each system configuration. However, it minimizes the total number of calculations by rejecting those configurations that would result in a decreasing reliability or in costs exceeding the cost constraints, etc.

For the interested reader, Appendix A describes the theoretical basis for the dynamic programming approach and provides an example of its application to a reliability allocation problem.

The dynamic programming optimization technique has application potential in other areas of reliability analysis. For example, useful models have been developed for determining an optimal number of redundant units (subsystems) subject to restraints such as weight, cost, volume, opposing failure modes, etc. Also, a dynamic programming model has been developed for providing a systems approach to test planning, i.e., planning for an optimal number of tests.

The important point to remember is that the dynamic programming approach can be readily computerized, and a number of computer models are available.

6.4 RELIABILITY PREDICTION

6.4.1 INTRODUCTION AND GENERAL INFORMATION

Reliability prediction is the process of quantitatively assessing whether a proposed, or actual, equipment/shelter design will meet a specified reliability requirement. The real value of the quantitative expression lies in the information conveyed with this value and the use which is made of that information. Predictions do not, themselves, contribute significantly to system reliability. They do, however, constitute decision criteria for selecting courses of action which affect reliability.

The primary objective of reliability prediction is to provide guidance, relative to expected inherent reliability of a given design. Reliability predictions are most useful and economical during the early phase of a system design and acquisition, before hardware is constructed and tested.

During design and development, predictions serve as quantitative guides by which design alternatives can be judged for reliability. Basically, the purpose of reliability prediction includes feasibility evaluation, comparison of alternative configurations, identification of potential problems during design review, logistics support planning and cost studies, determination of data deficiencies, tradeoff decisions, allocation of requirements, and also provides criteria for reliability growth and demonstration testing.

Some important uses of reliability prediction include:

(1) Establishment of firm reliability requirements in planning documents, preliminary design specifications and requests for proposals, as well as determination of the feasibility of a proposed reliability requirement

(2) Comparison of the established reliability requirement with state-of-the-art feasibility for guidance in budget and schedule decisions

(3) Providing a basis for uniform proposal preparation and evaluation and ultimate contractor selection

(4) Evaluation of potential reliability through predictions submitted in technical proposals and reports in precontract transactions

(5) Identification and ranking of potential problem areas and the suggestion of possible solutions

(6) Allocation of reliability requirements among the subsystems and lower level items

(7) Evaluation of the choice of proposed parts, materials, units, and processes

(8) Conditional evaluation of the design for prototype fabrication during the development phase

(9) Provides a basis for tradeoff analysis

Thus, reliability prediction is a key to system development and allows reliability to become an integral part of the design process. To be effective, the prediction technique must relate engineering variables (the language of the designer) to reliability variables (the language of the reliability engineer).

In general, there is a hierarchy of reliability prediction techniques available to the designer depending upon (1) the depth of knowledge of the design and (2) the availability of historical data on equipment and component part reliabilities. As the system design proceeds from the Conceptual, through Full Scale Development, to the Production phase, data describing the system design evolves from a qualitative description of system functions to detailed specifications and drawings suitable for hardware production. Therefore, a hierarchy of reliability prediction techniques have been developed to accommodate the different reliability study and analysis requirements and the availability of detailed data as the system design progresses. These techniques can be roughly classified in five categories, depending on the type of data or information availability for the analysis. The categories are:

(1) Similar Equipment Techniques. The equipment under considera-
     tion is compared with similar equipments of known reliability
     in estimating the probable level of achievable reliability

(2) Similar Complexity Techniques. The reliability of a new
     design is estimated as a function of the relative complexity
     of the subject item with respect to a "typical" item of
     similar type

(3) Prediction by Function Techniques. Previously demonstrated
     correlations between operational function and reliability are
     considered in obtaining reliability predictions for a new
     design

(4) Part Count Techniques. Equipment reliability is estimated as
     a function of the number of parts, in each of several part
     classes, to be included in the equipment

(5) Stress Analysis Techniques. The equipment failure rate is
     determined as an additional function of all individual part
     failure rates, and considering part type, operational stress
     level, and derating characteristics of each part

Figure 6.4.1-1 is a partial list of a radar system hierarchy and the
life cycle phase of the system development. As the program progresses
from the conceptual to the detailed design phase, details become
available at progressively lower levels of the system hierarchy.
Concurrently, reliability prediction procedures become more detailed and
accurate as the design proceeds.

Subsequent paragraphs of this section describe in more detail each of
the above mentioned prediction techniques, following a brief discussion
of some of the underlying mathematical principles of reliability
prediction for electronic systems.

6.4.2 MATHEMATICAL MODELS FOR RELIABILITY PREDICTION

For the simplest case of equipment/system consisting of N independent
elements/subsystems in series, the reliability equation is:

$$R_s = \prod_{i=1}^{N} R_i \qquad (6.21)$$

where

   R_s is the equipment/system reliability
   R_i is the reliability of each of the elements/subsystems

Eq. (6.21) refers simply to the probability of success; it is most
applicable to devices whose failure rate changes with time, or one-shot
devices. For the case where time is a factor

$$R_s(t) = \prod_{i=1}^{N} R(t)_i \qquad (6.22)$$

Reliability Prediction Techniques	Similar Equipment(of Known Reliability) Similar Complexity	• Similar Equipment • SIMILAR COMPLEXITY PREDICTION BY FUNCTION	• Part Counts • Gross Stress Analysis	• Stress Analysis
	System j=1 Radar System	Subsystem j=2 Transmitter Receiver Stalo	Assembly j=3 Power Output Amplifier Low Power Amplifier Power Supplies	Part j=4 TWT Transistors Capacitors Resistors
	Early Trade Studies	Conceptual Design	Early Design	Detailed Design

FIGURE 6.4.1-1: RADAR SYSTEM HIERARCHY (PARTIAL LISTING)

where

$R_s(t)$ = The probability that the system will not fail before time t. (In this case a "system" is considered to be any device consisting of n elements, none of which can fail without system failure.)

$R(t)_i$ = The probability that the ith element of the system will not fail before time t.

Finally, if one assumes that each of the $R(t)_i$'s is exponentially distributed with constant failure rate, λ_i

$$R_S(t) = \prod_{i=1}^{N} e^{-\lambda_i t} \qquad (6.23)$$

$$= \exp\left(- \sum_{i=1}^{N} \lambda_i t\right) \qquad (6.24)$$

Also,

$$\lambda_S = \sum_{i=1}^{N} \lambda_i \qquad (6.25)$$

where

λ_S = system failure rate

λ_i = failure rate of each of the independent elements of the system

And,

$$MTBF = \frac{1}{\lambda_S} = \frac{1}{\sum\limits_{i=1}^{N} \lambda_i} \qquad (6.26)$$

Eqs. (6.24), (6.25), and (6.26) are the basic equations used in the reliability prediction of electronic equipment/systems.

The use of the exponential distribution of time to failure for complex systems is usually justified because of the many forces that can act upon the system and produce failure. For example, different deterioration mechanisms, different part hazard-rate functions, and varying environmental conditions often result in, effectively, random system failures.

Another justification for assuming the exponential distribution in long life complex systems is the so called "approach to a stable state," wherein the system hazard rate is effectively constant regardless of the failure pattern of individual parts. This state results from the mixing of part ages when failed elements in the system are replaced or repaired. Over a period of time, the system hazard rate oscillates, but this cyclic movement diminishes in time and approaches a stable state with a constant hazard rate.

A third justification for assuming the exponential distribution is that the exponential can be used as an approximation of some other function over a particular interval of time for which the true hazard rate is essentially constant.

Finally, the exponential distribution has been validated over the past twenty five years on a number of electronic equipments and systems by providing results which correlate fairly closely with actual field data.

The preceding paragraphs are not intended to imply that the exponential assumption is generally valid. Because of its mathematical simplicity and the extensive theory developed by many researchers, the exponential density plays a prominent role in reliability work. However, if observed failure data do not support the exponential assumption or if such factors as wearout are expected to be significant, the exponential assumption can be erroneous. In such cases, other distributions, such as the lognormal, gamma and Weibull distributions are available for performing more valid predictions. These more complex situations will not be treated in this section. For information concerning the application of such techniques, the reader is directed to References 1, 4, 5, 6, 7, 8.

Furthermore, if a system contains redundant items, the reliability formula will be more complex even though the individual items follow an exponential distribution of failure times. However, all systems can be reduced to combinations and/or modifications of basic configurations. These configurations and combinations are:

(1) Series configurations

(2) Parallel (redundant) configurations

(3) Mixed (series and parallel) configurations

(4) Partially redundant configurations

(5) Standby redundancy configurations

The subject of redundancy as a design technique is treated in more detail in Section 7 and in Appendix A of that section.

As an example let us use the block diagrams of Figure 6.4.2-1 to develop some simple models. Figure 6.4.2-1 as with Figure 6.4.1-1, shows the evolution of the detailed system block diagram, going from the weapon system level (I) down to the part level (V).

Progressing from Level I to Level V, for example, System Reliability, R_s = $R_1 \times R_2 \times R_3 \times R_4$ where

$$R_4 = R_a \times R_b \times R_c \times R_d \times R_e$$

$$R_c = R_i \times R_{ii} [1 - (1-R_v)(1-R_{iii}R_{iv})][1 - (1-R_{vi})^3]$$

$$R_{ii} = R_X R_L R_C R_R [1-Q_C^2][1-Q_X^2][1-Q_D^2]^2$$

LEVEL I

MAJOR SYSTEM

5

1   2   3   4

LEVEL II

SYSTEM

a   b   c   d   e

LEVEL III

SUBSYSTEM

i   ii

iii   iv

v

vi

vi

vi

LEVEL IV

UNIT

X   L   C   R

C
C

X
X

D
D

D
D

LEVEL V

PART STRESS ANALYSIS AND
FAILURE MODE DIAGRAM

λ_o λ_f λ_s

STRESS
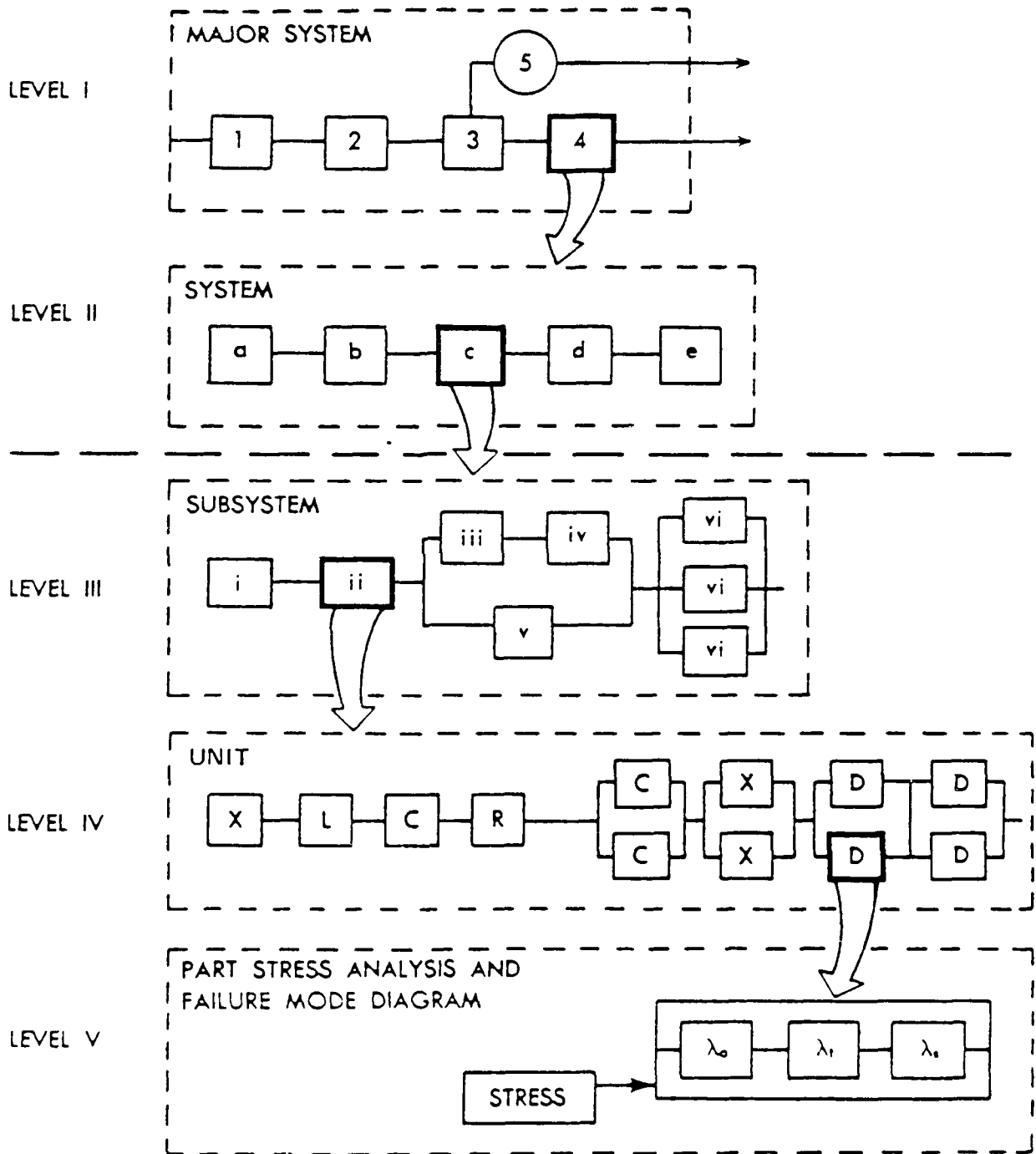
FIGURE 6.4.2-1:   PROGRESSIVE EXPANSION OF RELIABILITY BLOCK DIAGRAM
AS DESIGN DETAIL BECOMES KNOWN

where

$Q \qquad = 1-R, \text{ e.g., } Q_D = 1-R_D$

$R_D \qquad = e^{-\lambda_D t} \text{ for a particular part}$

$\lambda_D \qquad = \lambda_o + \lambda_t + \lambda_s$

Subscripts o, t, and s denote open, tolerance, and short modes of failure, respectively.

Looking at the Level III diagram of Figure 6.4.2-1 and using the decomposition method discussed in the previous section, the following notations are appropriate:

Let $\quad R_i = a; R_{ii} = b; R_{iii} = c; R_{iv} = d; R_v = e; R_{vi} = f;$
and $\quad (1-R_i) = \bar{a}; (1-R_{ii}) = \bar{b}; (1-R_{iii}) = \bar{c}; (1-R_{iv}) = \bar{d};$
$\qquad (1-R_v) = \bar{e}; (1-R_{vi}) = \bar{f}$

Then, dividing the Level III diagram into three groups, there is the following tabulation for all possible combinations of successful performance.

Group 1: $\quad R_1 = ab$ (a and b required)

Group 2: $\quad R_2 = cde + cd\bar{e} + c\bar{d}e + \bar{c}de + \bar{c}\bar{d}e$ (either c and d, or e, required)

Group 3: $\quad R_3 = 1 - \bar{f}^3$ (at least 1 out of 3 required)

Combining: $R_{III} = R_1 \times R_2 \times R_3$

Example

Reliability estimates have been derived for all units of subsystem c, the guidance and control package, of a new air-to-air missile to be developed for an aircraft weapon system. For a flight time of 80 seconds, the following component reliabilities and corresponding UNreliabilities have been estimated.

Group 1. $\quad a = R_i \quad = .99 \quad \bar{a} = (1-R_i) \quad = .01$
$\qquad\qquad b = R_{ii} \quad = .98 \quad \bar{b} = (1-R_{ii}) \quad = .02$

Group 2: $\quad c = R_{iii} \quad = .95 \quad \bar{c} = (1-R_{iii}) \quad = .05$
$\qquad\qquad d = R_{iv} \quad = .95 \quad \bar{d} = (1-R_{iv}) \quad = .05$
$\qquad\qquad e = R_v \quad = .90 \quad \bar{e} = (1-R_v) \quad = .10$

Group 3: $\quad f = R_{vi} \quad = .90 \quad \bar{f} = (1-R_{vi}) \quad = .10$

$R_1 \quad = \quad ab = (.99)(.98) = .97$

$R_2 \quad = \quad cde + cd\bar{e} + c\bar{d}e + \bar{c}de + \bar{c}\bar{d}e$
$\qquad = \quad (.95)(.95)(.90) + (.95)(.95)(.10)$
$\qquad\qquad + (.95)(.05)(.90) + (.05)(.95)(.90)$
$\qquad\qquad + (.05)(.05)(.90)$
$\qquad = \quad .99$

$R_3 \quad = \quad 1 - f^3 = 1 - 0.001 = .999$

Estimated reliability feasibility for a guidance subsystem of this particular design configuration is then:

$$R_{III} = R_1 \times R_2 \times R_3 = (.97)(.99)(.999) = .96$$

Having described the mathematical model used for prediction, let us now return to a description of each of the types of prediction techniques used.

6.4.3 SIMILAR EQUIPMENT TECHNIQUES

Several techniques have been developed and used in performing very early predictions of equipment reliability before any characteristics of the system design have been established. The most basic of these techniques involves a simple estimate of equipment reliability in terms of MTBF, failure rate, or similar parameters, based on experience gained from operational equipments of similar function.

In general, these similar equipment prediction techniques involve the following steps:

(1) Defining the new equipment in terms such as general equipment type (e.g., radar), operational use (e.g., ground based) and other known characteristics

(2) Identifying an existing equipment or class of equipments that most nearly compares with the new equipment

(3) Obtaining and analyzing historical data generated during operation of the existing equipment to determine as nearly as possible the reliability of the equipment under the stated operating environment

(4) Drawing conclusions concerning the level of reliability that will be demonstrated by the new equipment. Such conclusions assume that similar equipment will exhibit similar reliability and that reliability achievement evolves in an orderly manner from one generation of equipments to the next. These reliability prediction techniques permit very early estimation of the failure rate of a new equipment based on experience gained from operational equipments of similar function. The accuracy of the estimates, however, depends on the quality of historical data and the similarity between the existing and new equipments.

Obviously, more meaningful and accurate results are achieved if a technique based on field results of similar products is used. Also, other factors such as design practices and production techniques are more likely to be similar to those on past equipments designed and built by the same manufacturer than those of another manufacturer.

In most cases, prediction techniques such as this are used in estimating the feasibility of meeting some minimum reliability objective within the constraints of the current state-of-the-art.

6.4.4 SIMILAR COMPLEXITY TECHNIQUES

Several techniques have been developed in the past for performing reliability predictions based on the complexity of the equipment of interest. These techniques have been developed as a result of analyses that indicate a direct and predictable correlation between equipment complexity and reliability. However, such predictions are complicated somewhat by the influence of the equipment type or different environments in which the equipment will be operated. Therefore, methods for predicting reliability as a function of equipment complexity include provisions for compensating for use environment factors.

The most commonly used similar complexity technique involves the use of graphical procedures relating failure rate to active element group count and use environment. This technique can be used to obtain a quick estimate of equipment reliability from a knowledge of the number of nonredundant active elements. Active elements are defined as vacuum tubes, transistors, relays, and rectifier diodes. The expected mean time between failures is plotted in Figure 6.4.4-1 as a function of the number of active elements. In Table 6.4.4-1. the various classes of equipment are subdivided into low, average, and high quality. The reliability function can be obtained from the mean time between failures by use of the formula

$$R(t) = e^{-t/m} \qquad\qquad (6.27)$$

where t is the time period of interest and m is the mean time between failures.

TABLE 6.4.4-1: ELECTRONIC EQUIPMENT RELIABILITY CLASSIFICATIONS

Type of Equipment	Reliability Class		
	Low Quality	Average Quality	High Quality
Airborne, vacuum tube	A_1	A_2	A_3
Airborne, transistorized	B_1	B_2	B_3
Ground-based, vacuum tube	B_1	B_2	B_2
Ground-based, transistorized	C_2	C_3	D_1
Mobile, vacuum tube	A_2	A_3	B_1
Mobile, transistorized	B_2	B_3	C_1
Missile, vacuum tube	A_1	A_2	A_3
Missile, transistorized	B_1	B_2	B_3
Ship-borne, vacuum tube	B_1	B_2	B_3
Ship-borne, transistorized	C_1	C_2	C_3
Space-borne, vacuum tube	B_1	B_2	B_3
Space-borne, transistorized	C_1	C_2	C_3
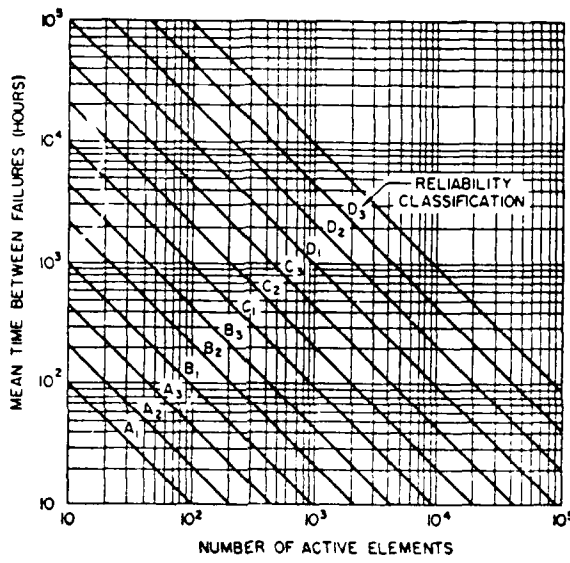
FIGURE 6.4.4-1: <u>MEAN TIME BETWEEN FAILURES VERSUS NUMBERS OF ACTIVE ELEMENTS FOR VARIOUS</u>
<u>RELIABILITY CLASSES.</u>

Let us assume that one would like to estimate the reliability of an airborne transistorized equipment of high quality, containing 500 active elements. Table 6.4.4-1 gives the classification B_3 for this case. Entering Figure 6.4.4-1 and finding the intersection of the diagonal B_3 line with the vertical line for 500 active elements, we read the estimated MTBF as 90 hours.

Unfortunately, this technique has not been updated recently to incorporate the widespread application of microcircuits. However, it may still be somewhat useful for relative comparisons of complex designs.

6.4.5 PREDICTION BY FUNCTION TECHNIQUE

This refers to a prediction technique which relates expected reliability with the functional characteristics of the equipment or subsystem. The technique is based upon a statistical correlation between significant functional characteristics and the observed operational reliability of an equipment. The result is a series of regression equations which relate the more significant (from a reliability viewpoint) equipment functions to the expected equipment reliability.

The original series of equations were developed during the 1960s (Ref. 9) and are probably no longer valid. The most recent work was done in 1974 (Ref. 10) and may still be considered somewhat valid. During this study, regression equations were developed for:

(1) radars
(2) computers
(3) displays
(4) communications equipment

For example, the radar regression equation is given by:

$$\ln P = -0.8277 + 0.397 \times 10^{-2} \, (DY) + 3.586 \times 10^{-1} \, (MTR)$$
$$+ \; 3.87 \times 10^{-2} \, (DR) + 6.959 \times 10^{-2} \, (PW) + 7.603 \times 10^{-1} \, (HP)$$
$$- \; 4.71 \times 10^{-3} \, (MTR)(DR) - 2.2 \times 10^{-4} \, (DR)(RDR) \qquad (6.28)$$

where

ln	= natural logarithm
P	= average number of component parts
DY	= design year, e.g., 1970
MTR	= multiple target resolution (kilofeet)
DR	= detection range (nautical miles)
PW	= pulse width (microseconds)
HP	= half power beam width (degrees)
RDR	= receiver dynamic range (dB)

Having calculated P, one can then find the expected MTBF from

$$MTB \cdot = \frac{1}{(FR)(P)} \qquad (6.29)$$

where

P = average number of component parts
FR = average failure rate per part

Let us run through a typical calculation for an airbo⟨ e radar having the design characteristics shown in Table 6.4.5-1. Plugging the design values into Eq. (6.28) we get:

$$\ln P = -0.8277 + (0.00307)(1970) + (0.3586)(0.1) + (0.0387)(150)$$
$$+ (0.06959)(4) + (0.7603)(1) - (0.00471)(0.1)(150)$$
$$- (0.00022)(150)(60)$$
$$= 10.0491$$

$$P = e^{10.0491} = 23,134 \text{ parts}$$

TABLE 6.4.5-1: RADAR SYSTEM DESIGN CHARACTERISTICS

Design Parameter	Units	Value
Design Year (DY)	--	1970
Detection Range (DR)	NMI	150.0
Receiver Dynamic Range (RDR)	dB	60.0
Multiple Target Resolution (MTR)	K ft.	0.1
Pulse Width (PW)	usec	4.0
Half Power, Azimuth Beam (HP)	deg.	1.0

In order to calculate the equipment failure rate we need information on the distribution of parts per equipment, the generic failure rate per part, and the environmental K factor for an airborne environment. These are given in Tables 6.4.5-2 and 6.4.5-3.

TABLE 6.4.5-2: PARTS DISTRIBUTION

Part Type	Radar	Computer	Display	Comm.
CAP	0.1855	0.1508	0.1399	0.3912
RES	0.3130	0.2709	0.2272	0.3416
DIODE	0.2169	0.1372	0.2553	0.0682
XSTR	0.1127	0.0532	0.1420	0.0717
IC	0.1158	0.3610	0.1706	0.0130
IND	0.0393	0.0132	0.0527	0.1076
TUBE	0.0079	0	0.0122	0
HYBRID	0.0089	0.0137	0.0001	0.0067

TABLE 6.4.5-3: MIL-HDBK-217 PART RELIABILITY DATA

Part Type	Failure Rate $(\times 10^6)$	ENVIRONMENTAL K-FACTOR		
		Airborne K_A	Ground K_G	Shipboard K_S
CAP	0.0496	8.646	1.0766	5.907
RES	5.810	3.111	0.21446	0.101
DIODE	1.000	4.322	0.874	1.29
XSTR	1.190	8.004	1.5008	0.363
IC	6.000	7.000	1.000	3.000
IND	0.34	1.000	1.000	1.000
TUBE	1.313	6.002	1.000	1.000
HYBRID	12.000	7.000	1.000	3.000

Thus,

$$\lambda_e = P[(0.1855)(0.0496)(8.646) + (0.313)(5.81)(3.111) +$$

$$(0.2169)(1.0)(4.322) \ldots + (0.0089)(12)(7)]$$

$$= P(13.4341 \text{ failures}/10^6 \text{ hrs.})$$

Substituting the previously derived value for P (23,134) we get:

$$\lambda_e = (23,134)(13.3828 \text{ failure}/10^6 \text{ hrs})$$

$$= 310798 \text{ failures}/10^6 \text{ hrs}$$

$$MTBF = \frac{1}{\lambda_e} = 3.2 \text{ hours}$$

The regression equation for computers is given by:

$$\ln \overline{\lambda} = 371.4264 - 1.8263 \times 10^{-1} (DY) - 7.981 \times 10^{-1} (AST)$$
$$+ 1.1 \times 10^{-3} (PD) - 1.564 \times 10^{-2} (INST)$$
$$+ 5.99 \times 10^{-3} (AST) INST) - 4.3 \times 10^{-4} (MS)(PD) \qquad (6.30)$$

where

$$\overline{\lambda} = \text{equipment failure rate}$$
DY = design year
AST = add/subtract time (microseconds)
PD = power dissipation (watts)
INST = number of instructions
MS = memory speed (microseconds)

and

$$MTBF = \frac{1}{\overline{\lambda}} \qquad (6.31)$$

Thus, one could perform a similar calculation for a computer example as was previously done for the airborne radar example, using Eqs. (6.30) and (6.31).

As was stated previously, Reference 10 contains the details on this technique and its application to other types of equipment. Admittedly, Tables 6.4.5-2 and 6.4.5-3 probably require updating to reflect the latest state of the art, however, the technique is still useful in the conceptual phase of development when one usually has little knowledge of the numbers and types of component parts that will be used in the equipment design. It is particularly useful in comparing alternate designs during proposed evaluation, as well as determining the realism of a proposed design.

6.4.6 PART COUNT TECHNIQUE

This technique is used when one has a "feel" for the number of component parts (actual or estimated) by class or type that will be used in an equipment/system but does not have enough data as to the stresses to which each part will be subjected in the final design. It involves counting the number of parts of each class or type, multiplying this number by the generic failure rate for each part class or type, and summing these products to obtain the failure rate for the equipment. The procedure distinguishes a part class as being all parts of a given function (e.g., resistors, capacitors, transformers). Part types are used to further define parts within a class (e.g., fixed composition resistors, fixed wire wound resistors).

The information needed to apply the method is (1) generic part types (including complexity for microelectronics) and quantities, (2) part quality levels, and (3) equipment environment. The general expression for equipment failure rate with this method is:

$$\lambda_{EQUIP} = \sum_{i=1}^{i=n} N_i \, (\lambda_G \pi_Q)_i \qquad\qquad (6.32)$$

for a given equipment environment where:

λ_{EQUIP} = total equipment failure rate (failures/10^6 hr.)

λ_G = generic failure rate for the ith generic part (failures/10^6 hr.)

π_Q = quality factor for the ith generic part

N_i = quantity of ith generic part

n = **number of different generic part categories**

Eq. (6.32) applies if the entire equipment is being used in one environment. If the equipment comprises several units operating in different environments (such as avionics with units in airborne inhabited (A_I) and uninhabited (A_U) environments), then Eq. (6.32) should be applied to the portions of the equipment in each environment. These "environment-equipment" failure rates should be added to determine total equipment failure rate.

The generic (average) failure rate (λ_G) and the quality factor (π_Q) are obtained from the latest version of MIL-HDBK-217 which is the basic document used for reliability prediction of military electronic equipment. MIL-HDBK-217 contains a number of tables of generic failure rates for various classes and types of parts, as well as the associated quality factors. Tables 6.4.6 1 and 6.4.6-2 (from MIL-HDBK-217D) are specific examples of generic failure rates and quality factors for resistors.

TABLE 6.4.6-1: GENERIC FAILURE RATE λ_G, (f./10^6 hr.) FOR RESISTORS

(See Table 6.4.6-2 for π_Q Values)

CONSTRUCTION	STYLE	MIL-R-	USE ENVIRONMENT									
			M_{FA}	M_{FF}	M_P	N_H	N_S	N_{SB}	N_U	N_{UU}	S_F	U_{SL}
RESISTORS, FIXED												
Composition	RCR	39008	.012	.0077	.0051	.0096	.0038	.0029	.030	.0048	.00051	.015
"	RC	11	.06	.039	.026	.048	.019	.015	.15	.024	.0025	.075
Film	RLR	39017	.017	.013	.012	.018	.062	.0055	.026	.17	.00048	.034
"	RL	22684	.086	.064	.058	.092	.031	.028	.13	.083	.0024	.17
"	RNR	55182	.02	.015	.013	.022	.0072	.0065	.031	.018	.00057	.037
"	RN	10509	.1	.073	.063	.11	.036	.032	.15	.091	.0029	.19
", Power	RD	11804	.2	.15	.13	.22	.061	.061	.21	.23	.012	.41
", Network	RZ	83401	.51	.38	.27	.53	.18	.16	1.5	.26	.025	.79
Wirewound, Accurate	RBR	39005	.16	.11	.1	.16	.046	.046	.18	.16	.013	.31
	RB	93	.78	.55	.52	.8	.23	.23	.91	.82	.064	1.6
Wirewound, Power	RWR	39007	.28	.2	.18	.28	.08	.08	.37	.24	.021	.53
	RW	26	1.4	1.0	.89	1.4	.4	.4	1.8	1.2	.11	2.6
Wirewound, Ch. Mount	RER	39009	.14	.11	.093	.14	.044	.044	.2	.12	.0079	.26
	RE	18546	.72	.53	.47	.72	.22	.22	1.0	.6	.04	1.3
RESISTORS, VARIABLE												
Wirewound, Trimmer	RTR	39015	.34	.24	.21	.35	.086	.086	.31	.32	.014	.64
	RT	27208	1.7	1.2	1.1	1.7	.43	.43	1.5	1.6	.071	3.2
W. W., Prec.	RR	12934	32.	23.	20.	33.	7.5	7.5	21.	29.	.84	60.
W. W., Semi-Prec.	RA	19	*	*	5.7	13.	3.3	3.3	*	7.5	.31	*
M. W. Prec.	RK	39002	*	*	*	*	*	*	*	*	*	*
M. W., Power	RP	22	*	*	5.2	9.1	2.4	2.4	*	8.9	*	*
Non-W.W., Trimmer	RJR	39035	.54	.39	.36	.56	.12	.12	.41	.54	.020	1.1
	RJ	22097	2.7	1.9	1.8	2.8	.60	.60	2.1	2.7	.10	5.3
Composition	RV	94	4.4	3.2	2.8	4.5	1.1	1.1	5.7	3.8	.12	8.2
Non-N.W. Prec.	RQ	39023	2.7	1.9	1.6	2.7	.71	.71	3.2	2.2	.086	4.8
Film	RVC	23285	2.7	1.9	1.8	2.8	.74	.74	2.3	2.6	.096	5.2

* - not normally used in these environments.

TABLE 6.4.6-2 π_Q FACTOR FOR RESISTORS AND CAPACITORS

FAILURE RATE LEVEL	$*\pi_Q$
L	1.5
M	1.0
P	.3
R	.1
S	.03

*For Non-ER parts (Style with only 2 letters in Table 6.4.6-2), π_Q = 1 providing parts are procured in accordance with the part specification; if procured as commercial (NON-MIL) quality, use π_Q = 3. For ER parts (Styles with 3 letters), use the π_Q value for the "letter" failure rate level procured.

This technique is usually more accurate than the prediction by function technique since more "fine grained" data, e.g., actual or estimated number of component parts, is available. It is most useful in the early design stage of an equipment/system before the actual stresses on each component are known.

An example of how this technique might be applied to predict the MTBF and reliability of a ground search radar is shown in Figure 6.4.6-1. Admittedly, the example might be considered technologically obsolete; however, the basic methodology is still the same.

6.4.7 STRESS ANALYSIS TECHNIQUE

The previous method described was based upon average failure rates for each component part type. It is a well known fact that part failure rates vary significantly with applied stresses, sometimes by several orders of magnitude. For example, a 110 volt light bulb does not operate very long when subjected to 220 volts. It is this interaction between strength of the component and the stress level at which the component operates which determines the failure rate of a component in a given situation. Thus, at different stress levels component parts assume different failure rates. This is the rationale for the stress analysis prediction technique. The technique is based upon a knowledge of the stress to which the part will be subjected, e.g., temperature, humidity, vibration, etc., and the effect of those stresses on the part's failure rate. Application of this technique is the same as was shown for the parts count technique except that each individual component's failure rate is modified to reflect the anticipated or actual stress environment to which it will be subjected. Thus, it can be seen that the technique is more laborious and time consuming, although it does provide the most accurate results. It requires the use of MIL-HDBK-217, which contains the necessary charts and tables to estimate the failure rate for each component part under the anticipated stresses.

The procedure for extracting failure rate data from MIL-HDBK-217 differs according to part class and type. In general, however, the following steps are required:

(1) A base failure rate is determined for each part. This value is established from the appropriate chart in MIL-HDBK-217 and is a function of part type, environmental temperature, and the relative level of the more significant operational stresses.

(2) The values of one or more multiplicative or additive factors are determined from tables or charts in MIL-HDBK-217. These factors define the relationship between the base failure rate and the predicted failure rate for the specific application of interest.

(3) The part failure rate is calculated using the established base failure rate and the modifying factors.

SAMPLE RELIABILITY CALCULATION

Part Type	Quantity used	Failure rate per 10 hours	Total failures per 10 hours
Tubes, electron, receiving	96	6	576.00
Tubes, electron, transmitting (power tetrode)	12	40	480.00
Tubes, electron, magnetrons	1	200	200.00
Tubes, electron, CRT's	1	15	15.00
Crystals, diode	7	2.98	20.86
Capacitors, fixed ceramic, high K	59	0.18	10.62
Capacitors, fixed tantalum foil	2	0.45	0.90
Capacitors, fixed, mica molded	89	0.018	1.60
Capacitors, fixed, paper	108	0.01	1.08
Resistor, fixed, carbon composition	467	0.0207	9.67
Resistor, fixed, power film	2	1.6	3.20
Resistors, fixed, wire-wound	22	0.39	8.58
Resistors, variable, composition	38	7.0	266.00
Resistors, variable, wire-wound	12	3.5	42.00
Connectors, coaxial	17	13.31	226.47
Inductors	42	0.938	39.40
Meters, electrical	1	1.36	1.36
Motors, blower	3	630	1,890.00
Motors, synchro	13	0.8	10.40
Relays, crystal can	4	21.28	85.12
Relays, contactor	14	1.01	14.14
Switches, toggle	24	0.57	13.66
Switches, rotary	5	1.75	8.75
Transformers, power and filter	31	0.0625	1.94
Summation			3,926.57

$$\text{MTBF (m)} = \frac{10^6}{3,926.57} = 255 \text{ hr}$$

Probability of successful operation for 100 hours without failure:

$$R(100) = e^{-100/255} = e^{-0.392} = 0.676 = 67.6\%$$

FIGURE 6.4.6-1   SAMPLE RELIABILITY CALCULATION

The following relatively simple example indicates the methodology used.

Example

Given: Silicon diode, JANTX grade, in fixed ground service at 0.6 rated maximum current and 40 percent rated voltage in power rectifier operation at 60°C case temperature, T_C. Device rated at 5 amps, T_S = 100°C case temperature and T_{MAX} = 150°C and has a metallurgically bonded contact.

The formula for determining the failure rate is:

$$\lambda_p = \lambda_b \left(\pi_E \times \pi_Q \times \pi_R \times \pi_A \times \pi_{S2} \times \pi_C \right) \text{ failures}/10^6 \text{ hrs}$$

where

λ_b = base failure rate
π_E = multiplier due to environment
π_Q = multiplier due to quality level
π_R = multiplier due to current rating
π_A = multiplier due to application
π_{S2} = multiplier due to voltage stress
π_C = multiplier due to construction factor

The first step is to find the stress ratio factor (S) which is equal to the maximum rated current times the convection factor (CF). In other words,

$$S = 0.6 \text{ (CF)}$$

where, for devices with $T_S > 25^\circ$C and $T_{MAX} < 175^\circ$C,

$$CF = \frac{T_{max} - T_S}{150} = \frac{150 - 100}{150} = 0.33$$

$$S = (0.6)(0.333) \quad 0.2$$

The next step is to solve for T where

$$T = T_C + (175 - T_{MAX})$$
$$= 60 + (175 - 150) = 85$$

Given T and S, one follows the following steps indicated to arrive at the final value for the failure rate for this particular device under the stated conditions:

Step (1) From Figure 6.4.6-2 (Table 5.1.3.4-7) for T = 85°C and S = 0.2, λ_b = 0.00076 failures/10^6 hours

Step (2) From Figure 6.4.6-2 (Table 5.1.3.4-1) fixed ground, π_E = 3.9

Step (3) From Figure 6.4.6-2 (Table 5.1.3.4-2) JANTX grade, π_Q = 0.3

TABLE 5.1.3.4-7
MIL-S-19500 DIODES, GROUP IV, SILICON
BASE FAILURE RATE, λ_b, IN FAILURES PER 10^6 HOURS

T (°C)	.1	.2	.3	.4	.5	.6	.7	.8	.9	1.0
0	.00010	.00014	.00020	.00027	.00037	.00049	.00065	.00085	.0011	.0016
10	.00012	.00018	.00025	.00033	.00045	.00059	.00076	.0010	.0014	.0022
20	.00016	.00023	.00031	.00041	.00053	.00070	.00092	.0013	.0019	.0031
25	.00018	.00025	.00033	.00045	.00059	.00076	.0010	.0014	.0022	.0039
30	.00020	.00027	.00037	.00049	.00065	.00085	.0017	.0016	.0025	
40	.00025	.00033	.00045	.00059	.00076	.0010	.0014	.0022	.0039	
50	.00031	.00041	.00053	.00070	.00092	.0013	.0019	.0031		
55	.00033	.00045	.00059	.00076	.0010	.0014	.0022	.0039		
60	.00037	.00049	.00065	.00085	.0011	.0016	.0025			
65	.00041	.00053	.00070	.00092	.0013	.0019	.0031			
70	.00045	.00059	.00076	.0010	.0014	.0022	.0039			
75	.00049	.00065	.00085	.0011	.0016	.0025				
80	.00053	.00070	.00092	.0013	.0019	.0031				
85	.00059	.00076	.0010	.0014	.0022	.0039				
90	.00065	.00085	.0011	.0016	.0025					
95	.00070	.00092	.0013	.0019	.0031					

TABLE 5.1.3.4-1
Group IV Diodes
Environmental Mode Factors

Environment	π_E
G_B	1
S_F	1
G_F	3.9
N_{SB}	4.8
N_S	4.8
A_{IT}	12
M_P	12
M_{FF}	12
M_{FA}	17
G_M	18
N_H	19
N_{UU}	20
A_{UT}	20
N_U	21
A_{IF}	25
A_{RW}	27
U_{SL}	36
A_{UF}	40
M_L	41
C_L	690

TABLE 5.1.3.4-2
π_Q, QUALITY FACTOR

Quality Level	π_Q
JANTXV	0.15
JANTX	0.3
JAN	1.5
Lower*	7.5
Plastic**	15.0

*Hermetic packaged devices.
**Devices sealed or encapsulated with organic material.

TABLE 5.1.3.4-3
π_R FOR GROUP IV DIODES

Current Rating (amps.)	π_R
≤ 1	1
> 1 to 3	1.5
> 3 to 10	2.0
>10 to 20	4.0
>20 to 50	10.0

FIGURE 6.4.6-2: MIL-HDBK-217D (Typical Tables)

TABLE 5.1.3.4-4
π_A FOR GROUP IV DIODES

Application	π_A
Analog Circuits($\leq$500 ma.)	1.0
Switching (< 500 ma.)	0.6
Power Rectifier ($\geq$500 ma.)	1.5
Power Rect. (H.V. Stacks) V max > 600	2.5/junction

TABLE 5.1.3.4-5
π_{S2} FOR GROUP IV DIODES

Voltage Stress, $S_2 = \dfrac{\text{Applied } V_R}{\text{Rated } V_R} \times 100$
V_R = diode reverse voltage.

S_2 (Percent)	π_{S2}
0 to 60	0.70
70	0.75
80	0.80
90	0.90
100	1.0

TABLE 5.1.3.4-6
π_C, CONSTRUCTION FACTOR

Contact Construction	π_C
Metallurgically Bonded	1
Non-metallurgically Bonded (Spring loaded contacts)	2

FIGURE 6.4.6-2: MIL-HDBK-217D (Typical Tables) (CONT'D)

Step (4)   From Figure 6.4.6-2 (Table 5.1.3.4-3) 5 amps, $\pi_R = 2.0$

Step (5)   From Figure 6.4.6-2 (Table 5.1.3.4-4) power rectifier, $\pi_A = 1.5$

Step (6)   From Figure 6.4.6-2 (Table 5.1.3.4-5) at 40 percent of rated voltage, $\pi_{S2} = .70$

Step (7)   From Figure 6.4.6-2 (Table 5.1.3.4-6) for metallurgically bonded contacts, $\pi_C = 1.0$

Step (8)   Perform the calculation:

$$\lambda_p = \lambda_b \left(\pi_E \times \pi_Q \times \pi_R \times \pi_A \times \pi_{S2} \times \pi_C \right)$$

$$\lambda_p = 0.00076 \left(3.9 \times 0.3 \times 2.0 \times 1.5 \times 0.7 \times 1.0 \right)$$

$$\lambda_p = 0.0019 \text{ failures}/10^6 \text{ hours}$$

After one has calculated the failure rate for each component, the equipment failure rate is given by:

$$\lambda_{EQUIP} = \sum_{i=1}^{n} \lambda_i \qquad (6.33)$$

and the MTBF is

$$MTBF = \frac{1}{\lambda_{EQUIP}} \qquad (6.34)$$

Stress analysis failure rate predictions such as this permit extremely detailed analyses of equipment or system reliability. However, since details of the system design are required in determining stress ratios, temperature and other application and environmental data, these techniques are only applicable during the late stages of design. Because of the high level of complexity of modern systems, the application of the procedure is time consuming.

However, there are computerized MIL-HDBK-217 models such as ORACLE (Ref. 11) which will perform this detailed analysis for DoD organizations and contractors, given the part types and the anticipated stresses.

6.4.8   MODIFICATION FOR NONEXPONENTIAL FAILURE DENSITIES (GENERAL CASE)

Although the exponential technique indicated in the previous sections can be used in most application with little error, it must be modified (1) if the system contains parts for which the density function of failure times cannot be approximated by an exponential over the time period of interest; or (2) if the parts which are the dominant factor in overall system unreliability do not follow an exponential density function of times to failure. Mechanical parts such as gears, motors, and bearings usually fall in this category.

In these cases, one cannot add the failure rates of all parts because there are some parts whose failure rates vary significantly with time. The method used is to consider separately within each block diagram the portion of the block containing parts with constant failure rates, and the portion containing parts with varying failure rates. If the former portion contains x parts, then the reliability of this portion is

$$R_1(t) = \exp\left[-\left(\sum_{i=1}^{x} \lambda_i\right) t\right] \qquad (6.35)$$

The reliability of the second portion at time t is formed by using the appropriate failure density function for each part whose parameters have been determined through field experience or testing. If this portion contains B parts, then

$$R_2(t) = \prod_{i=1}^{B} R_i(t) \qquad (6.36)$$

where

$$R_i(t) = \exp -\int_0^t h_i(T) \, dT \qquad (6.37)$$

and h(t) is the time varying hazard rate of each of the B parts.

The reliability for the block diagram, under the assumption of independence between the two portions, is

$$R(t) = R_1(t)R_2(t) \qquad (6.38)$$

By solving for various levels of t, the block and system reliability function can be plotted. Often the shape of the curve will be very similar to that for an exponential, and the system mean life can be estimated graphically by finding the time interval over which the reliability is equal to 0.37. Remember for the exponential distribution the mean life is 0.37.

For example, consider the failure rates of two elements X and Y that make up a system. Let X have a constant failure rate λ of $1,000 \times 10^{-6}$ failures per hour, and Y a hazard rate h(t) that varies with time and is given by $(500 \times 10^{-6} + 0.01t)$. Thus,

$$R_Y(t) = \exp\left[-\int_0^t (500 \times 10^{-6} + 0.01r) \, dr\right]$$

The reliability of a system composed of these two independent elements would be obtained through

$$R(t) = R_X(t)R_Y(t)$$

$$= [\exp(-10^3 \times 10^{-6})t] \left\{ \exp \left[- \int_0^t (500 \times 10^{-6} + 0.01r)\, dr \right] \right\}$$

$$= \exp \left[- \left(1,500 \times 10^{-6}t + \frac{0.01t^2}{2} \right) \right]$$

Evaluation of the above equation for several discrete points in time permits construction of the reliability function.

For those systems which have a reliability curve appreciably different from the exponential, the mean life is equal to:

$$\theta_S = \int_0^\infty R(t)\, dt \qquad (6.39)$$

Reliability prediction methods for those cases in which the equipment/system contains parts which are predominantly mechanical or electromechanical and for which the exponential approximation is not valid are given in References 12, 13 and 14. The prediction methods described are applicable to these components which exhibit Normal, Weibull, Lognormal, or Extreme Value distributions of failure times.

For those nonelectronic devices where the exponential approximation of failure times is valid, Reference 15 contains a listing of failure rates for various types of nonelectronic devices. It can be used to supplement the MIL-HDBK-217 failure rate data, which is restricted to electrical and electronic parts.

6.4.9 MODIFICATION TO INCLUDE NONOPERATING FAILURE RATES

The component failure rates in MIL-HDBK-217 and in the Nonelectronic Parts Data Book (Ref. 15) are based upon operating time. There are equipment/systems in which nonoperating time represents a significant portion of the useful life, e.g., missiles, fuzes, projectiles. For these equipment/systems the failure rate should be modified to include nonoperating, or dormant, failure rates. The simplest modification includes a nonoperating or dormant failure rate correction so that the model becomes

$$\lambda_T = \lambda_{op} d + (1 - d) \lambda_{nop} \qquad (6.40)$$

where

λ_T = total failure rate

λ_{op} = operating failure rate

λ_{nop} = nonoperating failure rate

d = ratio of operating to nonoperating time

As was mentioned, this modification is particularly important for those systems which spend a significant portion of their useful lives in a nonoperating or dormant state, e.g., missiles.   For example, Ref. 16 formulates the following general reliability prediction equation for a missile:

$$R_{LC}(t) = R_{NO}\,(t_{NO}) \cdot R_0\,(t_0) \cdot R_L(t_L) \cdot R_F(t_F)$$
$$= e^{-\lambda_{NO}t_{NO}} \cdot e^{-\lambda_0 t_0} \cdot e^{-\lambda_L t_L} \cdot e^{-\lambda_F t_F}$$

$$(6.41)$$

where

$R_{LC}(t)$ is the missile's life cycle reliability

λ_{NO} is the unit's failure rate during transportation and handling, storage and dormant time (nonoperating time)

t_{NO} is the sum of all nonoperating and dormant time

λ_0 is the unit's failure rate during checkout, test or system exercise during which components have electrical power applied (operating)

t_0 is the sum of all operating time excluding launch and flight

λ_L is the unit's failure rate during powered launch and flight (*Propulsion System Active*)

t_L is the powered launch and flight time

λ_F is the unit's failure rate during unpowered flight

t_F is the unpowered flight time

t is the sum of t_{NO}, t_0, t_L and t_F

Reference 16 also contains a methodology for performing a "parts count" reliability prediction of a missile system reliability as well as tables of λ_{NO}, λ_0, λ_L, λ_F for various classes of missile components.   Reference 17 contains nonoperating failure rates for electrical and electronic devices.   Reference 18 contains nonoperating failure rates for avionics equipment used in USAF aircraft.

Finally, the U.S. Army Command, Redstone Arsenal, AL 35809, maintains a Storage Reliability Data Bank.   This data bank consists of a computerized data base with generic part storage reliability data and a storage reliability report library containing available research and test reports of nonoperating reliability research efforts.

6.4.10 <u>COMPUTERIZED RELIABILITY PREDICTION METHODS</u>

Reliability predictions for complex systems frequently require a large amount of tedious computation. A number of computer programs have been developed for performing reliability predictions. A detailed listing of programs is presented in Table 6.4.10-1. Some of them may be proprietary or have restrictions on their dissemination. A check should be made at one's computer installation to determine which programs are available and which can be obtained before performing any laborious manual calculations.

The programs listed in Table 6.4.10-1 are those which are solely devoted to performing reliability predictions and analyses. Computer programs for performing system availability analysis and life cycle cost analysis (using R&M parameters) are listed in Section 10 of this handbook.

In addition to the computer programs listed in Table 6.4.10-1, the following paragraphs provide brief descriptions of some computer programs not listed in Table 6.4.10-1:

6.4.10.1 <u>RADC ORACLE (OPTIMIZED RELIABILITY AND COMPONENT LIFE ESTIMATES)</u>

RADC ORACLE is a software package (computer program) for performing reliability predictions, developed to mechanize the implementation of MIL-HDBK-217 (Reliability Prediction of Electronic Equipment). It is interactive in nature and structured such that a reliability engineer can, with a few days' training, be able to productively exercise it.

The program provides queries to the user, guiding him in program execution and in the development of proper data inputs. Insofar as the last is concerned the program directly queries the user for appropriate data parameters (such as part numbers, part type, stress, temperature, etc.), checks the inputs for completeness, and automatically formats and records the results in the appropriate data file.

Through the input of an electronic parts list, the computer program generates many needed reliability design parameters for electronic systems. The program determines the MIL-HDBK-217 parameters and selects the proper prediction algorithm needed to calculate the part failure rate. The output lists each part and its corresponding failure rate, the sum of the failure rates for all of the parts corresponding to a system or a subsystem, the Mean Time Between Failures (MTBF) for the system or subsystem. ORACLE can also perform tradeoff analyses through the modification of the parts application conditions such as the operating temperature, the screening level, and the operating environment.

ORACLE is available only to DOD agencies, and can be provided, upon request, to DoD contractors.

    Contact: RADC/RBET
                Griffiss AFB, NY 13441-5700

TABLE 6.4.10.1: SUMMARY OF PROGRAMS IN THE RELIABILITY AREA

Program Description	Organizations (Originator or User/Sponsor)	References
Computerized Reliability Assessment Method	ARINC/NASA	19
PESCRIPT (Not a specific program but a reliability-oriented progamming language for prediction)	Computer Concepts, Inc.	20
Automated Reliability Tradeoff Program for balancing cost vs. predicted reliability	Collins Radio	21
Reliability Prediction of majority voter logic by Monte Carlo methods	IBM	22
Reliability Prediction of systems by combining failure rates	Radiation Inc.	23
Reliability Prediction of systems by combining failure rates	Lockheed-Georgia	24
Reliability Prediction of systems by programmed prediction equation	Marine Engineering Lab.	25
Reliability Prediction and crew safety analysis for complex aerospace systems from input logic models	Grumman/NASA	26
Reliability Prediction program for computing mission success and crew safety for Gemini launch Vehicle; prediction equations required	Martin-Baltimore	27
Reliability Prediction by simulation	Air Force Institute of Technology	28
Special purpose program for prediction of Apollo mission success by simulation	GE-Tempo/NASA	29
Reliability Analysis and Prediction Independent of Distributions	Lear Siegler/NASA	30
Automatic Reliability Mathematical Model	NAA	31
Reliability Prediction of power systems	Westinghouse	32
Reliability Prediction of space vehicle by Monte Carlo simulation	NAA/NASA	33
Simulation of Failure Responsive Systems	Westinghouse/NASA	34
Weibull Analysis Program - Conducts Weibull Reliability Analysis	Motorola	34
Reliability program; computer success probability; several components; different distributions; includes correlation between lifetimes	Service Bureau Corp.	35
Reliability program; computer system reliability estimates of components	Service Bureau Corp.	35
Mathematical Automated Reliability and Safety Evaluation Program	Mathematica/Sandia	36,37
Predictors - Integrated Suite of Reliability Design Software Programs	Management Services Incs.	38, 41
RELCOMP: A Computer Program for Calculating System Reliability and MTBF	Interstate Electronics Co.	39
Computer Program for Approximating System Reliability	Research Triangle Institute	40

6.4.10.2 SPARCS - 2 (SIMULATION PROGRAM FOR ASSESSING THE RELIABILITY OF COMPLEX SYSTEMS)

SPARCS - 2 is a PL/1 computer program for assessing (establishing interval estimates for) the reliability and the MTBF of a large and complex system of any modular configuration. The system can consist of a complex logical assembly of independently failing attribute (binomial-Bernoulli) and time-to-failure (Poisson-exponential) components, without any regard to their placement. Alternatively, it can be a configuration of independently failing modules, where each module has either or both attribute and time-to-failure components.

The raw data for assessments are the component failure history data and the system configuration. The historical data are "successes and failures" for binomial-Bernoulli components and "failures and testing time (normalized to 'mission equivalent units')" for time-to-failure components. The configuration data consist of a list or lists of minimal paths ("minimal path sets" and "tie sets") or else a list of minimal cuts ("minimal cut sets") for the system as a list of modules and for each modules as a list of components. If the MTBF assessment option is selected, the system "mission time" is also needed.

    Contact: AFWAL/AFFDL
                  Wright Patterson AFB, OH 45433

6.4.10.3 ERSION 3 RELIABILITY GOAL STATUS

The ERSION program is basically a prediction type program which allows the user to input component level reliability indices and compute overall reliability values at the subsystem, system, and unit level. Basically, the program substitutes the input indices in the SCOPE (MFS-16410) generated equation for the subsystem to obtain a subsystem reliability. A set of subsystem level indices are obtained in this manner and are substituted in the associated system SCOPE equation determined by system/subsystem ID code to obtain a system reliability index. Finally, after a complete set of system level reliability indices are generated, numbers are substituted in the SCOPE equation to produce the overall unit reliability. The program allows the user to update a previously generated data set if the only difference between what is needed and what is available from the previous data set is in the component reliabilities. In this case, the user merely codes the numbers of differences on the system or subsystem control card and places the new reliabilities after the basic component set. The component program will apportion the new reliability to the phases of operation in the same proportion as the old values were apportioned. Since phase reliabilities are assumed independent, the overall reliability is the product of the phase reliabilities.

    Contact: Computer Software Management & Information Center
                  (COSMIC)
                  112 Barrow Hall
                  University of Georgia
                  Athens, Georgia 30602

6.4.10.4 SCOPE (SYSTEM FOR COMPUTING OPERATIONAL PROBABILITY EQUATIONS)

SCOPE is a system for determining the probability of success or failure for a given network. SCOPE computes from a logic block diagram, success or failure modes, success or failure equations, and probability of success or failure probability indices. SCOPE will merge a pert type path generator with an algorithm for combining failure or success modes to obtain failure or success equations. This allows the user to analyze a system's reliability. The mathematical model for the SCOPE program is based on its extension to cases of more than two events. This program can be used to determine the reliability of any large network or system where the functioning of the system is dependent on each step.

    Contact: COSMIC
                112 Barrow Hall
                University of Georgia
                Athens, Georgia 30602

6.4.10.5 APRDCT (APPORTIONMENT/PREDICTION)

This is a general program which utilizes weighting, failure rates, time, reliability equations, and system contractual stage goals to establish phase predicted indices and phase apportioned reliabilities at the component, subsystem, and system levels. The weighting factors used in this apportionment reflect Thurstone-Mosteller weightings derived from analyses of components with respect to conditions of use, phase stress conditions, and item capabilities. The phase reliability equations are determined from phase reliability networks by a computer program called "System for Computing Operational Probability Equations," (SCOPE). (See previous item.)

    Contact: COSMIC
                112 Barrow Hall
                University of Georgia
                Athens, Georgia 30602

6.4.10.6 RELIABILITY COMPUTATION FROM RELIABILITY BLOCK DIAGRAMS

This program package consists of a probability calculation program used to calculate the probability of system success from an arbitrary reliability block diagram. The class of reliability block diagrams that can be handled include any active standby combination of redundancy, and the computations include the effects of dormancy and switching in any standby systems. Four factors to be considered in calculations of this type are active block redundancy, standby block redundancy, partial redundancy, and the presence of equivalent blocks in the diagram. The probability of successful operation for a system involving active redundancy is found by using the probability tree method. The principle that is used in computing standby redundancy is simple, but difficulty occurs in applying the principle to complex circuits; methods and equations are presented in the program documentation. Partial redundancy is handled by manually setting up the problem in terms of

equivalent blocks. Equivalent blocks occur when the same piece of physical hardware appears more than once in the reliability block diagram. When this happens, the program assumes that if the block worked in one occurrence, it will work in the other and vice versa. To accommodate storage capacity (on the UNIVAC 1108), the following program limitations exist: (1) maximum of 50 blocks to a block diagram, (2) maximum of 200 success paths, (3) there can only be one output block, and (4) maximum of 14 inputs and 14 outputs per block. (The first three restrictions can be overcome by grouping blocks and/or success paths, by routing output blocks through one final success block.) The program is written to be used on a UNIVAC 1108 time sharing system with 65K core storage and a UNIVAC 1108 FORTRAN V compiler. The program can be run in either batch or interactive mode.

        Contact: COSMIC
                    112 Barrow Hall
                    University of Georgia
                    Athens, Georgia 30602

6.4.10.7 EXACT MINIMAL PATH AND MINIMAL CUT TECHNIQUES FOR DETERMINING SYSTEM RELIABILITY

This is a generalization of a family of techniques for determining by exact methods the probability of successfully operating a system using tree type logical analysis of the configuration of the elements. The system is deemed to be successful if a path of unbroken strings of connected branches corresponding to operating elements and assemblies can be traced from one end of the tree to another. The minimal paths are a subset of the paths and generate all the others; the minimal cuts are the subset of the failure states that generate all the others. The reliability of the system is the probability that at least one path obtains failure (success). The unique feature of these techniques is that one can find the system reliability if only either set of minimal states is known. By a recursive process, a system reliability (or unreliability) equation is generated as a function of the reliabilities (unreliabilities) of the elements using the complete set of minimal paths (cuts). The system reliability (unreliability) is formed by substitution into this equation.

        Contact: COSMIC
                    (see above)

6.4.10.8 RAM - RELIABILITY ANALYSIS MODEL

The Reliability Analysis Model (RAM) Program is an integrated Systems Design Analysis Program whose primary purpose is to combine the results of various Saturn V analyses into a single effective and comprehensive program. The RAM Program can be readily applied to determine the probability of success for one or more given objectives for any complex system. RAM can be applied to analyzed complex systems. The Reliability Analysis Model Program is also applicable to determining the effect of human factors on reliability. The RAM program includes failure mode and effects, criticality and reliability analyses, and some aspects of operations, safety, flight technology, systems, design

engineering, and configuration analyses. The unique advantage of this methodology and its associated programs is that the results of all these analyses are fed into a single data bank in term of impact on mission objectives, so that comparison, correlation, and tradeoffs may be made between the results of the various analyses. The basic output of the RAM program is the identification of those components that are critical to primary flight mission (no abort), vehicle integrity (no physical destruction of the vehicle), and crew safety. In addition to identifying those components that are critical to a specific objective, this program can rank them in order of importance (probability of primary flight mission success, vehicle integrity, and crew safety -both as an overall number and as a profile with respect to mission time). The criticality determination technique (CD technique) used in conjunction with RAM is a more general method. Criticality numbers can be assigned to components, subsystems, systems, stages, missions, and crews for any given failure distribution, such as the exponential, Weibull, Gamma, or truncated normal, where applicable.

      Contact: COSMIC
                 112 Barrow Hall
                 University of Georgia
                 Athens, Georgia 30602

6.4.10.9 BAYESIAN INTERACTIVE GRAPHICS RELIABILITY ASSESSMENT PROCEDURE (BIGRAP)

BIGRAP is a package of interactive graphics programs, written for use in the graphics terminal TEKTRONIX 4014 connected to the ARRADCOM CEC 6500/6600 computer configuration. This package consists of a set of intricate programs that allow a user to input component success/failure data as a Boolean expression depicting system reliability logic for the purpose of assessing system reliability. The computer converts the logic expression to an algebraic expression for the system reliability as a function of the individual component reliabilities. A Bayesian statistical algorithm is then employed to provide the user with point and confidence interval estimates of system reliability. In addition, the graphics feature of the package displays histograms and corresponding Beta distributions involved in the analysis.

      Contact: ARRADCOM
                 Attn: DRDAR-QAS
                 Dover, New Jersey 07801

6.5 STEP-BY-STEP PROCEDURE FOR PERFORMING RELIABILITY PREDICTION AND ALLOCATION

In summary, the following basic steps apply to the prediction and allocation of reliability requirements:

Step (1)   Definition of equipment

Step (2)   Definition of failure

Step (3)   Definition of operational and maintenance conditions

Step (4)   Develop the reliability block diagram(s)

Step (5)   Establish mathematical model(s)

Step (6)   Compilation of part lists

Step (7)   Performance of "parts count" or "parts stress analysis" reliability prediction

Step (8)   Assignment of failure rates or reliability

Step (9)   Combination of failure rates or reliability

Step (10)   Computation of equipment reliability

Step (11)   Allocate failure rates and reliability

Step (12)   Allocate among redundant configurations

Step (13)   Evaluate feasibility of allocated requirements

The procedures for making predesign or interim reliability predictions are basically the same as for final design predictions except that the difference lies in the degree of precision (and details) with which the basic steps are implemented.

For predictions made at any stage of development, each of the steps will be carried out to the maximum extent possible. The system failure and operating and maintenance conditions should be defined as explicitly as possible. Reliability block diagrams are constructed to the lowest identifiable function, and appropriate system reliability formulas are established.

Precise parts lists, of course, cannot be compiled prior to design of an equipment. It is necessary, however, to make the best possible estimate of the parts complements of the various item subdivisions (blocks on the reliability diagram).

Stress analyses obviously cannot be made prior to design. Therefore, for portions of the equipment that have not been designed, gross stress analyses can be accomplished. Stress levels may be assumed and failure rate estimates can be made by applying failure rate vs. stress tradeoffs to the assumed failure rate data.

The process of combining part failure rates to obtain preliminary block failure rates or reliabilities, of adjusting block rates or probabilities, and of computing equipment reliability is the same for predesign and interim predictions as for final predictions.

Step 1: Definition of Equipment. The initial step in a reliability prediction is to define the system or other item for which the prediction is being accomplished. The task of defining the item, then, consists of explicitly describing its purpose, intended function, or mission and physical boundaries of the items which compose the item. Particular attention must be devoted to interfaces among items so that all items will be considered in a prediction and there will be no unwanted duplication of coverage in predictions.

Step 2: Definition of Failure. Equipment failure is considered as the occurrence of any condition which renders the equipment incapable of operating within its specified performance parameter limits. The task of defining failure consists of listing or referencing the appropriate limits.

Step 3: Definition of Operational and Maintenance Conditions. Operating conditions include the equipment operational profile and the environmental conditions prevailing during the various periods of operation. The operational profile should be defined in terms of elapsed mission times or mission phases at which the equipment is turned on and the duration of operation during each phase. The sequence of functions necessary for success and the duty cycles of items within the equipment are also elements of the operational profile which must be defined.

During each period of operation, the pertinent environmental conditions must be established by test, reference, or assumption. Definition of environmental conditions encompasses all the factors that might affect reliability, whether or not their effects can be quantitatively assessed.

The maintenance conditions expected to affect reliability will be established. Pertinent items include: replacement schedules for parts with known or estimated limited lives; other preventive maintenance schedules; identification of items which may be replaced or repaired during a mission; requirements for special equipments or facilities; and so on. Also items that include redundancy will be identified. For those redundant items that can be repaired during a mission, maintainability predictions are required.

Step 4: Develop the Reliability Block Diagram(s). A reliability block diagram may be considered a logic chart which, by means of the arrangement of blocks and lines, depicts the effect of failure of equipment subdivisions on the equipment's functional capability. Items whose failure causes equipment failure are shown in series with other items. Items whose failure causes equipment failure only when some other item has also failed are drawn in parallel with the other items.

One of the first tasks in constructing a block diagram is to determine the complexity of equipment items which are to be shown as separate blocks. For a complex system it is often convenient to have several block diagrams. The first would be a simple diagram showing the first-order subdivision breakdown of the equipment. Separate block diagrams are then constructed for each of the first-order subdivisions. This process of diagramming goes on until individual blocks represent an order complexity such that their failure rates, or reliabilities, can be readily estimated from part level data.

It is frequently not possible to convey all of the pertinent information merely by the arrangement of blocks and interconnecting lines. Therefore, appropriate notation must be included on the diagram or in accompanying verbal descriptions. The notation should describe types of redundancy where it is not obvious from the diagram. Where failure of a redundant element degrades performance or places additional stresses on the items in alternate paths, it should be so noted. Also, operating times or cycles of the individual blocks should be noted if different from equipment operating time. In addition, items that may be repaired or replaced during a mission should be identified and monitoring intervals for those items should be stated.

If equipment operation varies during a mission (or specified operating time), this variation must be considered in determining the equipment failure pattern. For this purpose, mission time is divided into intervals, during which the equipment configuration is constant. Separate diagrams or sets of diagrams should be developed for each interval.

It is necessary to go within each block of the system block diagram to develop a reasonable approximation of a subsystem diagram containing those units required to perform the subsystem function. To the extent that design information is available at the early stage of system planning, it may be desirable to go further down into the system to block diagram specific design configurations at the subsystem and lower item levels -especially if planned features of the design concept include the application of redundancy or unique devices at these lower levels.

In the development of a block diagram, items that are predominantly electronic in function are classified and symbolized as electronic units, even though mechanical elements may be involved in the performance of an output function. Items that are predominantly mechanical or otherwise essentially nonelectronic in nature are identified accordingly. Any redundancy contemplated in the system planning stage should be shown, as well as any planned provisions for alternate mode capability. To the extent practicable, the block diagram should be constructed so that each item can be assumed functionally independent of its neighboring item so far as its specific transfer function is concerned.

Figure 6.5-1 shows the evolution of the detailed block diagram - going from the weapon system level down to the part level - as a function of design evolution.
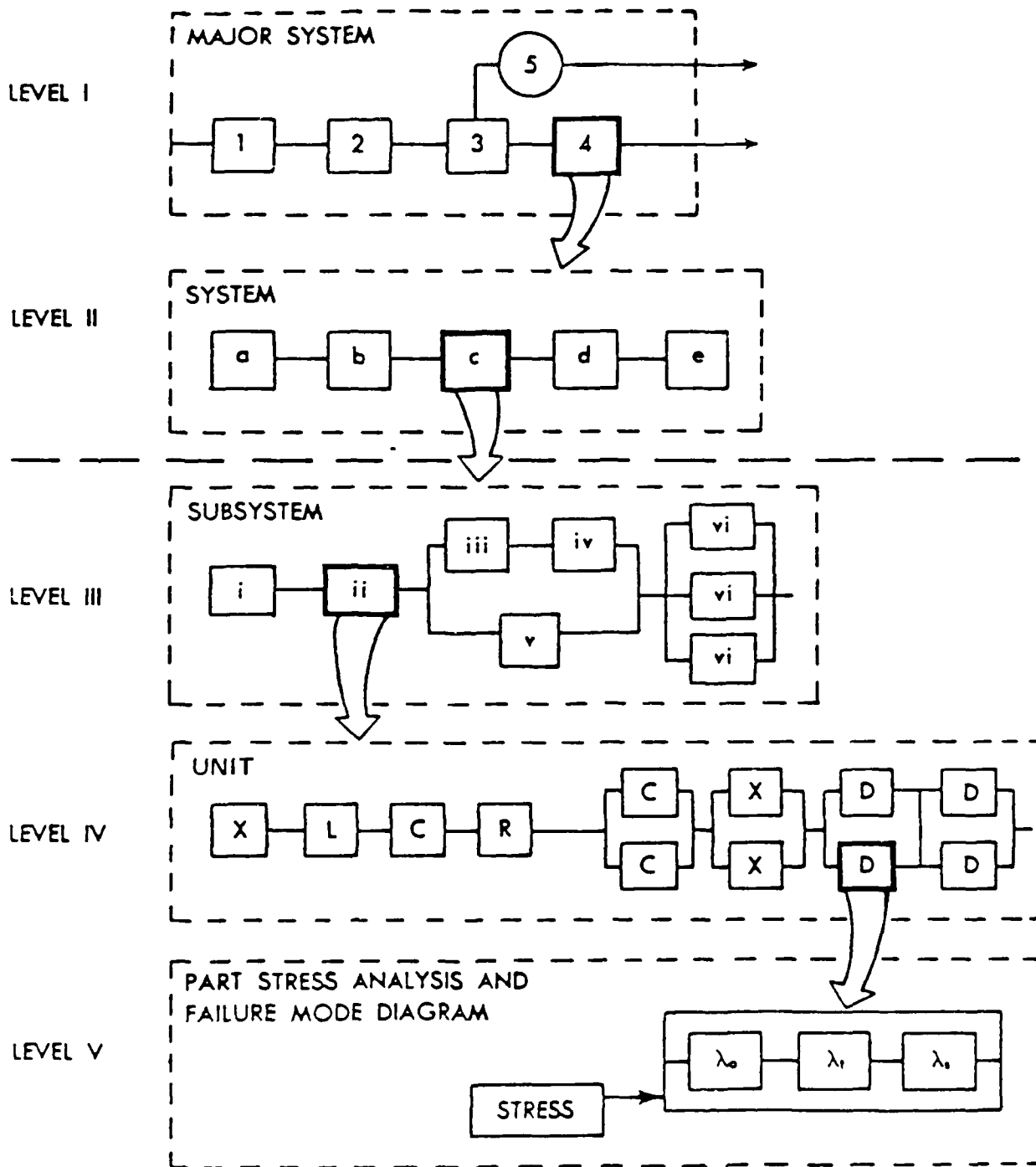
FIGURE 6.5-1: <u>PROGRESSIVE EXPANSION OF RELIABILITY BLOCK DIAGRAM AS DESIGN BECOMES KNOWN</u>

Levels I and II diagrams are usually producible from information available in the system planning phase. They are considered adequate for preliminary feasibility estimation and reliability allocation.

The Level III diagram is usually producible in the early design proposal stage.

The Level IV diagram is producible after a period of design formulation and review in which a definitive design has resulted.

Level V represents the failure mode diagram at the part level, where it becomes practicable to perform stress analyses and failure mode studies on individual parts within the system. Such detailed information may be available in the early planning phase on certain critical parts known to be essential to the success of the system concept.

MIL-STD-756 and the cited references provide additional guidelines on how to construct a reliability model, including drawing a reliability block diagram.

Step 5: Establish Mathematical Model(s). The mathematical model is a mathematical expression relating equipment reliability to the reliabilities of the equipment subdivisions depicted as blocks on the reliability diagram. In the simple cases where all blocks are in a series, the reliability equation may be merely:

$$R_e = R_1 R_2 \ldots, R_n$$

where

R_e is equipment reliability and

R_1, R_2, $\ldots$, R_n are reliabilities of

blocks 1, 2, $\ldots$, n, respectively.

Where there are no items whose failure rates change with time, no one-shot devices, etc., the equation may be even simpler, i.e.,

$$R_E(t) = e^{-\sum_{i=1}^{n} \lambda_i t_i}$$

where

λ_i is the failure rate of the ith block

t_i is the operating time of the ith block in system operating time t

If an equipment includes redundant items, items whose failure rates change with time, one-shot devices, provision for replacement of failed redundant elements, etc., the reliability formula will be more complex.

Section 6.4.2, MIL-STd-756 and the cited references (1, 4, 5, 6, 7, 8) provide guidelines for reliability modeling.

Step 6: Compilation of Parts List. For each block on the reliability block diagram, individual parts should be listed in some convenient order. If the block contains several low order subdivisions (such as assemblies or subassemblies), parts will be listed by circuit symbol within part type within block subdivision. All parts within a block should be listed, with appropriate notation to identify those whose failure will not cause the block to fail. If, for some parts, only particular failure modes will affect the block, those parts and the pertinent failure modes will also be identified.

In addition to identifying the parts within blocks, lists serve as basic worksheets for determining stresses and part failure rates, or reliability estimates. Therefore, parts lists should include part descriptions and pertinent ratings. They should also include space for entering operating voltages, currents, power dissipation, stress indexes, and failure rates or probabilities of survival. An example of an appropriate parts list is shown in Figure 6.5-2. This worksheet has been patterned after information derived from MIL-HDBK-217 and is used in Step 7 also.

For predesign predictions, estimate numbers of parts by type within each block. For interim predictions, compile parts lists for blocks, or subdivisions thereof, for which design information is available. Estimate parts complements for equipment subdivisions which have not been designed as stated above for predesign predictions.

Step 7: Performance of "Parts Count" or "Parts Stress Analysis" Reliability Prediction. Perform "Parts Count" analyses when applicable; during bid proposal and early design phases according to MIL-HDBK-217. Utilize generic part types and quantities, quality levels of parts, and equipment environment which has been determined in previous steps. For early trade studies and conceptual efforts, similar equipment of known complexity and parts content can be utilized for estimating reliability values.

Perform Parts Stress Analysis Prediction when most of the design is completed, detail parts are known, and when part stresses are available in accordance with MIL-HDBK-217. During early design, it may be feasible to advance from the "Parts Count" technique to a "gross stress analysis" based upon rough parts count, assumed stressed levels, etc.

Part selection and control activities include the determination of actual part stress levels in the intended circuit application. They also include failure rate calculations per MIL-HDBK-217 and employment of appropriate derating factors consistent with reliability prediction studies.

STRESS ANALYSIS – RELIABILITY PREDICTION WORKSHEET

FIGURE 6.5-2: STRESS ANALYSIS - RELIABILITY PREDICTION WORKSHEET

Additional improvement in part and, ultimately, equipment reliability can be realized by applying the techniques of derating. Derating can be defined as the operation of a part at less severe stresses than those for which it is rated. In practice, derating can be accomplished either by reducing stresses or by increasing the strength of the part. Selecting a part of greater strength is usually the most practical approach.

Derating is effective because the failure rate of most parts tends to decrease as the applied stress levels are decreased below the rated value. The reverse is also true; the failure rate increases when a part is subjected to higher stresses and temperature. The failure rate model of most parts is stress and temperature dependent. As a general rule, the specific derating should not be conservative to the point where costs rise excessively (e.g., higher than necessary parts are selected). Neither should the derating criteria be so loose as to render reliable part application ineffective. Optimum derating occurs at below the point where a rapid increase in failure rate is noted for a small increase in stress. Derating may require consideration of other constraints such as size, weight and power.

Step 8: Assignment of Failure Rates or Reliability. Failure rates or other appropriate measures of reliability will then be assigned to the individual parts. For most part types the measure of reliability will be obtained from the data in MIL-HDBK-217. Thus, they will usually be in the form of constant failure rates. The stress ratio determined in the preceding step, temperatures, derating, and other pertinent information are used to obtain these failure rates. If the stress ratio or temperatures vary during a mission, a separate failure rate for each mission phase must be assigned to each affected part.

Data applicable to parts whose failure rates change with time and one-shot devices or other parts whose reliability are not time dependent are usually expressed in the form of probabilities. They will be recorded as such on the parts lists. If the reliabilities are time dependent, appropriate values will be recorded for each of the time periods of interest (determined by previous steps).

Where part failure rate or reliability are estimated by part type (as in the parts count method), the generic failure rates for the devices in the prediction must account for differences in use environment.

Step 9: Combination of Failure Rates or Reliability. For blocks which contain only series parts with constant failure rates, the part failure rates will be added to obtain the block failure rate. If a block includes series parts which do not have constant failure rates, the reliability for these parts will be substituted in the reliability mathematical model to obtain the block reliability.

If part failure rates or reliability vary during a mission, they will be appropriately combined to obtain a block reliability for each mission phase, subphases, or other periods of interest determined in previous steps.

Step 10: Computation of Equipment Reliability. Compute the equipment's reliability in the form of mean-time-between-failures or reliability for the specified time intervals. Where all part failure rates are constant and there is no redundancy, the MTBF is the reciprocal of the sum of the block failure rates. If the blocks of the diagram represent one-shot devices, other parts whose reliability is not time dependent, parts whose failure rates change with time, redundant items, etc., reliabilicy is computed accurding to the guidelines and formulae in MIL-STD-756 and the cited references (1, 4, 5, 6, 7, 8).

Step 11: Allocate Failure Rates and Reliability. The previous section discussed reliability allocation techniques. One simple technique is to allocate on the assumption of equality of improvement feasibility (a slight modification of the ARINC technique). To allocate permissible failure rates among subsystems of the system, allocation is made by using as proportionality constants the ratios of individual subsystem's failure rates to total system failure rate. Thus, if a given subsystem now contributes 10% of the total system failure rate, it is reasoned that it should not be permitted to exceed 10% of the total failure rate allowable under the new requirement.

To allocate failure rates among systems, subsystems, or units, compute the ratio of the smaller block failure rate to the next larger block rate. For example, in Figure 6.5-1, assume that System 4 (Level 1) has an observed reliability of 0.8 for a 3 hour mission and each of the subsystems (a, b, c, d, e) have observed reliabilities and failure rates as shown in the table below:

Subsystem	Observed Reliability	Observed Failure Rate (10^6 hrs)	% of Total
a	0.96	13,600	18.38
b	0.97	9,000	12.16
c	0.92	28,800	38.92
d	0.96	13,600	18.38
e	0.97	9,000	12.16
TOTAL	0.8	74,000	100

Suppose that the new system has a reliability requirement of 0.9 for 3 hrs. The new failure rates and reliabilities of each of the subsystems would be allocated on the basis of the percentage of total failure rate contribution of each of the original subsystems. For example

$$R'_4(3) = 0.9 = e^{-3\lambda'_4}$$

$$\lambda'_4 = \frac{-\ln 0.9}{3} = 35,120 \text{ failure}/10^6 \text{ hours for System 4}$$

The new allocated failure rate for subsystem c would be

$$\lambda'_c = (0.3892)(35,120) = 13,677$$

and its allocated reliability would be

$$R'_c(3) = e^{-3\lambda'_c} = e^{-(3)(0.01367)} = 0.96$$

Repeating this procedure to find $R'_a(3)$, $R'_b(3)$, $R'_d(3)$ and $R'_e(3)$, we obtain the table below which shows the reallocated failure rates and reliabilities based upon the new system requirement.

Subsystem	Observed Reliability	Observed Failure Rate (10^6 hrs)	% of Total
a	0.98	6,455	18.38
b	0.99	4,270	12.16
c	0.96	13,670	38.92
d	0.98	6,455	18.38
e	0.99	4,270	12.16
TOTAL	0.9	35,120	100

Caution must be exercised when operational GFE items are part of the system reliability model. Oftentimes, the specified failure rate (or reliability) of such GFE items is used in lieu of the actual failure rate (or reliability) experienced in fleet usage. If the actual GFE failure rate is significantly higher than its specified failure rate, as is the usual case, then the reliability allocation of the non-GFE items under development is inadequate to satisfy the system reliability requirement. On the other hand, if the actual GFE failure rate is significantly less than its specified failure rate, then the reliability allocation of the non-GFE items under development is more severe and costly than is necessary to satisfy the system reliability requirement.

Step 12: Allocate Among Redundant Configurations. If the redundant elements are known to be part of the system concept, the above allocation method must be modified to account for the planned redundancy.

The following modification is applicable for any type of subsystem and system reliability function. The only necessary statistical or probability assumptions are that failure of any of the subsystems considered will result in system failure and that the failure probability of each subsystem is independent of all other subsystems. This will allow the use of the product formula for system reliability upon which the method is based.

One method of allocation when redundancy is present in the subsystem follows:

(1) Draw a reliability block diagram of the subsystem in question. Also construct an equivalent (functional) non-redundant subsystem.

(2) Select the number of hours, T, over which a high system reliability is desired. T would be defined by the mission requirements or the average time interval before corrective maintenance or unit replacement.

(3) Using estimated base failure rates, evaluate R(T) for both the redundant and non-redundant configurations described in (1) above.

6-66

(4) The failure rate factor for the redundant subsystem is estimated by:

$$\lambda_r = \frac{R(T)_s}{R(T)_r} \lambda_s$$

where

λ_r is the estimated failure rate for the redundant subsystem

λ_s is the failure rate for the equivalent non redundant subsystem

$R(T)_s$ is the calculated reliability at time T of the non redundant subsystem

$R(T)_r$ is the calculated reliability at time T of the redundant subsystem

(5) Specify $R^*(T)$, the desired system reliability at time T, and compute the total system failure rate,

$$\lambda_o = \sum_i \lambda_i$$

where λ_i is the failure rate of the ith subsystem.

(6) The allocated reliability for Subsystem i is

$$R^*_i(T) = R^*(T)^{\lambda_i / \lambda_o}$$

NOTE: For non redundant subsystems, the allocated failure rate is

$$\lambda^*_i = \frac{-\ln R^*_i(T)}{T}$$

(7) Check the allocation against the required system $R^*(T)$.

Example: Assume the reliability block diagram of a system is as shown in Figure 6.5-3. Each box represents a complex equipment for which the failure rates and the estimated mean lives are:

Subsystem	Failure Rate x 10^{-6}	Mean Life
S_1	20,000	50 hours
S_2	15,000	67 hours
S_3	a)10,000	100 hours
	c)20,000	50 hours

(a) Establish equivalent non redundant units. S_1 and S_2 subsystems are non redundant with all constituent elements in series. S_3 has two parallel elements in series with another element. Since only one of the two parallel elements is necessary for performing the system function, we have S_3, as shown in Figure 6.5-4.
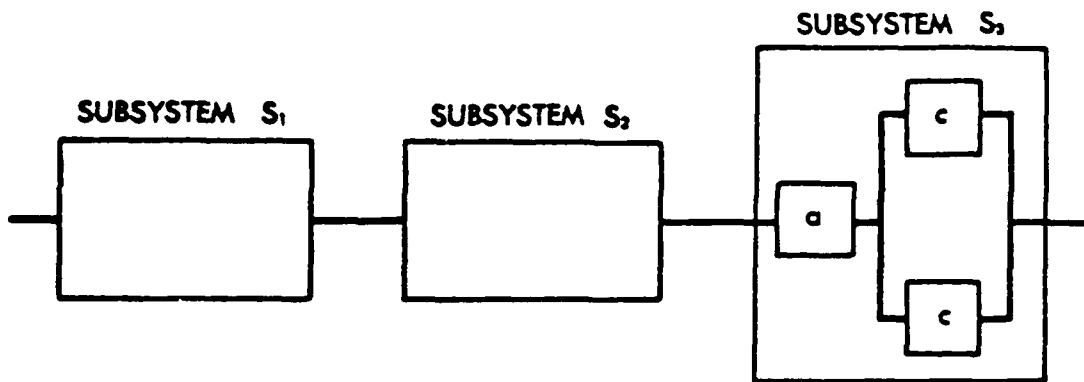
FIGURE 6.5-3: RELIABILITY BLOCK DIAGRAM WITH REDUNDANT ELEMENTS
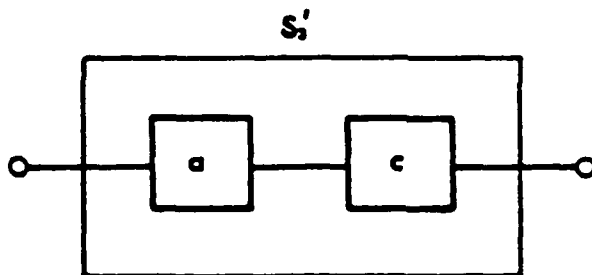
FIGURE 6.5-4: EQUIVALENT NON-REDUNDANT UNIT

(b) Determine critical time period. Assume corrective maintenance is performed every 50 hours; hence, T = 50.

(c) Compute $R(T)_s$ for non redundant units and $R(T)_r$ for redundant units at T = 50 hours.

Non Redundant Unit:

$$R(T)_s = R(T)_a \times R(T)_c$$

$$= e^{-T/100} \times e^{-T/50}$$

$$= .606 \times .368 = .223$$

Redundant Unit:

$$R(T)_r = R(T)_a \times R(T)_c [2 - R(T)_c]$$

$$= .606 \times .368 [2 - .368] = .364$$

(d) Compute base failure rate factor for redundant unit, with

$$\lambda_s = (10,000 + 20,000) \times 10^{-6}$$

$$= 30,000 \times 10^{-6}$$

$$R(T)_s = .223$$

$$R(T)_r = .364$$

Then,

$$\lambda_r = \left[\frac{R(T)_s}{R(T)_r} \right] \lambda_s$$

$$= \left(\frac{.223}{.364} \right) 30,000 \times 10^{-6}$$

$$= 18,379 \times 10^{-6}$$

(e) Convert desired reliability to total system failure rate. Assume that at 50 hours, the reliability requirement is specified to be .75. Hence, $R*(T) = .75$.

$$\lambda_1 = 20,000 \times 10^{-6}$$

$$\lambda_2 = 15,000 \times 10^{-6}$$

$$\lambda_3 = 18,379 \times 10^{-6}$$

$$\lambda_0 = \sum_i \lambda_i = 53,379 \times 10^{-6}$$

(f) Allocate reliability.

$$R^*_i(T) = R^*(T)^{\lambda_i/\lambda_o}$$

$$R^*_1(50) = (.75)^{200/534} = .898$$

$$R^*_2(50) = (.75)^{150/534} = .922$$

$$R^*_3(50) = (.75)^{183/534} = .906$$

(g) Check allocation against $R^*(T) = .75$.

$$R^*_i(50) \; R^*_2(50) \; R^*_3(50) = .7501$$

The allocated system failure rates for non-redundant Subsystems 1 and 2 are:

$$\lambda^*_1 = \frac{-\ln .898}{50} = 2150 \times 10^{-6}$$

$$\lambda^*_2 = \frac{-\ln .922}{50} = 1620 \times 10^{-6}$$

Step 13: <u>Evaluate Feasibility of Allocated Requirement</u>. In previous steps, the system reliability permitted by operational requirements was distributed by an allocation procedure among subsystems within the new system. There are assumptions in the allocation procedures (e.g., reliability prediction techniques) which establish the allocation as tentative only; that is, for use as an initial basis in the specification of reliability requirements at the next lower level of equipment.

The allocation of requirements to the next level of definition results in the process being reiterated and further allocations of requirements in the hardware breakdown structure. The allocations, therefore, must be reviewed and adjusted as soon as details at the next level of reiteration disclose discrepancies between allocated improvement feasibility.

It may turn out, for example, that a ten-to-one reduction in failure rate of one unit is entirely feasible, whereas a two-to-one reduction in another unit would be beyond state-of-art capability. The reallocation of reliability requirements must therefore ultimately consider improvement feasibility within the constraints of available time and funds.

REFERENCES

1. AMCP 706-196, Engineering Design Handbook: Design for Reliability, AD#A027370, January 1976.

2. Reliability of Military Electronic Equipment, Advisory Group on Reliability of Electronic Equipment, Office of the Assistant Secretary of Defense (Research & Engineering), June 1957.

3. Von Alven, W.H., Ed., Reliability Engineering, Prentice-Hall Inc., Englewood Cliffs, NJ, 1964.

4. AMCr 706-197, Engineering Design Handbook: Reliability Prediction, AD#A032105, January 1976.

5. NAVAIR 01-1A-32, Reliability Engineering Handbook, Naval Air Systems Command, Washington DC, July 1977.

6. Lloyd, R.K., and M. Lipow, Reliability: Management, Methods, and Mathematics, 2nd edition, Redondo Beach, California, 1977.

7. Shooman, M., Probabilistic Reliability: An Engineering Approach, McGraw Hill Book Co., New York, 1968.

8. Mann, N., R. Schafer and N. Singpurwalla, Methods of Statistical Analysis of Reliability and Life Data, John Wiley & Sons, New York, 1974.

9. Mazzili et al., RADC Reliability Notebook, Vol. 1, RADC-TR-67-108, November 1968, AD#845304.

10. James, L.E., et al., Study of Reliability Prediction Techniques for Conceptual Phases of Development, RADC-TR-74-235, October 1974.

11. Klion, J., and G. Lyne, "RADC ORACLE," Proceedings of the 1981 Annual Reliability and Maintainability Symposium, January 1981.

12. Lipson, C., et al., Reliability Prediction -- Mechanical Stress/Strength Interference Models, RADC-TR-68-403, March 1967.

13. Lipson, C., et al., Reliability Prediction -- Mechanical Stress/Strength Interference (nonferrous), RADC-TR-68-403, December 1968.

14. Yurkowsky, W., Nonelectronic Reliability Notebook, RADC-TR-69-458, March 1970.

15. Nonelectronic Parts Reliability Data (NPRD-2), Reliability Analysis Center, Griffiss AFB, NY 13441, Summer 1981.

16. Missile Materiel Reliability Prediction Handbook, Parts Count Prediction, LC-78-1, U.S. Army Missile Research & Development Command, Redstone Arsenal, AL 35809, February 1978.

17. Storage Reliability of Missile Material Program, Volume 1, Electrical and Electronic Devices, LC-78-2, U.S. Army Missile Research and Development Command, Redstone Arsenal, AL 35809, January 1978.

18. Kern, G., et al., Nonoperating Failure Rates for Avionics Study, RADC-TR-80-136, April 1980.

19. Van Tijn, D.E., "Description of the Computerized Reliability Analysis Method (CRAM)," Monograph 11, ARINC Research Corp., Washington, DC, 1964.

20. Whiteman, I.R., "RESCRIPT -- A Computer Programming Language for Reliability," presented at Fifth Annual West Coast Reliability Symposium, Los Angeles, California, 1964.

21. Parr, Van B., "Automated Reliability Trade-off Program - ARTOP II," Proceedings of the 1967 Annual Symposium on Reliability, 1967, pp. 847-857.

22. Coffelt, R.B., "Automated System Reliability Prediction," Proceedings of the 1967 Annual Symposium on Reliability, 1967, pp. 302-304.

23. House, J.F., and J. LaCapra, "Systems Reliability Analysis and Prediction Through the Application of a Digital Computer," pre-sented at National Symposium on Space Electronics and Telemetry, Miami Beach, Florida, 1962.

24. Shelley, B.F., and D.O. Hamilton, "A Mechanized Aircraft Reliability Analysis Model," Proceedings of the Tenth National Symposium on Reliability and Quality Control, 1964, pp. 560-566.

25. McFaul, C., "Deep Submergence Rescue Vessel Reliability Prediction," Technical Memo 415/65, U.S. Navy MEL, Annapolis, Maryland, 1965.

26. Weisburg, S.A., and J.H. Schmidt, "Computer Technique for Estimating System Reliability," Proceedings of the 1966 Annual Symposium on Reliability, 1966, pp. 87-97.

27. Kiefer, F.P., et al., "Man-rating the Gemini Launch Vehicle (Crew Hazard and Mission Analysis)," Proceedings of the 1966 Annual Symposium on Reliability, 1966, pp. 250-268.

28. Finch, R.E., "An SPS Subroutine as a Simulation Aid," School of Engineering, Air University, Wright-Patterson AFB, 1963, AD#425237.

29. "Survey of Studies and Computer Programming Efforts for Reliability, Maintainability, and System Effectiveness," Report OEM 1, Office of the Director of Defense Research and Engineering, September 1965, AD#622676.

30. Bryant, R.O., "Variability Prediction -- A New Method," Proceedings of the 1967 Annual Symposium on Reliability, 1967, pp. 181-188.

31. McKnight, C.W., et al., "An Automatic Reliability Mathematical Model," Proceedings of the Eleventh National Symposium on Reliability and Quality Control, 1965, pp. 518-532.

32. Patton, A.D., et al., "Power System Reliability II - Applications and a Computer Program," IEEE Transactions on Power Apparatus and Systems PAS-84, July 1965, pp. 636.

33. Hershkowitz, B.H., et al., "Reliability Simulation Model," Proceedings of the Tenth National Symposium on Reliability and Quality Control, 1964, pp. 186-200.

34. Hannigan, J.M., "A Computer Program for the Simulation of Failure-Responsive Systems," Technical Report No. 6, Westinghouse Defense and Space Center, 1966, N66-26880.

35. "Reliability Engineering at SBC," Service Bureau Corporation, Computing Sciences Division, Palo Alto, California, 1966.

36. "A Description of the MARSEP Program - A Mathematica Report," Mathematica, Inc., Princeton, NJ, July 1969.

37. Breipohl, A.M., and R.A. Hernquist, "A Computer Program for Performing Reliability Analyses," Report SC-TM-65-523, Sandia Laboratory, Albuquerque, New Mexico, December 1965.

38. Blemel, K.G., "Computer Software Synergism Integrates R/M Design," Proceedings of the 1974 Annual Reliability and Maintainability Symposium, 1974, pp. 68-72.

39. Fleming, J.L., "Relcomp: A Computer Program for Calculating System Reliability and MTBF," IEEE Trans. Reliability R-20, August 1971, pp. 102-107.

40. Nelson, A.C., Batts, J.R., and R.L. Beadles, "A Computer Program for Approximating System Reliability," IEEE Trans. Reliability R-19, May 1970, pp. 61-65 and R-20, May 1971, pp. 88-90.

41. Blemel, K.G., "Functional Analysis - A Methodology," Proceedings of the 1985 Reliability Conference, Birmingham England.

APPENDIX A

DYNAMIC PROGRAMMING APPROACH TO RELIABILITY ALLOCATION

INTRODUCTION TO DYNAMIC PROGRAMMING

To serve as a basis for formulation of such problems, a brief summary of the essential elements of the dynamic programming procedure follows:

(1) The dynamic programming technique is applicable to multi-stage (or sequential) decision problems. The technique converts such a problem to a series of single-stage optimization problems.

(2) In addition to defining the stages of such a process, four attributes of the problem must be identified if the technique is to be applied:

   (1) S_k is the set of all possible states of stage k. Its elements are designated as s_k, i.e., $s_k \in S_k$.

   (2) D_k is the set of all possible decision alternatives available at stage k. Its elements are designated as $d_k \in D_k$.

   (3) $T_k(s_k, d_k)$ is a function transforming s_k to s_{k-1} depending on the existing state, s_k, of stage k and the decision alternative, d_k, selected at stage k.

   (4) $R_k(s_k, d_k)$ is a function defining the return realized at stage k resulting from state s_k and alternative d_k.

(3) An n-stage process is displayed by Figure A-1.

(4) The multi-stage decision problem may then be converted to a series of single-stage decision problems as reflected by a set of recursion equations.

$$f_k(s_k) = \min_{d_k \in D_k} [Q_k(s_k, d_k)], \quad k = 1, 2, \ldots, n \qquad (A.1)$$

$$Q_k(s_k, d_k) = R_k(s_k, d_k), \quad k = 1 \qquad (A.2)$$

$$= R_k(s_k, d_k) \cdot f_{k-1}(s_{k-1}), \quad k = 2, 3, \ldots, n$$

where $\cdot$ may be interpreted as either an addition or multiplication operator. However, it is used as a multiplication operator on condition that the operands are non-negative.

(5) Then

$$f_n(s_n) = \min_{d_n D_n} [R_n(s_n, d_n) \cdot f_{n-1}(s_{n-1})] \qquad (A.3)$$
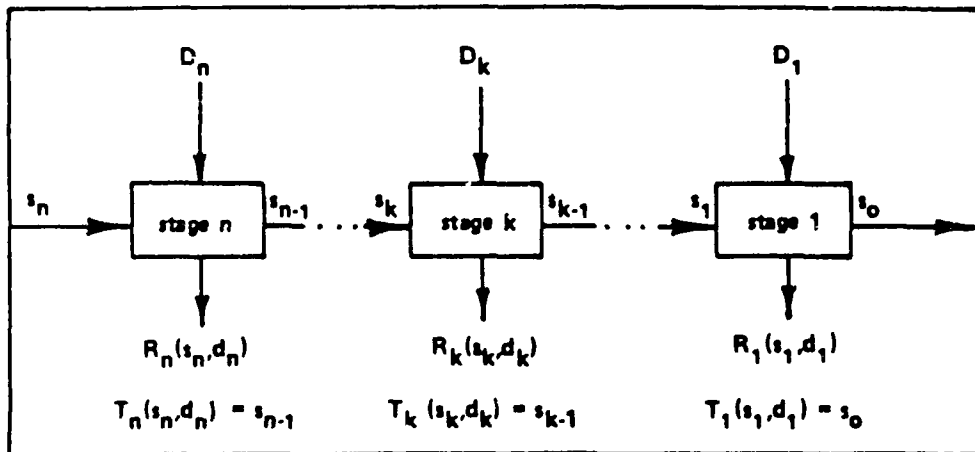
FIGURE A-1: $\bar{n}$-STAGE DYNAMIC PROGRAMMING REPRESENTATION

is the total return which results from the optimal set of decision alternatives.

$$d^* = (d^*_1, d^*_2, \ldots, d^*_n) \tag{A.4}$$

(6) The above formulation may be applied to a maximization objective by the substitutions of max for min.

SUBSYSTEMS OPERATING IN SERIES

The dynamic programming formulation contained herein pertains to apportionment of system reliability requirements among series subsystems in such a manner as to minimize the total expenditure of development effort. Some basic assumptions which are fundamental to the formulation are discussed below:

(1) At any particular stage of the development program (at time of apportionment), the system can be partitioned into n subsystems and the present reliability level can be estimated for each subsystem. Failure of any subsystem will cause system failure. In addition, it is assumed that the subsystem goal cannot be less than its estimated present level.

(2) The n subsystems function independently so that expected system reliability resulting from the subsystem goals can be expressed as the product of these subsystem goals:

$$y = \prod_{i=1}^{n} y_i \tag{A.5}$$

where y is the system reliability goal and y_i is the goal for the ith subsystem.

(3) An effort function can be identified for each subsystem, defining the number of units of development effort required to raise its reliability level from the present value to any potential reliability goal. The effort may represent a single important resource or a combination of resources, if these can be expressed by a common unit. The effort function may be either continuous or discrete. A continuous mathematical function allows the reliability goal to assume any value between the estimated present level and one. A discrete function limits potential subsystem goals to particular values.

Consider a proposed system comprised of n subsystems, each of which are to be developed independently. These subsystems are to function independently and in series. What reliability goal should be assigned to each subsystem in order that the system goal be satisfied at a minimum expenditure of development effort? Symbols to be used in problem formulation are defined as:

$\bar{y}$ = system reliability goal, $0 \le \bar{y} \le 1$

x_i = reliability level of subsystem i at the present state of development $0 \le x_i \le 1$

y_i = reliability goal apportioned to subsystem i, $x_i \le y_i \le 1$

$G_i(x_i,y_i)$ = units of development effort required to raise the reliability level of subsystem i from x_i to y_i

n = number of subsystems

y^*_i = reliability goal apportioned to subsystem i such that total development effort is minimized

The problem may be formulated as:

$$\text{minimize} \quad \sum_{i=1}^{n} G_i (x_i, y_i) \qquad (A.6)$$

$$\text{subject to} \quad \prod_{i=1}^{n} y_i = y \qquad (A.7)$$

$$x_i \le y_i \le 1, \quad i = 1, 2, \ldots, n$$

The problem may be converted to a dynamic programming problem as follows:

(1)   Identify each of the n subsystems as a stage such that an apportionment goal must be determined at each stage. A specific numbering sequence for the stages (subsystems) is not necessary, but each subystem must maintain its assigned identity throughout the entire procedure.

(2)   Define the set, S_k, of all possible states, s_k, at stage k such that:

$$1 = s_n \ge s_{n-1} \cdots \ge s_1 \ge s_0 = y$$

(3)   Define the set, D_k, of all possible decision alternatives, $d_k = y_k$, at stage k such that:

$$x_k \le y_k \le 1, \quad k = 1, 2, \ldots, n$$

(4)   Define the transformation function for stage k:

$$T_k(s_k, d_k): \quad s_k y_k = s_{k-1}, \quad k = 1, 2, \ldots, n$$

(5)   Define the return realized at stage k as the function:

$$R_k(s_k, d_k) = G_k(x_k, y_k), \quad k = 1, 2, \ldots, n$$

The problem is displayed in Figure A-2. The resulting recursion equations are:

$$f_k(s_k) = \min_{y_k} [Q_k(s_k, y_k)] \quad k = 1, 2, \ldots, n \tag{A.8}$$

$$Q_k(s_k, y_k) = G_k(s_k, y_k), \quad k = 1$$

$$= G_k(s_k, y_k) + f_{k-1}(s_{k-1}), \quad k = 2, 3, \ldots, n \tag{A.9}$$

and the optimal set of apportioned goals will be defined as:

$$d^* = (y^*_1, y^*_2, \ldots, y^*_n)$$

This problem can be solved by means of a digital computer.

EXAMPLE USING DYNAMIC PROGRAMMING APPROACH

To exemplify the use of the technique, consider a proposed weapon system which is to be developed as three independent subsystems. The system can be functionally successful if, and only if, each of the three subsystems function properly. In order that the system fulfill its intended role, it should be 0.90 reliable. Based on engineering analysis and historical information of similar type equipment, estimates of the state-of-the-art reliability levels of the subsystems are 0.95, 0.95, and 0.97. What reliability goal should be assigned to each subsystem in order to minimize the total expenditure of development funds? The estimated effort (funds) functions for the three subsystems are contained in Figure A-3 where $G_i(x_i, y_i)$ is expressed in $1000 units. Potential apportioned goals are limited to those contained in these tabled functions.

First, $(0.95)(0.95)(0.97) = 0.875425 < 0.90$ indicates that further development is necessary to meet the system goal.

$$n = 3$$

$$\bar{y} = 0.90$$

$$x_1 = 0.95$$

$$x_2 = 0.95$$

$$x_3 = 0.97$$

The general formulation follows:

$$\min G_1(0.95, y_1) + G_2(0.95, y_2) + G_3(0.97, y_3)$$
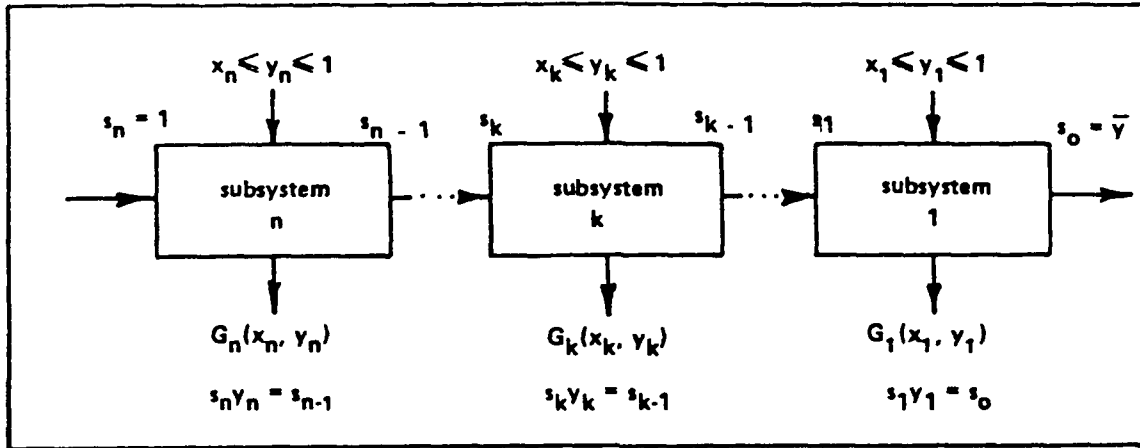
FIGURE A-2: DYNAMIC PROGRAMMING APPORTIONMENT FORMULATION

y_1	$G_1(0.95, y_1)$	y_2	$G_2(0.95, y_2)$	y_3	$G_3(0.97, y_3)$
0.95	0	0.95	0	0.97	0
0.96	1.0	0.96	20.0	0.98	25.0
0.97	3.9	0.97	46.0	0.99	55.6
0.98	16.5	0.98	81.2	0.995	99.7
0.99	34.0	0.99	126.8		
0.995	65.0	0.995	179.8		

FIGURE A-3: TABLE OF EFFORT FUNCTIONS

subject to $\prod\limits_{i=1}^{3} y_i \geq 0.9$

y_1 = 0.95, 0.96, 0.97, 0.98, 0.99 or 0.995

y_2 = 0.95, 0.96, 0.97, 0.98, 0.99 or 0.995

y_3 = 0.97, 0.98, 0.99 or 0.995

Since discrete effort functions allow only specific values to be considered as potential subsystem goals, the system goal might not be met as an equality; hence, the inequality constraint.

The dynamic programming format and elements are shown in Figure A-4.

The recursion equations are:

$$f_1(s_1) = \min_{y_1} [G_1(0.95, y_1)]$$

$$f_2(s_2) = \min_{y_2} [G_2(0.95, y_2) + f_1(s_1)]$$

$$f_3(s_3) = \min_{y_3} [G_3(0.97, y_3) + f_2(s_2)]$$

Figures A-5a, b, and c contain the calculated state transformations for Stages 3, 2 and 1, respectively, utilizing the following relations.

s_3 = 1

s_2 = $s_3 y_3$

s_1 = $s_2 y_2$

s_0 = $s_1 y_1$

Figure A-6a shows the calculated $Q_1(s_1, y_1)$ for Stage 1.

$$Q_1(s_1, y_1) = G_1(0.95, y_1)$$

The values shown in blocks are

$$\min_{y_1} [Q_1(s_1, y_1)] = f_1(s_1)$$

The blanks represent s_0 values which do not satisfy the problem constraint that

$$s_0 \geq 0.90$$

Figure A-6b shows the calculated $Q_2(s_2, y_2)$ for Stage 2.

$$Q_2(s_2, y_2) = G_2 (0.95, y_2) + f_1(s_1)$$
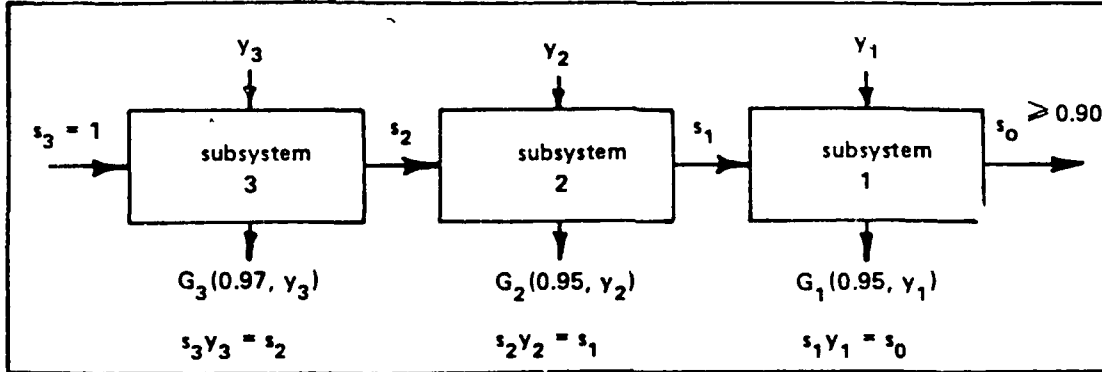
FIGURE A-4: DYNAMIC PROGRAMMING FORMULATION EXAMPLE

s_2	Y_3			
	0.97	0.98	0.99	0.995
$s_3 = 1$	0.97	0.98	0.99	0.995

a. State Transformations for Stage 3

s_1	Y_2					
	0.95	0.96	0.97	0.98	0.99	0.995
0.97	0.9215	0.9312	0.9409	0.9506	0.9603	0.9652
0.98	0.9310	0.9408	0.9506	0.9604	0.9702	0.9751
s_2						
0.99	0.9405	0.9504	0.9603	0.9702	0.9801	0.9851
0.995	0.9453	0.9552	0.9652	0.9751	0.9851	0.9900

b. State Transformations for Stage 2

FIGURE A-5: STATE TRANSFORMATIONS FOR STAGES 1, 2, AND 3.

s_0	y_1					
	0.95	0.96	0.97	0.98	0.99	0.995
0.9215	0.8754	0.8846	0.8939	0.9031	0.9123	0.9169
0.9310	0.8845	0.8938	0.9031	0.9124	0.9217	0.9263
0.9312	0.8846	0.8940	0.9033	0.9126	0.9219	0.9265
0.9405	0.8935	0.9029	0.9123	0.9217	0.9311	0.9358
0.9408	0.8938	0.9032	0.9126	0.9220	0.9314	0.9361
0.9409	0.8939	0.9033	0.9127	0.9221	0.9315	0.9362
0.9453	0.8979	0.9074	0.9169	0.9263	0.9358	0.9405
0.9504	0.9029	0.9124	0.9219	0.9314	0.9409	0.9456
0.9506	0.9031	0.9126	0.9221	0.9316	0.9411	0.9458
0.9552	0.9074	0.9170	0.9265	0.9361	0.9456	0.9504
0.9603	0.9123	0.9219	0.9315	0.9411	0.9507	0.9555
0.9604	0.9124	0.9220	0.9316	0.9412	0.9508	0.9556
0.9652	0.9169	0.9265	0.9362	0.9458	0.9555	0.9603
0.9702	0.9217	0.9314	0.9411	0.9508	0.9605	0.9653
0.9751	0.9263	0.9361	0.9458	0.9556	0.9653	0.9702
0.9801	0.9311	0.9409	0.9507	0.9605	0.9703	0.9752
0.9851	0.9358	0.9456	0.9555	0.9653	0.9752	0.9801
0.9900	0.9405	0.9504	0.9603	0.9702	0.9801	0.9851

(s_1 labels the left column rows)

c.   State Transformations for Stage 1

FIGURE A-5:   (CONT'D)

$Q_1(s_1,y_1)$	y_1					
	0.95	0.96	0.97	0.98	0.99	0.995
0.9215	-----	-----	-----	16.5	34.0	65.0
0.9310	-----	-----	3.9	16.5	34.0	65.0
0.9312	-----	-----	3.9	16.5	34.0	65.0
0.9405	-----	1.0	3.9	16.5	34.0	65.0
0.9408	-----	1.0	3.9	16.5	34.0	65.0
0.9409	-----	1.0	3.9	16.5	34.0	65.0
0.9453	-----	1.0	3.9	16.5	34.0	65.0
0.9504	0	1.0	3.9	16.5	34.0	65.0
0.9506	0	1.0	3.9	16.5	34.0	65.0
0.9552	0	1.0	3.9	16.5	34.0	65.0
0.9603	0	1.0	3.9	16.5	34.0	65.0
0.9604	0	1.0	3.9	16.5	34.0	65.0
0.9652	0	1.0	3.9	16.5	34.0	65.0
0.9702	0	1.0	3.9	16.5	34.0	65.0
0.9751	0	1.0	3.9	16.5	34.0	65.0
0.9801	0	1.0	3.9	16.5	34.0	65.0
0.9851	0	1.0	3.9	16.5	34.0	65.0
0.9900	0	1.0	3.9	16.5	34.0	65.0

s_1

a. Returns for Stage 1

FIGURE A-6: RETURNS FOR STAGES 1, 2, and 3.

$Q_2(s_2,y_2)$	y_2					
	0.95	0.96	0.97	0.98	0.99	0.995
0.97	0 + 16.5 = 16.5	20.0 + 3.9 = 23.9	46.0 + 1.0 = 47.0	81.2 + 0 = 81.2	126.8 + 0 = 126.8	179.8 + 0 = 179.8
0.98	0 + 3.9 = 3.9	20.0 + 1.0 = 21.0	46.0 + 0 = 46.0	81.2 + 0 = 81.2	126.8 + 0 = 126.8	179.8 + 0 = 179.8
s_2 0.99	0 + 1.0 = 1.0	20.0 + 0 = 20.0	46.0 + 0 = 46.0	81.2 + 0 = 81.2	126.8 + 0 = 126.8	179.8 + 0 = 179.8
0.995	0 + 1.0 = 1.0	20.0 + 0 = 20.0	46.0 + 0 = 46.0	81.2 + 0 = 81.2	126.8 + 0 = 126.8	179.8 + 0 = 179.8

b. Cumulative Returns for Stage 2

$Q_3(s_3,y_3)$	y_3			
	0.97	0.98	0.99	0.995
$s_3 = 1$	0. + 16.5 = 16.5	25.0 + 3.9 = 28.9	55.6 + 1.0 = 56.6	99.7 + 1.0 = 100.7

c. Cumulative Returns for Stage 3

FIGURE A-6: (CONT'D)

A-12

The values shown in blocks are

$$f_2(s_2) = \min_{y_2} [Q_2(s_2, y_2)]$$

Figure A-6c shows the calculated $Q_3(s_3, y_3)$ for Stage 3.

$$Q_3(s_3, y_3) = G_3(0.97, y_3) + f_2(s_2)$$

The blocked value is

$$f_3(s_3) = \min_{y_3} [Q_3(s_3, y_3)]$$

Then the optimal decision at Stage 3 is

$$y^*_3 = 0.97$$

as indicated by the blocked value in Figure A-6c and

$$s_2 = s_3 y^*_3 = 0.97$$

The optimal decision at Stage 2, given $s_2 = 0.97$, is

$$y^*_2 = 0.95$$

as indicated in Figure A-6b, and

$$s_1 = s_2 y^*_2 = 0.97(0.95) = 0.9215$$

Similarly, the optimal decision at Stage 1, given that $s_1 = 0.9215$, is

$$y^*_1 = 0.98$$

as indicated by Figure A-6a, and the resulting

$$s_0 = s_1 y^*_1 = 0.9215(0.98) = 0.903$$

which meets the system reliability goal.

Summarizing the optimal reliablity subsystem goals are

$$y^*_3 = 0.97$$

$$y^*_2 = 0.95$$

$$y^*_1 = 0.98$$

and the total required expenditure of development funds to achieve these goals is

$$\$1000 f_3(s_3) = \$1000(16.5) = \$16,500$$

as indicated in Figure A-6c.

7.0 RELIABILITY ENGINEERING DESIGN GUIDELINES

7.1 INTRODUCTION

Reliability engineering is the technical discipline of estimating, controlling, and managing the probability of failure in devices, equipment and systems. In a sense, it is engineering in its most practical form, since it consists of two fundamental aspects:

(1) paying attention to detail
(2) handling uncertainties

However, merely to specify, allocate, and predict reliability is not enough. One has to do something about it in terms of having available a family of design procedures which the designer can use to achieve a desired reliability. These are provided in this section.

During development a design is formulated to meet quantitative reliability requirements previously defined. The results of these activities provide inputs for all future actions. The importance of designing in the required degree of reliability initially cannot be overemphasized, for once the design is approved inherent reliability is fixed. Less than perfect compliance with required actions from this point may result in an achieved reliability level less than the fixed inherent level.

There are a host of design principles and tools of which the designer should be aware and should *utilize* as *required* to achieve the design of a reliable electronic equipment/system. They include:

(1) part selection and control
(2) part derating
(3) reliable circuit design
(4) redundancy
(5) environmental design
(6) human factors design
(7) failure modes and effects analysis (FMEA)
(8) fault tree analysis (FTA)
(9) sneak circuit analysis
(10) design reviews

Each of the above items will be briefly discussed in this section in terms of its role in the design of reliable equipment/systems.

7.2 PART SELECTION AND CONTROL

Component parts are the basic building blocks of systems. The system can be no stronger from a reliability viewpoint than the basic building blocks from which it is built. Therefore, the most crucial part of the design process is the selection, specification, application, and control

of the component parts to be used in the system. Numerous criteria and guidelines have been developed for the selection and control of component parts.

The general rule for part selection is that wherever possible standard parts should be used. Standard parts have become the subject of Military (MIL) specifications. MIL specifications, which thoroughly delineate a part's substance, form, and operating characteristics, exist or are in preparation for practically every known part type of electronic component.

Wherever possible, the designer should strive to incorporate standard parts in the equipment design, since they have been proven to be more reliable than their nonstandard counterparts and their application in an equipment design helps to minimize logistic support costs.

Even among certain families of standard parts (e.g., semiconductors, microcircuits), some standard parts are preferred over others, usually those standard parts representing the more recent technologies.

The basic equipment specifications such as MIL-E-4158, MIL-E-5400 and MIL-E-16400 provide a listing of specifications, standards and publications to be used in the design and construction of electronic and associated equipment. The parts, materials, and processes covered in these documents are considered "standard" and should be used whenever they are suitable for the applicable equipment specification invoked in the contract. Parts, materials and processes which are considered "standard" must be designated by the procuring activity.

Parts, materials, and processes not covered in the basic equipment specification are considered "nonstandard." Nonstandard parts, materials, and processes should be used sparingly and, when used, should be interchangeable with a standard equivalent and should be as reliable as a standard equivalent. Approval for the use of nonstandard parts must be obtained prior to their use in an equipment. The procedure for obtaining this approval is spelled out in MIL-STD-965.

Table 7.2-1 provides some general ground rules for parts selection and control.

TABLE 7.2-1: GROUND RULES FOR PARTS SELECTION AND CONTROL

a) Determine part type needed to perform the required function and the environment in which it is expected to operate.

b) Determine part criticality.

   o Does part perform critical functions, i.e., safety or mission critical?
   o Does part have limited life?
   o Does part have long procurement lead time?
   o Is the part reliability sensitive?
   o Is the part a high cost item or does it require formal qualification testing?

c) Determine part availability.

   o Is part on a Preferred Part List?
   o Is part a Standard MIL item available from a qualified vendor?
   o What is the part's normal delivery cycle?
   o Will part continue to be available throughout the life of the equipment?
   o Is there an acceptable in-house procurement document on the part?
   o Are there multiple sources available?

d) Estimate expected part stress in its circuit application.

e) Determine reliability level required for the part in its application.

f) Select the appropriate burn-in or other screening methods for improving the part's failure rate (as required).

g) Prepare an accurate and explicit part procurement specification, where necessary. Specifications should include specific screening provisions, as needed, to assure adequate reliability.

h) Determine actual stress level of the part in its intended circuit application. Include failure rate calculation per MIL-HDBK-217.

i) Employ appropriate derating factors consistent with reliability prediction studies.

j) Determine need for nonstandard part and prepare a request for approval as outlined in MIL-STD-965.

An essential element of parts control is the application of quality and screening tests during production in order to improve the reliability of the component parts. Quality tests are those that reduce the number of defective devices from production lines by means of inspection and conventional testing. The screens are those which remove inferior devices and reduce the hazard rate by methods of stress application.

The need for screening tests, the theoretical basis for screening tests, the types of screening tests, and the most effective screening tests for specific classes of components are covered in great detail in Section 11 of this handbook.

7.3 DERATING

Derating can be defined as the operation of an item at less severe stresses than those for which it is rated. In practice, derating can be accomplished by either reducing stresses or by increasing the strength of the part. Selecting a part of greater strength is usually the most practical approach.

Derating is effective because the failure rate of most parts tends to decrease as the applied stress levels are decreased below the rated value. The reverse is also true. The failure rate increases when a part is subjected to higher stresses and temperature. The failure rate model of most parts is stress and temperature dependent.

Electronic parts are prone to premature failure due to thermal (temperature) overstress. MIL-HDBK-217 failure rate data shows that failure rates vary significantly with temperature. Certain parts are more temperature sensitive than others. Decreases in failure rate can be achieved in these cases by reduction of stress (temperature) with adequate thermal design.

Derating of electronic parts and materials (MIL-STD-454 Requirement 18) shall be accomplished as necessary to assure that the required equipment reliability is within specification. Derating procedures vary with different types of parts and their application. Resistors are derated by decreasing the ratio of operating power to rated power. Capacitors are derated by maintaining the applied voltage at a lower value than the voltage for which the part is rated. Semiconductors are derated by keeping the power dissipation below the rated level.

Derating electronic parts involves the use of derating curves. These curves usually relate derating levels to some critical environmental or physical factor or mathematical models which quantify a base failure rate in terms of a stress ratio, temperature, and other parameters related to the part under consideration.

Manufacturers of solid state d... .. .,.. provide useful thermal data, including curves of operating parameters vs. temperature, maximum and minimum storage temperatures, maximum junction operating temperature, and pertinent thermal resistances. Unless specially selected premium parts are specified, deviation from the nominal observed values can be large. Maximum junction operating temperature must be derated by circuit designers with reference to failure rate vs. temperature data, so that the desired reliability is achieved. A common design error is to compute worst case semiconductor junction temperatures and assume that the thermal design is adequate, if the manufacturer's maximum operating junction temperature is not exceeded. While the device may function under such conditions, its reliability, or life, will generally be so low as to be unacceptable. Maximum allowable semiconductor junction temperatures are meaningless unless related to required system reliability. This normally will require considerable derating of the manufacturer's data.

In addition to the requirements of system reliability, maximum junction temperature derating is advisable to provide some margin of analytical error. This allows for nonuniform heating without catastrophic failure and allows for system electrical transients.

Figure 7.3-1 (taken from MIL-HDBK-217) shows a table of base failure rates for a NPN silicon transistor. Figure 7.3-2 is derived from this table of failure rates, showing the relationship between the base failure rate (λ_b) and temperature and stress. The stress ratio, S, is the ratio of the operating electrical stress to rated electrical stress. These figures illustrate a rapid increase in failure rate as electrical stress and temperature increase. Also, a 6 to 1 increase in failure due to low temperature can be obtained (160°C to 40°C stress level) for the NPN silicon transistor at the 10 percent stress ratio.

Since semiconductors as well as most electronic parts are sensitive to temperature, the thermal analysis of any design should accurately provide the ambient temperatures needed for proper application of the part. Of course, lower temperatures produce better reliability but can also produce increased penalties in terms of added loads (or constraints) on controlling the system's environment. The thermal analysis should be part of the design process and included in tradeoff studies covering equipment performance, reliability, weight, volume, environmental control requirements and cost.

As a general rule, derating should not be conservative to the point where costs rise excessively. Neither should the derating criteria be so loose as to render reliable part application ineffective. Optimum derating occurs at or below the point on the stress temperature curve where a rapid increase in failure rate is noted for a small increase in temperature or stress. There is, however, a practical minimum to derating. At some minimum stress level, circuit complexity may be necessarily increased to gain performance, thus offsetting the reliability gain accomplished by derating.

T (°C)	STRESS RATIO(S)									
	.1	.2	.3	.4	.5	.6	.7	.8	.9	1.0
0	.0034	.0041	.0048	.0057	.0067	.0079	.0095	.011	.014	.018
10	.0038	.0046	.0054	.0064	.0075	.0089	.010	.013	.017	.023
20	.0043	.0051	.0060	.0071	.0084	.010	.012	.015	.020	.029
25	.0046	.0054	.0064	.0075	.0089	.010	.013	.017	.023	.033
30	.0048	.0057	.0067	.0079	.0095	.011	.014	.018	.025	
40	.0054	.0064	.0075	.0089	.010	.013	.017	.023	.033	
50	.0060	.0071	.0084	.010	.012	.015	.020	.029		
55	.0064	.0075	.0089	.010	.013	.017	.023	.033		
60	.0067	.0079	.0095	.011	.014	.018	.025			
65	.0071	.0084	.010	.012	.015	.020	.029			
70	.0075	.0089	.010	.013	.017	.023	.033			
75	.0079	.0095	.011	.014	.018	.025				
80	.0084	.010	.012	.015	.020	.029				
85	.0089	.010	.013	.017	.023	.033				
90	.0095	.011	.014	.018	.025					
95	.010	.012	.015	.020	.029					
100	.010	.013	.017	.023	.033					
105	.011	.014	.018	.025						
110	.012	.015	.020	.029						
115	.013	.017	.023	.033						
120	.014	.018	.025							
125	.015	.020	.029							
130	.017	.023	.033							
135	.018	.025								
140	.020	.029								
145	.023	.033								
150	.025									
155	.029									
160	.033									

Example:
6:1 decrease in failure rate due to low temperature at a 10% stress level.

Based on the typical maximum junction temperature of 175° C (fully derated) and 25° C for the maximum temperature at which full rated operation is permitted.

FIGURE 7.3-1: MIL-S-19500 TRANSISTORS, GROUP I, SILICON, NPN BASE FAILURE RATE λ_b IN FAILURES PER 10^6 HOURS
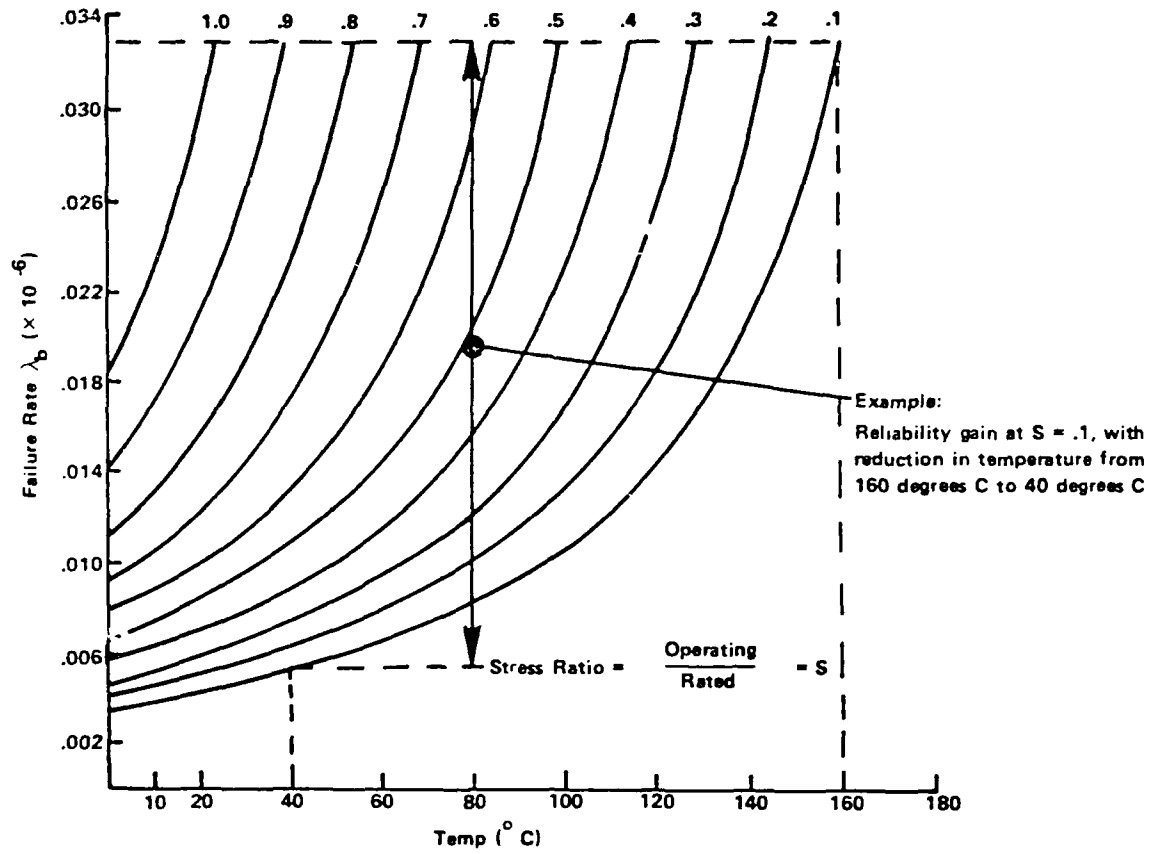
FIGURE 7.3-2: FAILURE RATE/TEMPERATURE RELATIONSHIP FOR GROUP I
TRANSISTOR (SILICON, NPN)

The most comprehensive, up-to-date information on electrical and electronic device derating is contained in Air Force Systems Command Pamphlet 800-27.

For electronic devices, data on failure rates vs. stress is available for a number of parts. This data can be used to determine the reliability improvement through derating. The same is not true of mechanical and structural parts, as can be seen in the following subsection.

7.3.1 DERATING OF MECHANICAL AND STRUCTURAL COMPONENTS

For mechanical and structural components, such failure rate versus stress data may be obtainable from the manufacturer or users, but time rate data may not be available. In using a manufacturer's rating and single design stress values, the design engineer must keep in mind that they are really distributions, not single values. Either the worst case "tolerances" for both stress and strength or a plot of the distributions must be utilized. When there is time dependency for the distributions (e.g., degradation, wear out), the stress and strength distributions must be related to the cyclic or time operation in the intended environment.

The classical approach to mechanical and structural design is to give every part enough strength to handle the worst stress it will encounter. Several references, such as MIL-HDBK-5 are available, providing data on the strength of materials. Some of these provide limited data on strength degradation with time, resulting from fatigue. Effective design procedures should provide for evaluating alternative configurations with respect to reliability. Since failure is not always related to time, the designer needs techniques for comparing stress vs. strength, and determining the quantitative reliability measure of the design. The traditional use of safety factors and safety margins is inadequate for providing a reliability measure of design integrity.

The concept of stress strength in design recognizes the reality that loads or stresses and strengths of particular items subjected to these stresses cannot be identified as a specific value but have ranges of values with a probability of occurrence associated with each value in the range. The ranges of values (variables) may be described witn appropriate statistical distributions for the item. Stress/strength design requires knowledge of these distributions. After the strength and stress distributions are determined, a probabilistic approach can be used to calculate the quantitative reliability measure of the design, including confidence limits.

To illustrate the concept of stress and strength distributions related to reliable design, assume that a large number of tests of the strength of a given manufactured item have been run, with each test being run to failure. A relationship (frequency distribution) between the number failing at any particular value of strength (or band of values) and the value can be determined. Figure 7.3.1-1(a) shows a generalized frequency distribution of the results. If the exact relationship were known, the probability of a randomly selected specimen failing at a
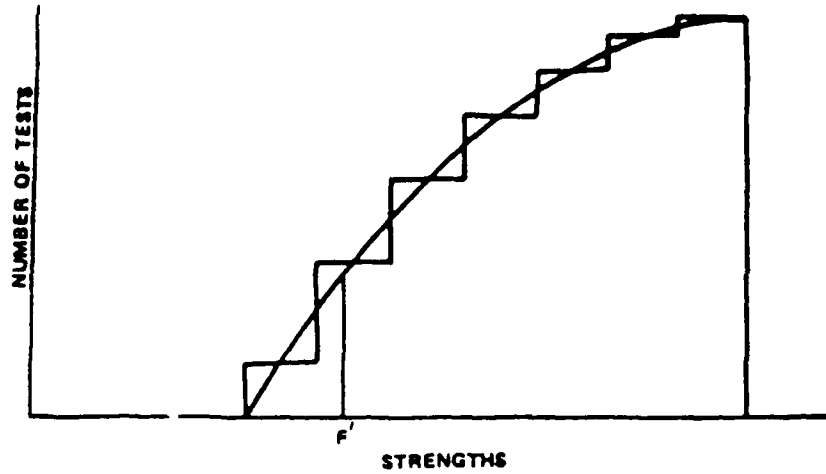
a) Strength Frequency Distribution

b) Stress Frequency Distribution
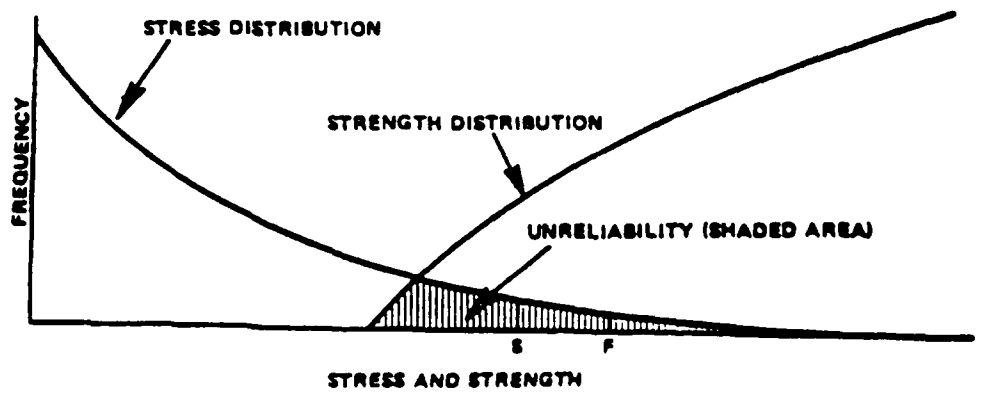
c) Probability of Stress Exceeding Strength

FIGURE 7.3.1-1: STRESS-STRENGTH DISTRIBUTIONS AND UNRELIABILITY IN DESIGN

particular value of stress F' could be predicted. It would be that fraction of the population, whose strength was equal to or less than a stress F'. Similarly if a large number of experiments were conducted, and the stress was recorded on each experiment, a relationship between the relative frequency of stresses and the stress can be established. This relationship is shown in Figure 7.3.1-1(b). If the exact relationship were known, the probability that on any randomly selected trial the stress would exceed a strength S' could be predicted. This would be the fraction of the population (of possible trials) in which the stress exceeded the strength S'. With both of these distributions defined, unreliability is determined as the probability that the stress is greater than the strength. Unreliability can be determined analytically, graphically, by numerical integration or by probabilistic techniques such as "Monte Carlo" provided the form or shape of the two probability distribution functions are known. The curves from Figure 7.3.1-1(a) and 7.3.1-1(b) are combined in Figure 7.3.1-1(c) to illustrate the region of the unreliability given by the shaded area where stress exceeds strength. Figure 7.3.1-2 illustrates normal (gaussian) stress and strength distributions, where the stress and strength variables are identified as Kips (a thousand pounds).

Looking at Figure 7.3.1-2, two things may happen with time and repeated stress. The variance of the strength distribution may change; for example the curve may extend from 13 to 23 Kips rather than the original 16 to 20 Kips. This would result in an increased unreliability since the shaded area would now extend from 13 to 20 Kips. This is shown in Figure 7.3.1-3(a). The other factor that could change with time and stress is that the mean of the strength distribution might be lowered, to say 15 Kips. This, in turn, would result in a decreased reliability as shown by the shaded area of Figure 7.3.1-3(b).

The purpose of stress strength analysis is to improve the reliability of the design. That is, to find the optimum comparison of stress and strength that will have an acceptable probability of success and compete favorably with other contraints such as weight, cost, availability of material.

There are four basic procedures the designer may use to increase reliability.

(1) Increase Average Strength. This approach is tolerable if size and weight increases can be accepted or if a stronger material is available.

(2) Decrease Average Stress. Occasionally the average stress on a component can be reduced without greatly affecting its capability.

(3) Decrease Stress Variation. The variation in stress is usually hard to control. However, the stress distribution can be effectively truncated by putting limitations on use conditions.

(4) Decrease Strength Variation. The inherent part-to-part variation in strength can be reduced by improving the basic process, holding tighter control over the process, or by utilizing tests to eliminate the less desirable parts.
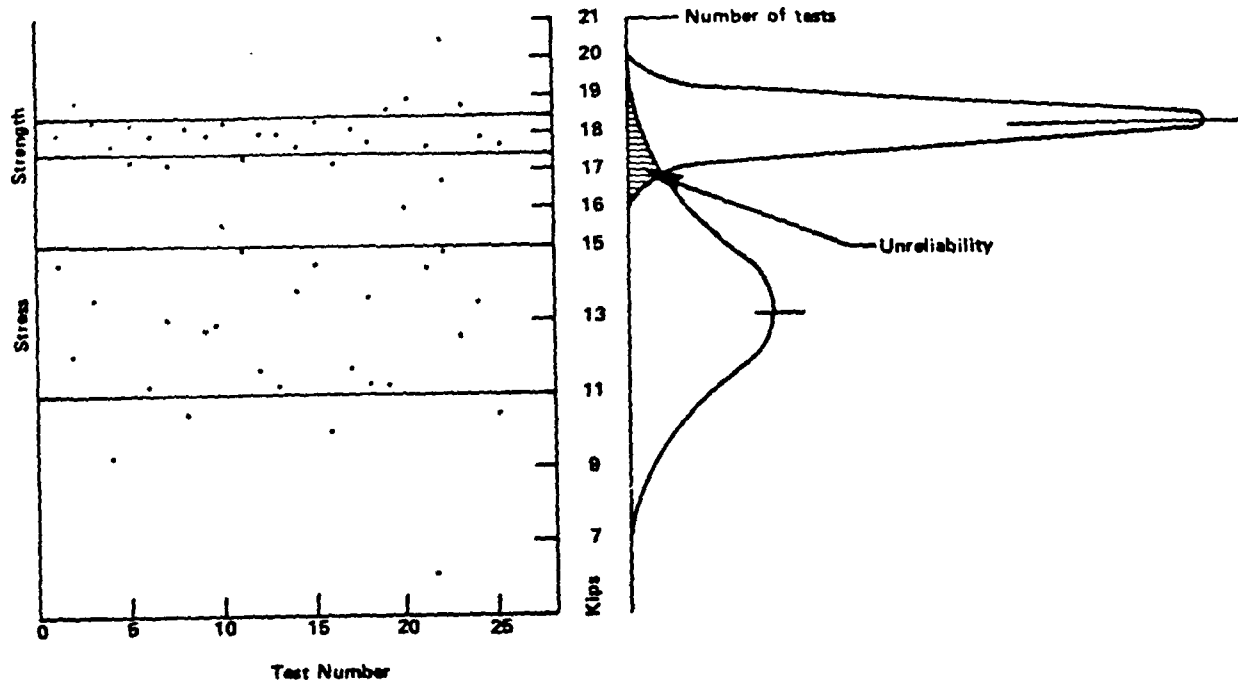
FIGURE 7.3.1-2: <u>NORMAL (GAUSSIAN) STRESS-STRENGTH DISTRIBUTIONS</u>
<u>AND UNRELIABILITY IN DESIGN</u>
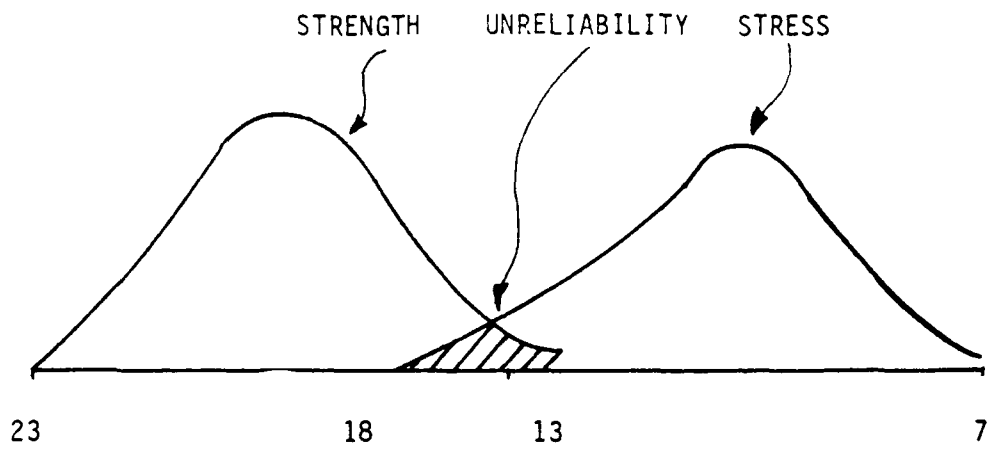
(a) RESULT OF INCREASE OF VARIANCE IN STRENGTH WITH TIME & STRESS
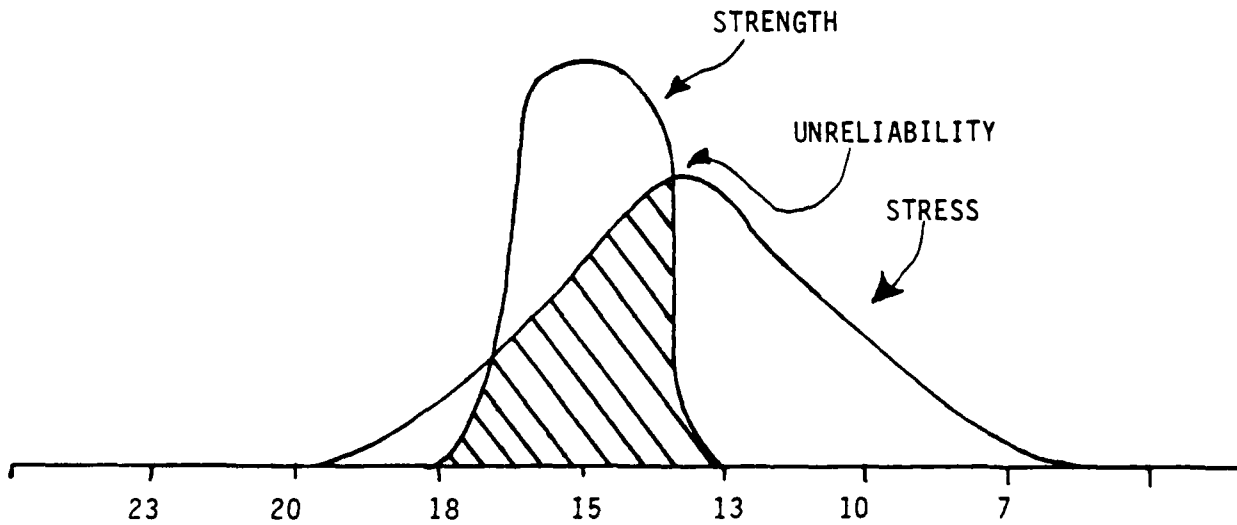
(b) RESULT IN DECREASE IN STRENGTH WITH TIME & STRESS

FIGURE 7.3.1-3

Factors Effecting Unreliability

References 2, 3 and 4 provide more details on this procedure and its application to mechanical and structural components.

7.4 RELIABLE CIRCUIT DESIGN

7.4.1 INTRODUCTION

This section cannot possibly cover all of the aspects of circuit design. In addition to a number of design textbooks, there are handbooks available (e.g., Refs. 5, 6) which can be used to solve almost any circuit design problem. Reference 6 is highly recommended since it concentrates on a unified approach to the design of reliable transistor circuits.

The only thing that this section can accomplish in the limited space available is to outline some of the circuit design methods available to ensure high reliability. They are by no means comprehensive; circuit designers should consult their own organizations' design rules, component application notes, the cited references and other relevant sources. The methods outlined in this section are intended as a guide to the points which reliability engineers and circuit designers need to consider.

In order to produce a reliable circuit design, the designer must consider the following reliability design criteria:

    (1)   component derating (discussed in the previous section)
    (2)   design simplification
    (3)   use of standard parts and circuits
    (4)   transient and overstress protection
    (5)   parameter degradation and analysis
    (6)   minimizing design errors
    (7)   fundamental design limitations

Except for component derating, which was discussed in the previous section, the following paragraphs discuss each of the above mentioned critiera.

7.4.2 DESIGN SIMPLIFICATION

Since reliability is a function of complexity (as was shown in Section 5), anything that can be done to reduce complexity will, as a rule, increase reliability. Put simply, if a component part can be eliminated from the design, the effects of its failure have been eliminated. Design simplification may be inherent in the design process (and practiced). However, it may not be a planned and deliberate procedure for improvement and achievement of optimal reliability. During design reviews (Section 7.11), attention should be directed towards a determination that all items and circuits are required in order to perform the intended function(s), i.e., design simplicity. Design simplicity contributes to optimal reliability by making system success dependent on fewer components and the resultant decrease in potential of failures. Caution must be exercised to insure that: (1) higher stresses or unusual performance requirements are not

imposed on the remaining components; and (2) the designer, in his zeal to use a single part to perform multiple functions, may replace proven, reliable parts with unproven, untried parts.

One example of simplification is the simplification of logic functions by the use of Boolean algebra techniques. This way, unnecessary terms are identified and removed. Boolean reduction, a minimization technique, is a well established tool for incorporating reliability into design through simplification. With this minimization technique, superfluous elements can be eliminated from a logic design where improved reliability is a criteria of the minimization (simplification).

As an example, consider the logic design shown in Figure 7.4.2-1. The corresponding Boolean expression for this design is:

$$E = A\bar{B} + C + \bar{A}\bar{C}D + B\bar{C}D \qquad (7.1)$$

By using the Boolean relationships*

(1) $A + \bar{A}B = A + B$
(2) $AB + AC = A(B+C)$
(3) $\overline{AB} = \bar{A} + \bar{B}$

the original expression can be reduced to

$$E = A\bar{B} + C + D \qquad (7.2)$$

as follows:

Applying relationship (1) to the last three terms, we find

$$E = A\bar{B} + C + \bar{A}D + BD$$

Rearranging and applying relationships (2) and (3)

$$E = A\bar{B} + C + D(\bar{A} + B)$$
$$= A\bar{B} + C + D\ (\overline{A\bar{B}})$$

And applying relationship (1) again

$$E = A\bar{B} + C + D$$

the resultant logic diagram for Eq (7.2) is shown in Figure 7.4.2-2.

Note that by simplification the number of inverters was reduced from 3 to 1, the number of "AND" gates from 3 to 1, and the number of "OR" gates from 2 to 1, not to mention the reduction in the number of circuit connectors. Also eliminated is a potential signal delay problem that might occur with signals reading and passing through the superfluous components.

*Basic relationships which can be found in texts on Boolean Algebra techniques.
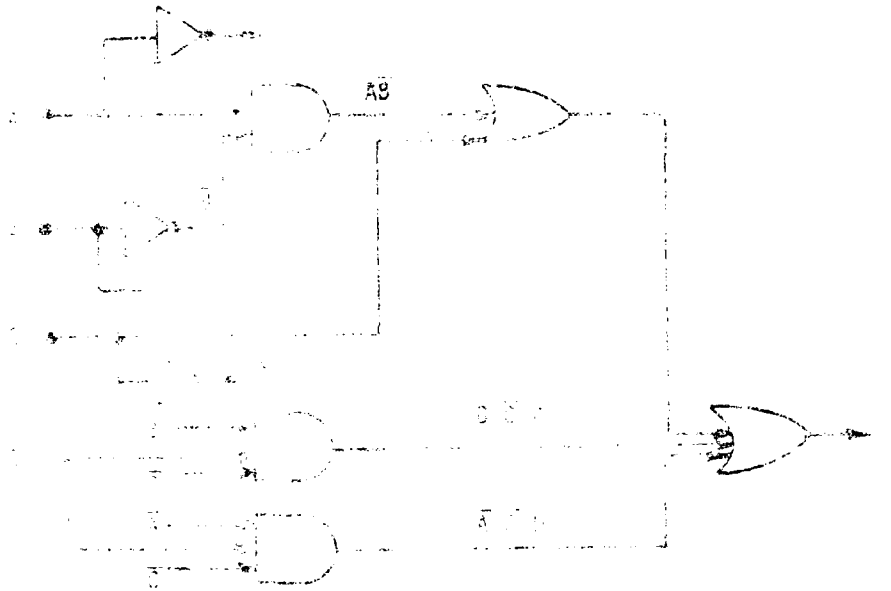
LOGIC REPRESENTATION OF
E = AB + C + D
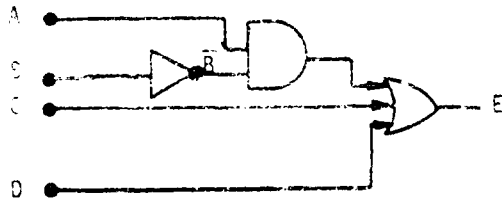
FIGURE 7.4.2-2:   LOGIC REPRESENTATION OF
E = AB + C + D

LEGEND

= "AND" Logical Gate

= "OR" Logical Gate

= Logical Inverter

A, B, C, D = Inputs

$\overline{A}, \overline{B}, \overline{C}, \overline{D}$ = Inversions of Inputs

E = Output

Another example is represented by Figure 7.4.2-3. The original logic diagram is represented by this figure and the corresponding Boolean expression is:

$$D = \bar{C} (A + \bar{B}) + \bar{A} (\bar{B} + C) + B (A + C) \qquad (1)$$

Two equivalent reductions are found for this equation. The sum-of-products form

$$D = \bar{A} \bar{B} + A \bar{C} + B C \text{ or } D = \bar{B}\bar{C} + \bar{A}C + AB \qquad (2)$$

is the basis for Figure 7.4.2-3(b), which is simpler than Figure 7.4.2-3(a). Still simpler is the product-of-sums form of reduction

$$D = (A + \bar{B} + C) (\bar{A} + B + \bar{C}) \qquad (3)$$

which is shown in Figure 7.4.2-3(c).

Design results can be written to assist in minimizing component types, by constraining designers to preferred standard approaches. Component type reduction should also be made an objective of design review, particularly of initial designs, before prototypes are made or drawings frozen for production.

7.4.3 USE OF STANDARD COMPONENTS AND CIRCUITS

As was mentioned in Section 7.4.3, designers of military electronic systems should use standard components produced in accordance with the appropriate military specifications and taken from preferred parts lists. Numerous studies have shown that the use of standard components results in the most reliable equipment design. The term "component" today includes rather complex circuit elements, e.g., microprocessors. In fact, they are complete circuits in themselves, and one might argue that, except for high power and high frequency applications, the systems of tomorrow will be designed using standard circuits as the basic building blocks.

Design reliability can be improved by the use of proven circuits with known reliability. Information is available concerning reliability of many unit configurations and circuits. There are electronic design handbooks available, for example, illustrating standard circuitry which should be used in preference to unique designs. Just as with electronic designs, proven mechanical and fluid system design concepts can be categorized and proven configuration given first preference. In some instances the preferred circuit may be modified to meet the specific requirements of the equipment. Reference 75 should be considered in the design of electronic equipment.

(a) LOGIC DIAGRAM FOR
    EQUATION 1
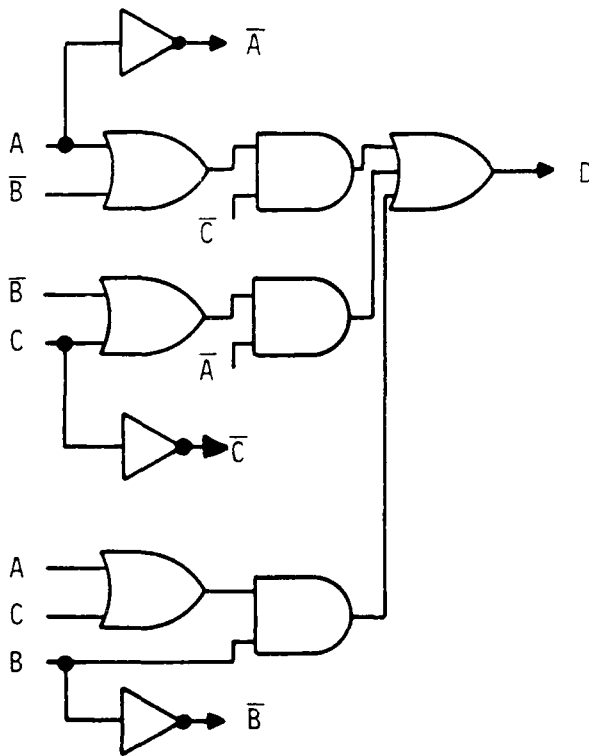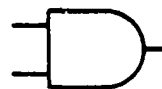
(b) LOGIC DIAGRAM FOR
    EQUATION 2
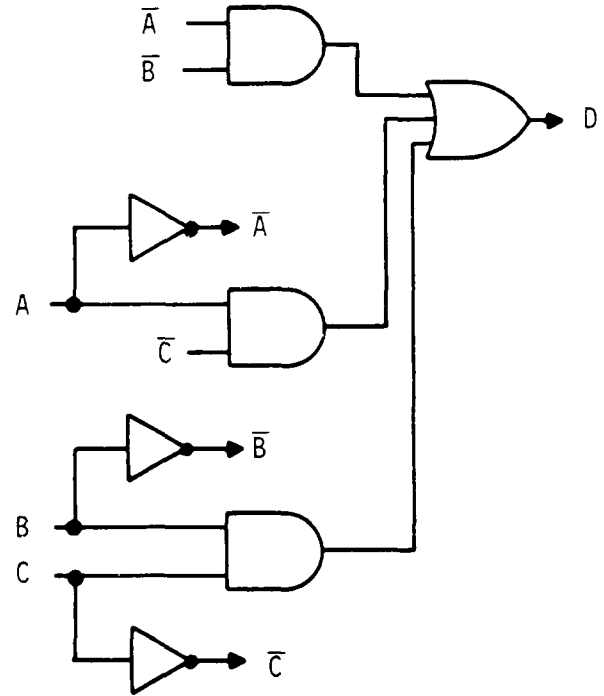
(c) LOGIC DIAGRAM FOR
    EQUATION 3
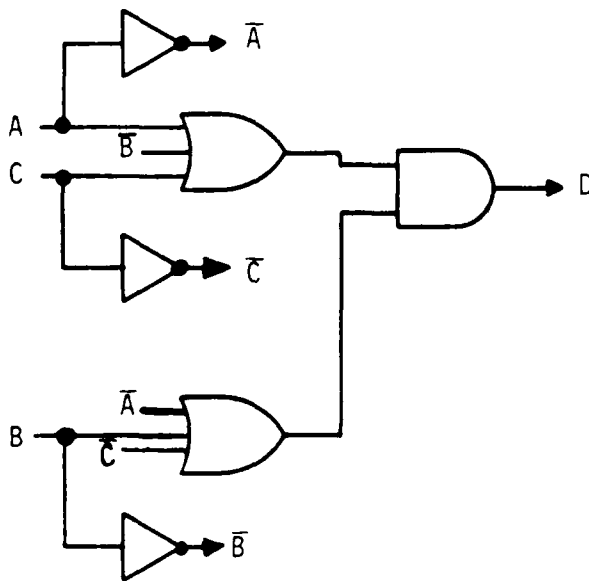
LEGEND

= "AND" Logical Gate

= "OR" Logical Gate

= Logical Inverter

A, B, C   = Inputs

$\overline{A}$, $\overline{B}$, $\overline{C}$ = Inversions of Inputs

D   = Output

FIGURE 7.4.2-3: BOOLEAN REDUCTION OF LOGIC ELEMENTS

Additionally, benefits in design reliability can be realized if a contractor's in-house organization collects and utilizes reliability and parts data to maintain a file of preferred circuits with proven performance and reliability for use by their design organizations.

The Navy Standard Electronic Modules (SEM) Program (MIL-M-28787) is intended to provide circuit module standardization. SEM usage can reduce design and fabrication time and provide proven reliability. These modules were developed to be cost effective in level of repair decisions to discard rather than repair at failure. The use of these standard functional modules may require tradeoffs where volumetric (volume, weight) penalties are primary concerns of the item in design. In some cases, the size and weight limitations may be acceptable, such as in ground support and test equipment or larger aircraft. In others, the weight size penalties may be best met by resorting to custom designed circuit modules. MIL-M-28787 provides a range of highly reliable standard modules, designed to reduce logistic costs.

7.4.4 TRANSIENT AND OVERSTRESS PROTECTION

Electronic components are often prone to damage by short duration voltage transients, caused by switching of loads, capacitive or inductive effects, static electricity, power supply ripple, testing, etc. Small semiconductor components are particularly vulnerable, owing to the very low thermal inertia of their wire bonds. MOS devices are very vulnerable to static electricity, and require special protection.

The subject of electrostatic discharge (ESD) is treated very thoroughly in other sources, and will only be summarized here. It is becoming an increasingly important and recognizable problem with the trend toward the development of integrated circuits of greater complexity and higher component densities. Some of today's microcircuits can be damaged by ESD voltages as low as 20 volts. The smaller the part, the less power it can dissipate or the lower the breakdown voltage, and the more likely it is to be damaged by an electrostatic discharge (ESD). Certain parts are considered highly susceptible and their chances for damage are great. These include metal oxide semiconductor (MOS) parts with a direct access to the MOS junction, high frequency parts produced by the Schottky barrier process, many bipolar and field-effect microcircuits like RAMs, ROMs, and PROMs utilizing small active area junctions, thin dielectrics, metalization crossovers, and N+ guard ring structures, precision film resistors and similar parts. A detailed list of electrostatic discharge sensitive (ESDS) parts and their voltage sensitivity ranges are provided in DOD-STD-1686 and DOD-HDBK-263. They also describe control programs that can be applied to minimize component failures due to ESD.

In addition to ESD, the designer must cope with the other causes of transient generation described in the first paragraph.

Semiconductor device circuit malfunctions can arise from two general sources: (1) transient circuit disturbances and (2) component burnout. Generally, transient upsets are the controlling factors, because they can occur at much lower energy levels.

Transients in circuits can prove troublesome in many ways. Flip-flop and Schmitt triggers can be inadvertently triggered, counters can change count, memory can be altered due to driving current or direct magnetic field effect, one-shot multivibrators can pulse, the transient can be amplified and interpreted as a control signal, switches can change state, semiconductors can latch-up, requiring reset, etc. The effect can be caused by transients at the input terminals, output terminals, on the supply terminals, or on combinations of these. Transient upset effects can be generally characterized as follows:

(1) Circuit threshold regions for upset are very narrow. That is, there is a very small amount of voltage amplitude difference between signals which have no probability of causing upset and signals which will certainly cause upset.

(2) The dc threshold for response to a very slow input swing is calculable from the basic circuit schematic. This can establish an accurate bound for transients that exceed the dc threshold for times longer than the circuit propagation delay (a manufacturer's specification).

(3) Transient upsets are remarkably independent of the exact wave-shape, and depend largely on the peak value of the transient and the time duration over which the transient exceeds the dc threshold. This waveform independence allows relatively easy experimental determination of circuit behavior with simple waveforms (square pulse).

(4) The input leads (or signal reference leads) are generally the ones most susceptible to transient upset.

Logic devices which interface with inductive or capacitive loads, or which "see" test connections, require transient voltage protection. This can be provided by: a _capacitor_ between the voltage line to be protected and ground to absorb high frequency transients, _diode protection_ to prevent voltages from rising beyond a fixed value (clamping) and _series resistances_ to limit current values.

The transient voltage levels which can cause failure of semiconductor devices are referred to as VZAP. VZAP values depend upon transient duration. Passive devices can also be damaged by transient voltages, but the energy levels required are much higher than for small semiconductor devices. Therefore, passive devices do not normally need individual protection.

There are many techniques available for transient suppression in semiconductor devices and circuits. Some of these are illustrated in Figures 7.4.4-1 through 7.4.4-6 and apply in the following areas:

(1) Transistors
(2) Silicon Controlled Rectifiers (SCRs)
(3) CMOS
(4) TTL Protection
(5) Diode Protection

These techniques are representative of generally applicable methods and are not intended as an exhaustive list.

7.4.5 PARAMETER DEGRADATION AND ANALYSIS

Part parameters (e.g., operating characteristics, values) are known to change with time under aging effects and stress. Part parameter changes can have a harmful effect on circuit performance and must be recognized as a significant cause of system failure.

Failure rate data which appears in MIL-HDBK-217 is not based on part changes due to aging. Parts such as resistors and capacitors are, however, known to change with age and stress so that degradation due to aging can result in out-of-tolerance failures of a system. As a result of gradual parameter changes due to aging, a point in time is reached where the collective effect of parameter changes causes system performance to be unacceptable.

In quantity manufacturing all parts characteristics have statistical distributions. Characteristics (e.g., resistance) have a nominal or mean value and a variance above and below it. The extreme values of the variance are called "tolerances." The part distributions are basically affected by the manufacturing lot, and by techniques for selection of close tolerance parts out of wide tolerance lots.

In addition to manufacturing distributions, there are distributions of each characteristic resulting from environment (temperature, etc.) stress (pressure voltage, etc.), and time (cold flow, drift, aging, etc.). Such distributions or tolerances must be added to the manufacturing distributions or tolerances in order to determine the real operational distribution.

The design process must ensure that the distributions cr tolerances cannot combine in such a way as to interfere with the intended function. In a circuit, mechanism, or structure it is necessary to consider the overall effect of the expected range of manufacturing tolerance, operational environment, stresses, and the effect of time. The item design, therefore, should operate satisfactorily at the parameter extremes of its associated parts.

Several examples of part parameter changes are shown in Figures 7.4.5-1 and 7.4.5-2. These figures show the average change from initial value vs. time, and the standard deviation of change from initial value vs.

(A) Current Limiting Resistor (R_B) And Transient Suppression Capacitor (C_1)

(B) Low Gain Filter (R_B, C_B) And Transient Suppression Capacitor (C_1)

(C) Transient Limiter (R_B, D_1, D_Z) And Transient Suppression Capacitor (C_1)

(D) Transient Suppression For Base And Collector (R_B, D_{Z1}, D_{Z2})

(E) Reverse And Forward Transient Limiter (R_B, D_{Z1}, D_{Z2}) And Transient Capacitor

(F) Complete Transient Protection (R_B, D_1, D_2, D_Z, C_1)
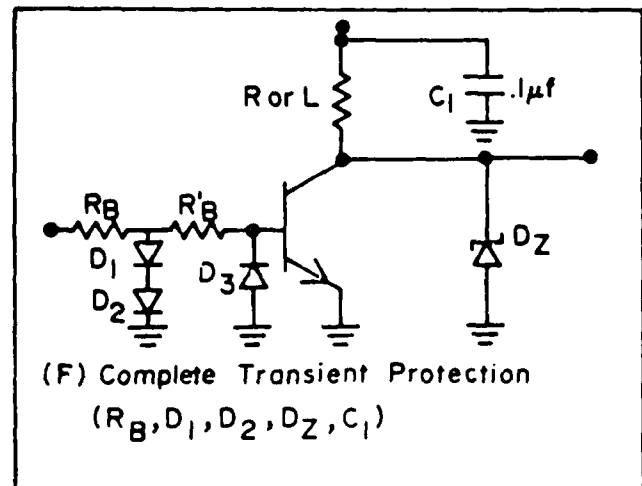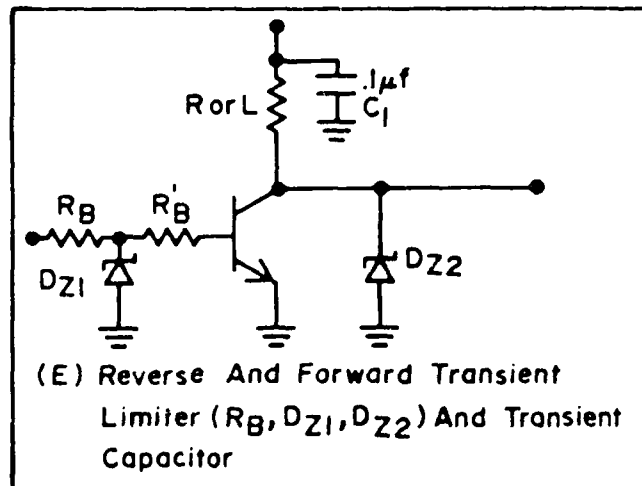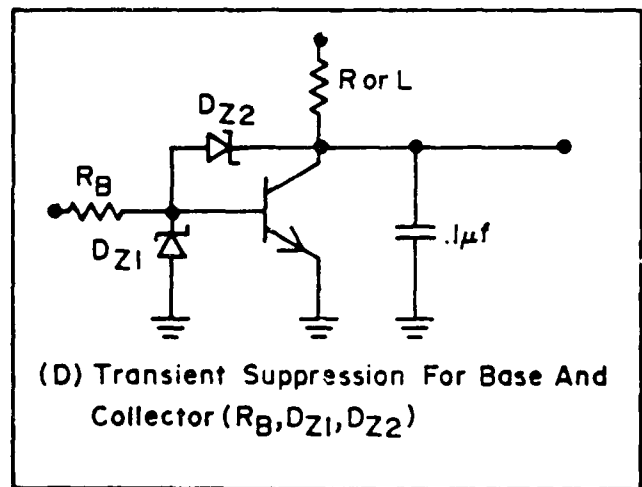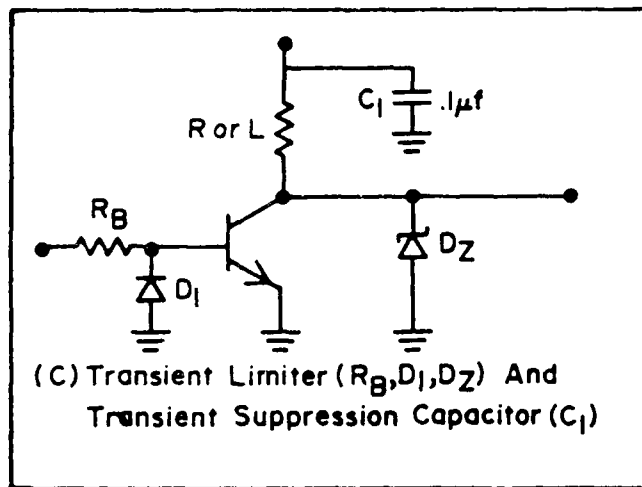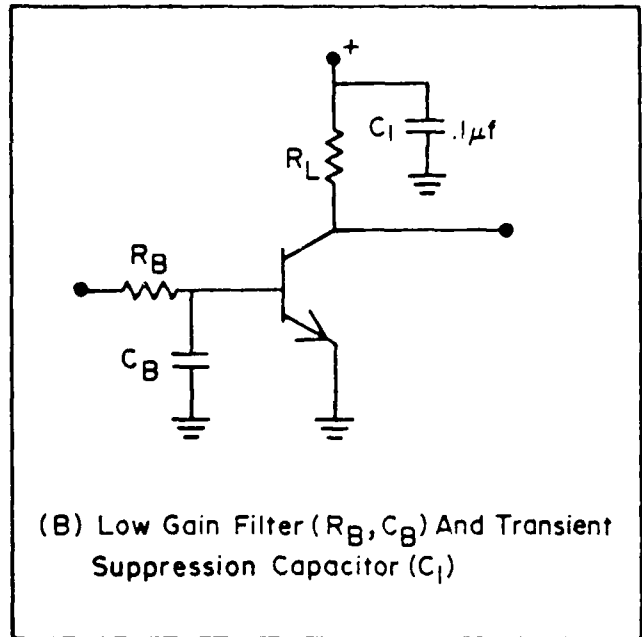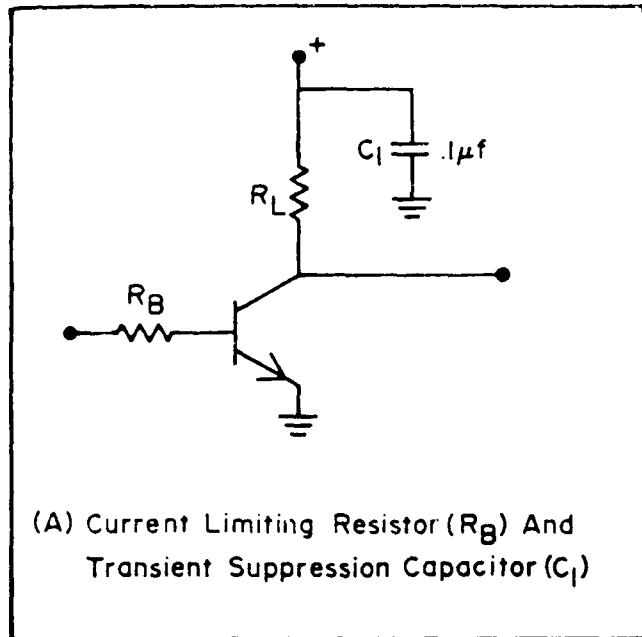
FIGURE 7.4.4-1: <u>TRANSISTOR PROTECTION</u>
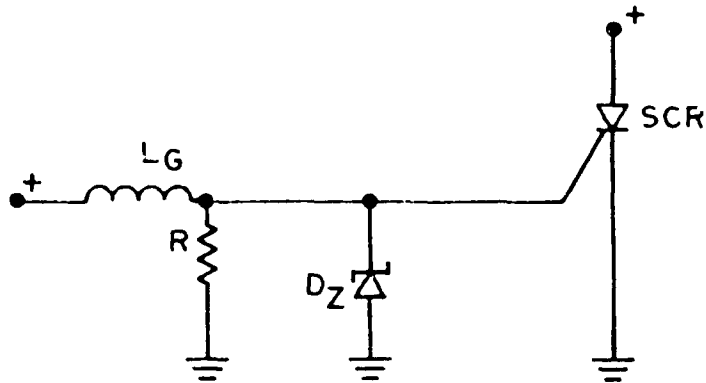
(A) Integrator (Lg,R) Serves To Limit The Initial Surge Current When The Gate Is Turned On. Diode Dz Protects Against Voltage Transients. The PIV of the SCR Should Be Chosen To Provide Sufficient Anode To Cathode Protection.
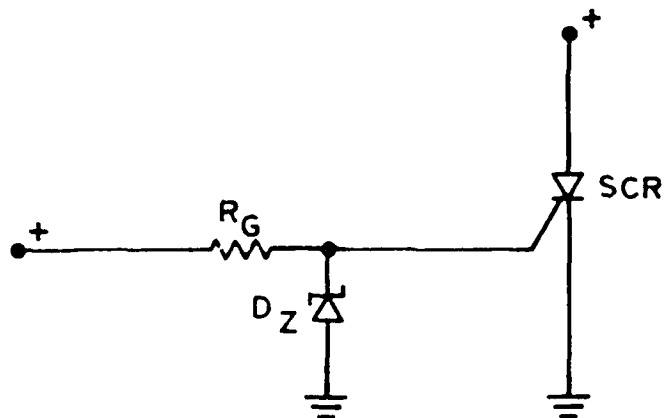
(B) Resistor R_G Limits The Gate Current Of The SCR and Diode Dz Protects The Gate Against Voltage Transients

FIGURE 7.4.4-2: SCR PROTECTION
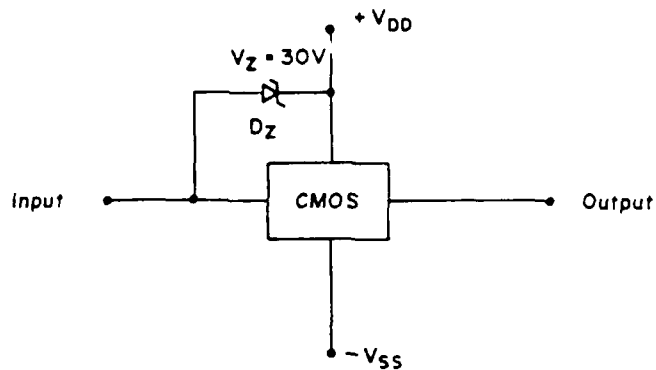
a) Single Diode Clamps Positive Input Voltage To V_{DD} And Negative Input Voltages To $V_{DD} - 30$ Volts Thus Preventing Gate Breakdown.
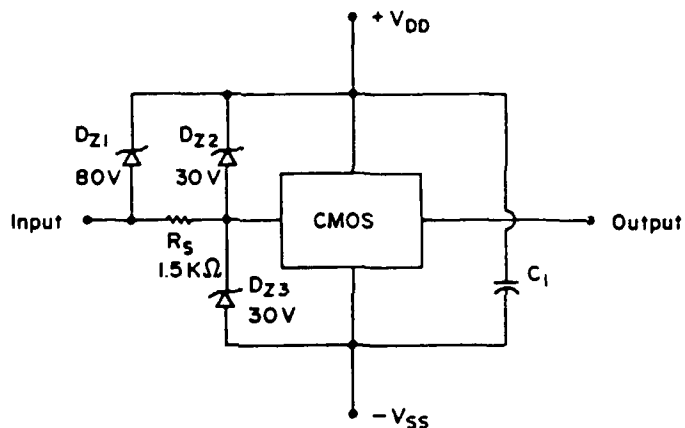
b) Diode D_{Z2} And D_{Z3} Clamps Positive Input To V_{DD} And Negative Input To V_{SS} Diode D_{Z1} And R_S Provide Time Delay And Current Limit Action. Capacitor C_1 Prevents High Frequency Transient From Entering The Device Through The Power Supply.

FIGURE 7.4.4-3: CMOS PROTECTION

a) Store Unused Devices In Conductive Foam Or Use Any Method That Shorts All Leads Together.

b) Use Grounded Soldering Iron.

c) Ground All Test Equipment.

d) All Unused Device Inputs Should Be Connected To V_{DD} Or V_{SS}.

e) All Low Impedance Equipment Should Be Disconnected From Device Inputs Before DC Power Supplies Are Turned Off.

FIGURE 7.4.4-4: CMOS HANDLING PRECAUTIONS
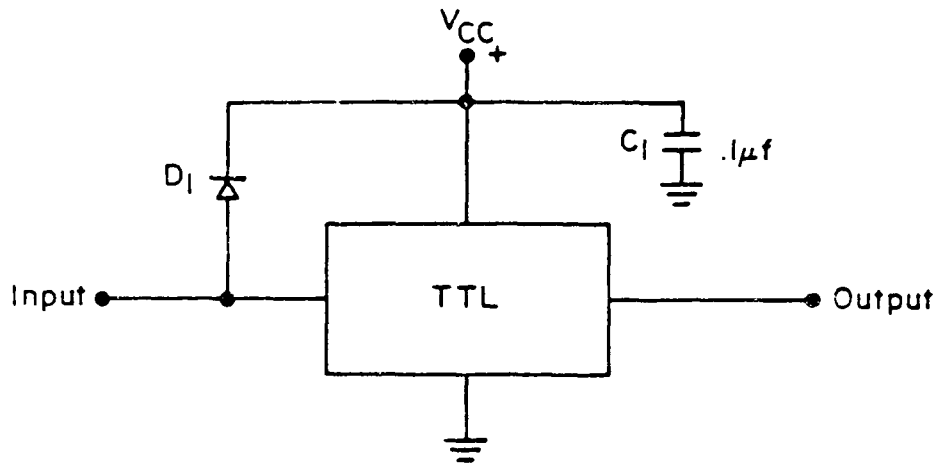
(A) Diode D_1 prevents Input From Becoming Greater Than V_{CC} And Capacitor C_1 Absorbs High Frequency Transients On The Power Supply Line
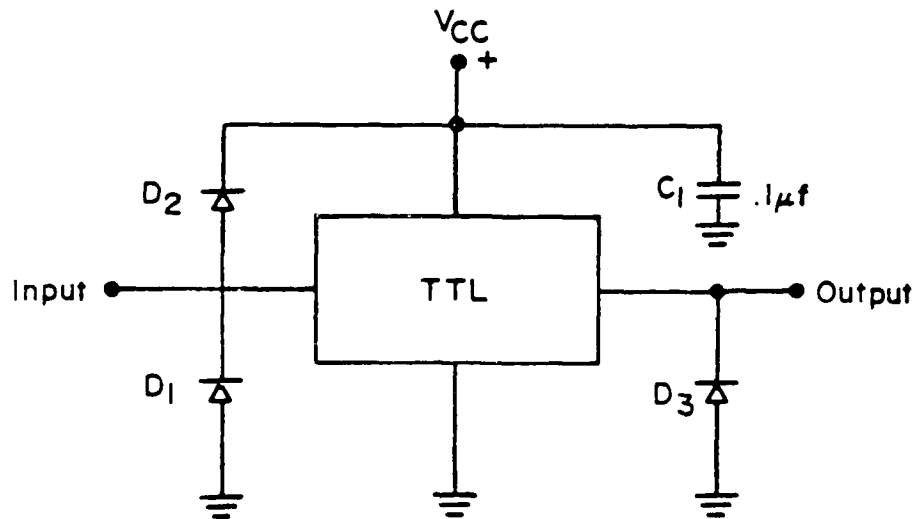
(B) Diodes D_1 And D_2 Clamp The Positive Input To V_{CC} And The Negative Input To Ground. Diode D_3 Prevents The Output From Going Below Ground. C_1 Absorbs High Frequency Transients On The Power Supply Line.

FIGURE 7.4.4-5: TTL PROTECTION

(A) Surge Current Limit Resistor (R_l)

(B) Surge Current Limit Resistor (R_l) and Transient Suppression Capacitor (C_l)
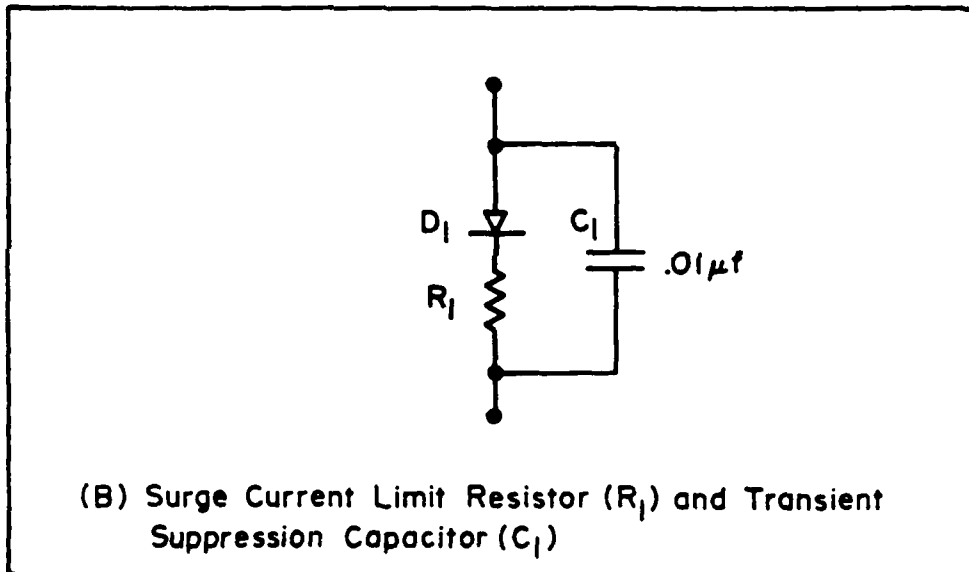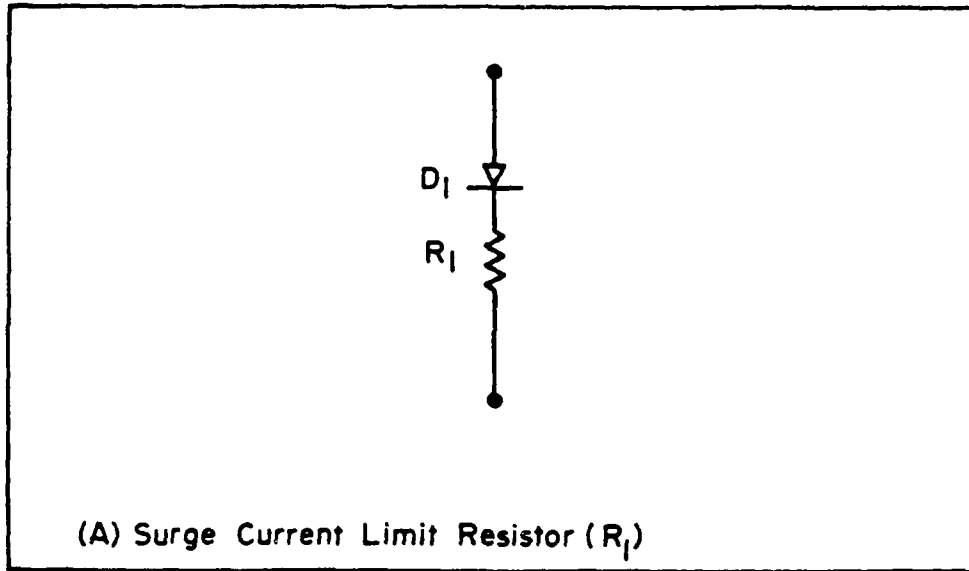
Note: The Best Protection For A Diode Is Sufficient Overrating Of The Reverse Breakdown Voltage (PIV), Forward Surge Current (I_s) And Power Dissipation Capability (P)

FIGURE 7.4.4-6: <u>DIODE PROTECTION</u>
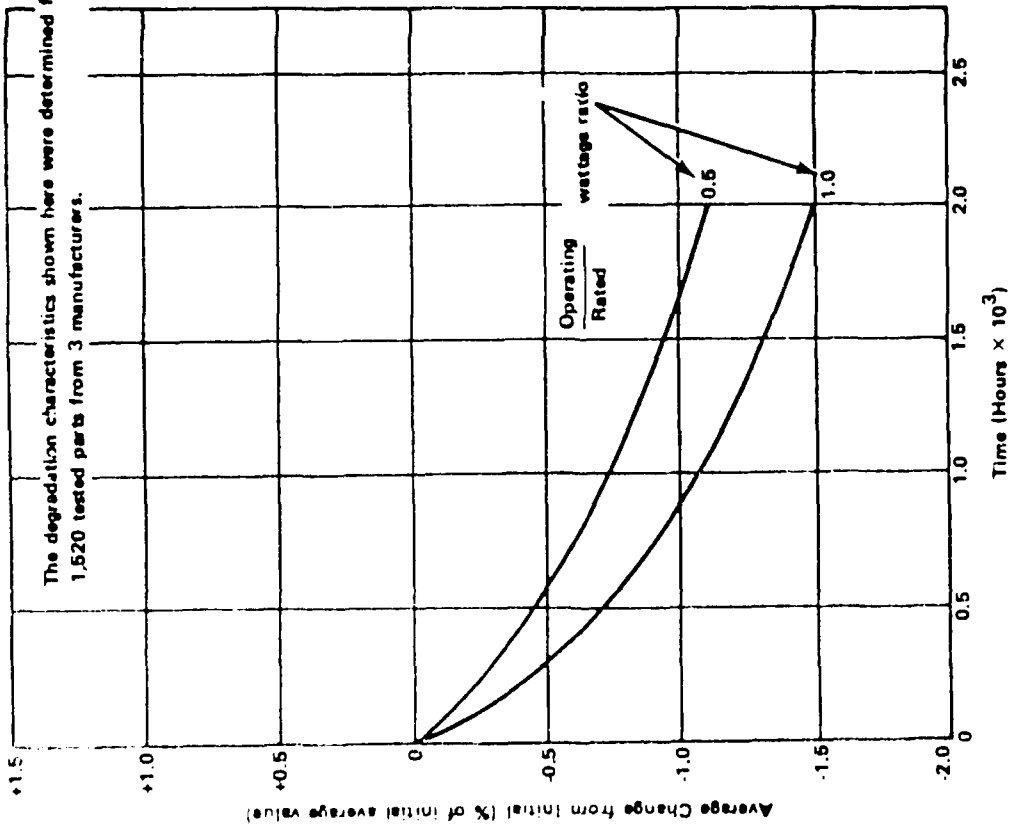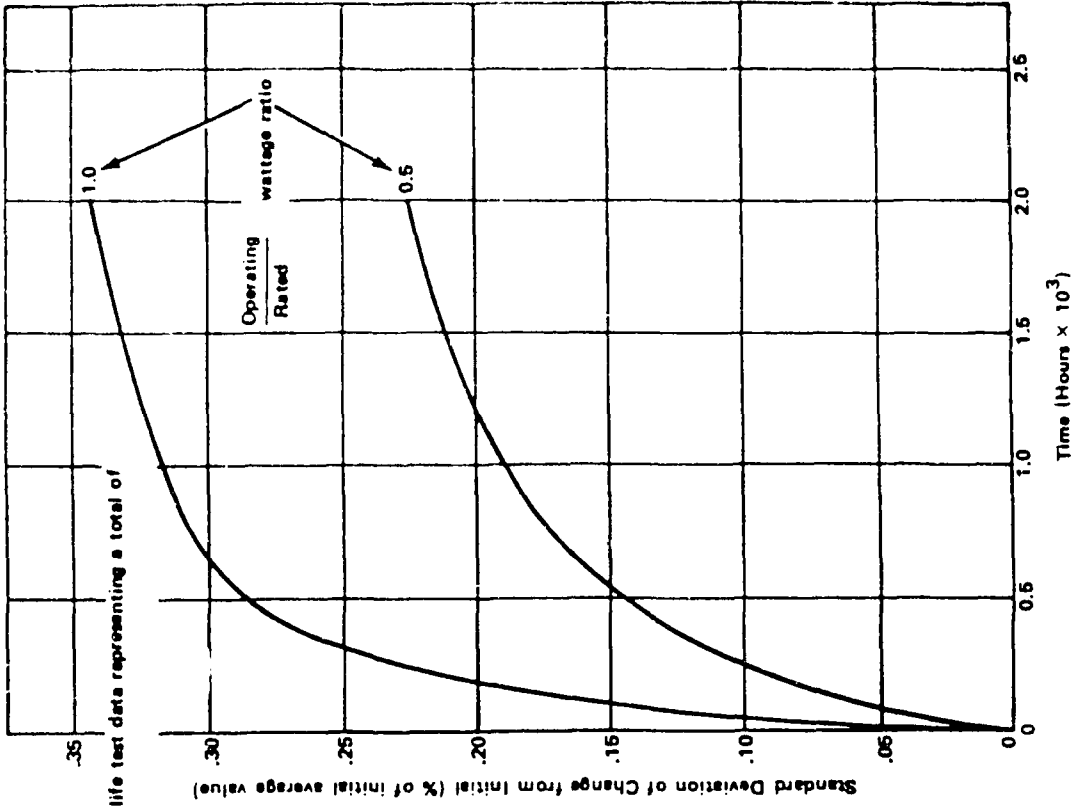
FIGURE 7.4.5-1: RESISTOR PARAMETER CHANGE WITH TIME (TYPICAL)
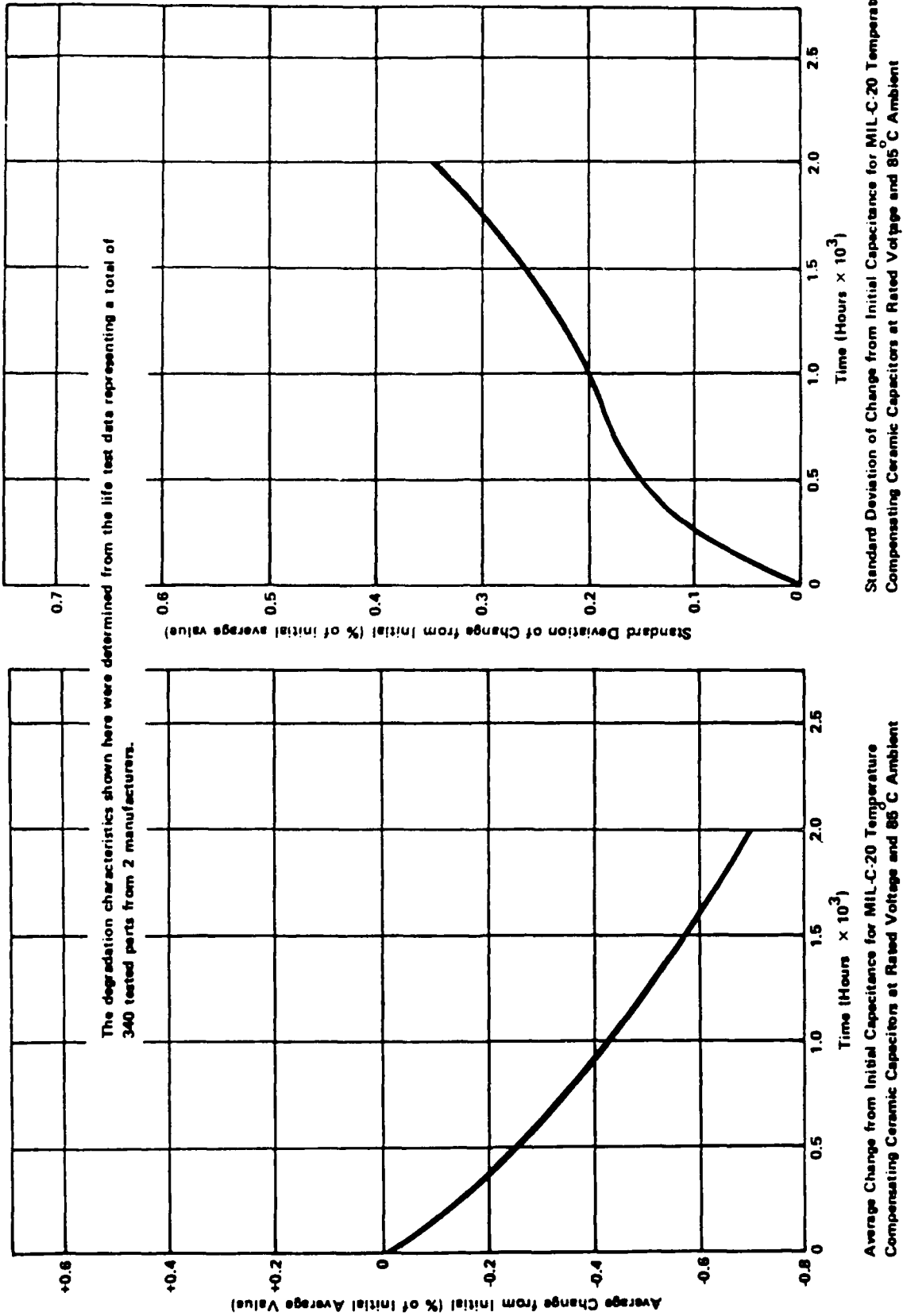
FIGURE 7.4.5-2: CAPACITOR PARAMETER CHANGE WITH TIME (TYPICAL)

The degradation characteristics shown here were determined from the life test data representing a total of 340 tested parts from 2 manufacturers.

Average Change from Initial Capacitance for MIL-C-20 Temperature Compensating Ceramic Capacitors at Rated Voltage and 85°C Ambient

Standard Deviation of Change from Initial Capacitance for MIL-C-20 Temperature Compensating Ceramic Capacitors at Rated Voltage and 85°C Ambient

time for the resistance of a particular resistor type. They also show
the change in capacitance of a particular capacitor type. The resistor
data is plotted for two stress levels, while the capacitor data is
plotted at rated voltage. Another type of presentation (Figure 7.4.5-3)
shows the initial tolerance and nominal value for a parameter and then
plots the change in these parameters under one specified stress and
temperature condition for a period of time.

There are two approaches utilized to overcome degradation problems.
These are:

(1) To control device and material parameter changes to hold them
     within specified limits for a specified time under specified
     conditions

(2) To design circuits and systems sufficiently tolerant of device
     and material parameter changes so that they accomodate antici-
     pated drifts and degradations with time.

In the first approach, it is necessary to control not only the parameter
value specified, but also to control its life history. Screening, such
as burn-in or preconditioning, can be used to eliminate or reduce a mode
of change in a part parameter. This screening produces more stability
in the part parameter, so that there is less chance of failure of the
item where it is used, due to part parameter changes.

Parameter change control thus requires detailed testing and control of
materials going into parts. It requires strict control of processes,
proven designs, and device testing to obtain valid parameter change data
over the useful life of the parts. Both parameter value distribution
for a single part and for a quantity of parts (population), related to
changes in time and stress severity must be considered.

The second approach is to design circuits which are tolerant of part
parameter changes. Two different techniques for tolerant circuit design
are the use of feedback to electrically compensate for parameter
variation and thus provide for performance stability; and the design of
circuitry that provides the minimum required performance, even though
the performance may vary somewhat due to aging. The latter approach
makes use of analyses procedures such as:

(1) Worst case analysis

(2) Parameter variation

(3) Moment

(4) Monte Carlo

A comparison of these methods is shown in Table 7.4.5-1; they are
described in detail, with examples in Refs. 7 and 8.

Resistance Change of 1/8 watt, fixed metal film Resistors
during 2000 hours of operation (Percentage Change in Resistance)
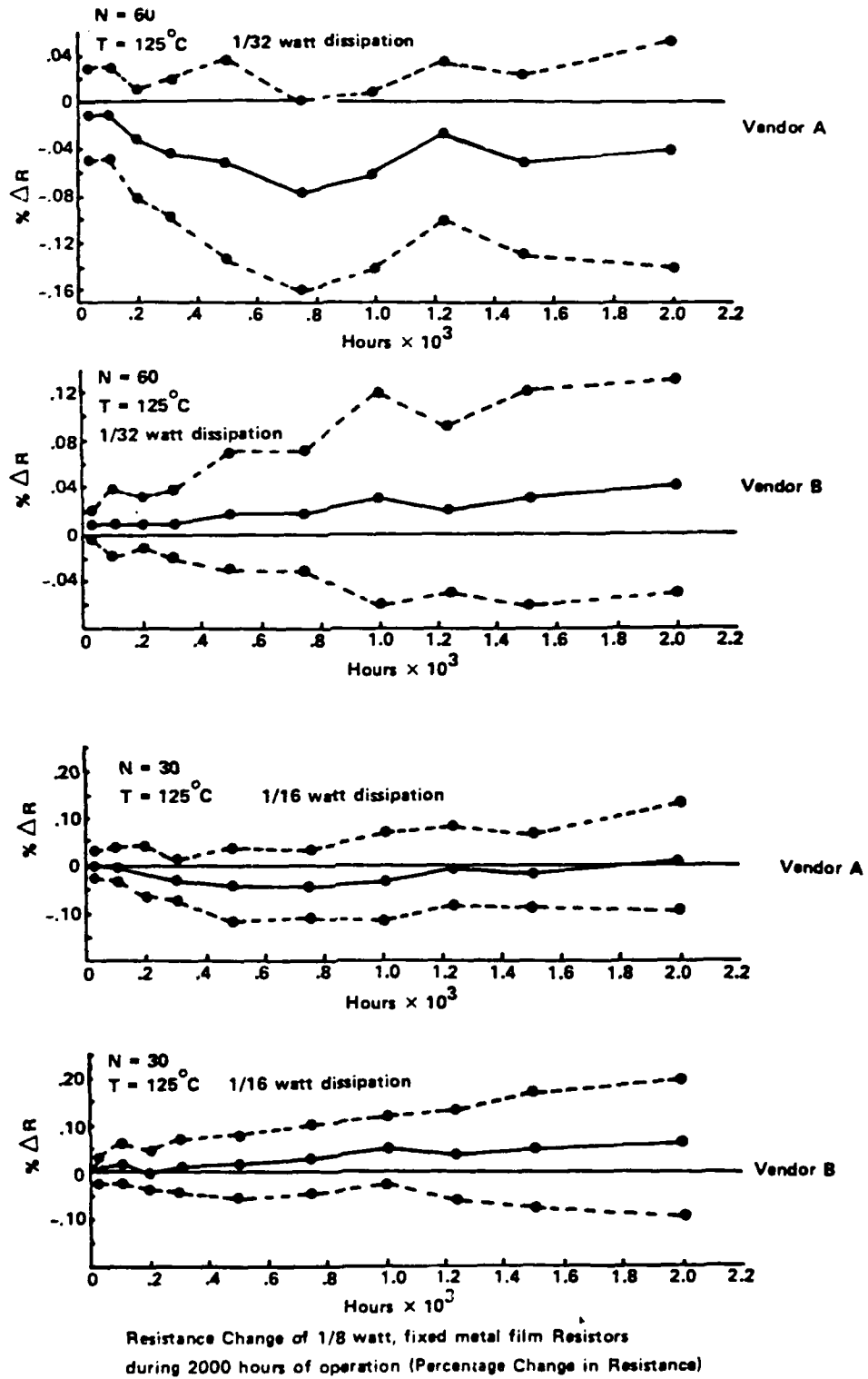
FIGURE 7.4.5-3: RESISTOR PARAMETER CHANGE WITH STRESS AND TIME (TYPICAL)

TABLE 7.4.5-1: COMPARISON OF VARIABILITY ANALYSIS METHODS

Method of Analysis	Type of Model	Class	Program Output	Objectives
Worst-case	Mathematical	Nonstatistical	Worst-case values for outputs with all parameters at cumulative worst case limits	Determine if failure is possible and under what conditions
Parameter variation	Mathematical	Nonstatistical	Range of variability data for schmoo plots	Establish realistic tolerance limits for parameters
Moment	Mathematical	Statistical	Mean values of outputs, indices of variability and redesign information	Reliability estimate Redesign if necessary
Monte Carlo	Mathematical	Statistical	Output histograms	Reliability estimates

The objective may be either of those discussed below.

(1) Examine the circuit specification and determine the allowable limits of each part parameter variation. Considering the anticipated environments, select each part accordingly.

(2) Examine the amount of parameter variation expected in each part and range of inputs. Then determine the outputs under worst case combinations, statistically expectant combinations, or other type combinations. Examine the results to determine the circuit tolerance or resistance to degradation as probability of surviving for a period time.

The worst case method of variability analysis is a nonstatistical approach (Ref. 8) that can be used to determine whether it is possible, with given parameter tolerance limits, for the system performance characteristics to fall outside specifications. The answer is obtained by using system models in which parameters are set at either their upper or lower tolerance limits. Parameter values are chosen to cause each performance characteristic to assume first its maximum and then its minimum expected value. If those performance characteristic values fall within specifications, the designer can be sure that the system has high drift reliability. If specifications are exceeded, drift type failures are possible, but the probability of their occurrence remains unknown.

The parameter variation analysis method provides means for determining the maximum and minimum values for the input parameters of a circuit, which will result in satisfactory circuit operation. Input parameters, either one-at-a-time or two-at-a-time, are varied in steps from their maximum to minimum limits or vice versa, while all other input parameters are held at the nominal value. From this process data are generated for developing safe operating envelopes, known as Schmoo Plots, for the input parameters. If the values of the input parameters are maintained within the limits determined from the Schmoo Plots, the circuit will function successfully.

Figure 7.4.5-4 is an example of a Schmoo plot of the input (R_1) and output (R_4) resistance variation of a particular circuit. The cross hatched area indicates the acceptable region of circuit operation.

Statistics are combined with system analysis techniques in the moment method to estimate the probability that performance will remain within specified limits. The method applies the propagation-of-variance formula to the first two moments of component part frequency distributions to obtain the moments of performance characteristic frequency distributions. On the basis for this information, the probability that specific system parameters drift out of their acceptable range, or drift reliability, can be computed.

In the Monte Carlo method a large number of alternate replicas of a system are simulated by mathematical models. Component values are selected randomly, and the performance of each replica is determined for its particular set of components. The performance of the replicas are compared with specification limits to yield an accurate estimate of system reliability.
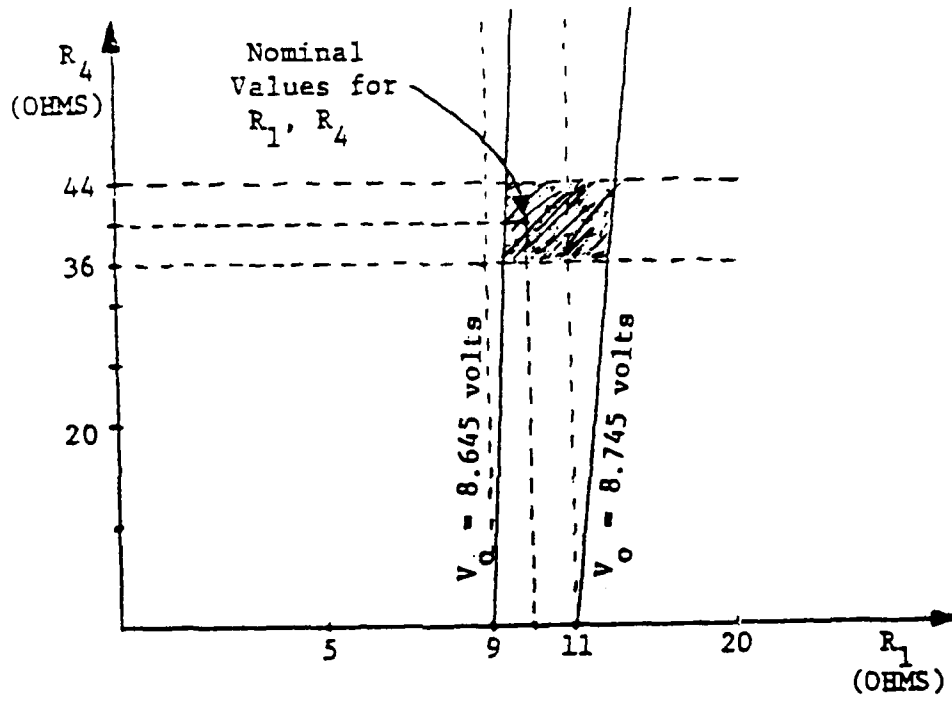
FIGURE 7.4.5-4: SCHMOO PLOT OF THE PAIR (R_1, R_4)

Each of these methods and their basic mathematical theory are discussed in Reference 8.

The fundamental approach in each method involves the systematic manipulation of a suitably arranged system model to give the desired information. All depend on the speed and accuracy afforded by the modern digital computer to manipulate the model and to process the data resulting from this manipulation.

The nonstatistical, worst case approach is designed to give basic information concerning the sensitivity of a configuration to variability in the parameters of its component parts. This information is useful to the designer in selecting economical but adequately stable components for the circuit and in modifying the configuration to reduce the critical effects on certain parameters. On the other hand, the moment and Monte Carlo methods, which are statistical, use actual parameter variability data to simulate real life situations and predict the probability that performance is inside tolerance specifications. The moment method prediction of performance variability is usually less accurate than the Monte Carlo method, but still adequate for most purposes. The moment method provides information that is extremely useful to the designer in pinpointing sensitive area and reducing this sensitivity to parameter variability.

In addition to providing data on drift type failures, the techniques are all capable of giving "stress level" information of the type needed for estimating catastrophic failure rates. They are useful, powerful tools for predicting overall reliability.

Due to the variety of variations on a large number of parameters of even a small number of parts, many of these analysis methods have been computerized. Table 7.4.5-2 illustrates the features of some programs designed to accomplish analysis of reliable designs.

Since computer aided design is the standard procedure in use today, a number of computerized circuit design programs are available, not neces- sarily reliability oriented, to aid the designer. Reference 9 includes a detailed discussion of some of these programs, e.g., ASTAP, BELAC, CIRC, CIRCUS 2, ECAP, MARTHA, SCEPTRE, SYSCAP.

7.4.6 MINIMIZING DESIGN ERRORS

A feasible design is not necessarily a reliable or economic one. Often, under the pressure of deadlines, a designer's first thought could be carried toward final practice, unless a formal, or informal procedure is implemented to have the early circuit design checked for reliability design errors by other experienced designers and specialists. The "checkers," for instance, might include not only other designers, but also component and reliability engineers. This differs from a formal design review which will be discussed later in this section. It is less formal and limited to communication directly between the designers and "design checkers."

TABLE 7.4.5-2: TYPICAL CIRCUIT ANALYSIS TECHNIQUES

Analysis Technique	Type of Analysis	Mathematical Model Necessary	Parts' Data Necessary	Output Information Received	Type of Circuits Suitable
MANDEX Worst-Case Method	Steady state ac and dc worst-case	Circuit's simultaneous equations or matrix equation	Nominal value and end-of-life limits	Worst-case value of output variable compared with allowable value	Class A amplifiers, power supplies, all biasing (dc) circuits, logic circuits, etc.
Moment Method	Statistical	Circuit's simultaneous equation or matrix equation	Mean (or nominal) value and standard deviation or variance of each input parameter and correlation coefficients when they exist	The mean and variance of the distribution of each output parameter	Any circuit for which a mathematical model can be derived
Monté Carlo Method	Statistical; predicts output variable distribution at any time; steady state ac or dc (transient may be performed if formula is available)	Circuit's simultaneous equation, matrix equation, transfer function (any mathematical representation including input parameter)	Complete distribution of each input parameter at a time	20 cell histogram for each output variable	Any circuit for which a mathematical model can be derived
VINIL Method	VINIL Method	Piece-wise linear equivalent circuits	Application curves over operating and environmental ranges along with drift data	Input characteristics (maximum and minimum), transfer characteristics (max. and min.), output characteristics (max. and min.)	Digital; linear analog
Parameter Variation Method	General, determines allowable parameter variation before design fails to function. Considers both one and two-at-a-time parameter variation	Circuit's simultaneous equation or matrix equation	A nominal value for each parameter and a range (in per cent)	Failure points for one and two-at-a-time parameter variation Schmoo plot determines safe operating envelope for design	Any steady state ac or dc circuit
SPARC (AEM-1, AEM-2, AEM-3) System of Programs	DC analysis, ac analysis; transient analysis	Equivalent circuits, equations, or matrices	Nominal (mean); Minimum (-3σ), Maximum (+3σ)	Solution of unknown in floating point fixed decimal output	All types, dc, bias, switching, nonlinear effects, ac response and distributed parameter circuit servo loops and feedback systems
SCAN DC Method	Linear static, nonlinear static	Linear or nonlinear equations in appropriate matrix form with reasonable estimates of values of the unknowns affects by nonlinear equations	Nominal (mean), Minimum (-3σ); Maximum (+3σ)	Nominal solutions, partial derivatives of unknowns with respect to knowns, worst case values, and the probability of the unknowns being outside of specified limits	All circuits that can be described by linear and nonlinear equations
SCAN AC Method	Linear sinusoidal dynamic analysis	Simultaneous complex variable equations with the real and the imaginary parts of the equations separated	Nominal (mean), Minimum (-3σ), Maximum (+3σ)	Families of frequency response curves; statistical variation of unknowns at any selected frequency; +3σ, -3σ and mean of unknowns vs frequency assumed	Any linear circuit that contains frequency-dependent devices and which is driven or is significantly analyzed with sinusoidal driving functions
SCAN Transient Method	Linear and nonlinear transient analysis, time dependent solution	Simultaneous differential equations	Nominal parts data, alternate sets of parts data, parts data for the switched states	Time response of linear or nonlinear systems	All circuits for which the transient determining effects can be modeled

Here the term "design error" includes deficiencies of the design which cause performance, overstress, testability or maintainability problems. Clearly, bench testing or even environmental testing will reveal only a fraction of the problems. Long term production, system operation and maintenance will certainly reveal all of those problems. Early critical examination of a proposed design, together with advisory programs, is the only reasonable course of action to reduce design errors. Following are some examples:

(1) TTL (Transistor-Transistor-Logic) system design problems are few since a sound system of standardization has been developed from experience with, and the maturity of, these devices. The general lack of problems has, however, led to carelessness; errors vary from simple oversights (excessive fanout) and ignoring design rules (no isolation) to subtle test or system difficulties. As an example of a test problem, the flip-flop shown in Figure 7.4.6-1 has both its set and reset inputs tied to a common isolation resistor. With a single resistor the element cannot be set into a defined state and the logic card cannot be initialized easily prior to test. Often, a significant part of the test time can be consumed by applying a homing sequence to initialize the logic card under test. As an example of the subtle type of overstress problem is the requirement of open collector drivers (shown in Figure 7.4.6-2) to have V_{CC} (Nominal, of 5V) applied if the output transistors are to retain their rated maximum breakdown voltage. Unless V_{CC} is applied before the 30V stress, the output transistor breaks down at its V_{CEO} which is much lower than its rated V_{CER}. Supply sequence sensitive circuits pose severe test maintenance and design problems. A lack of appreciation of the limitations of integrated circuits is all too common, and is usually due to the communications gap between vendors and users.

(2) MOS (Metal Oxide Semiconductor) LSI products are growing in complexity and playing a much greater part in current designs. Unfortunately, several interface, handling and application problems have become apparent. Some of these difficulties are due to a poor appreciation by the user of the true internal structure of the device.

The charge injection problems of LSI MOS dynamic shift registers are typical of interfacing problems encountered. The example shown in Figure 7.4.6-3 involves a P-channel MOS shift register which requires a high level clock driver.

Positive going clock spikes result in stored data through parasitic PNP transistor action. Such spikes therefore require special attention which involve adding clamp diodes to the circuit. More recently, microprocessors have taken a significant place in circuit designs. One of the most popular of these requires a 5V and a -9V supply. Unfortunately, the component is supply sequence sensitive such that, unless the 5V line rises before the -9V line the internal reset circuitry does not operate and a long software initializing sequence is required prior to use.
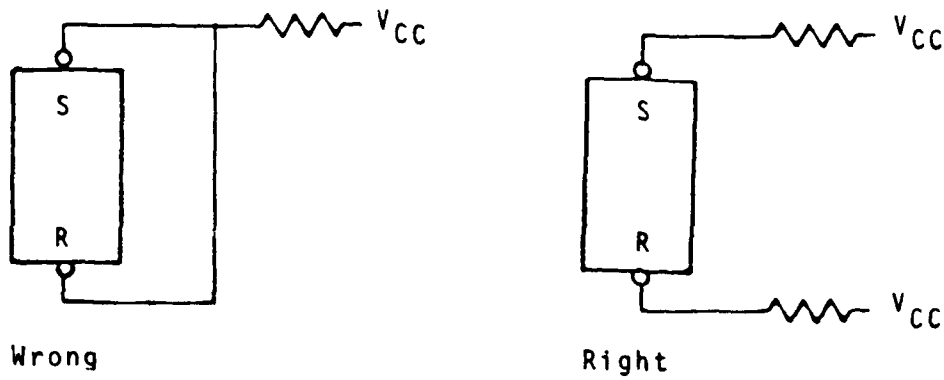
FIGURE 7.4.6-1: <u>TESTABILITY HAZARD</u>
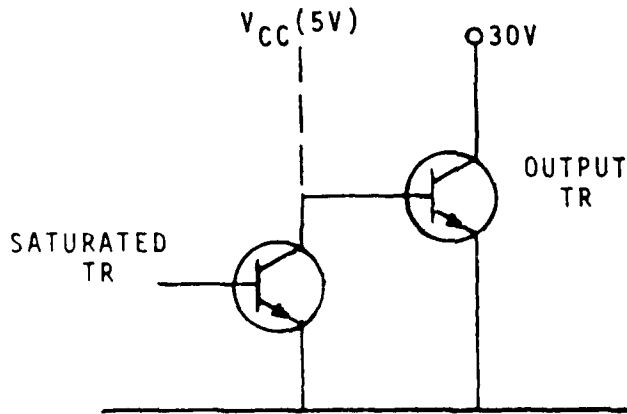
FIGURE 7.4.6-2: <u>OUTPUT STRUCTURE OF A TTL DECODER/DRIVER</u>
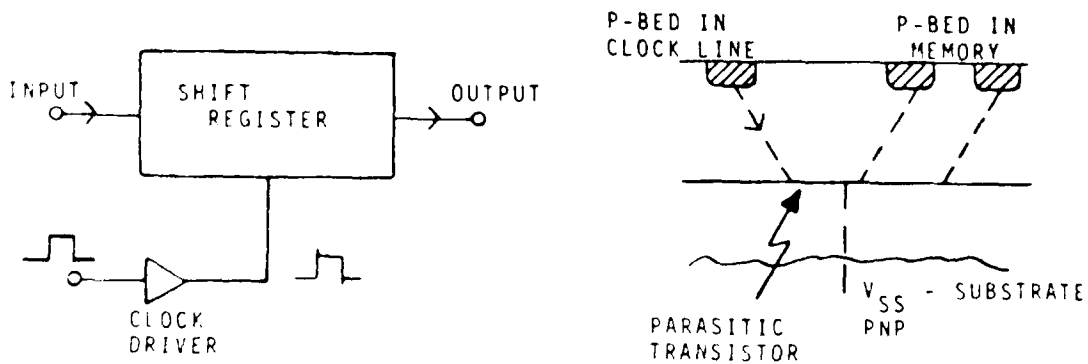
FIGURE 7.4.6-3: <u>CLOCK SPIKE PROBLEMS IN P-CHANNEL SHIFT REGISTERS</u>

(3) Discrete component circuit design seems to be a dying art. Consequently, it is an area in which a wide range of mistakes are made. Judging by field failure reports, most of the component failures occur in circuits which have high (or hidden) transient stresses as were previously discussed. The examples following have been chosen to illustrate this latter factor. However, errors of setting tolerances, failure to account for component aging and electrical noise problems are quite common. Following are some specific examples.

The first relay drive circuit shown in Figure 7.4.6-4 uses a single diffused transistor, no base emitter resistor, a catching diode, and common ground for both the logic supply and the power ground. The diode can have several unwanted effects, the worst of which is a serious reduction in relay contact life due to long relay release times and contact bounce. The lack of a base emitter resistor lowers the breakdown voltage of the transistor, increases the switch-off time of the transistor, and thereby increases the dissipation of the transistor which is single diffused and, therefore, least qualified to handle it. The common ground of the first design is a special hazard to TTL circuitry, since TTL is sensitive to ground borne noise. The new design attempts to solve the problems by using a damping resistor which allows the relay to drop out fairly quickly. A base emitter resistor preserves the high breakdown voltage of the triple diffused device, and a separate ground is used for the power circuits. It is important to note that in a simple bench test the difference between the circuits is not apparent.

The left circuit in Figure 7.4.6-5 has a higher voltage stress due to the absence of the catching diode. In terms of computed mean-time-to failure, the first circuit offers 530,000 hours and the second almost 1,000,000 hours (Ref. 10).

7.4.7 FUNDAMENTAL DESIGN LIMITATIONS

Probably the first and prime step in the establishment of reliability criteria is the establishment of the boundaries which represent the limitations on the controlled characteristics for the component or device in question. Some of the limitations are commonly known: breakdown voltage, power dissipation limitation, current density limitations, and similar factors. Many, however, are either poorly known, or possibly not known at all. Often it is these factors which cause difficulties in circuits.

If one examines the behavior of components in systems, one finds that there normally is a region of operation in which failures are rare or unlikely, but when operating conditions reach a possibly undefinable level, the probability of failure rises substantially. Conversely, with any given configuration, improvements in reliability as a result of redesign may be easy to obtain to a certain level of improvement, and then become progressively more difficult to obtain.
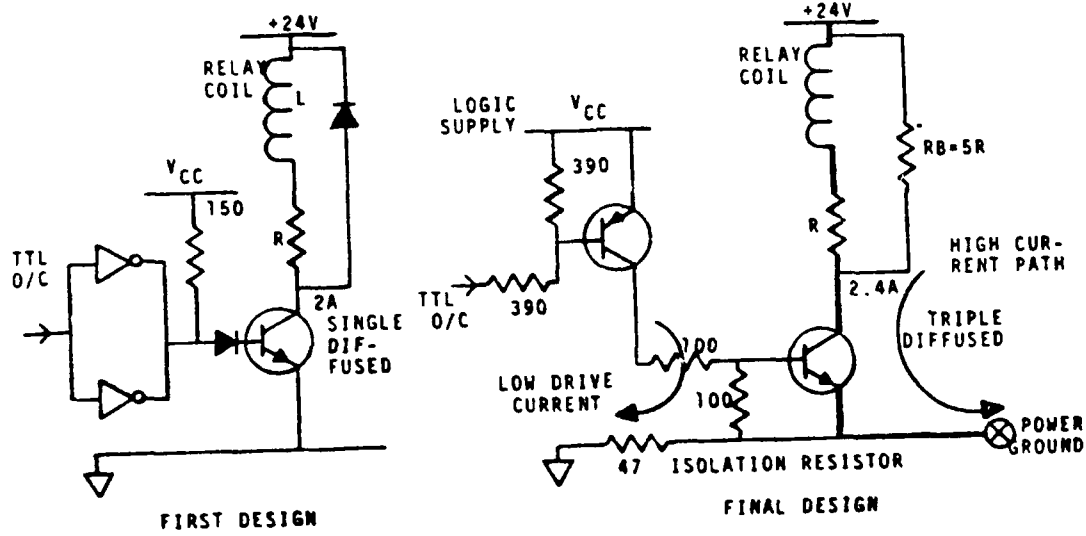
FIGURE 7.4.6-4: <u>RELAY DRIVERS</u>
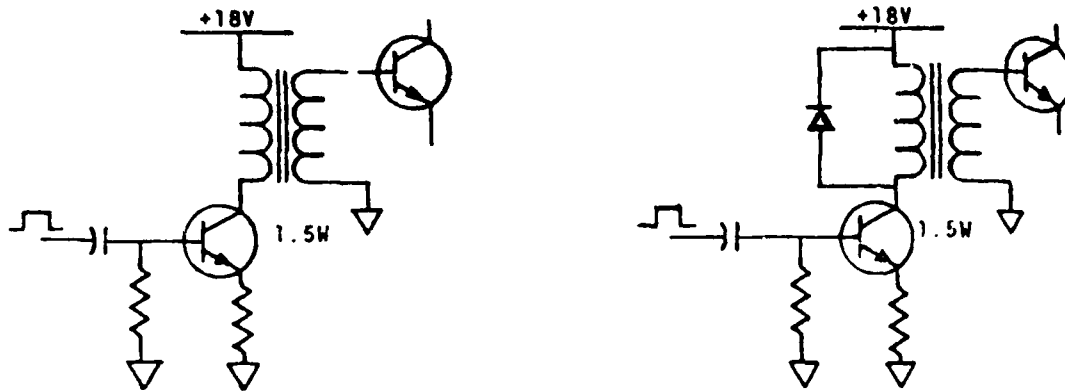
FIGURE 7.4.6-5: <u>CATCHING DIODE REDUCES TRANSIENT STRESS</u>

Improvement of reliability in terms of these criteria generally makes more sense than either attempting to attain an excessively high value for all components or being satisfied with an excessively small value based on the poor reliability of the few components. Limitation of collector supply voltage to the minimum which permits the devices to perform as required provides a very economical way of improving the reliability of a given circuit. Typically, this may require that the collector and the base supply voltages be provided from separate sources, with the base supply providing a substantially higher voltage but at a sharply reduced current level. The voltage level required for the base supply will be about the same as is used normally for the entire circuit.

The optimization of the reliability of a system on a circuit-by-circuit basis might appear to be an excessively time consuming and difficult problem. Actually, however, such need not be the case, since it is entirely practical to test at the design state (on paper) the effects of voltage reduction on circuit performance. Since it is necessary to limit voltage gain for reasons of circuit stability, proceeding in this manner might lead to an occasional additional amplifier circuit but it should at the same time lead to substantially reduced power consumption and substantially reduced cooling problems. Both of these are important criteria for reliability.

The following paragraphs discuss some fundamental design limitations which are important to designers of military electronic equipment.

The Voltage Gain Limitation

The development of radar brought with it the need to be able to amplify very weak signals in the presence of strong ones, and for the first time made the question of stability and freedom from ringing a prime consideration in tuned amplifiers. These tuned amplifiers frequently were required to have voltage amplifications as great as a million overall, with no change in operating frequency permitted.

The basic criterion which must be satisfied, both for each individual amplifier stage and for the amplifier as a whole, is that the loop amplification of individual elements as well as of the assembled groups of elements must be rigidly limited to assure that stability will not be impaired. This stability problem is essentially a phase-sum problem. If an input voltage is applied to the amplifier or stage in question, then the voltage returned through feedback to be summed into the input voltage is the product of this voltage by the amplification "around the loop" from input back to input

$$K_L = K_U \times K_f \tag{7.3}$$

where K_U is the forward voltage amplification to the output, and K_f is the feedback "amplification" from the output back to the input on an

open-loop basis. The modified forward amplification K' then takes the form:

$$K'_U = K_U/(1 - K_U K_f) \qquad\qquad (7.4)$$

and the phasor term $(1 - K_U K_f)$ determines both the variation of the signal amplitude and the signal phase.

Clearly, one of the requirements of any amplifier to which Eq. (7.3) applies is that $|K_U K_f|$ must be small compared to unity, or a potentially unstable situation can develop. In addition, significant phase shift in the output circuit compared to the input can occur even with relatively small values of $|K_U K_f|$ values as small as 0.1 or 0.2, for example. In such a situation, as much as 5 to 10 degree phase discrepancy per stage can be encountered.

Where phase stability is of prime importance, it is evident that values of $|K_U K_f|$ should be less than 0.01 if at all possible, as then there is reasonable chance that the cumulative phase angle discrepancy in a system may be limited to a fraction of a radian. The design of an amplifier meeting this limitation can be both difficult and painstaking, and the mechanical realization of the calculated design can be even more difficult. The design techniques described in Reference 35 offer possibly one of the best ways of achieving the required results.

Early radar experience quickly showed that the limit on per stage gain K_U for achieving amplitude and phase stability with minimum to modest ringing proved to be approximately 10. (It is possible to get device gains of 100 with common grid or common base circuits, but the required impedance transformation required to match the input circuit for the succeeding amplfier typically reduces the overall stage gain back to approximately 10.) This means that the maximum permitted value for K_f is approximately 0.01 to 0.02, for a power isolation possibly as much as 40 dB. Where phase stability is of primary importance, the maximum permitted value for K_f is nearer 0.001 than 0.01.

It is very important to control and restrain the circulation of carrier frequency currents throughout any multistage amplifier, since if five stages overall are involved, the isolation from output back to input must be about 0.01^5 or $10^{\pm 10}$. This is the reason that radar IF amplifiers were designed to receive power in the vicinity of the middle stage, and R-C decoupling was used in both directions for supply voltages, and L-C decoupling for heater currents. All voltage feed points were in addition individually bypassed, and grounds grouped within the channel in such a way as to prevent circulation of carrier frequency currents in the channel.

Clearly, there is really nothing magic about the value of K_U of 10. The magic number, if one exists, is in fact the "invariant" $K_U \times K_f$ whose value must be sufficiently small to limit the phase and amplitude excursions in the signal. This is the basic stability criterion. But there definitely is an upper limit on the value of K_U, at least in

a practical way, since there is a lower practical limit on how small K_f can be made successfully in production type equipment. The internal stage voltage gain from input to output on control separation amplifiers can be significantly higher, since the input admittances for these devices are sufficiently high that the return feedback gain is severely reduced.

This limitation on voltage gain has very interesting consequences, particularly in design for reliable operation. It is shown in Eq. (7.5).

$$K_\upsilon = \kappa \Lambda I_C Z_L \qquad (7.5)$$

where

K_υ = forward voltage amplification

I_C = collector current

Z_L = load impedance

κ = efficiency factor

Λ = q/kT

q = electron charge

k = Boltzmann's constant

T = absolute temperature

In this equation, it is evident that $I_C Z_L$ represents a value of a voltage, namely, the instantaneous voltage across the load impedance Z_L.

It is possible to relate the voltage $I_C Z_L$ to the minimum possible supply voltage V_{CC} which can be used with the ideal device in question to produce the required operating characteristics. The minimum supply voltage may then be defined in terms of the equation

$$I_C Z_L = K_\eta V_{CC} \qquad (7.6)$$

where K_η is a parameter which relates the output load voltage to the supply voltage. K_η normally has a value between 0.2 and 1.0. Substituting Eq. (7.6) in Eq. (7.5) gives the result:

$$K_\upsilon = \kappa K_\eta \Lambda V_{CC} \qquad (7.7)$$

This equation may be solved for the minimum supply voltage V_{CC} (neglecting saturation voltage) for a device in a circuit to give

$$\left|V_{CC}\right| = \left|K_\upsilon\right|(\kappa K_\eta \Lambda)^{-1} + V_{Csat} \qquad (7.8)$$

In Eq. (7.8), the value of κ_v ranges between roughly 0.0001 and 2.0, typical values of κ_n are less than unity, and V_{Csat} is the maximum saturation voltage. As a result, with bipolar transistors, the minimum value of supply voltage required for a circuit can be expected to be roughly a twentieth of the voltage gain. This means that the range of required supply voltage is between 0.5 and 10V, the lower voltage limit applying to the common emitter configuration, and the higher to the common base configuration.

The significance of this relation cannot be overemphasized. The properties of the device and its associated circuitry are controlled largely by the current level selected for operation, and there is little point to selecting a supply voltage for the output circuit which is more than marginally greater than calculated by Eq. (7.8). Selection of a higher voltage leads either to excessive power dissipation, excessive gain with its inherent instability, or combinations of these conditions. In short, the selected supply voltage should be as small as possible consistent with the demands on the circuits.

This discussion should not be implied necessarily to mean that the base supply voltage provided for base bias current and voltage necessarily can be as small as that for the collector. Since crude stabilization of circuits is frequently obtained by controlling the base current in a transistor, the supply voltage provided for this function must be sufficiently large to assure that an adequate constancy of current level can be achieved. This and this alone is the justification for use of a large voltage, yet the current requirement for these circuits is sufficiently small that a substantial decrease in power dissipation and a substantial improvement in reliability could be achieved through the use of separate power sources for these two functions. In comparison, then, one source of high current and low voltage is required, and one of higher voltage but substantially smaller current also is required. Using a common source for both clearly leads to the worst failures of each!

Current Gain Limitation Considerations

The voltage gain limitation is electrostatic, or charge control, in nature. It is particularly important with transadmittance* devices, which tend to have a relatively high input impedance and tend to become regenerative by passing through a zero admittance (infinite impedance) condition. It is important further because it has the smallest rate of decay with distance known from static fields.

The network dual of the voltage gain limitation is the current gain limitation. It is technically possible for this also to be critical, but at present its consequences are much less severe than its dual.

*transadmittance is defined as $y'_f = \kappa \wedge I_C$

Probably the principal reason for this is the rapidity of decay of magnetic fields associated with currents. Additional reasons are the dependence on rate-of-change of current (since only changing fields create voltage and currents), and the nonexistence of true transimpedance devices.

The control of magnetic fields proves to be one of control of fluctuating currents. The more that can be done to keep current fluctuations isolated and out of wires and shielding structures, the more freedom there is from coupling currents and fields. Size of loops carrying fluctuating currents should be kept to an absolute minimum unless the inductive properties of the loop are essential to the operation at hand. Even then the loop or coil should be so designed and so installed that it generates its field efficiently, so that an adequate quality factor, or Q, is obtained, and so that coupled fields and circulating currents induced and generated by the field are limited to regions where they are required and otherwise kept to a practical minimum.

Thermal Factors

One of the major problems in the use of transistor circuits is the stabilization of operating conditions so that the circuit can give the required performance over an adequate range of environmental conditions.

There are two principal thermal factors that affect the stability of transistor circuits. The first of these thermal factors is the reverse leakage current of the collector base junction, so called I_{co}, and the second the variation of V_{be} (base emitter voltage) with temperature. The leakage current increases rapidly as the temperature of the transistor is increased. This effect limits the conditions under which the transistor can provide effective operation (Figure 7.4.6-6). This current, in conjunction with the current gain of the transistor, limits the minimum usable current through the common emitter amplifier, thereby restricting the available range of operation.

Even though it is possible to use the transistor in the common emitter circuit with very small values of currents, the nonlinearity of the device when the base current has a reverse polarity is so pronounced that it is not practical to attempt to do so.

The variation of the base-to-emitter voltage with temperature for fixed magnitudes of base and emitter current is the second important thermal property of a transistor requiring compensation. The voltage between base and emitter affects the static operation of the transistor, and it also affects the small signal operation. Because the static, or Q-point for the transistor varies rapidly with temperature if the base voltage is fixed, it is necessary to fix the Q-point in a way to assure that a full range of operating conditions is available over the required range of operating temperature. The static stability must be determined in terms of the practical circuit in use, and the circuit must be designed to provide the required stability.
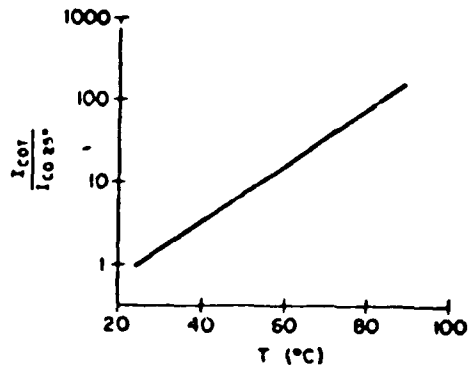
FIGURE 7.4.6-6: RATIO OF I_{CO} OVER TEMPERATURE T TO I_{CO} AT T = 25^OC

Reference 6 provides detailed design procedures for thermal stabilization of circuits, as well as design procedures to prevent thermal runaway.

7.5   REDUNDANCY

7.5.1   REDUNDANCY AS A DESIGN TECHNIQUE

In reliability engineering, redundancy can be defined as the existence of more than one means for accomplishing a given task. In general, all means must fail before there is a system failure.

Thus, if we have a simple system consisting of two parallel elements as shown in Figure 7.5.1-1 with A_1 having a probability of failure q_1 and A_2 having a probability of failure q_2, the probability of total system failure is

$$Q = q_1 q_2$$

Hence the reliability or probability of no failure is

$$R = 1 - Q = 1 - q_1 q_2$$

For example, assume that A_1 has a reliability r_1 of 0.9 and A_2 a reliability r_2 of 0.8. Then their unreliabilities q_1 and q_2 would be

$$q_1 = 1 - r_1 = 0.1$$

$$q_2 = 1 - r_2 = 0.2$$

and the probability of system failure would be

$$Q = (0.1)(0.2) = 0.02$$

Hence the system reliability would be

$$R = 1 - Q = 0.98$$

which is a higher reliability than either of the component parts acting singly. Parallel redundancy is therefore a design tool for increasing system reliability when all other approaches have failed.
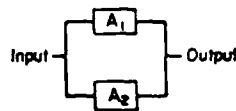
FIGURE 7.5.1-1:   Parallel Network

It should be pointed out that whole redundancy reduces mission failures and increases logistics failures. In general, with m components in parallel, the overall probability of failure in time t is

$$Q(t) = q_1(t) \cdot q_2(t) \cdots q_m(t) \tag{7.9}$$

and the probability of operating without failure is

$$R(t) = 1 - Q(t) = 1 - q_1(t)q_2(t) \cdots q_m(t) \tag{7.10}$$

which can also be given as

$$R(t) = 1 - [1 - r_1(t)][1 - r_2(t)] \cdots [1 - r_m(t)] \tag{7.11}$$

because $q_i(t) = 1 - r_i(t)$ for each component. Where each of the component reliabilities is equal, the above equations reduce to

$$Q(t) = [q(t)]^m \tag{7.12}$$

$$R(t) = 1 - [q(t)]^m \tag{7.13}$$

$$= 1 - [1 - r(t)]^m \tag{7.14}$$

So far it has been assumed that parallel components do not interact and that they may be activated when required by ideal failure sensing and switching devices. Needless to say, the latter assumption, in particular, is difficult to meet in practice. Therefore, the potential benefits of redundancy cannot be realized fully. The reader is referred to the cited references, e.g., Refs 11 and 12, for detailed treatment of redundancy with sensing and switching devices which are most ideal. The subject is also treated in Appendix A of this section.

Most cases of redundancy encountered will consist of various groupings of series and parallel elements. Figure 7.5.1-2 typifies such a network. The basic formulas previously given can be used to solve the overall network reliability R_{AC}. This was done in Section 5 of this handbook. Network decomposition methods are also treated in Appendix A of this section, and in more detail in Reference 12.
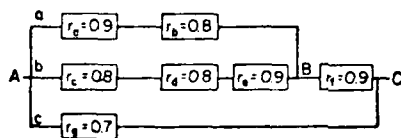
FIGURE 7.5.1-2: SERIES-PARALLEL REDUNDANCY NETWORK

7.5.2 REDUNDANCY IN TIME DEPENDENT SITUATION

The previous discussion of reliability at a point in time did not consider the time dependent reliability function. As a rule, the results given above can be extended to the time dependent situation. For example, returning to Figure 7.5.1-1, assume that A_1 and A_2 have constant failure rates of λ_1 and λ_2 and exponential time-to-failure distributions. Then the overall reliability is given by

$$R(t) = 1 - q_1(t)q_2(t) \tag{7.15}$$

$$= 1 - (1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t})$$

$$= e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$$

because for each element $r(t) = e^{-\lambda t}$; hence $q(t) = 1 - e^{-\lambda t}$.

The basic redundancy formulas previously given can then be used to solve for the case of parallel components as well as any series-parallel combinations.

An important point to be remembered, however, is that the constant failure rates of the elements in a redundant configuration cannot be combined in the usual manner (addition) to obtain the system failure rate. This is because the system failure rate is not constant but increases with time because the number of paths for successful operation decreases as each redundant path fails. The system mean life, however, is found from equation

$$\theta_s = \int_0^\infty R(t)dt \tag{7.16}$$

For the example given in Eq. (7.15), the redundant system mean life would be

$$\theta_s = \int_0^\infty e^{-\lambda_1 t}\, dt + \int_0^\infty e^{-\lambda_2 t}\, dt - \int_0^\infty e^{-(\lambda_1 + \lambda_2)t} dt$$

$$= \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} \quad \text{for } \lambda_1 \neq \lambda_2 \tag{7.17}$$

$$= \frac{3}{2\lambda} \quad \text{for } \lambda_1 = \lambda_2 = \lambda \tag{7.18}$$

Thus it can be seen that the mean life of a redundant system containing two parallel elements of equal reliability is 1.5 times the mean life of a single element. For n equal components in parallel

$$\theta_s = \frac{1}{\lambda} + \frac{1}{2\lambda} \cdots + \frac{1}{n\lambda} \tag{7.19}$$

$$R_p(t) = 1 - (1 - e^{-\lambda t})^n \tag{7.20}$$

7.5.3 REDUNDANCY CONSIDERATIONS IN DESIGN

Depending on the specific application, a number of approaches are available to improve reliability through redundant design. These approaches are classified on the basis of how the redundant elements are introduced into the circuit to provide a parallel signal path.

In general, there are two (2) major classes of redundancy:

(1) <u>Active Redundancy</u>. External components are not required to perform the function of detection, decision and switching when an element or path in the structure fails.

(2) <u>Standby Redundancy</u>. External elements are required to detect, make a decision and switch to another element or path as a replacement for a failed element or path.

Techniques related to each of these two classes are depicted in the simplified tree structure shown in Figure 7.5.3-1.
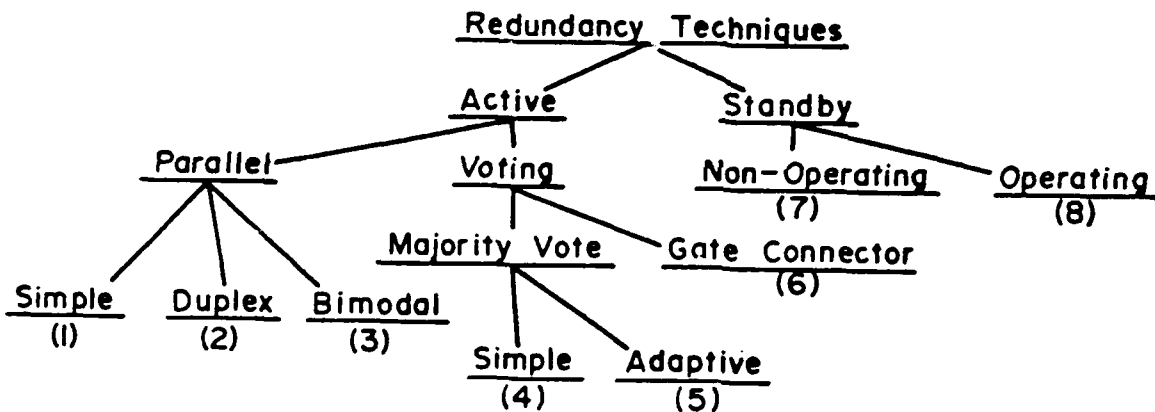
FIGURE 7.5.3-1: REDUNDANCY TECHNIQUES

Table 7.5.3-1 further defines each of the eight techniques identified in Figure 7.5.3-1 by number.

TABLE 7.5.3-1: REDUNDANCY TECHNIQUES

Simple Parallel Redundancy
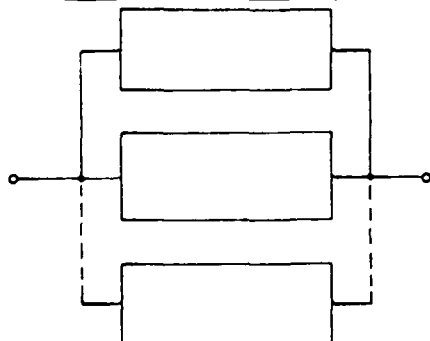
In its simplest form, redundancy consists of a simple parallel combination of elements. If any element fails open, identical paths exist through parallel redundant elements.

Duplex Redundancy
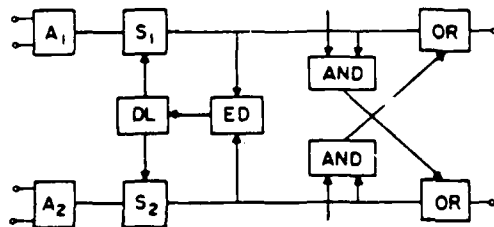
This technique is applied to redundant logic sections, such as A1 and A2 operating in parallel. It is primarily used in computer applications where A1 and A2 can be used in duplex or active redundant modes or as a separate element. An error detector at the output of each logic section detects noncoincident outputs and starts a diagnostic routine to determine and disable the faulty element.

(a) Bimodal Parallel/ Series Redundancy
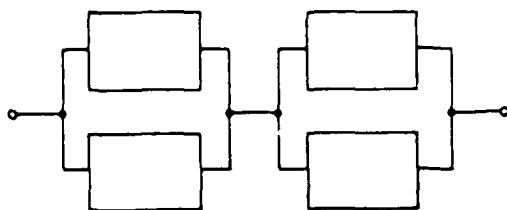
A series connection of parallel redundant elements provides protection against shorts and opens. Direct short across the network due to a single element shorting is prevented by a redundant element in series. An open across the network is prevented by the parallel element. Network (a) is useful when the primary element failure mode is open. Network (b) is useful when the primary element failure mode is short.

(b) Bimodal Series/ Parallel Redundancy
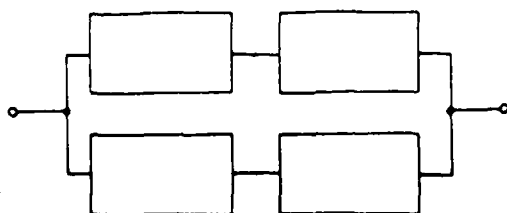
TABLE 7.5.3-1: REDUNDANCY TECHNIQUES (Cont'd)

Majority Voting Redundancy
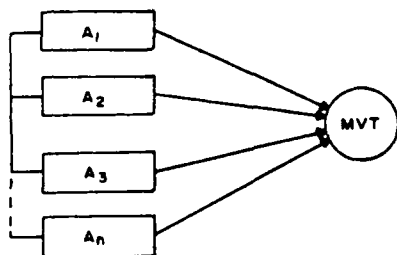
Decision can be built into the basic parallel redundant model by inputting signals from parallel elements into a voter to compare each signal with remaining signals. Valid decisions are made only if the number of useful elements exceeds the failed elements.

Adaptive Majority Logic
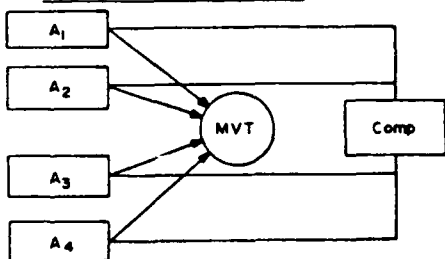
This technique exemplifies the majority logic configuration discussed previously with a comparator and switching network to switch out or inhibit failed redundant elements.

Gate Connector Redundancy
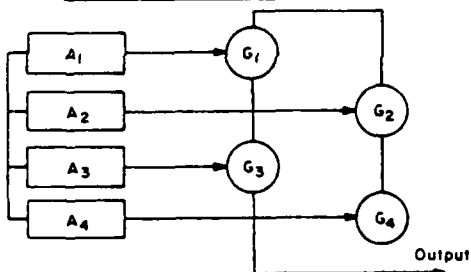
Similar to majority voting. Redundant elements are generally binary circuits. Outputs of the *binary elements are fed to switch-like gates* which perform the voting function. The gates contain no components whose failure would cause the redundant circuit to fail. Any failures in the gate connector act as though the binary element were at fault.

Standby Redundancy
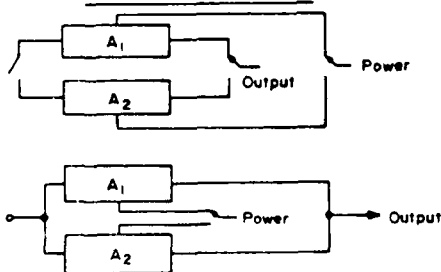
A particular redundant element of a parallel configuration can be switched into an active circuit by connecting outputs of each element to switch poles. Two switching configurations are possible.

1) The element may be isolated by the switch until switching is completed and power applied to the element in the switching operation.
2) All redundant elements are continuously connected to the circuit and a single redundant element activated by switching power to it.

Operating Redundancy
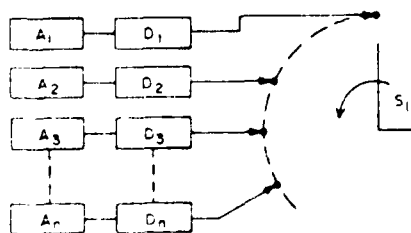
In this application, all redundant units operate simultaneously. A sensor on each unit detects failures. When a unit fails, a switch at the output transfers to the next unit and remains there until failure.

Appendix A contains a description of the more common types of redundant configurations available to the designer (including most of those shown in Table 7.5.3-1), with applicable block diagrams, mathematical formulae, and resulting reliability functions. This was done so that this section could be devoted to a discussion of some of the fundamental design considerations in using redundancy.

The decision to use redundant design techniques must be based on analysis of the tradeoffs involved. Redundancy may prove to be the only available method, when other techniques of improving reliability, e.g., derating, simplification, better components, have been exhausted, or when methods of item improvement are shown to be more costly than duplications. When preventive maintenance is planned, the use of redundant equipment can allow for repair with no system downtime. Occasionally, situations exist in which equipments cannot be maintained, e.g., satellites; then redundant elements may be the best approach to prolonging operating time significantly.

The application of redundancy is not without penalties. It will increase weight, space requirements, complexity, cost, and time to design. The increase in complexity results in an increase in unscheduled maintenance. Thus, safety and mission reliability is gained at the expense of adding an item(s) in the unscheduled maintenance chain. The increase in unscheduled maintenance may be counteracted by reliability improvement techniques such as design simplification, derating, and the use of more reliable components, as discussed elsewhere in this Handbook.

In general, the reliability gain for additional redundant elements decreases rapidly for additions beyond a few parallel elements. As illustrated by Figure 7.5.3-2 for simple parallel redundancy, there is a diminishing gain in reliabilty and MTBF as the number of redundant elements is increased. As shown for the simple parallel case, the greatest gain achieved through addition of the first redundant element is equivalent to a 50% increase in the system MTBF. Optimization of the number of parallel elements is discussed in Appendix A.

In addition to maintenance cost increases due to repair of the additional elements, reliability of certain redundant configurations may actually be less than that of a single element. This is due to the serial reliability of switching or other peripheral devices needed to implement the particular redundancy configuration. Care must be exercised to insure that reliability gains are not offset by increased failure rates due to switching devices, error detectors and other peripheral devices needed to implement the redundancy configurations. One case where the reliability of switching devices must be considered is that of switching redundancy. This occurs when redundant elements are energized but do not become part of the circuit until switched in after the primary element fails. Figure 7.5.3-3 is an example of redundancy with switching for two parallel elements. The mathematical model for this block diagram, written in terms of unreliability (R), considers two modes of failure associated with the switching mechanism.
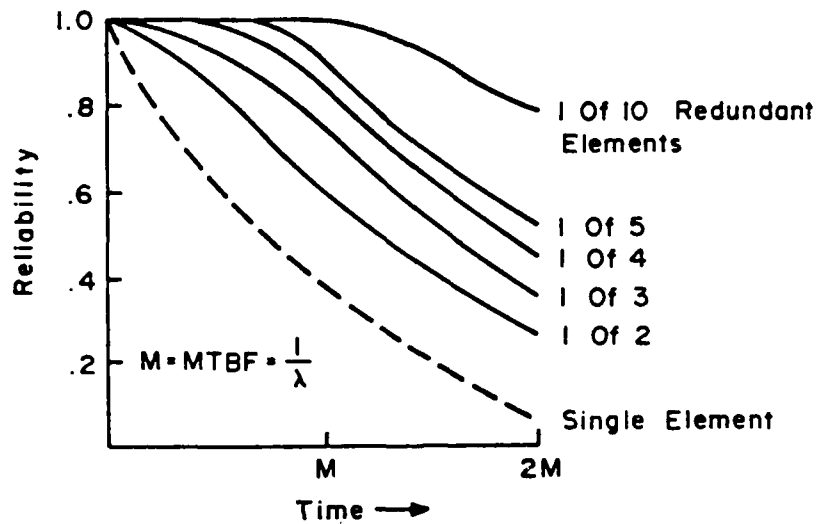
(a) Simple Active Redundancy For
One Of n Element Required
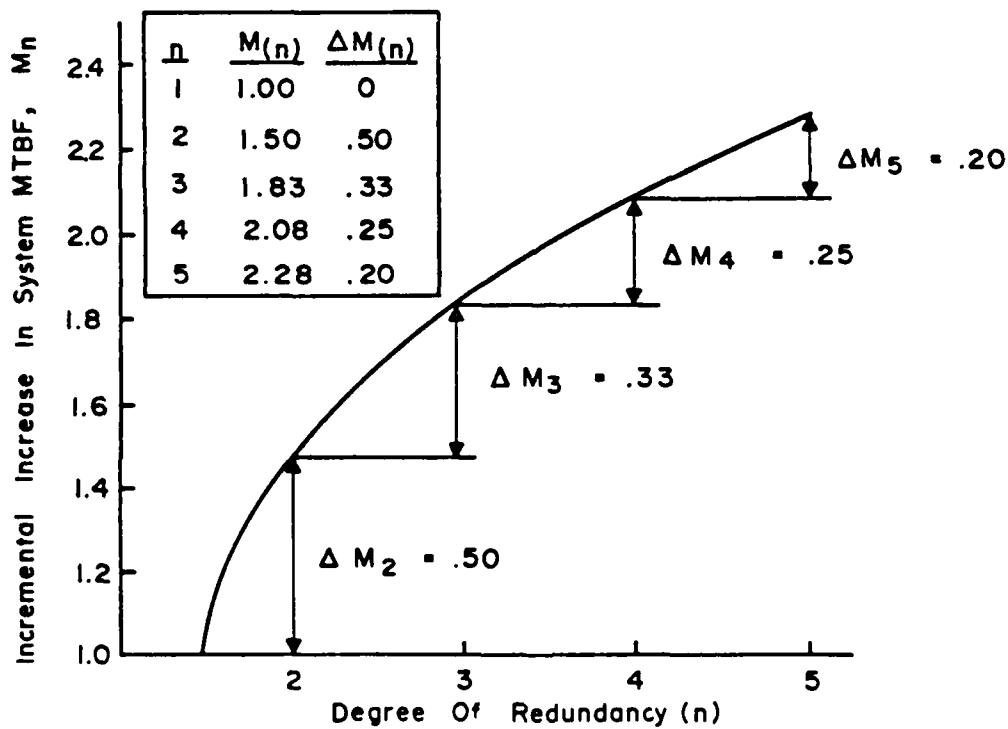
(b) Incremental Increase In System MTBF For n Active Elements

FIGURE 7.5.3-2: DECREASING GAIN IN RELIABILITY AS NUMBER OF ACTIVE ELEMENTS INCREASES

This equation indicates that the redundancy gain is limited by the failure mode(s) of the switching device, and the complexity increases due to switching.

The effectiveness of certain redundancy techniques (especially standby) can be enhanced by repair. Standby redundancy allows repair of the failed unit (while operation of the good unit continues uninterrupted) by virtue of the switching function built into the standby redundant configuration (see Appendix A). Through continuous or interval monitoring, the switchover function can provide an indication that failure has occurred and operation is continuing on the alternate channel. With a positive failure indication, delays in repair are minimized. A further advantage of switching is related to built-in test (BIT) objectives. Built-in test can be readily incorporated into a sensing and switchover network for ease of maintenance purposes.

An illustration of the enhancement of redundancy with repair is shown in Figure 7.5.3-4. The achievement of increased reliability brought about by incorporation of redundancy is dependent on effective isolation of redundant elements. Isolation is necessary to prevent failure effects from adversely affecting other parts of the redundant network. The susceptibility of a particular redundant design to failure propagation may be assessed by application of failure mode and effects analysis as discussed in Section 7.8. The particular techniques addressed there offer an effective method of identifying likely fault propagation paths.

Increased reliability brought about by incorporation of redundancy is dependent on effective isolation of redundant elements. Isolation is necessary to prevent failure effects from adversely affecting other parts of the redundant network. In some cases, fuses or circuit breakers, overload relays, etc., may be used to protect the redundant configuration. These items protect a configuration from secondary effects of an item's failure so that system operation continues after the element failure.

Redundancy may be incorporated into protective circuits as well as the functional circuit which it protects. Operative redundancy configurations of protection devices (e.g., fuse, circuit breaker) can be used to reduce the possibility that the "protected" circuit is not completely disabled should the protective circuit device open prematurely or fail to open due to overcurrent.

Caution must be exercised in the selection and use of various redundancy configurations in specific applications. Consider a parallel series (Table 7.5.3-1) configuration which protects against both open and short failure modes. In this case, it is a quad redundant configuration, where the elements are identical. Utilizing Appendix A, the reliability of the parallel series configuration is found to be

$$R = 2e^{-2\lambda t} - e^{-4\lambda t}$$

For comparison, Figure 7.5.3-5 shows a reliability plot of both single element reliability and the quad redundant configuration reliability.
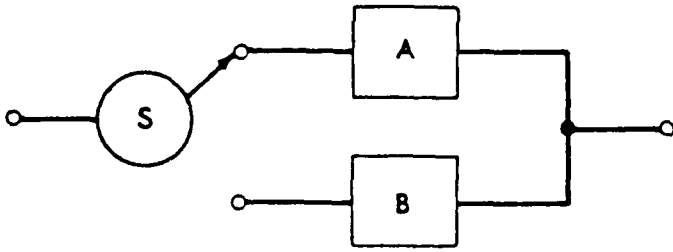
$$\overline{R} = p_a q_b q'_s + q_a p_b q_s + q_a q_b$$

where: q_s = probability of switch failing to operate when it is supposed to

q'_s = probability of switch operating without command (prematurely)

$q_{a,b}$ = probability of failure or unreliability of element A or B

$p_{a,b}$ = probability of success or reliability of element A or B

FIGURE 7.5.3-3: REDUNDANCY WITH SWITCHING
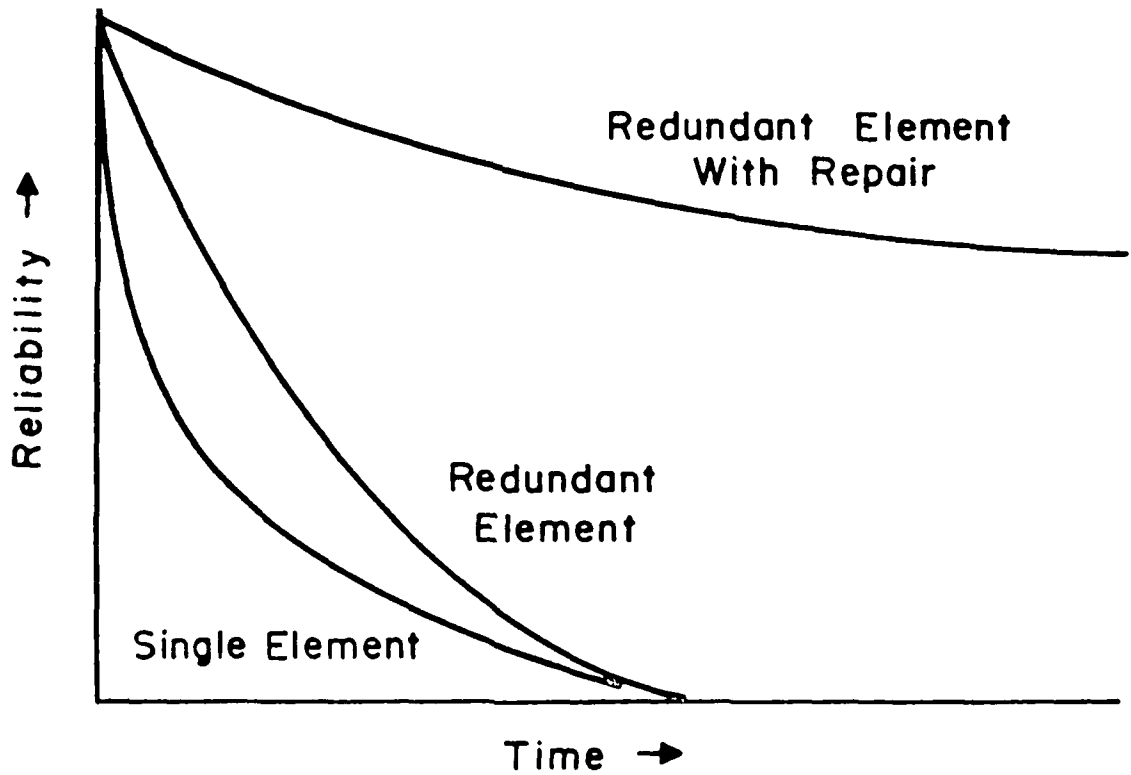
FIGURE 7.5.3-4: RELIABILITY GAIN FOR REPAIR OF SIMPLE PARALLEL ELEMENT AT FAILURE

Parallel-Series Configuration
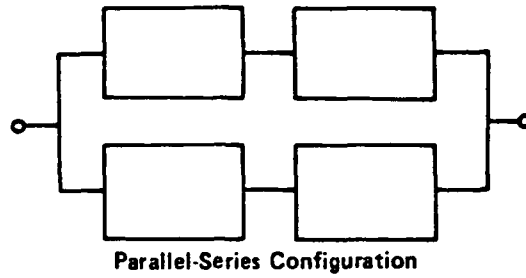
Parallel-Series Configuration Model $R = 2e^{-2\lambda t} - e^{-4\lambda t}$
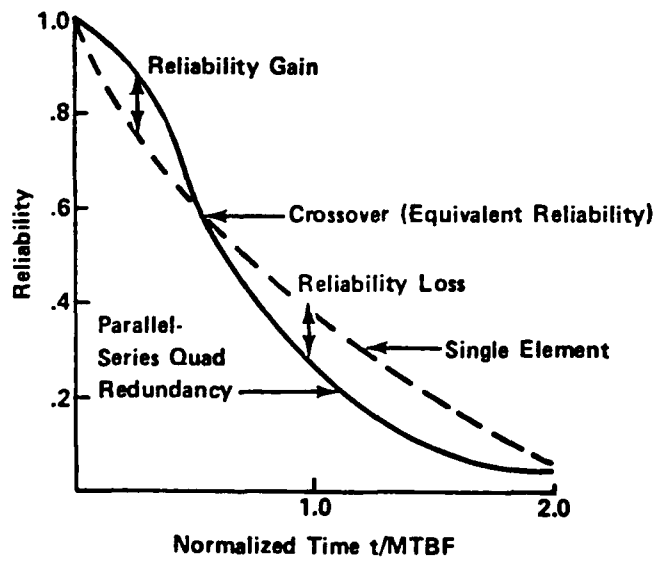
FIGURE 7.5.3-5: <u>PARALLEL-SERIES REDUNDANCY RELIABILITY GAIN</u>

The crossover point of the two curves illustrates that reliability gain is provided by the parallel series configuration up to the crossover point. Beyond the crossover point, there is a reliability loss associated with the parallel series arrangements compared with the use of the single nonredundant configuration. The normalized time, t/MTBF, for elements in this configuration determines where the reliability advantage is lost, i.e., the point where reliability for the single element is the same as for the redundant configuration.

Figure 7.5.3-6 shows an example of parallel series redundancy at the circuit level. The quadruple redundant configuration is centered about a transistor circuit with its biasing network. This configuration protects against both "fail open" and "fail short" failure modes. The mathematical model for this example assumes that opens and shorts are equally likely to occur. If they are not equally likely, the model would be more complicated. For a "no output" failure mode of the redundant configuration, either A and B, or A and D, or B and C, or C and D must fail open. This requires a double failure. For an "erroneous output" failure mode of the redundant configuration, either A and C, or B and D must fail short. Therefore, there are four combinations for a "no output" failure mode and two combinations for an erroneous output failure mode. Also double failures are required in each case to cause failure of the primary function.

Both the advantages and disadvantages of redundancy must be considered prior to incorporation in a system design. The previous mentioned major disadvantages of using redundancy to solve a reliability problem are weight, cost, and complexity. Addition of back up systems and/or lower level items adds the weight and cost of the added hardware. This weight and cost may be reduced by application of redundancy to the lower levels of the hardware breakdown structure (e.g., parts) rather than assemblies. A more harmful effect may be increased complexity which would negate the search for reliability improvement. For example, sensing, activation, and switching hardware added for back up item energization may reduce the overall reliability below that of the primary item.

There are many cases where deliberate redundancy provides reliability improvement with cost reduction. It does not necessarily follow that simple backup redundancy is the most cost effective way to compensate for reliability inadequacy. The design engineer has the responsibility to determine what balance of redundancy alternatives is the most effective to use. In the trade-off process, it may be determined that redundancy, by the duplication of hardware, may impact the cost of preventive maintenance. This is a significant factor in total life cycle cost considerations for equipment worth. Redundancy may be easy if a designed item is available, cheaper if the item is economical in comparison to redesign, too expensive if the item is costly, too heavy if aircraft limitations are exceeded, etc. These are all factors which the designer must consider. In any event, the designer should consider redundancy for reliablity improvement of critical items (of low reliability) for which a single failure
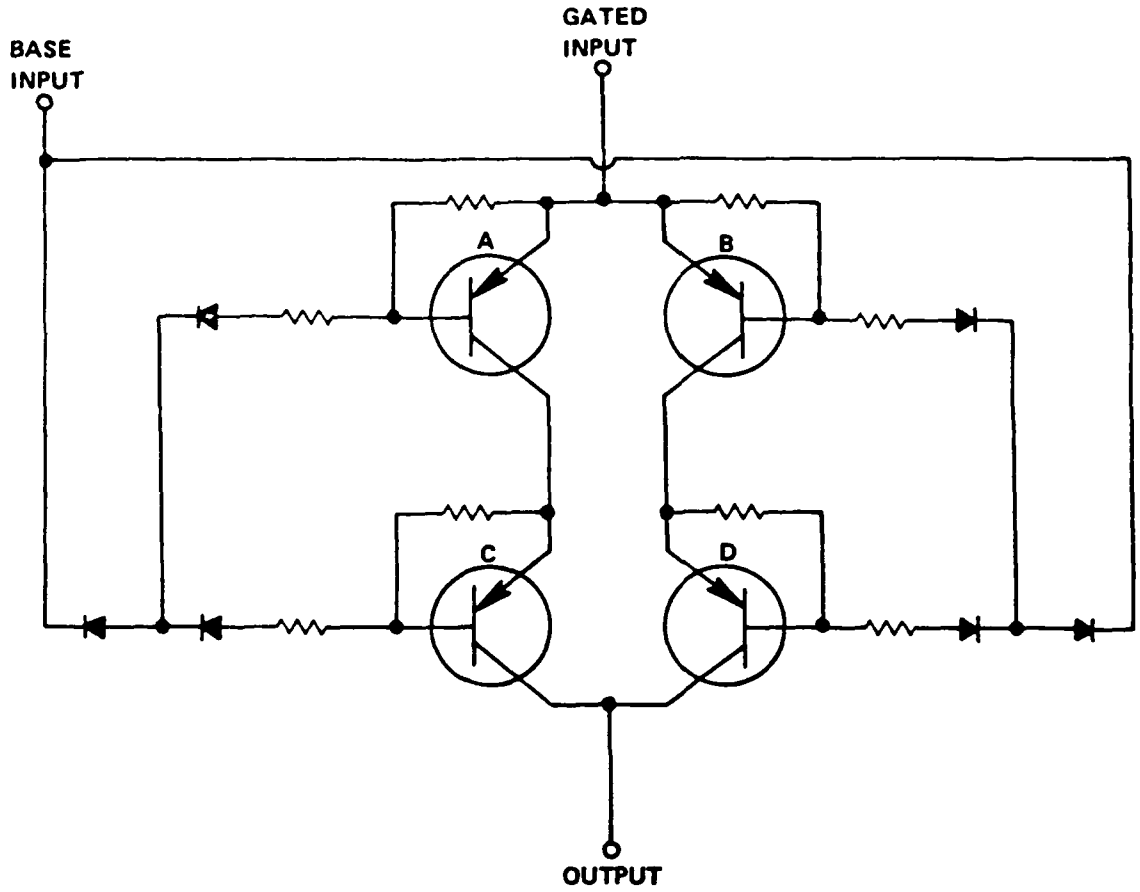
Basic Schematic Diagram
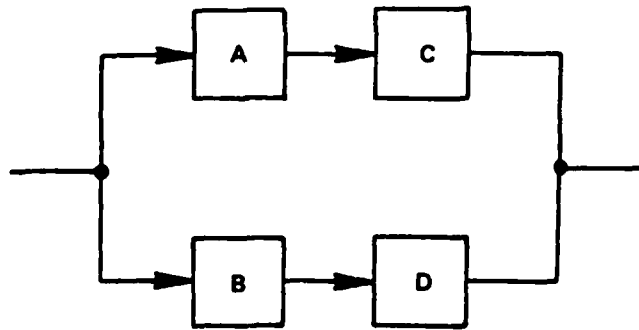
Reliability Block Diagram
Parallel-Series

$$R = 2e^{-\lambda t} - e^{-4\lambda t}$$

Parallel-Series Mathematical Model

FIGURE 7.5.3-6:   PARALLEL-SERIES REDUNDANCY CIRCUIT EXAMPLE

could cause loss of a system or one of its major functions: loss of control, unintentional release or inability to release armament stores, failure of weapon installation items, or could provide a crew safety hazard.

The incorporation of redundancy into a design must take into account "checkable redundancy." Due to redundancy inclusion, some circuits may not be checkable prior to mission start. Therefore, for some functional test prior to mission start it can only be assumed that only an item with noncheckable redundancy is functional. This does not mean that all of the redundant elements are operational. In this sense, pre-mission failures could be masked in a redundant item. This appears contradictory to the purpose of adding redundancy to improve reliability. If it is not known that redundant elements are operational prior to mission start, then the purpose of redundancy is defeated. The possibility exists of starting a mission without the deliberate redundancy designed for (a reliability loss). The designer must take into account for built-in test planning, inclusion of test points, packaging, etc., when redundancy is used in system design.

7.5.3.1   DESIGN EXAMPLES

This section presents examples of current applications of redundancy to avionics equipment. The particular examples discussed are listed below:

(1)   Simple parallel redundant precision voltage supply
(2)   Quad redundant computer building block
(3)   Majority voter redundant   8 counter
(4)   Standby redundant channels in an RF receiver

The basic mathematical derivations are given in Appendix A.

Example 1: Simple Parallel Redundancy

This example considers application of simple parallel redundancy at the circuit level centered around a precision regulated voltage supply. The circuit diagram for the basic nonredundant configuration plus part failure rates are shown in Figure 7.5.3-7.

For the nonredundant circuit, the total failure rate is given by:

$$\lambda_{Total} = \Sigma\lambda_{parts} = 10.548 \times 10^{-6} \text{ failures/hour}$$

Using an operating time of 2000 hours, the reliability for the nonredundant configuration is:

$$R = e^{-\lambda_{total}t} = e^{-(10.548 \times 10^{-6})(2 \times 10^{3})}$$

$$R = 0.979$$

Figure 7.5.3-8 shows the configuration for the redundant supply. The basic circuit is shown within the dotted lines in Figure 7.5.3-7.

Part	n	Failure Rate $(x\ 10^{-6})$	$n\ (x\ 10^{-6})$
Resistor, carbon composition	10	0.002	0.020
Capacitor, solid tantalum	4	0.038	0.152
Transformer, power	1	0.056	0.056
Transistor, silicon PNP	1	1.6	1.600
Transistor, silicon NPN	3	0.98	2.94
Diode, general purpose	6	0.68	4.08
Diode, zener	2	0.85	1.700
		TOTAL	10.548
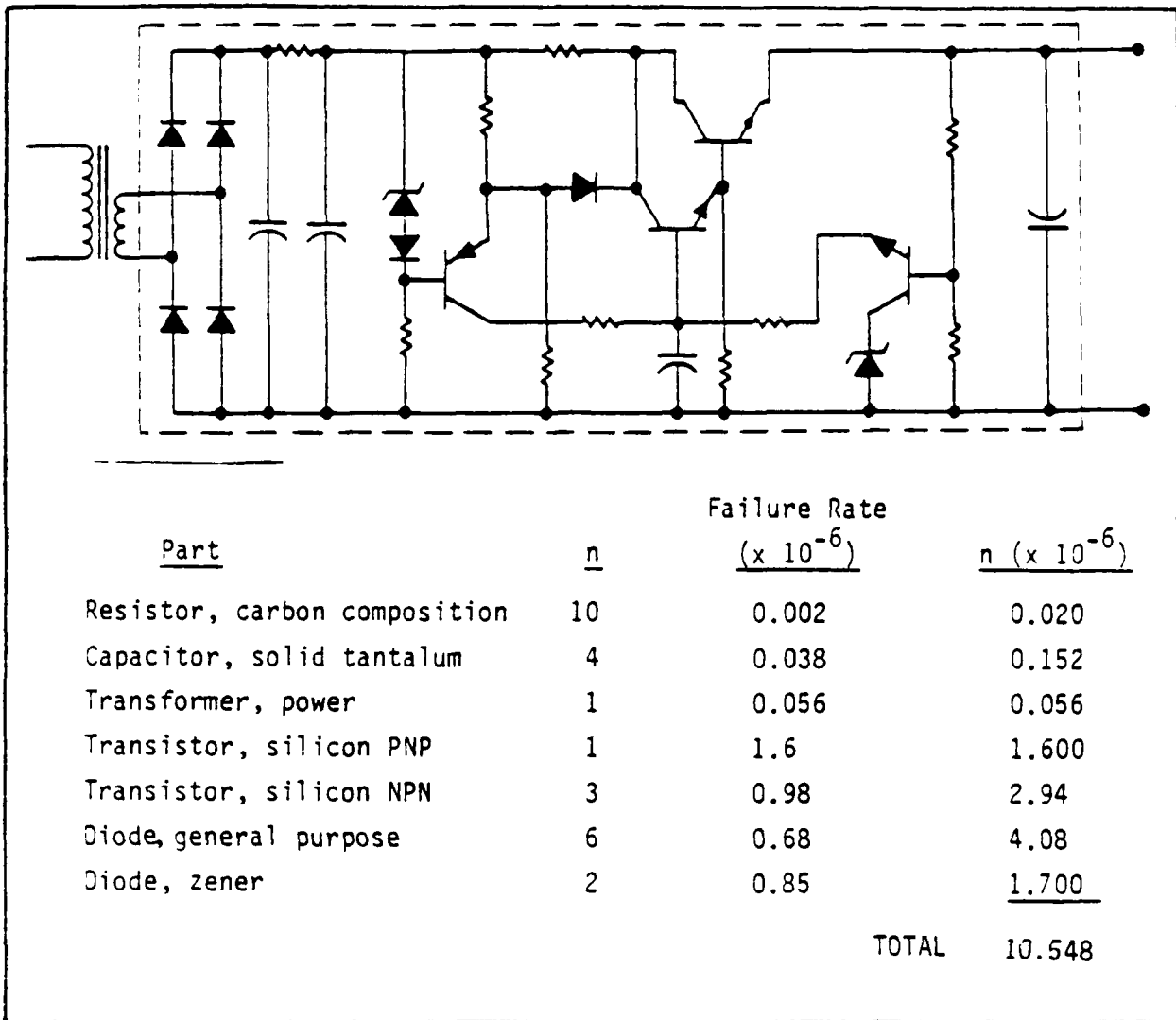
FIGURE 7.5.3-7: PRECISION REGULATED VOLTAGE SUPPLY

Redundant Circuit Configuration   Reliability Block Diagram

$$R = 2\epsilon^{-\lambda t} - \epsilon^{-2\lambda t}$$

Mathematical Model
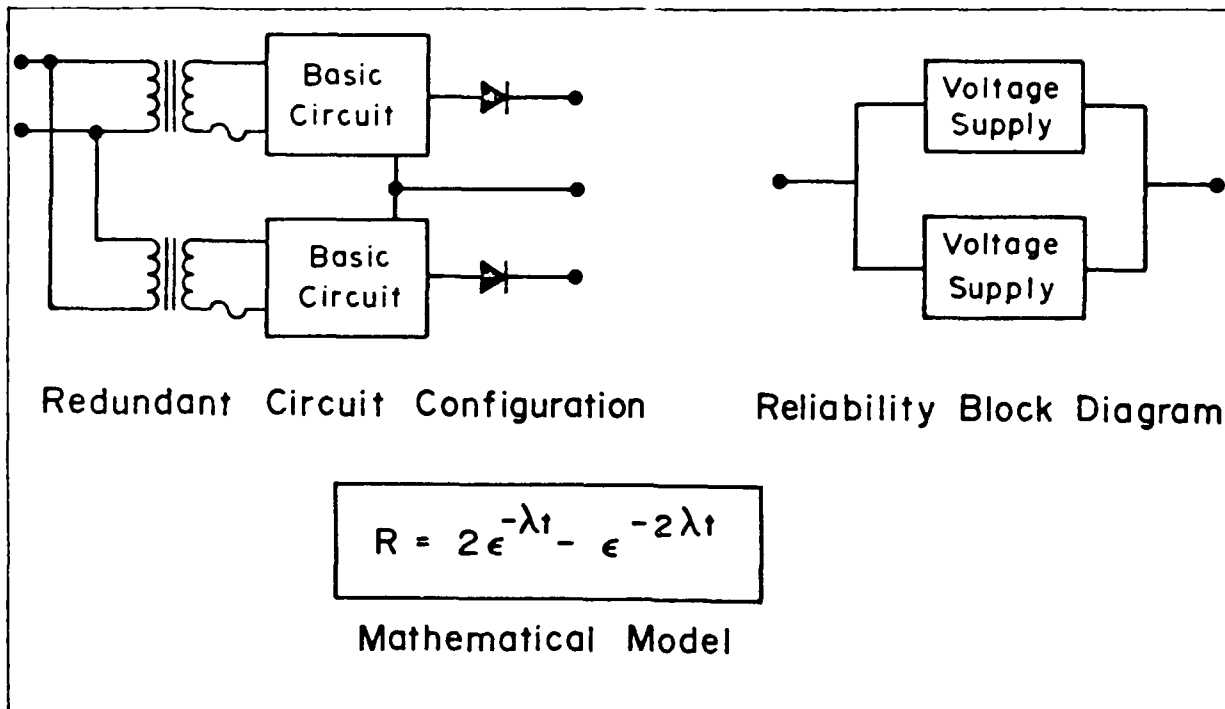
FIGURE 7.5.3-8:   REDUNDANT VOLTAGE REGULATOR SUPPLY

Using the mathematical model given in Figure 7.5.3-8, the reliability of the redundant configuration is:

$$R = 1 - (1-e^{-\lambda t})^2$$

$$R = 0.99956$$

As indicated previously, the time period used is 2000 hours. A side-by-side comparison of reliability versus time for both configurations is given in Figure 7.5.3-9 for mission times above 2000 hours. Figure 7.5.3-9 uses an expanded time axis plus a log scale on the time axis to provide greater resolution between the two curves.

Example 2: Bimodal Redundancy -- Quad Configuration

This example examines redundancy at the part level. The example chosen depicts application of a quad redundant configuration centered around a transistor and its associated biasing network. The advantage of the quad configuration is that, at the part level, it protects against both open and short failure modes. A circuit diagram and a list of failure rates is given in Figure 7.5.3-10 for the nonredundant circuit.

For the circuit shown in Figure 7.5.3-10, the total failure rate is:

$$\lambda_{total} = \Sigma\lambda_{parts} = 1.021 \times 10^{-6} \text{ failures/hour}$$

Using an operating time of 2000 hours, the reliability of the circuit is:

$$R = e^{-\lambda_{total}t} = e^{-(1.021) \times 10^{-6}) (2 \times 10^3)}$$

$$R = 0.9980$$

This circuit finds wide application in computers and other digital equipment. If 25 such circuits were to be used within an equipment and all were required to operate successfully for 2000 hours, the reliability could be expressed by

$$R = (0.9980)^{25}$$

$$R = 0.9512$$

Figure 7.5.3-11 shows the circuit diagram for the redundant quad configuration. The reliability block diagram and mathematical model are also included. Since the quad redundant circuit is used to protect against short and open failure modes, their probability of occurrence must appear in the mathematical model. However, for purposes of this example, both shorts and opens will be assumed equally likely to occur. Thus, the mathematical model used here (see Figure 7.5.3-11) is greatly simplified in contrast to a model which includes different failure mode probabilities.
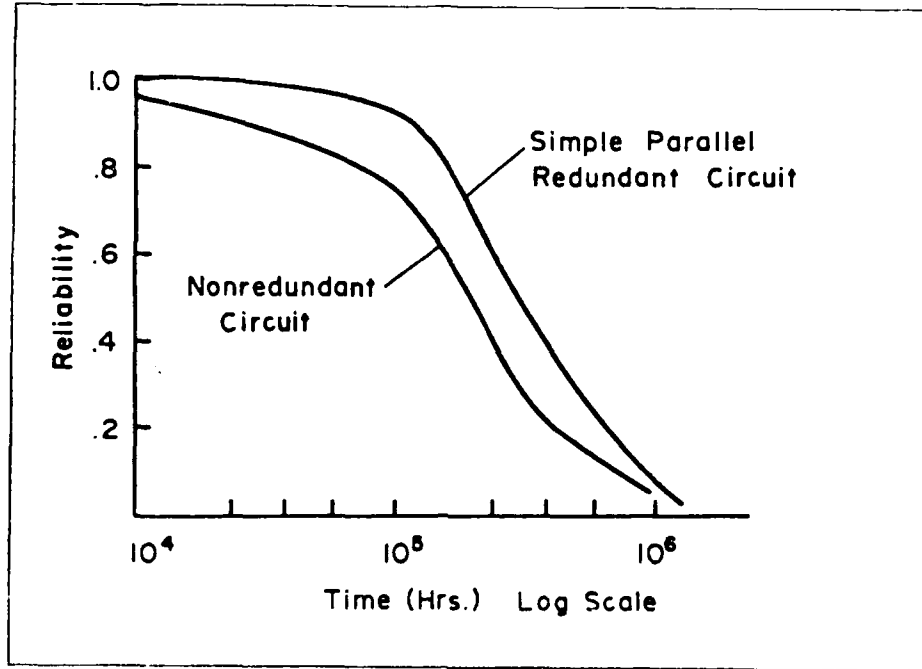
FIGURE 7.5.3-9: RELIABILITY COMPARISON OF SIMPLE REDUNDANT AND NONREDUNDANT VOLTAGE SUPPLIES
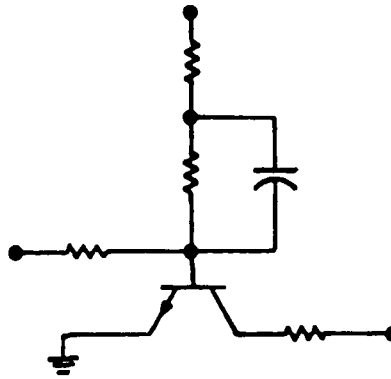
Part	n	Failure Rate $\lambda(\times 10^{-6})$	$n\lambda$
Resistor, carbon composition	4	0.002	0.008
Capacitor, ceramic	1	0.033	0.033
Transistor, NPN silicon	1	0.98	0.980
			$\overline{1.021 \times 10^{-6}}$

FIGURE 7.5.3-10: BASIC TRANSISTOR CIRCUIT

Transistor Block

Transistor Block

Transistor Block
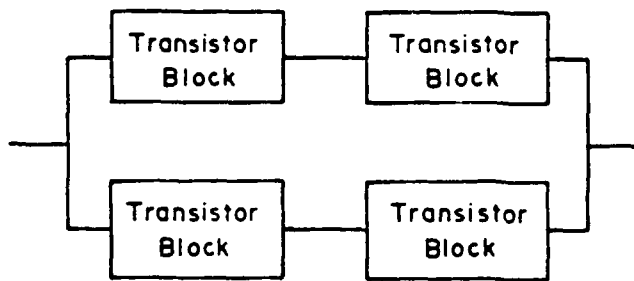
Transistor Block

Reliability Block Diagram
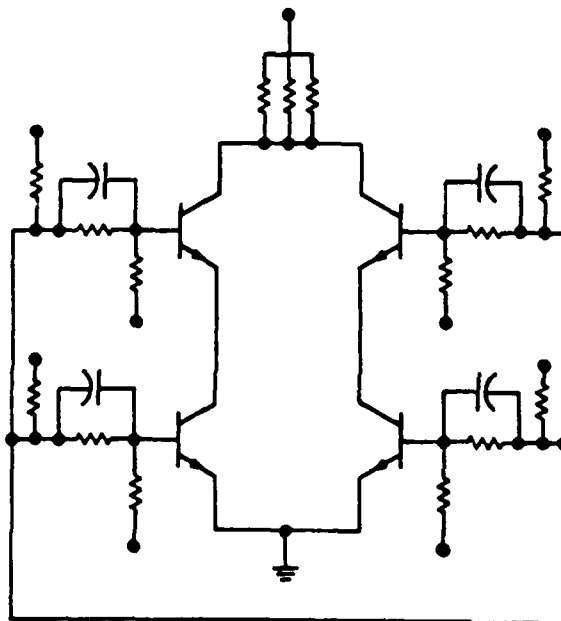
Quad Redundant Building Block

$$R = 2e^{-\lambda t} - e^{-4\lambda t}$$

Mathematical Model

FIGURE 7.5.3-11: QUAD REDUNDANT TRANSISTOR CIRCUIT

Design of the quad circuit includes the selection of three parallel resistors in the collector circuit as shown in Figure 7.5.3-11. If it is assumed that the predominant failure mode of these resistors is open, the failure of any one resistor will have a minimal effect on the power supply voltage. For simplicity of calculation, the reliability of these three resistors has been considered as part of the basic configuration rather than separate parallel redundant elements.

Using the mathematical model given in Figure 7.5.3-11, the reliability of the quad redundant configuration is:

$$R = 2e^{-2\lambda t} - e^{-4\lambda t}$$

$$R = 0.99998$$

If 25 such circuits are used, the reliability of the aggregate is given by

$$R = (0.99998)^{25}$$

$$R = 0.99958$$

A graphical comparison of these results for a single quad circuit plus the aggregate of 25 quad circuits is shown in Figure 7.5.3-12. As described in the previous example, the time scale has been expanded to show results for operating times greater than 2000 hours. A log scale is used to provide resolution between the two curves.

<u>Example 3: Majority Vote Redundancy</u>

This example presents an application of majority voting redundancy. It uses a divider logic circuit as the vehicle to show the application of redundancy. Divider circuits are frequently used in timing applications for computers and space systems. Both the divider and voter circuit are assumed to be packaged within separate integrated circuits. Figure 7.5.3-13 presents the logic diagram for a ÷ 8 counter circuit.

For an application within an orbiting satellite having a mission life of 4500 hours (approximately six months), the reliability for the nonredundant ÷ 8 counter is given by:

$$R = e^{-\lambda t} = e^{-(0.14 \times 10^{-6}) (4.5 \times 10^{3})}$$

$$R = 0.994$$

Figure 7.5.3-14 shows the circuit diagram, reliability block diagram and mathematical model for the redundant majority voting configuration for the ÷ 8 counter. A two-out-of-three majority voting circuit processes the output selection. This means that any two of the three ÷ 8 counters need to operate correctly for a proper output. The resistor/transistor networks provide for comparison of ÷ 8 counter outputs. Should the output of any ÷ 8 counter fail to match that of the remaining counters, its output would be inhibited.

(a) Single Element
(b) 25 Elements
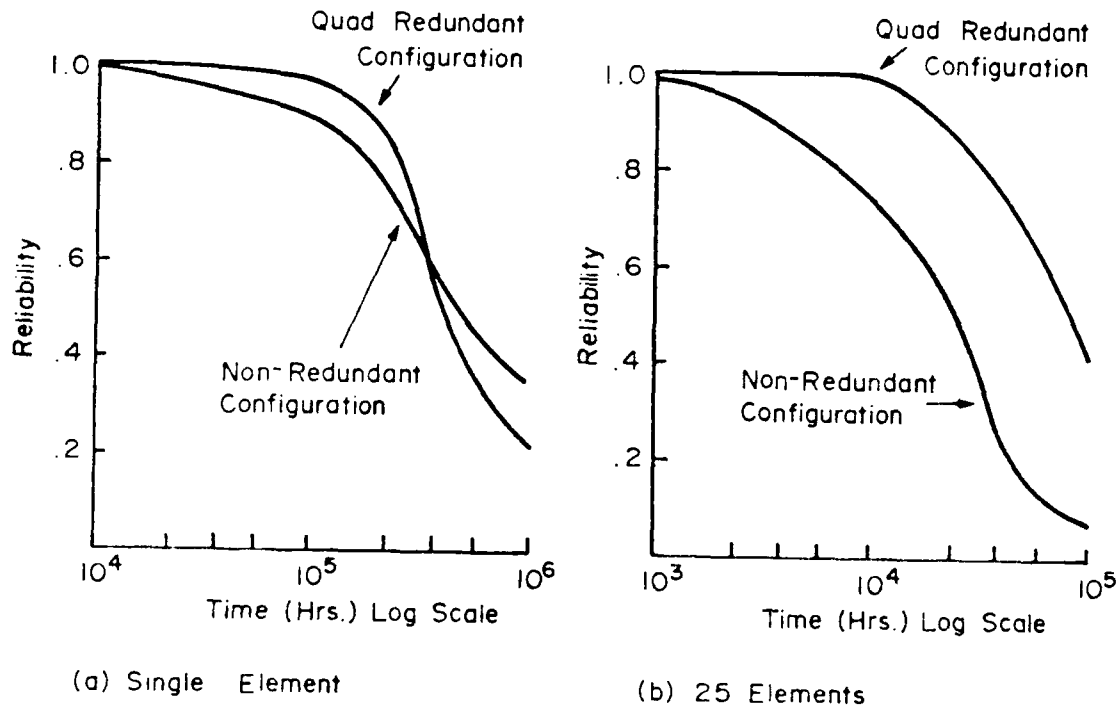
FIGURE 7.5.3-12: COMPARISON OF RELIABILITY FOR QUAD REDUNDANT AND NON-REDUNDANT TRANSISTOR CIRCUIT

It is assumed that the circuit shown above is available as a single integrated circuit.

$\lambda = 0.14 \times 10^{-6}$ failures/hour
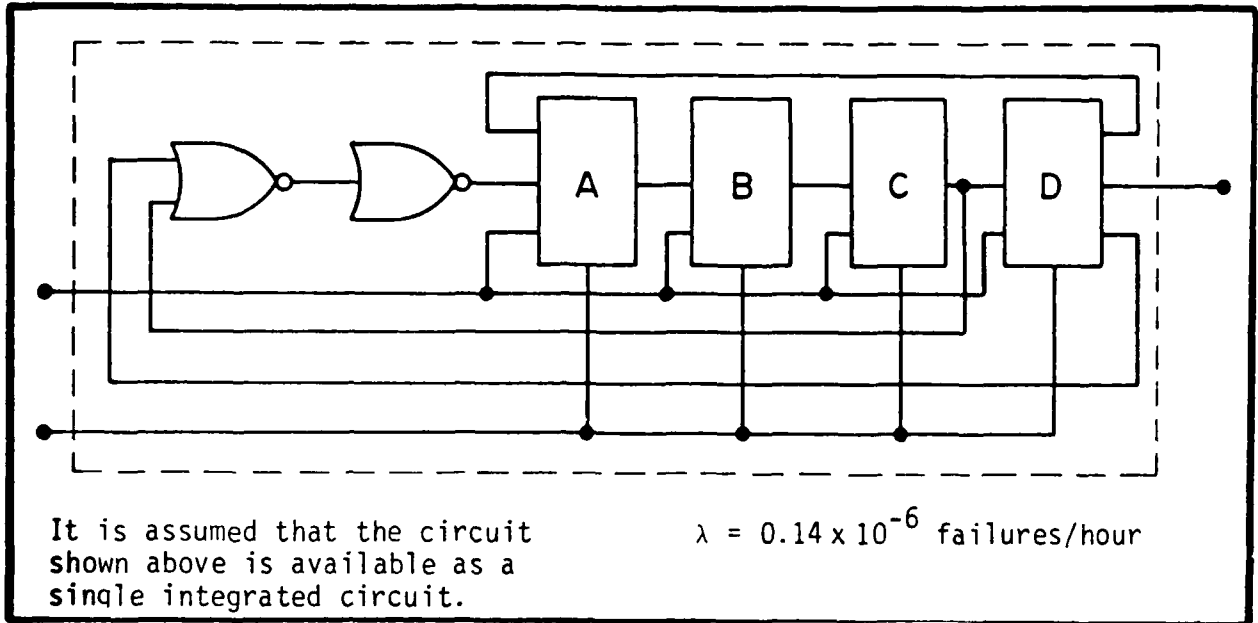
FIGURE 7.5.3-13: $\div 8$ COUNTER CIRCUIT

FIGURE 7.5.3-14:   TWO OUT OF THREE MAJORITY **VOTE REDUNDANT ÷** 8 COUNTER

Reliability Block Diagram

Redundant Circuit Schematic

Where λ_p = Failure Rate Of A Single Counter

λ_m = Failure Rate Of The Comparator Network

$$R = e^{-\lambda_m t}\left[e^{-3\lambda_p t} + 3e^{-2\lambda_p t}(1-e^{-\lambda_p t})\right]$$
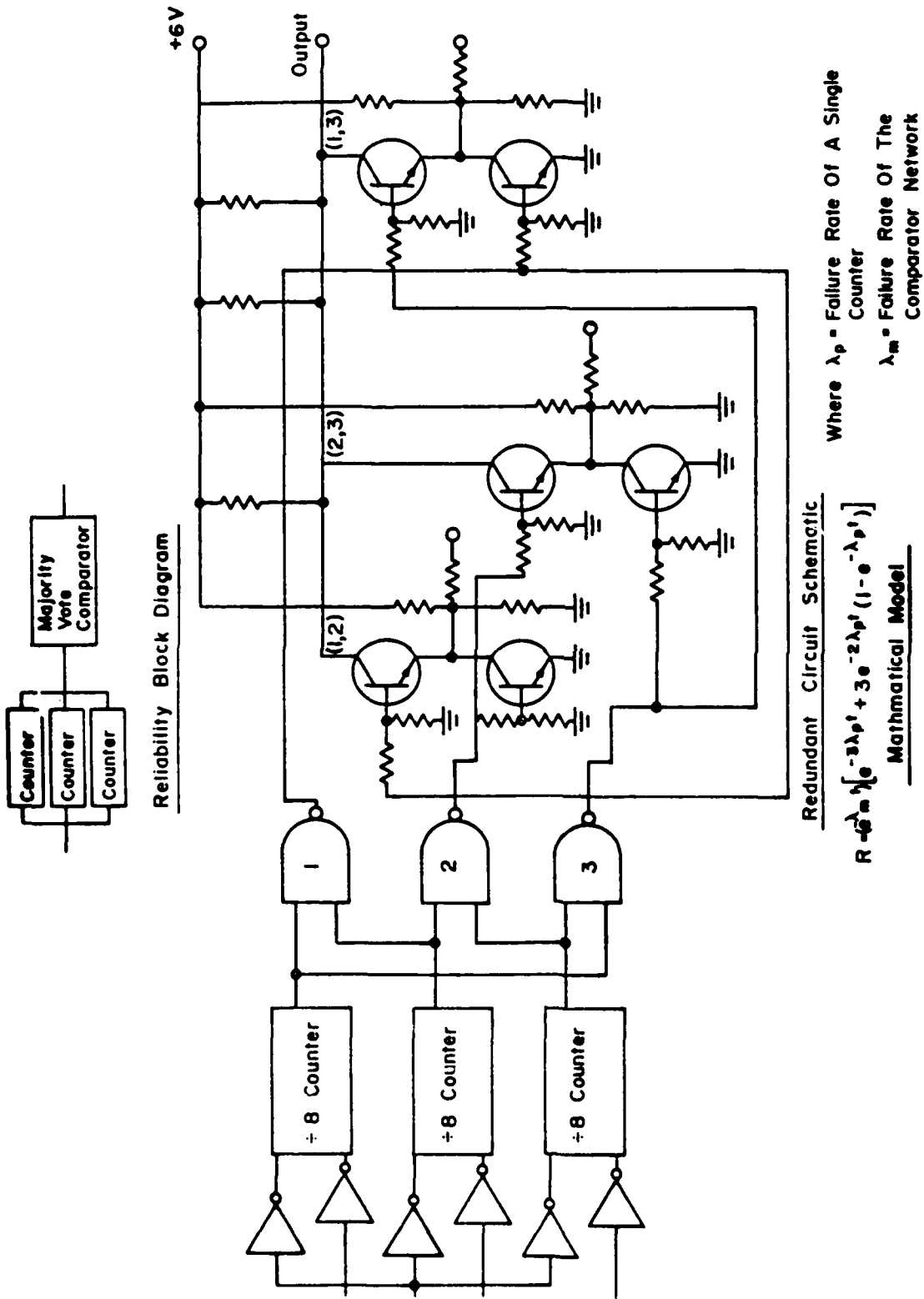
Mathmatical Model

Using the mathematical model shown in the figure, the reliability for the majority voting redundant circuit is given by:

$$R = e^{-\lambda_m t} \left[e^{-3\lambda_p t} + 3e^{-2\lambda_p t} (1 - e^{-\lambda_p t}) \right]$$

where λ_m is the total failure rate of the majority vote/integrated circuit comparator and is equal to 0.007×10^{-6} failures/hour.

For an operating time of 4500 hours,

$$R = 0.9999$$

A graphical comparison of these results in shown in Figure 7.5.3-15 for mission times above 4500 hours. Note also that the time axis has been expanded and a log scale used to provide resolution between the two curves.

Example 4: Standby Redundancy

This example shows an application of standby redundancy involving switching. This example utilizes functional R-F channels as the vehicle by which redundancy is applied. In this particular application, the redundant channels are isolated at the power input and at both the signal input and output. Switching is accomplished by MOSFETs driven by shift register stages of an address/decode circuit using high voltage amplifiers (Ref. 13). Each channel within the redundant configuration consists of:

    (1) R-F associated circuitry
    (2) Oscillator/mixer and associated circuitry
    (3) IF and associated circuitry
    (4) Detector and associated circuitry
    (5) High voltage amplifier
    (6) Shift register
    (7) MOSFETs

Figure 7.5.3-16 presents a diagram for a single (nonredundant) R-F receiver channel plus failure rates for the various functional circuits. The total failure rate for a single channel is:

$$\lambda_{Channel} = \Sigma \lambda_{circuits}$$
$$= 52.0 \times 10^{-6} \text{ failures/hour}$$

For a 2000 hour operating time, the reliability is:

$$R = e^{-\lambda_{ch} t} = e^{-(52.0 \times 10^{-6})(2000)}$$

$$R = 0.901$$

Figure 7.5.3-17 snows the circuit diagram, reliability block diagram and mathematical model for the two channel redundant configuration. The additional circuitry needed to implement the switching function and isolation between channels (λ_s) are listed below. Circuit failure rates are also given:
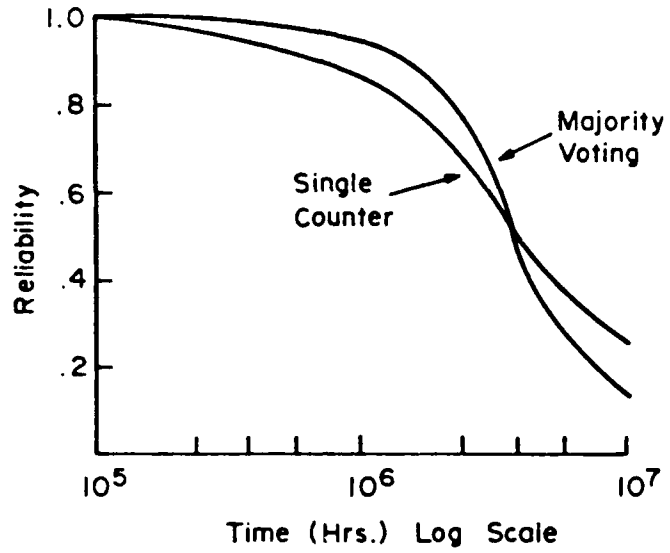
FIGURE 7.5.3-15: <u>RELIABILITY COMPARISON FOR REDUNDANCY & NON-REDUNDANT ÷8 COUNTER CONFIGURATION</u>
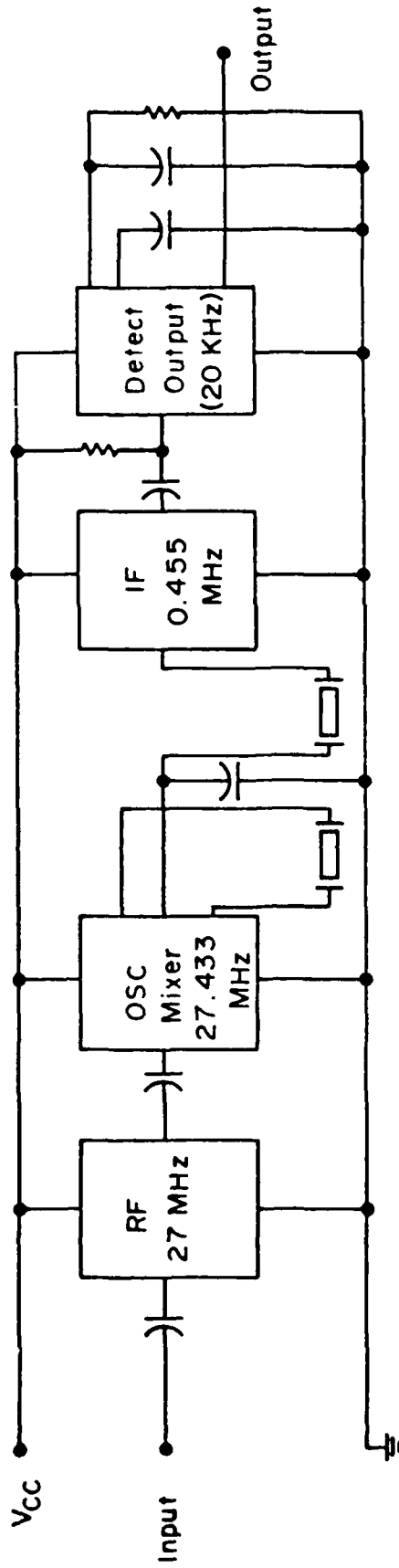
Circuit	Failure Rate ($\times 10^{-6}$)
RF Amplifier And Associated Circuitry	20.5
Oscillator / Mixer And Associated Circuitry	8.4
IF Amplifier And Associated Circuitry	16.2
Detector And Associated Circuitry	6.9
	52.0

FIGURE 7.5.3-16: NON - REDUNDANT RF AMPLIFIER CHANNEL

Reliability Block Diagram

Simplified Circuit Block Diagram

Redundant Circuit Block Diagram

Mathematical Model

$$R = e^{-\lambda CH t} \left[1 + \frac{\lambda CH}{\lambda_s} (1 - e^{-\lambda_s t_j}) \right]$$
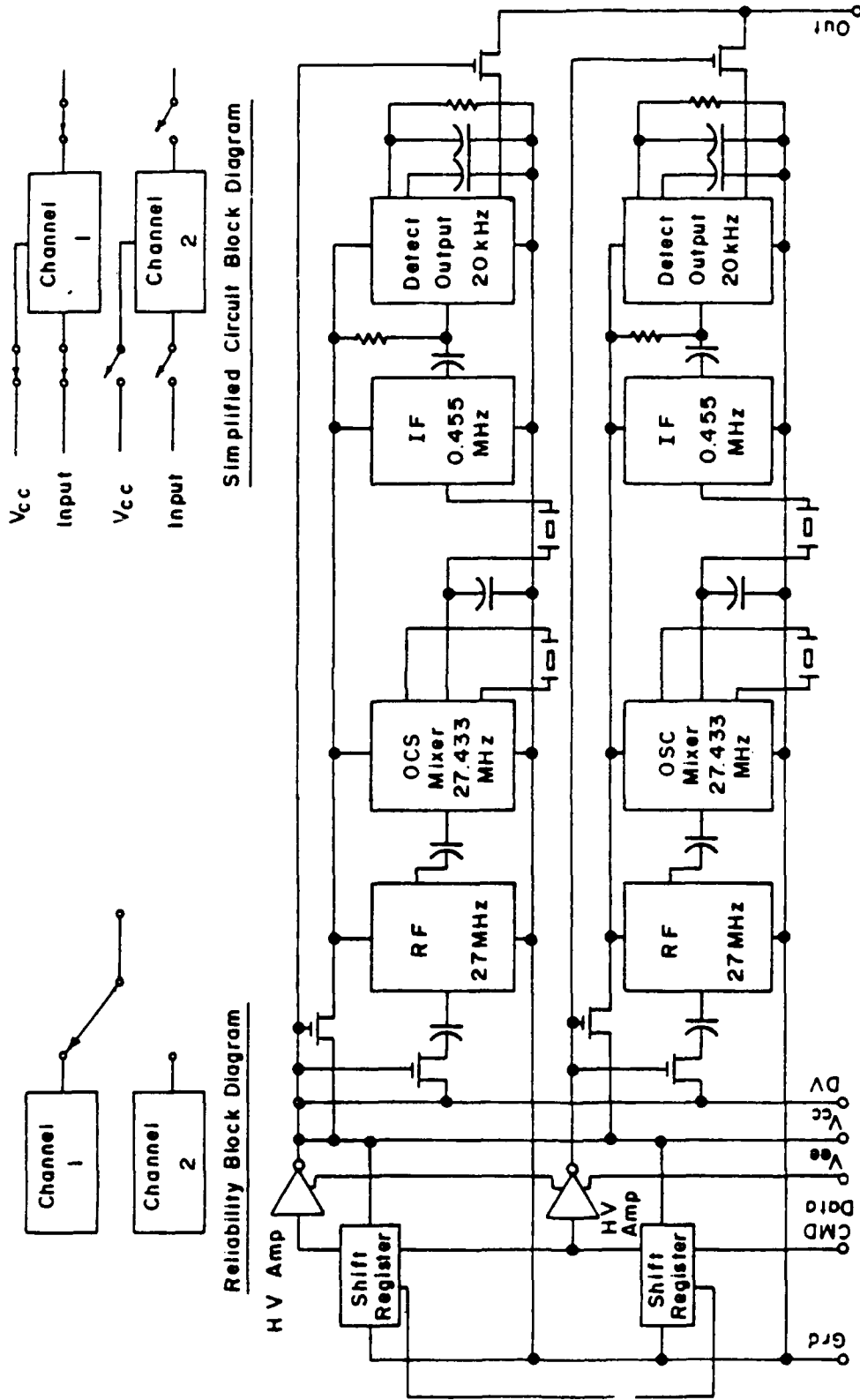
FIGURE 7.5.3-17: STANDBY REDUNDANT TWO CHANNEL R RECEIVER

Circuit	n	Failure Rate λ (x 10^{-6})	$n\lambda$
Shift register	1	0.23	0.23
High voltage amplifier	1	0.15	0.15
MOSFET output isolators	3	2.70	8.10

$$\text{Total} = 8.48 (\times 10^{-6}) = \lambda_s$$

Using the mathematical model shown in Figure 7.5.3-17, the reliability for the standby redundant R-F receiver is:

$$R = e^{-\lambda_{ch} t} \left\{ 1 + \left[1 + \frac{\lambda_{ch}}{\lambda_s} (1 - e^{-\lambda_s t}) \right] \right\}$$

$$R = 0.9939$$

The results of both redundant and nonredundant configurations are compared in Figure 7.5.3-18.

7.5.4 FURTHER REDUNDANCY CONSIDERATIONS

One has only to read the issues of the IEEE Transactions on Reliability in order to appreciate the diversity of redundancy reliability models.

See Appendix A for additional details on redundancy model and design techniques.
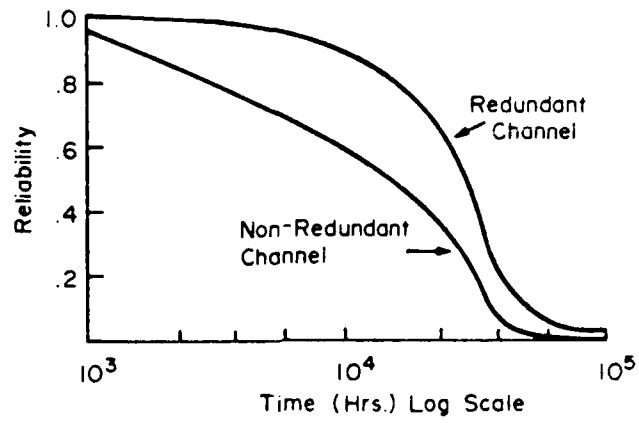
FIGURE 7.5.3-18: RELIABILITY COMPARISON OF REDUNDANT & NON-REDUNDANT RF RECEIVER CHANNELS

7.6 ENVIRONMENTAL DESIGN

7.6.1 INTRODUCTION

A series of Engineering Design Handbooks deals explicitly, and in great detail, with environmental design problems (Refs. 14-18). Those handbooks should be consulted for specific information. Also, Appendix B of this section provides some general considerations of environment in design, including environmental factors which exert a strong influence on reliability, and the effect of environment on hardware.

This section will concentrate on some general environmental design considerations against specific environments. Many of the details on environmental prediction and specific design methods are in the previously mentioned documents, particularly Appendiv B.

7.6.2 DESIGNING FOR THE ENVIRONMENT

Equipment failures have three convenient classifications:

  (1) Poor design or incorrect choice of materials or components
  (2) Inadequate quality control which permits deviations from design specifications
  (3) Deterioration caused by environmental effects or influences

Obviously, the first and third classes are related. Specifically, the careful selection of design and materials can extend item reliability by reducing or eliminating adverse environmental effects. Needless to say, this is not a profound thought, but merely one that is sometimes forgotten or perhaps relegated to mental footnotes. The environment is neither forgiving nor understanding; it methodically surrounds and attacks every component of a system, and when a weak point exists, the equipment reliability suffers. Design and reliability engineers, therefore, must understand the environment and its potential effects, and then must select designs or materials that counteract these effects or must provide methods to alter or control the environment within acceptable limits. Selecting designs or materials that withstand the environment has the advantage of not requiring extra components that also require environmental protection and add weight and costs.

In addition to the obvious environments of temperature, humidity, shock, and vibration, the design engineer will create environments by his choice of designs and materials. A gasket or seal, for example, under elevated temperatures or reduced pressures may release corrosive or degrading volatiles into the system. Teflon may release fluorine, and polyvinylchloride (PVC) may release chlorine. Certain solid rocket fuels are degraded into a jelly like mass when exposed to aldehydes or

ammonia, either of which come from a phenolic nozzle cone. These examples illustrate that internal environments designed into the system can seriously affect reliability.

Many aids are available to design and reliability engineers in selecting materials and components, e.g., the text, Deterioration of Materials, Causes and Preventive Techniques, by Glenn A. Greathouse and Carl J. Wessel. In addition, military specifications, standards, and handbooks provide both general and specific guidance on this subject.

7.6.3 TEMPERATURE PROTECTION

Heat and cold are powerful agents of chemical and physical deterioration for two very simple, basic reasons.

(1) The physical properties of almost all known materials are modified greatly by changes in temperature.

(2) The rate of almost all chemical reactions is influenced markedly by the temperature of the reactants. A familiar rule-of-thumb for chemical reactions (Ref. 8) is that the rate of many reactions doubles for every rise in temperature of $10^\circ C$; this is equivalent to an activation energy of about 0.6 eV.

Basically, heat is transferred by three methods: (1) radiation, (2) conduction, and (3) convection. One, or a combination of these three methods, therefore, is used to protect against temperature degradation. High temperature degradation can be minimized by passive or active techniques. Passive techniques use natural heat sinks to remove heat, while active techniques use devices such as heat pumps or refrigeration units to create heat sinks. Such design measures as compartmentation, insulation of compartment walls, and intercompartment and intrawall air flow can be applied independently or in combination. Every system component should be studied from two viewpoints:

(1) Is a substitute available that will generate less heat?

(2) Can the component be located and positioned so that its heat has minimum effect on other components?

For a steady temperature, heat must be removed at the same rate at which it is generated. Thermal systems such as conduction cooling, forced convection, blowers, direct or indirect liquid cooling, direct vaporization or evaporation cooling, and radiation cooling must be capable of handling natural and induced heat sources.

Passive sinks require some means of progressive heat transfer from intermediate sinks to ultimate sinks until the desired heat extraction has been achieved. Thus, when heat sources have been identified, and heat removal elements selected, they must be integrated into an overall heat removal system, so that heat is not merely redistributed within the system. Efficiently integrated heat removal techniques can significantly improve item reliability.

Besides the out-gassing of corrosive volatiles when subjected to heat, almost all known materials will expand or contract when their temperature is changed. This expansion and contraction causes problems with fit between parts, sealing, and internal stresses. Local stress concentrations due to nonuniform temperature are especially damaging, because they can be so high. A familiar example is a hot water glass that shatters when immersed in cold water. Metal structures, when subjected to cyclic heating and cooling, may ultimately collapse due to the induced stresses and fatigue caused by flexing. The thermocouple effect between the junction of two dissimilar metals causes an electric current that may induce electrolytic corrosion. Plastics, natural fibers, leather, and both natural and synthetic rubber are all particularly sensitive to temperature extremes as evidenced by their brittleness at low temperatures and high degradation rates at high temperatures. Table 7.6.3-1 summarizes some the basic precautions for reliability at low temperatures. An always present danger is that in compensating for one failure mode, the change will aggravate another failure mode.

TABLE 7.6.3-1: LOW TEMPERATURE PROTECTION METHODS

Effect	Preventive Measures
Differential contraction	Careful selection of materials Provision of proper clearance between moving parts Use of spring tensioners and deeper pulleys for control cables Use of heavier material for skins
Lubrication stiffening	Proper choice of lubricants: o Use greases compounded from silicones, diesters or silicone diesters thickened with lithium stearate o Eliminate liquid lubricants wherever possible
Leaks in hydraulic systems	Use of low temperature sealing and packing compounds, such as silicone rubbers
Stiffening of hydraulic system	Use of proper low temperature hydraulic fluids
Ice Damage caused by freezing of collected water	Elimination of moisture by: o Provision of vents o Ample draining facilities o Eliminating moisture pockets o Suitable heating o Sealing o Desiccation of air
Degradation of material properties and component reliability	Careful selection of materials and components with satisfactory low temperature capabilities

The preferred method for evaluating the thermal performance of electronic equipment (with respect to reliability) is a parts stress analysis method (per MIL-HDBK-217) which determines the maximum safe temperatures for constituent parts. The parts stress analysis method for evaluating system thermal performance is based on a determination of the maximum allowable temperature for each part. This determination is to be consistent with the equipment reliability and the failure rate allocated to that part.

A reduction in the operating temperature of components is a primary method for improving reliability. This is generally possible by providing a thermal design which reduces heat input to minimally achievable levels and provides low thermal resistance paths from heat producing elements to an ultimate heat sink of reasonably low temperature. The thermal design is often as important as the circuit design in obtaining the necessary performance and reliability characteristics of electronic equipment. Adequate thermal design maintains equipment and parts within their permissible operating temperature limits under operating conditions. Thermal design is an engineering discipline in itself, and will not be addressed in this section. The best existing document on thermal design is MIL-HDBK-251. It provides a very comprehensive review of the aspects of thermal design. Also, Chapter 9 of Ref. 19 discusses the subject in some detail.

7.6.4 SHOCK AND VIBRATION PROTECTION

Protection against mechanical abuse is generally achievable by use of suitable packaging, mounting, and structural techniques. The reliability impact of mechanical protection techniques is generally singular in that these measures do or do not afford the required protection against the identified mechanical abuse stresses. In most cases, tradeoff situations between the level of protection and reliability improvements are not as pronounced as in the case of thermal protection. The one exception may be the case of fatigue damage, where the level of protection would have a significant impact on reliability if, in fact, fatigue was a primary failure mechanism in the normal life of the equipment.

Basic structural design techniques, such as proper component location and selection of suitable materials, can aid in protecting an item against failure caused by severe environmental stresses from shock or vibration.

There are two approaches that may be taken when shock or vibration are present; either isolate the equipment or build it to withstand the shock or vibration. The problem with isolation is that effective, simultaneous control of both shock and vibration is difficult. When only one or the other is present, special mountings are often used. Protective measures against shock and vibration stresses are generally determined by an analysis of the deflections and mechanical stresses produced by these environment factors. This generally involves the determination of natural frequencies and evaluation of the mechanical stresses within

component and materials produced by the shock and vibration environment. If the mechanical stresses so produced are below the allowable safe working stress of the materials involved, no direct protection methods are required. If, on the other hand, the stresses exceed the safe levels, corrective measures such as stiffening, reduction of inertia and bending moment effects, and incorporation of further support members are indicated. If such approaches do not reduce the stresses below the safe levels, further reduction is usually possible by the use of shock absorbing mounts.

One factor, however, which is not often considered, is that the vibration of two adjacent components, or separately insulated subsystems, can cause a collision between them if maximum excursions and sympathetically induced vibrations are not evaluated by the designer. Another failure mode, fatigue (the tendency for a metal to break under cyclic stressing loads considerably below its tensile strength) is an area of reliability concern due to shock or vibration. This includes low cycle fatigue, acoustic fatigue, and fatigue under combined stresses. The interaction between multiaxial fatigue and other environmental factors such as temperature extremes, temperature fluctuations, and corrosion requires careful study. Stress-strength analysis of components and parameter variation analysis are particularly suited to these effects. Destruction testing methods are also very useful in this area. For one shot devices, several efficient nondestructive evaluation (NDE) methods are available - such as X ray, neutron radiography, and dye penetrant - which can be used to locate fatigue cracks. Developing a simple design that is reliable is much better than elaborate fixes and subsequent testing to redesign for reliability.

In addition to using proper materials and configuration, the shock and vibration experienced by the equipment ought to be controlled. In some cases, however, even though an item is properly insulated and isolated against shock and vibration damage, repetitive forces may loosen the fastening devices. Obviously, if the fastening devices loosen enough to permit additional movement, the device will be subjected to increased forces and may fail. Many specialized self locking fasteners are commercially available, and fastener manufacturers usually will provide valuable assistance in selecting the best fastening methods.

An isolation system can be used at the source of the shock or vibration, in addition to isolating the protected component. The best results are obtained by using both methods. Damping devices are used to reduce peak oscillations, and special stabilizers employed when unstable configurations are involved. Typical examples of dampeners are viscous hysteresis, friction, and air damping. Vibration isolators commonly are identified by their construction and material used for the resilient elements (rubber, coil spring, woven metal mesh, etc.). Shock isolators differ from vibration isolators in that shock requires stiffer springs and a higher natural frequency for the resilient element. Some of the types of isolation mounting systems are underneath, over-and-under, and inclined isolators.

A specific component may initially appear to be sufficiently durable to withstand the anticipated shock or vibration forces without requiring isolation or insulation. However, this observation can be misleading since the attitude in which a part is mounted, its location relative to other parts, its position within the system, and the possibility of its fasteners or another component fasteners coming loose can alter significantly the imposed forces. Another component, for example, could come loose and strike it, or alter the forces acting on it to the extent that failure results.

The following basic considerations must be included in designing for shock and vibration:

(1) The location of the component relative to the supporting structure (i.e., at the edge, corner, or center of the supporting structure).

(2) The orientation of the part with respect to the anticipated direction of the shock or vibration forces.

(3) The method used to mount the part.

7.6.5 MOISTURE PROTECTION

Moisture is a chemical and, considering its abundance and availability in almost all environments, is probably the most important chemical deteriorative factor of all. Moisture is not simply H_2O, but usually is a solution of many impurities; these impurities cause many of the chemical difficulties. In addition to its chemical effects, such as the corrosion of many metals, condensed moisture also acts as a physical agent. An example of the physical effects of moisture is the damage done in the locking together of mating parts when moisture condenses on them and then freezes. Similarly, many materials that are normally pliable at low temperatures will become hard and perhaps brittle if moisture has been absorbed and subsequently freezes. Condensed moisture acts as a medium for the interaction between many, otherwise relatively inert, materials. Most gases readily dissolve in moisture. The chlorine released by PVC plastic, for example, forms hydrochloric acid when combined with moisture.

Although the presence of moisture may cause deterioration, the absence of moisture also may cause reliability problems. The useful properties of many nonmetallic materials, for example, depend upon an optimum level of moisture. Leather and paper become brittle and crack when they are very dry. Similarly, fabrics wear out at an increasing rate as moisture levels are lowered and fibers become dry and brittle. Dust is encountered in environments and can cause increased wear, friction, and clogged filters due to lack of moisture.

Moisture, in conjunction with other environmental factors, creates difficulties that may not be characteristic of the factors acting alone. For example, abrasive dust and grit, which would otherwise escape, are trapped by moisture. The permeability (to water vapor) of some plastics

(PVC, polystryene, polyethylene, etc.) is related directly to their temperature. The growth of fungus is enhanced by moisture, as is the galvanic corrosion between dissimilar metals.

Some design techniques that can be used singly or combined to counteract the effects of moisture are: (1) elimination of moisture traps by providing drainage or air circulation; (2) using desiccant devices to remove moisture when air circulation or drainage is not possible; (3) applying protective coatings; (4) providing rounded edges to allow uniform coating of protective material; (5) using materials resistant to moisture effects, fungus, corrosion, etc.; (6) hermetically sealing components, gaskets and other sealing devices; (7) impregnating or encapsulating materials with moisture resistant waxes, plastics, or varnishes; and (8) separation of dissimilar metals, or materials that might combine or react in the presence of moisture, or of components that might damage protective coatings. The designer also must consider possible adverse effects caused by specific methods of protection. Hermetic sealing, gaskets, protective coatings, etc., may, for example, aggravate moisture difficulties by sealing moisture inside or contributing to condensation. The gasket materials must be evaluated carefully for outgassing of corrosive volatiles or for incompatibility with adjoining surfaces or protective coatings.

MIL-STD-454 provides common requirements for electronic equipment related to corrosion protection (Requirement 15), dissimilar metals (Requirement 16), and moisture pockets (Requirement 31).

7.6.6 SAND AND DUST PROTECTION

In addition to the obvious effect of reduced visibility, sand and dust primarily degrade equipment by:

(1) Abrasion leading to increased wear
(2) Friction causing both increased wear and heat
(3) Clogging of filters, small apertures, and delicate equipment

Thus, equipment having moving parts requires particular care when designing for sand and dust protection. Sand and dust will abrade optical surfaces, either by impact when being carried by air, or by physical abrasion when the surfaces are improperly wiped during cleaning. Dust accumulations have an affinity for moisture and, when combined, may lead to corrosion or the growth of fungus.

In the relatively dry regions, such as deserts, fine particles of dust and sand readily are agitated into suspension in the air, where they may persist for many hours, sometimes reaching heights of several thousand feet. Thus, even though there is virtually no wind present, the speeds of vehicles or vehicle transported equipment through these dust clouds can cause surface abrasion by impact, in addition to the other adverse effects of the sand or dust.

Although dust commonly is considered to be fine, dry particles of earth, it also may include minute particles of metals, combustion products, solid chemical contaminants, etc. These other forms may provide direct corrosion or fungicidal effects on equipment, since this dust may be alkaline, acidic, or microbiological.

Since most equipment requires air circulation for cooling, removing moisture, or simply functioning, the question is not whether to allow dust to enter, but, rather, how much or what size dust can be tolerated. The problem becomes one of filtering the air to remove dust particles above a specific nominal size. The nature of filters, however, is such that for a given working filter area, as the ability of the filter to stop increasingly smaller dust particles is increased, the flow of air or other fluid through the filter is decreased. Therefore, the filter surface area either must be increased, the flow of fluid through the filter decreased, or the allowable particle size increased, i.e., invariably, there must be a compromise. Interestingly enough, a study by R.V. Pavia (Ref. 20) showed that, for aircraft engines, the amount of wear was proportional to the weight of ingested dust, but that the wear produced by 100 m dust as approximately half that caused by 15 m dust. The 15 m dust was the most destructive of all sizes tried.

Sand and dust protection, therefore, must be planned in conjunction with protective measures against other environmental factors. It is not practical, for example, to specify a protective coating against moisture if sand and dust will be present, unless the coating is carefully chosen to resist abrasion and erosion, or is self healing.

7.6.7 EXPLOSION PROOFING

Protection against explosion is both a safety and reliability problem. An item that randomly exhibits explosive tendencies is one that has undesirable design characteristics and spectacular failure modes. This type of functional termination, therefore, requires extreme care in design and reliability analyses.

Explosion protection planning must be directed to three categories (not necessarily mutually exclusive) of equipment:

(1) Items containing materials susceptible to explosion
(2) Components located near enough to cause the explosive items to explode
(3) Equipment that might be damaged or rendered temporarily inoperative by overpressure, flying debris, or heat from an explosion.

The first category includes devices containing flammable gases or liquids, suspensions of dust in the air, hypergolic materials, compounds which spontaneously decompose in certain environments, equipment containing or subjected to high or low extremes of pressure (includes implosions), or any other systems capable of creating an explosive reaction. The second category is fairly obvious and includes many

variations on methods for providing an energy pulse, a catalyst, or a specific condition that might trigger an explosion. A nonexplosive component, for example, could create a corrosive atmosphere, mechanical puncture, or frictional wear on the side of a vessel containing high pressure air and thereby cause the air container to explode. The third category encompasses practically everything, including items in the first two categories, since a potentially explosive device (such as a high pressure air tank) can be damaged or made to explode by the overpressure from another explosion. Thus, some reasoning must be applied when considering devices not defined by the first two categories. From a practical standpoint, explosion protection for items in the third category ought to be directed to equipment that might possibly be near explosions. The sides of an electronic maintenance van, for example, will be subjected to overpressures from exploding enemy artillery rounds. If designed for protection against anything but a direct hit, the van would be extremely difficult to transport. Thus, mobility (and size) and protections against blast are traded off. On the other end of the compromise scale, however, is the bad effect on the reliability of internal equipment when explosion protection is minimal or nonexistent.

The possiblity of an explosive atmosphere leaking or circulating into other equipment compartments must be recognized. Lead acid batteries, for example, create hydrogen gas that, if confined or leaked into a small enclosure, could be exploded by electrical arcing from motor brushes, by sparks from metallic impacts, or by exhaust gases. Explosive environments, such as dust laden air, might be circulated by air distribution systems.

Explosion protection and safety are very important for design and reliability evaluations, and must be closely coordinated and controlled. Just as safe equipment is not necessarily reliable, neither is reliable equipment necessarily safe; but the two can be compatible, and often are.

7.6.8 ELECTROMAGNETIC RADIATION PROTECTION

The electromagnetic spectrum is divided conveniently into several categories ranging from gamma rays at the short wavelength end through X rays, ultraviolet, visible, infrared, and radio, to the long wavelength radiation from power lines. Solar radiation is the principal reliability concern. Damage near the surface of the earth is caused by the electromagnetic radiation in the wavelength range from approximately 0.15 to 5 m. This range includes the longer ultraviolet rays, visible light, and up to about midpoint in the infrared band. Visible light accounts for roughly one-third of the solar energy falling on the earth, with the rest being in the invisible ultraviolet and infrared ranges. The solar constant (the quantity of radiant solar heat received normally at the outer layer of the atmosphere of the earth) is, very roughly, about 1 kilowatt per square meter. In some parts of the world, almost this much can fall on a horizontal surface on the ground at noon.

Solar radiation principally causes physical or chemical deterioration of materials. Examples are the effects due to the increased temperature and deterioration of natural and synthetic rubber. These are mechanical effects. Radiation also can cause functional effects, such as the temporary electrical breakdown of semiconductor devices exposed to ionizing radiation. Considerations to include in a radiation protection analysis are the type of irradiated material and its characteristics of absorption and sensitivity to specific wavelengths and energy levels, ambient temperature, and proximity of reactive substances such as moisture, ozone, and oxygen. Some specific protection techniques are shielding, exterior surface finishes that will absorb less heat and are less reactive to radiation effects of deterioration, minimizing exposure time to radiation, and removing possibly reactive materials by circulation of air or other fluids or by careful location of system components. More extensive information is given in Reference 45.

Another form of natural electromagnetic radiation is that associated with lightning. It is estimated that lightning strikes the earth about 100 times each second, each stroke releasing large bursts of electromagnetic energy which encircle the globe. Most of this energy is concentrated at the low frequency end of the electromagnetic spectrum with the maximum power level being concentrated at about 3 kHz.

Manmade electromagnetic energy is another form and is of far greater importance when solar energy is excluded. Artificial electromagnetic radiators include power distribution systems, a multitude of uses in communications, and specialized detection and analytical applications. The development of lasers has introduced another intense source of electromagnetic radiation and, in military application, the electromagnetic pulse (EMP) associated with nuclear weapon detonations is of considerable importance.

The EMP spectrum is similar to that created by lightning with a maximum energy appearing at about 10 kHz but distributed with smaller amplitudes throughout a broad region of the frequency spectrum. EMP energy is of considerably greater magnitude than that observed in lightning and extends over a much larger area of the earth. Despite the similarities among EMP and lightning and other strong sources of electromagnetic energy, it cannot be assumed that protective measures consistent with these other electromagnetic radiation sources will protect material from the effects of EMP. The rapid rise time of the pulse associated with a nuclear detonation and the strength of the resulting pulse are unique.

A variety of effects of electomagnetic radiation on material are known, probably a number of effects are still unrecognized, and there are some poorly understood effects on man. Of course, one of the most important effects of electromagnetic radiation in the environment is the electromagnetic interference (EMI) it produces on the effective use of the electromagnetic spectrum. Well known examples are called radio

interference and radar clutter. Another important effect in the
military is the interaction of electromagnetic radiation with
electroexplosive devices used as detonators. Military as well as
civilian explosives are provided with detonators that often depend on
heating a small bridge wire to initiate the explosion. Absorbed
electromagnetic radiation can accidentally activate such fuzes.

Protection against the effects of electromagnetic radiation has become a
sophisticated engineering field of electromagnetic compatibility (EMC)
design. The most direct approach to protection is, in most cases, to
avoid the limited region in which high radiation levels are found. When
exposure cannot be avoided, shielding and filtering are important
protective measures. In other cases material design changes or
operating procedural changes must be instituted in order to provide
protection.

7.6.9 NUCLEAR RADIATION

Although a natural background level of nuclear radiation exists, the
only nuclear radiation that is of interest to design engineers is that
associated with manmade sources such as reactors, isotope power sources,
and nuclear weapons. The most important of these sources is nuclear
weapons, the effects of which can produce both transient and permanent
damaging effects in a variety of material.

X rays, gamma rays, and neutrons are the types of nuclear radiation of
most concern. As opposed to charged nuclear particles, which also
emanate from nuclear reactions, those forms of radiation listed have
long ranges in the atmosphere; thus, they can irradiate and damage a
variety of military material.

Among the nuclear effects that have been of most concern are those
called "transient radiation effects on electronics," often referred to
as TREE. These transient effects are due primarily to the
nonequilibrium free charged condition induced in material primarily by
the ionization effects of gamma rays and X rays. The separation of
transient and permanent effects is made on the basis of the primary
importance of the radiation effects. For example, a large current pulse
may be produced by ionizing radiation, and this current pulse may result
in permanent damage to a device by overheating. This is a transient
effect because the permanent damage results from overheating due to
excess current rather than to direct radiation induced material property
change. A large amount of information is available on specific
electronic components, circuits, and hardening methods.

It is impossible to completely protect material items from nuclear
radiation as can be accomplished for some other environmental factors.
The variety of effects produced by nuclear radiation for different
materials and components makes protective design difficult. The
procedure employed is to define a radiation hardness level in a given
material item and to design and test the item to that level.

Nuclear radiation hardening is a large and complex field with a variety of specialists required to deal with different aspects of the problem. This subject is treated extensively in the Design Engineers' Nuclear Effects Manual (Refs. 21-24).

Table 7.6.9-1 represents a summary of environmental effects and design techniques to overcome them. Appendix B of this section contains additional environmental design considerations.

7.7 HUMAN FACTORS

7.7.1 INTRODUCTION

All systems of concern in this handbook are of, by, and for humans. Analyses of the behavior and needs of humans are among the more controversial of the sciences; thus it is no surprise that there are several competing approaches to the handling and identification of people problems. References 25 and 26 analyze some of these approaches. Some disagreements exist about the comparisons themselves. It is convenient to classify four types of human interactions with a system; the classes are convenient, but not sharp and clear cut:

(1) Design and production of a system
(2) Operators and repairers as mechanical elements (human engineering)
(3) Operators and repairers as decision elements (human performance reliability)
(4) Bystanders (this classification is not considered further because it is largely a safety matter, not reliability).

An example of the fuzziness between classes is an operator's having to decide what to do, and then doing it; therefore, there is considerable interaction between the two activities.

An initial appraisal of the man/machine system must consider such aspects as: allocation of functions (man vs. machine), automation, accessibility, human tasks and their performance metrics, human stress characteristics, information presented to the human and the reliability of inferences coupled with the decisions on the basis of such information, and accessibility. The answers to these questions and the study of man/machine interactions and interfaces fall within the field variously called human factors, human engineering, or ergonomics (Ref. 29).

Human factors engineering is applied to research, development, test, and evaluation of systems to insure efficient integration of man into the system environment. This integration is intended to increase and preserve human and machine performance in the system during operation, control, maintenance, and support activities. Human engineering, therefore, becomes an active participant in the system engineering process and, consequently, must be weighed against safety, reliability, maintainability, and other system parameters to obtain tradeoffs providing increased system effectiveness. During the concept formulation phase, human factors data are used in predictions of system

TABLE 7.6.9-1: ENVIRONMENTAL STRESSES, EFFECTS AND RELIABILITY IMPROVEMENT
TECHNIQUES IN ELECTRONIC EQUIPMENT

Environmental Stress	Effects	Reliability Improvement Techniques
High Temperature	Parameters of resistance, inductance, capacitance, power factor, dielectric constant, etc. will vary; insulation may soften; moving parts may jam due to expansion; finishes may blister; devices suffer thermal aging; oxidation and other chemical reactions are enhanced; viscosity reduction and evaporation of lubricants are problems; structural overloads may occur due to physical expansions.	Heat dissipation devices, cooling systems, thermal insulation, heat-withstanding materials.
Low Temperature	Plastics and rubber lose flexibility and become brittle; electrical constants vary; ice formation occurs when moisture is present; lubricants gel and increase viscosity; high heat losses; finishes may crack; structures may be overloaded due to physical contraction.	Heating devices, thermal insulation, cold-withstanding materials.
Thermal Shock	Materials may be instantaneously overstressed causing cracks and mechanical failure; electrical properties may be permanently altered. Crazing, delamination, ruptured seals.	Combination of techniques for high and low temperatures.
Shock	Mechanical structures may be overloaded causing weakening or collapse; items may be ripped from their mounts; mechanical functions may be impaired.	Strengthened members, reduced inertia and moments, shock absorbing mounts.
Vibration	Mechanical strength may deteriorate due to fatigue or overstress; electrical signals may be mechanically and erroneously modulated; materials and structures may be cracked, displaced, or shaken loose from mounts; mechanical functions may be impaired; finishes may be scoured by other surfaces; wear may be increased.	Stiffening, control of resonance.

TABLE 7.6.9-1: ENVIRONMENTAL STRESSES, EFFECTS AND RELIABILITY IMPROVEMENT TECHNIQUES IN ELECTRONIC EQUIPMENT (Cont'd)

Environmental Stress	Effects	Reliability Improvement Techniques
Humidity	Penetrates porous substances and causes leakage paths between electrical conductors; causes oxidation which leads to corrosion; moisture causes swelling in materials such as gaskets; excessive loss of humidity causes embrittlement and granulation.	Hermetic sealing, moisture-resistant material, dehumidifiers, protective coatings.
Salt Atmosphere and Spray	Salt combined with water is a good conductor which can lower insulation resistance; causes galvanic corrosion of metals; chemical corrosion of metals is accelerated.	Nonmetal protective covers, reduced use of dissimilar metals in contact, hermetic sealing, dehumidifiers.
Electromagnetic Radiation	Causes spurious and erroneous signals from electrical and electronic equipment and components; may cause complete disruption of normal electrical and electronic equipment such as communication and measuring systems.	Shielding, material selection, part type selection.
Nuclear/Cosmic Radiation	Causes heating and thermal aging; can alter chemical, physical and electrical properties of materials; can produce gases and secondary radiation; can cause oxidation and discoloration of surfaces; damages electrical and electronic components especially semiconductors.	Shielding, component selection, nuclear hardening.
Sand and Dust	Finely finished surfaces are scratched and abraded; friction between surfaces may be increased; lubricants can be contaminated; clogging of orifices, etc.; materials may be worn, cracked, or chipped; abrasion, contaminates insulations, corona paths.	Air-filtering, hermetic sealing.
Low Pressure (High Altitude)	Structures such as containers, tanks, etc. are overstressed and can be exploded or fractured; seals may leak; air bubbles in materials may explode causing damage; internal heating may increase due to lack of cooling medium; insulations may suffer arcing and breakdown; ozone may be formed; outgasing is more likely.	Increased mechanical strength of containers, pressurization, alternate liquids (low volatility), improved insulation, improved heat transfer methods.

effectiveness and for initial function allocation studies. Human reliability studies during the contract definition phase are included in system reliability calculations, maintainability time and performance evaluations, system and subsystem safety analyses, and specific human engineering design criteria. The engineering development and production phases provide specific man/machine interactions for amplification of previous studies, isolate and define tradeoff and interaction problems not previously identified, and allow verification of prior design decisions on reliability, maintainability, safety, and other system parameters which interact with human factors.

7.7.2 DESIGN AND PRODUCTION

On the average, people are average. This truism is often forgotten by system designers, planners, and managers. Each wants to have well above average people in the tasks he is arranging. System designers do pay some attention to this problem when considering operators and repairers. But rarely it is considered in the design and manufacturing areas, although industrial and manufacturing engineers do deal with it in their constricted region of operation.

Beginning with the conception of a system, it is important to realize the limitations of the people involved all through the life cycle. Large organizations cannot and will not change rapidly, even though there is a management decree that the change will occur. People cannot adequately plan complete changes in a way of life or of work - there are too many unknown, unforeseen factors.

A system and its subsystem ought to be straightforward to design. Interfaces between subsystems ought to be as simple as possible. The more complexity, the more likely errors are to occur. Checklists are a valuable aid to designers. Design reviews and other product reviews help to overcome human limitations by putting some redundancy in the design system.

The designer of an equipment needs to consider how it will be produced, e.g., what kinds of quality control will be necessary, what machines/operators will actually perform a task. Reducing the occasion of very similar appearing parts, but which are different, can help avoid mistakes. A design that can accept looser tolerances might be better than one which requires tight tolerances, even though the latter would perform better if everything were right.

The designer needs to consider how the equipment actually will be repaired in the field. For example, if a repair when done right takes about 8 hr, and when done almost right takes 1 hr, which way will it be done under the pressures of understaffed maintenance crews many of whom are inexperienced? One cannot expect that field service personnel will have the knowledge about the system that the designers have. Even where the situation is understood, the officer in charge under the pressures of command might well choose to have the almost right repair that takes only 1 hr. The designer must always keep in mind that the equipments will be used and repaired by ordinary people who have other things in mind than "babying" the equipment. He must realize the difference between what people actually will do, and what he thinks they ought to do.

If the familiar production processes in a plant will have to change, then a quality assurance effort must be implemented to be sure the system does change and that it changes correctly.

A Cause-Consequence chart is a good tool for viewing the design-production process. It allows one to look at:

    (1) What can go wrong (causes)
    (2) How likely it is to go wrong
    (3) What happens when it does go wrong (consequences)
    (4) How to alleviate the severe consequences

Anywhere people are involved in doing something, the Cause-Consequences chart - even a very simple one - can help locate potential people problems.

System planners should be aware of the impact of administrative policies on the reliability of systems. In Reference 28 it is shown that many reported failures were not the result of either faulty design or human error (for the Air Force F-106 avionics systems), but were "required" by the procedural environment. Reference 28 ought to be read by every system planner.

7.7.3 HUMAN ENGINEERING

This areas deals largely with motor responses of operators and with varied human physical capabilities. MIL-STD-1472, MIL-H-46855 and Reference 29 covers this area adequately. Typical constraints are that:

    (1) An operation ought to be within the physical capabilities of the central 95% of the potential operators.

    (2) A person is not required to do something that his coordination will not allow him to do, e.g., something akin to patting his head with the left hand while rubbing his chest with the right hand.

    (3) Real people cannot easily use, read, and respond to controls and displays, especially in times of psychological stress.

Mock ups under realistic conditions are very helpful in uncovering forgotten constraints. For example, if an equipment must be used at night in extremely cold weather, have a person try to use it in a freezing, poorly lit room for several hours.

Military standards, regulations, specifications, and other publications contain guidelines, policies, and requirements for human factors, and human engineering. For example, requirements and policies for human engineering programs are presented in MIL-H-46855 and Reference 57.

MIL-STD-1472 give design criteria, requirements, and definitions for human engineering in military systems. Standardization, automation, visual and auditory displays, controls, labeling, workspace design, maintainability, remote handling devices, safety hazards, and environmental requirements are some of the subjects treated in these sources (Refs. MIL-STD-1472 and MIL-H-46855).

7.7.4 HUMAN PERFORMANCE RELIABILITY

The analysis of human factors recognizes that both human and machine elements can fail, and that just as equipment failures vary in their effect on a system, human errors can also have varying effects on a system. In some cases, human errors result from an individual's action, while others are a consequence of system design or manner of use. Some human errors cause total system failure or increase the risk of such failure, while others merely create delays in reaching system objectives. Thus, as with other system parameters, human factors exert a strong influence on the design and ultimate reliability of all systems having a man/machine interface. A good summary and critical review of human performance reliability predictive methods is given in Reference 25 which is a summary of Reference 26. Both references contain excellent bibliographies. Table 7.7.4-1 is taken from Reference 25 and lists the available predictive methods.

In the initial evaluation of a design, the man/machine system can be put into clearer perspective by answering the following two questions:

(1) In the practical environment, which of the many characteristics that influence human performance are truly important; which must be included in the design; and under what circumstances is each characteristic important?

(2) What effect will including or excluding particular characteristics have on the design of the system?

7.7.5 THE RELATIONSHIP BETWEEN HUMAN FACTORS AND RELIABILITY

Both reliability and human factors are concerned with predicting, measuring, and improving system performance. System failures are caused by human or equipment malfunctions. Thus, system reliability must be evaluated from the viewpoint that the system consists not only of equipment and procedures, but also includes the people who use them. The reliability engineer must analyze and provide for reliability in the equipment and procedures, and also must work closely with the human factors engineer to identify and plan for human reliability factors and their effects on the overall system reliability. Similarly, the human factor engineer is concerned, from the reliability viewpoint, with the reliability of humans in performing or reacting to equipment and procedure activities, and the effect that system reliability will have on human activities. When the man/machine interface is complex, for example, the possibility of human error increases, with an accompanying increase in the probability of system failure due to human error. Of particular concern to the reliability and human factors engineers are

TABLE 7.7.4-1: <u>LIST OF PREDICTIVE METHODS</u>

OPERABILITY METHODS

A. Analysis

1. American Institute for Research (AIR) Data Store
2. THERP-Technique for Human Error Rate Protection
3. TEEPS-Technique for Establishing Personnel Performance Standards
4. Pickrel/McDonald Method
5. Barry-Wulff Method
6. Throughput Method
7. Askren/Regulinski Method
8. DEI-Display Evaluative Index
9. Personnel Performance Metric
10. Critical Human Performance and Evaluative Progress (CHPAE)

B. Simulation

1. Digital Simulation Method
2. TACDEN
3. Boolean Predictive Technique
4. HOS-Human Operator Simulator
5. ORACLE-Operations Research and Critical Link Evaluator

MAINTAINABILITY METHODS

1. ERUPT-Elementary Reliability Unit Parameter Technique
2. Personnel Reliability Index
3. MIL-HDBK-472 Prediction Models

the frequency and modes of human failures, and the degree of adverse effect of human failures on the system. One obvious approach to eliminating failures due to human errors is to replace the human by a machine. This approach, however, must consider the complexity, reliability, interactions with other equipment, cost, weight, size, adaptability, maintainability, safety, and many more characteristics of a machine replacement for the human. An interesting facet of the human factors/reliability relationship (and which also concerns the maintainability engineer) is that the continuation of the system designed in reliability depends upon the detection and correction of malfunctions. This task usually is assigned to humans. Thus, system performance can be enhanced or degraded, depending upon whether or not the malfunction information is presented so that it is understood readily. By studying human response to various stimuli (audio, visual, etc.), the human factors engineer provides valuable guidance in the design of system malfunction indicators. Reference 30 contains additional information on human reliability and includes methods for collecting, analyzing, and using system failure data in quantitative approach to human reliability. A study of the feasibility of quantifying human reliability characteristics and subsequent development of a methodology for quantifying human performance, error prediction, control and measurement are discussed in References 33-39. Reference 35, Handbook of Human Performance Measures, is a comprehensive abstract of human performance measures.

7.7.6 HUMAN FACTORS THEORY

Basically, human behavior is a function of three parameters:

(1) Stimulus Input (S). Any stimuli, such as audio or visual signals, failure indications, or out of sequence functions which act as sensory inputs to an operator.

(2) Internal Reaction (O). The operator's act of perceiving and interpreting the S and reasoning a decision based upon these inputs.

(3) Output Response (R). The operator's response to S based upon O. Talking, writing, positioning a switch, or other responses are examples of R.

All behavior is a combination of these three parameters, with complex behavior consisting of many S-O-R chains in series, parallel, or interwoven and proceeding concurrently. Each element in the S-O-R chain depends upon successfully completing the preceding element. Human errors occur when the chain is broken, as, for example, when a change in conditions occurs but is not perceived as an S; when several S's cannot be discriminated by the operator; when an S is perceived but not understood; when an S is correctly recognized and interpreted, but the correct R is unknown (i.e., operator cannot reach a decision, or complete O); when the correct R is known but is beyond the operator's capabilities (i.e., operator completes O but cannot accomplish R); or when the correct R is within the operator's capabilities but is incorrectly performed.

Human factors, reliability, safety, maintainability, and other system engineering elements must be directed to a system design that contributes to proper operator responses by creating perceivable and interpretable stimuli requiring reactions within the operator's capabilities. Feedback ought to be incorporated into the design to verify that operator responses are correct. In other words, equipment characteristics should serve as both input and feedback stimuli to the operator. These relationships between human and equipment elements are depicted in Figure 7.7.6-1.

7.7.7 MAN/MACHINE ALLOCATION AND RELIABILITY

The functional block diagrams, allocation of task error rates, mathematical modeling of performance, prediction of performance reliability, and validation are applied to human subsystems in much the same manner as in the reliability of hardware subsystems. Stochastic modeling and quantification of human performance reliability can be done in either time discrete or time continuous domains. Particularly useful techniques are:

(1) Data generation and processing, including tests of randomness, stationarity, and ergodicity

(2) Failure modes and effects analysis

(3) Parameter variation analysis

(4) Cause-Consequence charts

(5) Estimation of suitable distributions for random variables

(6) Decision making methods such as hypothesis testing, multiple decision and sequential testing, and formulating rules for strategies.

Many of these techniques are discussed in greater detail in References 42-46.

Reliability of a system is affected by the allocation (not necessarily quantitative) of system functions to either the man, the machine, or both. Table 7.7.7-1 lists some of the salient characteristics of the humans and machines which are pertinent to the allocation choice. As is evident from studying Table 7.7.7-1, the prediction of human reliability is more difficult than the prediction of machine reliability. The machine's insensitivity to extraneous factors (Item 10 in Table 7.7.7-1) versus the human's sensitivity to these factors is one consideration, leading to human performance variability, and the subsequent capability to predict machine reliability more precisely. In fact, a human's response can be sufficiently influenced to vary from 0.0001 to 0.9999 reliability within conditions that would not affect a machine. The machine, for example, does not react to environments of combat which could produce severe psychological stress and breakdown in a human. Since the trade-off depends partly on the nature of the system and human functions and partly on the way the allocation problem is approached,

INPUTS (OTHER PERSONNEL)
INPUTS (PHYSICAL ENVIRONMENT)

EQUIPMENT   PERSONNEL

INPUTS
(ENVIRONMENTAL)   SENSING   DISPLAYS   SENSING

INPUTS
(OTHER
EQUIPMENT)

                   PROCESS-   PROCESS-
                     ING   ING

OUTPUTS
(OTHER
   EQUIPMENT)
OUTPUTS   ACTUATING   CONTROLS   ACTUATING
(EFFECTS ON THE
 EQUIPMENT
 ITSELF)   VERBAL AND OTHER RESPONSES
                   FEEDBACK
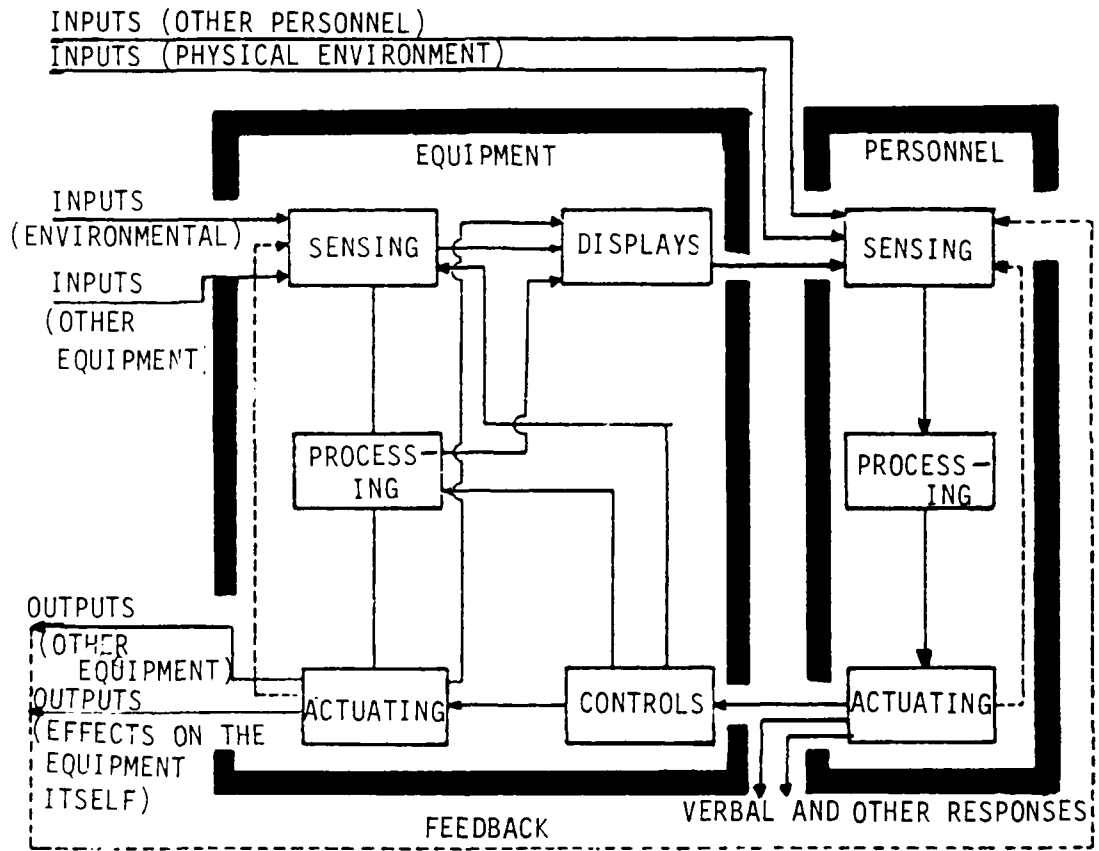
FIGURE 7.7.6-1:   THE MAN/MACHINE INTERACTION

TABLE 7.7.7-1: CHARACTERISTICS OF HUMANS AND MACHINES

Characteristics Tending to Favor Humans	Characteristics Tending to Favor Machines
1. Ability to detect certain forms of energy	1. Monitoring men or other machines
2. Sensitivity to a wide variety of stimuli within a restricted range	2. Performance of routine, repetitive, precise tasks
3. Ability to perceive patterns and generalize about them	3. Responding quickly to control signals
4. Ability to detect signals (including patterns) in high noise environments	4. Exerting large amounts of force smoothly and precisely
5. Ability to store large amounts of information for long periods and to remember relevant facts at the appropriate time	5. Storing and recalling large amounts of precise data for short periods of time
6. Ability to use judgment	6. Computing ability
7. Ability to improvise and adopt flexible procedures	7. Range of sensitivity to stimuli
8. Ability to handle low probability alternatives (i.e., unexpected events)	8. Handling of highly complex operations (i.e., doing many different things at once)
9. Ability to arrive at new and completely different solutions to problems	9. Deductive reasoning ability
10. Ability to profit from experience	10. Insensitivity to extraneous factors
11. Ability to track in a wide variety of situations	
12. Ability to perform fine manipulations	
13. Ability to perform when overloaded	
14. Ability to reason inductively	

each design situation requires a separate human factors analysis. Such variables as cost, weight, size, hazard levels, adaptability, and state of technology must be considered for each system.

One approach to the choice between man and machine is to compare the predicted reliabilities of each. This approach, however, should not be based solely on failure rates, since humans are sufficiently adaptable to recover quickly and correct some human induced malfunctions. Similarly, humans have the flexibility to handle unique situations that might cause system failure if an unadaptable machine were assigned the task. An approach based on reliability comparisons ought to use failure rates in conjunction with an analysis of man/machine characteristics and the desired task accomplishments.

Another approach to man/machine allocation is illustrated by Figure 7.7.7-1. This approach has three general steps:

(1) Develop a prediction model.
(2) Generate Task Equipment Analysis (TEA) data.
(3) Predict man/machine reliability using the TEA data as inputs to the prediction model.

The predictive model can be developed in either the time-discrete or time-continuous domains, depending on the nature of the human task. The human performance reliability is defined as (Ref. 47):

(1) Probability (task performance without error/stress) (discrete)
(2) Probability (task performance without error in an increment of time/stress) (continuous)

Embodied in the stress is the totality of all factors -- psychological, physiological, and environmental -- which affect human performance.

For discrete tasks such as pushing a button or throwing a lever, the task random variable has only discrete values (often, the positive integers). The reliability of some discrete repetitive task (assuming that the trials are statistically independent and have the same probability) can be estimated simply as the fraction of the trials which are a success. The discrete human performance unreliability sometimes can be approximated by the error rate multiplied by the time interval (Ref. 47).

The time-continuous quantification of human performance reliability is applied to such tasks as:

(1) Tracking a signal displayed on a screen
(2) Manually controlling the pitch, roll, and yaw of an aircraft
(3) Performing a vigilance task which might require, for example, the detection of the presence (or absence) of a specified event. In this type of task, the random variable is continuous in time over some domain.

INPUT

KNOWLEDGE OF MAN'S CAPABILITIES AND LIMITATIONS

REVISION OF TRAINING PROGRAM AND PERSONNEL SUBSYSTEM

DESCRIBE SYSTEM FUNCTIONS AND REQUIREMENTS

REVISION OF SYSTEM FUNCTIONS

ESTABLISH DISTRIBUTION OF FUNCTIONS BETWEEN MEN AND MACHINES

ESTABLISH DISTRIBUTION OF OPERATOR TASKS

PREDICT USE RELIABILITY

KNOWLEDGE OF MACHINE CAPABILITIES AND LIMITATIONS

REVISION OF MACHINE CAPABILITIES

FIGURE 7.7.7-1: PREDICTING MAN/MACHINE RELIABILITY

The time-to-error has a random distribution, just as time-to-failure of hardware; this distribution will have a probability density function, cumulative distribtuion function, and failure rate (error rate). Depending on the specific task, a measure of human performance reliability might be mean time-to-first-error, mean time-to-error, median time-between-errors, or something similar. Numerous other measures similarly can be formulated. For example, because of the capacity of the human to correct self generated errors, it is germane to model some performance function related to error correction. In Reference 61 such a performance measure is formulated as "correctability" and defined as:

> Probability (Completion of task error correction in a certain time/stress). The time-to-task-error-correction is analogous to time-to-repair and has a random distribution (and of course, all the descriptions of such a distribution). References 26, 31 and 49 provide a comprehensive treatment of man-machine reliability modeling in this context.

Examples of numerical evaluation of these probabilities are:

(1) The human subsystem (operator) is required to interconnect two machines in a decision sense. From TEA data it is determined that the probability of a successful interconnection on a single trial is 10% - a very difficult task.

(2) Radar operators who are tracking multiple target signals have two types of errors: missing a target which is displayed, or false alarming. TEA data might show that the time-to-first-false-alarm is lognormally distributed. The parameters of the distribution could be estimated (along with their uncertainties) from some sample data. The median time-to-first-alarm could then be calculated, as could any other point on the distribution.

7.7.8 INTERACTIONS AND TRADEOFFS

The principal determinant of man/machine performance is the complexity of human tasks within the system. A system design that requires frequent and precise adjustments by an operator may create reliability problems associated with wearout or misadjustment of the control device, or maintainability problems from repeated replacement of the worn control. On the other hand, a design providing an automatic adjusting mechanism may cause problems of cost, weight, size, reliability, maintainabiity, or safety due to the control's complexity. Similarly, for the same level of effectiveness, a system that through design, location, or environment is difficult to repair must necessarily be made more reliable than a system with a less complex man/machine interface. Thus, the man/machine interaction can contribute to, or detract from, the effectiveness of other disciplines depending upon tradeoffs and interactions selected during the system engineering process.

References 29, 50-53 give additional design guides and approaches for solving human factors problems and tradeoffs with other disciplines. A valuable consideration, the use of human factors information by designers, is discussed and illustrated with tests and examples in References 54-56.

7.7.9 THERP (TECHNIQUE FOR HUMAN ERROR RATE PREDICTION)

The human performance reliability model developed at Sandia Laboratories is defined as (Ref. 49):

"THERP is a method to predict human error rates and to evaluate the degradation to a man/machine system likely to be caused by human errors in association with equipment functioning, operational procedures and practices, and other system and human characteristics which influence system behavior."

There are five steps in applying the model.

(1) Define the system failures (consequences). Work with the failures one at a time.

(2) List and analyze the human operations related to each failure (task analysis).

(3) Estimate the appropriate error probabilities

(4) Estimate the effects of human errors on the system failure. Usually the hardware characteristics will have to be considered in the analysis.

(5) Recommend changes to the man/machine system and return to Step 2.

Reference 47 summarizes and explains the THERP model (and extolls its virtues). Reference 46 is an annotated bibliography of the Sandia Laboratories work in this area and will very helpful to anyone trying to estimate the effects of human frailty on a system. It lists 44 sources of further information.

7.8 FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

7.8.1 INTRODUCTION

Failure Mode and Effects Analysis is a reliability procedure which documents all possible failures in a system design within specified ground rules. It determines, by failure mode analysis, the effect of each failure on system operation and identifies single failure points, i.e., those failures critical to mission success or crew safety. It may also rank each failure according to the criticality category of failure effect and probability occurrence. This procedure is the result of two steps: the Failure Mode and Effect Analysis (FMEA) and the Criticality Analysis (CA).

In performing the analysis, each failure studied is considered to be the only failure in the system, i.e., a single failure analysis. The FMEA can be accomplished without a CA, but a CA requires that the FMEA has previously identified critical failure modes for items in the system design. When both steps are done, the total process is called a Failure Mode, Effects and Criticality Analysis (FMECA).

FMEA utilizes inductive logic on the "bottoms up" approach. Beginning at the lowest level of the system hierarchy, (e.g., component part), and from a knowledge of the failure modes of each part, the analyst traces up through the system hierarchy to determine the effect that each failure mode will have on system performance. This differs from fault tree analysis (discussed in the next section) which utilizes deductive logic on the "top down" approach. In fault tree analysis, the analyst assumes a system failure and traces down through the system hierarchy to determine the event, or series of events, that could cause such a failure.

The FMEA provides:

(1) The design engineer with a method of selecting a design with a high probability of operational success and crew safety

(2) Design engineering with a documented method of uniform style for assessing failure modes and their effect on operational success of the system

(3) Early visibility of system interface problems

(4) A list of possible failures which can be ranked according to their category of effect and probability of occurrence

(5) Identification of single failure points critical to mission success or to crew safety

(6) Early criteria for test planning

(7) Quantitative and uniformly formatted data input to the reliability prediction, assessment, and safety models

(8) A basis for design and location of performance monitoring and fault sensing devices and other built-in automatic test equipment

(9) A tool which services as an aid in the evaluation of proposed design, operational, or procedural changes and their impact on mission success or crew safety.

Items (5) and (8) are the two most important functions performed by an FMEA.

The FMEA is normally accomplished before a reliability prediction is made to provide basic information. It should be initiated as an integral part of the early design process and should be periodically

updated to reflect design changes. Admittedly, during the early stages, one usually does not have detailed knowledge of the component parts to be used in each equipment. However, one usually has knowledge of the "black boxes" which make up the system. Thus, at this stage, an FMEA might start at the "black box" level and be expanded as more detailed knowledge becomes available. This analysis may also be used to provide a model for analyzing already built systems. An FMEA is a major consideration in design reviews.

The principles of FMEA are straightforward and easy to grasp. The practice of FMEA is tedious, time consuming and very profitable. It is best done in conjunction with Cause-Consequence and Fault Tree Analysis. The bookkeeping aspects, namely, the keeping track of each item and its place in the hierarchy, are very important because mistakes are so easy to make.

The Cause-Consequence chart shows the logical relationships between causes (events which are analyzed in no more detail) and consequences (events which are of concern only in themselves, not as they in turn affect other events). The chart usually is represented with consequences at the top and causes at the bottom; and the words Top and Bottom have come into common use to describe those portions of the chart. A Failure Modes and Effects Analysis (FMEA) deals largely with the bottom part of the chart. A fault tree is a part of a Cause-Consequence chart. It consists of only one consequence and all its associated branches. The Cause-Consequence chart is created by super imposing the separately created fault trees. The Cause-Consequence chart can be used to organize one's knowledge about any set of causes and their consequences; its use is not limited to hardware oriented systems.

The FMEA consists of two phases which provide a documented analysis for all critical components of a system. First, however, definitions of failure at the system, subsystem, and sometimes even part level must be established.

Phase 1 is performed in parallel with the start of detail design and updated periodically throughout the development program as dictated by design changes. Phase 2 is performed before, or concurrently with, the release of detail drawings.

The Phase 1 analysis consists of the following steps:

(1)   Constructing a symbolic logic block diagram, viz., a reliability block diagram or a Cause-Consequence chart

(2)   Performing a failure effect analysis, taking into account modes of failure such as:

    (a)   Open circuits
    (b)   Short circuits
    (c)   Dielectric breakdowns
    (d)   Wear
    (e)   Part-parameter shifts

(3) Proper system and item identification

(4) Preparation of a critical items list

During Phase 2, the results of Phase 1 are revised and updated as required by design changes. In addition, all items on the system are analyzed to determine their criticality with respect to the system.

7.8.2 PHASE 1

During this phase the following detailed steps are performed:

(1) A Symbolic Logic Block Diagram is constructed. This diagram is developed for the entire system to indicate the functional dependencies among the elements of the system and to define and identify its subsystems. It is not a functional schematic or a signal flow diagram, but a model for use in the early analysis to point out weaknesses. Figures 7.8.2-1 and 7.8.2-2 show typical symbolic logic diagrams. Figure 7.8.2-1 illustrates the functional dependency among the subsystems, sets, groups, and units that make up the system. Figure 7.8.2-2 illustrates the functional dependencies among assemblies, subassemblies, and parts that make up one of the units in Figure 7.8.2-1.

(2) A failure effect analysis is performed for each block in the symbolic logic block diagram, indicating the effect of item failure on the performance of the next higher level on the block diagram. Table 7.8.2-1 shows a typical group of failure modes for various electronic and mechanical parts. The failure mode ratios are estimates and should be revised on the basis of the user's experience. However, they can be used as a guide in performing a detailed failure effect analysis.

It should be noted that integrated circuit failure modes are not addressed in Table 7.8.2-1. This is because of the complexity involved and the fact that they are so technology dependent.

To attempt to identify failure modes by methodically analyzing the schematic for such a complex device is not a viable approach for a number of reasons.

(1) The sheet complexity of analyzing a device such as a microprocessor containing over 20,000 gates is overwhelming. Even if it could be done vendors seldom (if ever) make available the documentation necessary to perform this type of analysis.

(2) Assuming the entire circuit was analyzed and the failure modes thus defined, this still would not necessarily represent an accurate failure mode distribution, since only those failures due to the chip itself would be considered. In general, a complete failure mode distribution must represent failure due to the following:

LEVEL

SYSTEM

SUBSYSTEM

SET

GROUP

UNIT

```
SYSTEM        ┌──────────────┐
              │      S       │
              └──────────────┘

SUBSYSTEM  ┌──────┐  ┌──────┐  ┌──────┐  ┌──────┐
           │  10  │──│  20  │──│  30  │──│  40  │
           └──────┘  └──────┘  └──────┘  └──────┘
                               ┌──────┐
                               │  50  │
                               └──────┘

SET        ┌──────┐  ┌──────┐  ┌──────┐
           │  11  │──│  21  │  │  31A │
           └──────┘  └──────┘  └──────┘
                               ┌──────┐
                               │  31B │        INPUT FROM
                               └──────┘        DIFFERENT
                                               SYSTEM
GROUP      ┌──────┐  ┌──────┐  ┌──────┐  ┌──────┐
           │  01A │──│  02  │──│  03  │──│  04  │
           └──────┘  └──────┘  └──────┘  └──────┘
           ┌──────┐
           │  01B │
           └──────┘

UNIT       ┌──────┐  ┌──────┐  ┌──────┐
           │ 01B1 │──│ 01B2 │──│ 01B3 │
           └──────┘  └──────┘  └──────┘
```
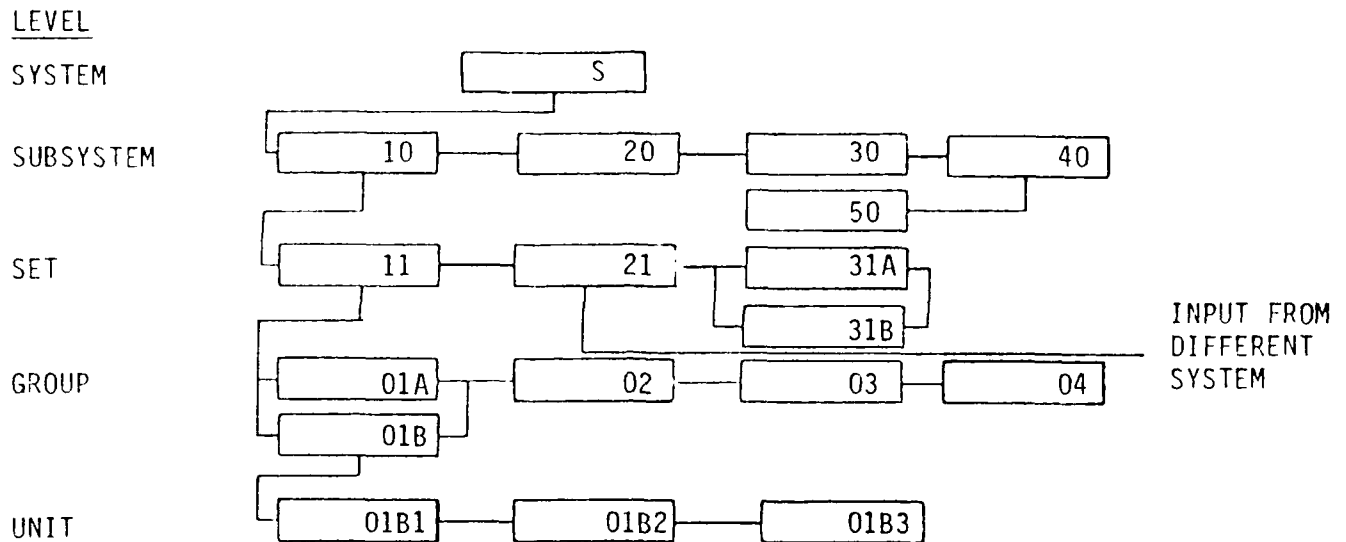
Notes:

1. The system depends on subsystems 10, 20, 30, and 40.

2. Subsystem 10 depends on sets 11, 21, 31A, and 31B

3. Set 11 depends on groups 01A, 01B, 02, 03, and 04.

4. Group 01B depends on units 01B1, 01B2, and 01B3.

5. Sets 31A and 31B are redundant.

6. Groups 01A and 01B are redundant

7. Subsystem 40 depends on subsystem 50.

8. Set 21 depends upon an input from another system.

FIGURE 7.8.2-1: TYPICAL SYSTEM SYMBOLIC LOGIC BLOCK DIAGRAM

FIGURE 7.8.2-2: TYPICAL UNIT SYMBOLIC LOGIC BLOCK DIAGRAM
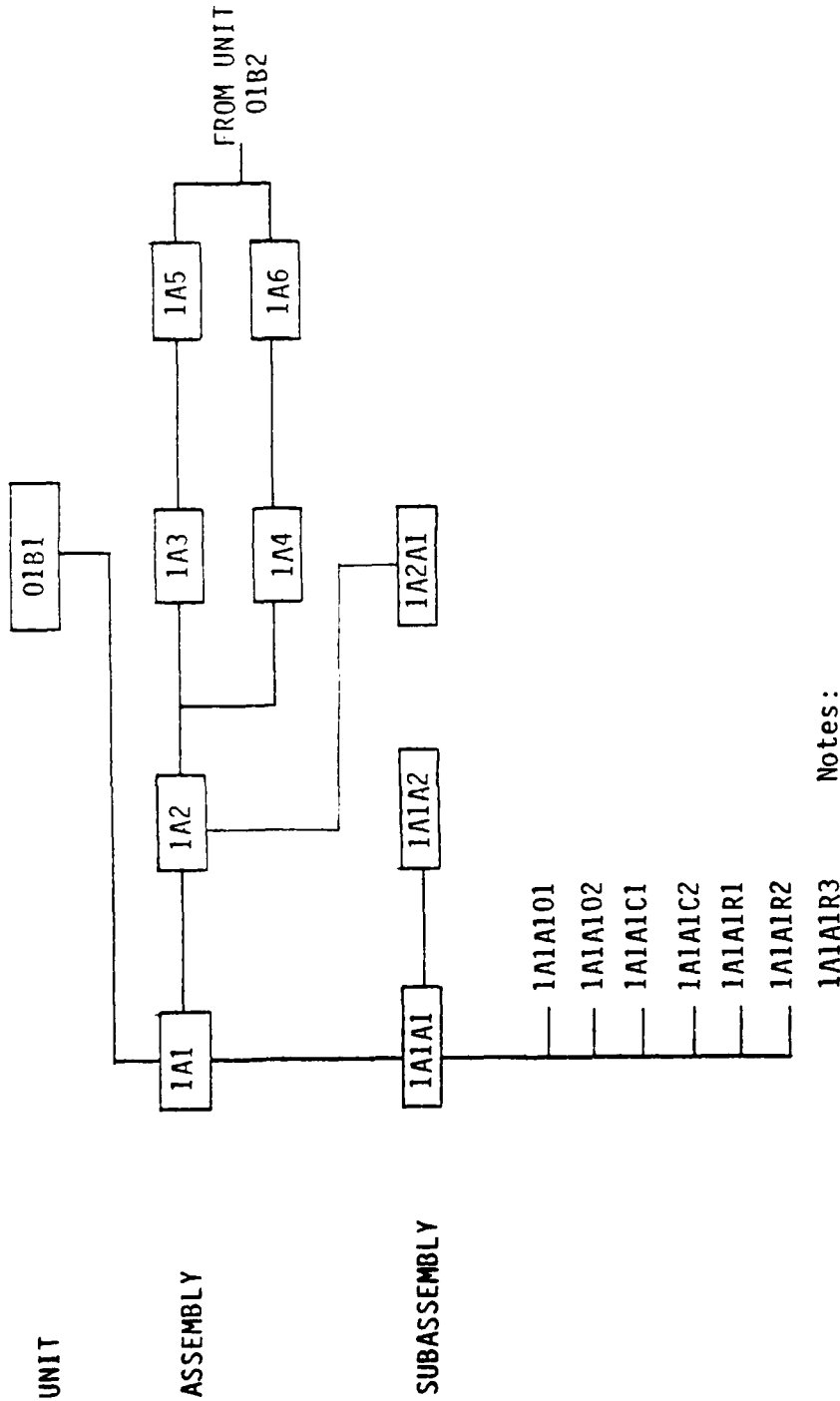
Notes:
1. Unit 01B1 depends on assemblies 1A1, 1A2 AND either '1A3 AND 1A5' OR '1A4 AND 1A6'
2. Assembly 1A1 depends on subassemblies 1A1A1 AND 1A1A2
3. Assembly 1A2 depends on subassembly. 1A2A1
4. Subassembly 1A1A1 depends on all parts contained therein

o   the semiconductor chip (technology dependent)
o   the packaging
     -    conductive particles
     -    wire bonds
o   the software
o   the environment
     -    physical (temperature, humidity, etc.)
     -    electrical (ESD, EMI, etc.)

In order to accurately address the failure modes of a given LSI microcircuit each of these factors must be accounted for. As an example, if the IC chip is packaged in a hermetic cavity package there is a possibility that one wire may break and short to an adjacent wire. If this same chip were encapsulated in a plastic package, this short could not occur, since the wire is constrained by the potting material. However, the potting material can have other detrimental effects on an IC chip.

Figure 7.8.2-3 illustrates a useful form of conducting a failure effect analysis. (See also Figure 7.8.3-2 for an example of its use.) For each component in the system, appropriate information is entered in each column. Column descriptions are given in Table 7.8.2-2.

A numerical reference for all items in the symbolc logic block diagram must be provided by using a standard coding system, such as that specified in MIL-STD-1629. All items below the set and group levels are identified using the scheme illustrated in Table 7.8.2-2. Items at and above the group and set levels are not subject to this standard nomenclature scheme. These items can be assigned a simple code such as that illustrated in Figure 7.8.2-1. In this illustration, the system is assigned a letter; and the subsystems, sets, and groups are assigned numbers in a specifically ordered sequence. As an example, the code S-23-01 designates the first group of the third set in the second subsystem of system S. The exact coding system used is not as important as making sure that each block in the diagram has its own number. Identical items (same drawing numbers) in different systems, or in the same system but used in different applications, should not be assigned the same code number.

(3) During the failure effects analysis, a number of changes to the block diagrams may be required. Therefore, to minimize the number of changes in the coding system, it is recommended that the failure effects analysis be completed before assignment of code numbers is finalized.

(4) Based on the failure effects analysis, a list of critical items should be prepared. This list will contain those items whose failure results in a possible loss, probable loss, or certain loss of the next higher level in the symbolic logic block diagram. All items that can cause system loss should be identified clearly in the list.

(1) ITEM	(2) CODE	(3) FUNCTION	(4) FAILURE MODE	(5) FAILURE EFFECT	(6) LOCS PROBABILITY, β

FIGURE 7.8.2-3: <u>FAILURE EFFECTS ANALYSIS</u>
<u>FORM</u>

TABLE 7.8.2-1: <u>FAILURE MODE DISTRIBUTION OF PARTS</u>[1]

PART	IMPORTANT FAILURE MODES AND APPROXIMATE PERCENTAGE OF OCCURRENCE	
Bearings	Deterioration of lubrication	45
	Contamination	30
	Misalignment	5
	Brinelling	5
	Corrosion	5
Blowers	Winding failures	35
	Bearing failures	50
	Sliprings, brushes, & commutators	5
Capacitors-Fixed Ceramic Dielectric	Short circuits	50
	Change of value	40
	Open circuits	5
Capacitors-Fixed Electrolytic Aluminum	Open circuits	40
	Short circuits	30
	Excessive leakage current	15
	Decrease in capacitance	5
Capacitors-Fixed,, Mica or Gloss Dielectric	Short circuits	70
	Open circuits	15
	Change of value	10
Capacitors-Fixed Metallized Paper or Film	Open circuits	65
	Short circuits	30
Capacitors-Fixed Paper Dielectric	Short circuits	90
	Open circuits	5
Capacitors-Fixed Electrolytic, Tantalum	Open circuits	35
	Short circuits	35
	Excessive leakage current	10
	Decrease in capacitance	5
Choppers	Contact failures	95
	Coil failure	5
Circuit Breakers	Mechanical failure of tripping device	70
Clutches-Magnetic	Bearing wear	45
	Loss of torque due to internal mechanical degradation	30
	Loss of torque due to coil failure	15
Coils	Insulation deterioration	75
	Open winding	25

[1] <u>Engineering Design Handbook</u>, AMCP-706-196, U.S. Army Material Command, Jan. 76

TABLE 7.8.2-1:   FAILURE MODE DISTRIBUTION OF PARTS (Cont'd)

PART	IMPORTANT FAILURE MODES AND APPROXIMATE PERCENTAGE OF OCCURRENCE	
Connectors	Shorts (poor sealing)	30
	Mechanical failure of solder joints	25
	Degradation of insulation resistance	20
	Poor contact resistance	10
	Miscellaneous mechanical failures	15
Connectors, Standard	Contact failure	30
	Material deterioration	30
	Mechanical failure of solder joints	25
	Miscellaneous mechanical failures	15
Crystal Units, Quartz	Opens	80
	No oscillations	10
Diodes, Silicon and Germanium	Short circuits	75
	Intermittent circuits	18
	Open circuits	6
Electron Tubes (subminiature)	Degradation (gm, 1hk, 1p, etc.)	90
	Catastrophic (shorts, opens, cracked envelopes, etc.)	10
Hose Assemblies (Rubber)	Material deterioration	85
	End fitting mechanical failure	10
Indicator Lights	Catastrophic (opens)	75
	Degradation (corrosion, solderability)	25
Insulators	Mechanical breakage	50
	Deterioration of plastic material	50
Lamps, Incandescent	Catastrophic (filament breakage, glass breakage)	10
	Degradation (loss of filament emission)	90
Magnetrons	Window puncturing	20
	Cathode degradation (resulting from arcing and sparking)	40
	Gassing	30
Meters, Ruggedized	Catastrophic (opens, glass breakage, open seals)	75
	Degradation (accuracy, friction, damping)	25
Motors, Drive and Generator	Winding failures	20
	Bearing failures	20
	Slipring brushes, and commutators	5

TABLE 7.8.2-1: FAILURE MODE DISTRIBUTION OF PARTS (Cont'd)

PART	IMPORTANT FAILURE MODES AND APPROXIMATE PERCENTAGE OF OCCURRENCE	
Motors, Servo and Tachometer	Bearing failures	45
	Winding failures	40
Oil seals (rubber)	Material deterioration	85
O-Rings (rubber)	Material deterioration	90
Relays	Contact failures	75
	Open coils	5
Resistors-Fixed, Carbon and Metal Film	Open circuits	80
	Change of value	20
Resistors-Fixed Composition	Change of value	95
Resistors-Variable, Composition	Erratic operation	95
	Insulation failure	5
Resistors-Variable, Wirewound	Erratic operation	55
	Open circuits	40
	Change of value	5
Resistors-Variable Wirewound, Precision	Open circuits	70
	Excessive noise	25
Switches, Rotary	Intermittent contact	90
Switches, Toggle	Spring breakage (fatigue)	40
	Intermittent contact	50
Synchros	Winding failures	40
	Bearing failures	30
	Slipring and brush failures	20
Thermistors	Open circuits	95
Transformers	Shorted turns	80
	Open circuits	5
Transistors Germanium and Silicon	High collector to base leakage current)	59
	Low Collector to emitter breakdown voltage (Bvceo)	37
	Open terminals	4
Valve-Check and Relief	Poppets sticking (open or closed)	40
	Valve seat deterioration	50

TABLE 7.8.2-1: FAILURE MODE DISTRIBUTION OF PARTS (Cont'd)

PART	IMPORTANT FAILURE MODES AND APPROXIMATE PERCENTAGE OF OCCURRENCE	
VariStors	Open circuits	95
Vibration Isolators (rubber type)	Material deterioration	85
Vibration Isolators (spring type)	Degradation of damping medium	80
	Spring fatigue	5
Vibrators	Contact failures	80
	Open winding	5
	Spring fatigue	15

TABLE 7.8.2-2: COLUMN DESCRIPTIONS FOR FIGURE 7.8.2-3

Column	Nomenclature	Description
1	Item	Item name
2	Code	Item identification or circuit designation code
3	Function	Concise statement of the item's function
4	Failure Mode	Concise statement of the mode(s) of item failure
5	Failure Effect	Explanation of the effect of each failure mode on the performance of the next higher level in the symbolic logic block diagram
6	Loss Probability,	Numerical index indicating the probability of system loss if the item fails in the mode indicated

7.8.3 PHASE 2

This phase is implemented by performing the following steps:

(1) The symbolic logic block diagram, failure effects analysis, coding, and critical items list are reviewed and brought up-to-date.

(2) Criticality is assigned, based on the item applicable failure mode, the system loss probability, the failure mode frequency ratio, and the item unreliability. The analysis of criticality is essentially quantitative, based on a qualitative failure effects analysis.

Criticality CR_i defined by the equation

$$(CR)_{ij} = \alpha_{ij} \beta_{ij} \lambda_i \qquad (7.21)$$

where

α_{ij} = failure mode frequency ratio of item i for the failure mode j (see Table 7.8.2-1 for an example), i.e., the ratio of failures of the type being considered to all failures of the item.

β_{ij} = loss probability of item i for failure mode j (i.e., the probability of system failure if the item fails). A suggested scale is Certain Loss - 1.00, Probable Loss - 0.1 to 1.0, Possible Loss - 0 to 0.10, No Effect - 0.0

λ_i = failure rate of item i

$(CR)_{ij}$ = system failure rate due to item i's failing in its mode j

The system criticality is given by Eq. (7.22)

$$(CR)_s = \sum_{i=1} \sum_{j=1} (CR)_{ij} \qquad (7.22)$$

where

$(CR)_s$ = system criticality (failure rate)

$\sum_j$ = sum over all failure modes of item i

$\sum_i$ = sum over all items

A form useful for conducting the criticality analysis is given in Figure
7.8.3-2. This form is a modification of Figure 7.8.2-3 to include the
failure mode frequency ratio and the failure rate. The example in the
next section and Figures 7.8.3-1 and 7.8.3-2 illustrate the procedure.

The CR value of the preamplifier unit is 6.851 per 10^6 hr. This number
can be interpreted as the predicted total number of system failures per
hour due to preamplifier failures, e.g., 6.851 x 10^{-6}. Whether or not
this number is excessive, and, thus, calls for corrective action,
depends upon the requirements for the system and the criticalities for
other units in the system. If the number is excessive, it can be
reduced by any of the following actions:

(1) Lowering the failure rates of parts in the system by derating

(2) Decreasing the failure mode frequency ratio through selection of
other parts

(3) Decreasing the loss probability by changing the system or preampli-
fier design

(4) Redesign using various techniques such as redundancy, additional
cooling, or switching
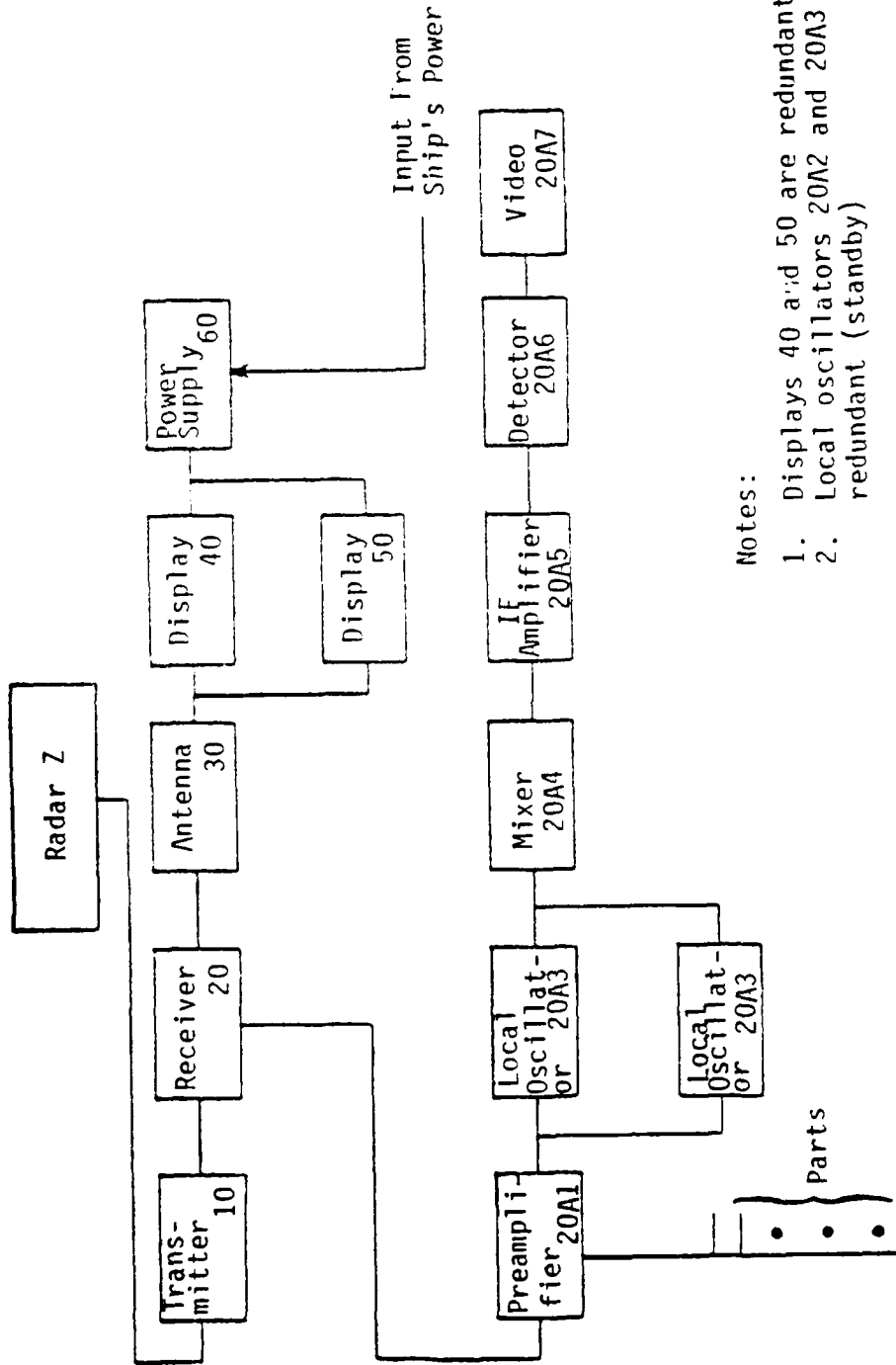
FIGURE 7.8.3-1: SYMBOLIC LOGIC BLOCK DIAGRAM OF RADAR EXAMPLE

Page 1 of 2

CRITICALITY WORK SHEET

SYSTEM Radar (Z)
SUBSYSTEM Receiver 20

UNIT Preamplifier 20A1
Parts

(1) Item	(2) Code	(3) Function	(4) Failure Mode	(5) Failure Effect	(6) Loss Probability (β)	(7) Failure Mode Frequency Ratio (α)	(8) Failure Rate (Per Million Hours) (λ)	(9) Criticality (CR)	(10) Comments
Resistor	20A1R1	Voltage Divider	Open	No Output	1.00	0.80	1.5	1.200	Film Resistor
Resistor	20A1R1	Voltage Divider	Change of Value	Wrong Output	0.10	0.20	1.5	0.030	Film Resistor
Resistor	20A1R2	Voltage Divider	Open	No Output	1.00	0.80	1.5	1.200	Film Resistor
Resistor	20A1R2	Voltage Divider	Change of Value	Wrong Output	0.10	0.20	1.5	0.030	Film Resistor
Capacitor	20A1C3	Decoupling	Open	No Effect	0.00	0.35	0.22	0.000	Tubular Tantalum
Capacitor	20A1C3	Decoupling	Short Circuit	No Output	1.00	0.35	0.22	0.077	Tubular Tantalum
Capacitor	20A1C3	Decoupling	High Leakage Current	No Effect	0.00	0.20	0.22	0.000	Tubular Tantalum
Capacitor	20A1C3	Decoupling	Decrease In Capacitance	No Effect	0.00	0.10	0.22	0.000	Tubular Tantalum
Diode	20A1CR3	Voltage Divider	Short Circuit	No Output	1.00	0.75	1.0	0.750	
Diode	20A1CR3	Voltage Divider	Intermittant Ckt.	No Output	1.00	0.20	1.0	0.200	
Diode	20A1CR3	Voltage Divider	Open Circuit	No Output	1.00	0.05	1.0	0.050	
Transistor	20A1Q4	Amplifier	High Collector In Base Leakage Current	No Output	1.00	0.60	3.0	1.800	
Transistor	20A1Q4	Amplifier	Low	No Output	1.00	0.35	3.0	1.05	
Transistor	20A1Q4	Amplifier	Open Terminals	No Output	1.00	0.05	3.0	0.150	
Transformer	20A1Q4	Coupling	Shorted Turns	Wrong Output	0.10	0.80	3.0	.24	

CRITICALITY TOTAL FOR UNIT 6.777

TOTAL 6.777

FIGURE 7.8.3-2: DETERMINATION OF PREAMPLIFIER CRITICALITY

CRITICALITY WORK SHEET

SYSTEM Radar (Z)
SUBSYSTEM Receiver 20
UNIT Preamplifier 20A1
Parts

(1) Item	(2) Code	(3) Function	(4) Failure Mode	(5) Failure Effect	(6) Loss Probability (β)	(7) Failure Mode Frequency Ratio (α)	(8) Failure Rate (Per Million Hours)	(9) Criticality (CR)	(10) Comments
Transformer	20A1O5	Coupling	Open Ckt.	No Output	1.00	0.20	0.30	0.06	Composition
Resistor	20A1R5	Bias	Open Ckt.	No Output	1.00	0.05	0.006	0.000	Composition
Resistor	20A1R6	Bias	Change of Values	No Effect	0.00	0.05	0.005	0.000	Composition
Capacitor	20A1R7	Bypass	Open Ckt.	No Effect	0.00	0.40	0.48	0.000	Aluminum
Capacitor	20A1R7	Bypass	Short Ckt.	Wrong Output	0.10	0.30	0.48	0.014	Electrolytic
Capacitor	20A1R7	Bypass	High Leakage Current	No Effect	0.00	0.20	0.48	0.000	
Capacitor	20A1R7	Bypass	Decrease in Capacitance	No Effect	0.00	0.10	0.48	0.000	

CRITICALITY TOTAL FOR UNIT 6.851   TOTAL 0.074

FIGURE 7.8.3-2: DETERMINATION OF PREAMPLIFIER CRITICALITY (Cont'd)

7.8.4 EXAMPLE

The detail design of a radar system required the use of FMEA to determine the effect of item failure on the system. The FMEA analysis must be performed at this time prior to freezing the design. Perform an FMEA analysis as follows:

Procedure	Example
(1) Develop a symbolic logic block diagram of the radar system. The units making up the receiver subsystem are shown in detail. In an actual analysis, symbolic diagrams must be constructed for all other subsystems.	See Figure 7.8.3-1
(2) Fill in the work sheets for all units in the receiver subsystem. Repeat this procedure for all subsystems.	See Figure 7.8.3-?
(3) Qualitatively estimate the values of loss probability for each part.	An analysis indicates that for this system the following values of β are applicable: 1.0, 0.1, and 0.
(4) Determine the failure mode frequency ratio for each failure mode of every part.	The resistor 20A1R1 is fixed, film (Fig. 7.8.3-2); from Table 7.8.2-1, it has two failure modes: open = 0.8 and drift = 0.2.
(5) Tabulate failure rates for each component.	λ(20A1R1) = 1.5 per 10^6 hr, for example.
(6) Compute the CR value for each failure mode of each part by Eq. (7.21). Ignore all values with more than 3 decimal places.	CR(20A1R1 - open) = 0.80×1.00 $\times 1.5 \times 10^6$ hr = 1.2 per 10^6 hr CR(20A1R1 - drift) = 0.20×0.10 $\times 1.5$ per 10^6 hr = 0.030 per 10^6 hr
(7) Compute the total CR for the unit (CR), by Eq. (7.22).	The total CR for the preamplifier unit is 6.851 per 10^6 hr (See Fig. 7.8.3-3).

MIL-STD-1629 contains detailed procedures and forms for performing FMEAs and FMECAs, as well as additional examples. The worksheet from MIL-STD-1629 (Figure 7.8.4-1) is slightly more complex than the one used to work the Radar Preamplifier example.

7.8.5 COMPUTER ANALYSIS

A computer can be quite useful in performing an FMEA, since a large number of computations and a large amount of record keeping are often required for systems of reasonable size.

In the failure effects portion of the analysis the computer is used primarily for function evaluation, using performance models. On the assumption that the computer program contains the design equations relating system outputs to various design parameters, each item is allowed to fail in each one of its modes, and the effect on the system is computed.

Several computer programs are available for evaluating circuits. The NET-1 (Ref. 58) network analysis program can be used for a failure effects analysis of a circuit containing transistors and passive circuit elements. The value of all of the circuit performance parameters would be printed out for each abnormal condition. NET-1 does not automatically consider failure modes of circuit parts such as shorts and opens; investigation of these require manually setting up a new run for each set of values of the parts. A shorted resistor would have zero resistance and an open resistor would have infinite resistance.

Circuit analysis programs such as ECAP (Electronic Circuit Analysis Program) (Ref. 59), which accept a topological input description of the circuit and synthesize the circuit equations, can be used to evaluate failure effects, but computer running time can become excessive since the circuit equations may have to be generated over again for each run. For extreme failure modes such as an open or a short of a part, the circuit configuration is changed and a completely new solution is required.

The AFMAP (Automated Failure Mode Analysis Program) (Ref. 60) is a circuit analysis program that automates the failure effect analysis for DC circuits. It repeatedly solves the circuit equations, computing and printing circuit mode voltages, for failure modes such as opens and shorts of parts and shorts between all node pairs. However, AFMAP includes only resistors, diodes, transistors, power supplies, and nodes. This automated approach to failure effects analysis can be used effectively in other types of systems such as structures and propulsion systems, but no programs are known which provide these capabilities.

Some other programs that can be used for FMEA are:

(1) IM 045-NAA: Analyzes failure mode effect at system, subsystem, or part level. (Ref. 61)
(2) IM 066-NAA: Revision of IM 045-NAA (Ref. 63)
(3) IM 063-NAAL: Analyzes failure mode effects at system, subsystem, or part level (Ref. 62)

CRITICALITY ANALYSIS

SYSTEM _____
FEATURE LEVEL _____
REFERENCE DRAWING _____
MISSION _____

DATE _____
SHEET _____ OF _____
COMPILED BY _____
APPROVED BY _____

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	SEVERITY CLASS.	FAILURE PROBABILITY FAILURE RATE DATA SOURCE	FAILURE EFFECT PROBABILITY (β)	FAILURE MODE RATIO (α)	FAILURE RATE (λ_p)	OPERATING TIME (t)	FAILURE MODE CRIT # $C_m = \beta\alpha\lambda_p t$	ITEM CRIT # $C_r = \Sigma(C_m)$	REMARKS

FIGURE 7.8.4-1: EXAMPLE OF A CRITICAL ANALYSIS WORKSHEET FORMAT

The most recent FMEA computer program was one developed for the space shuttle program (Ref. 64), and can be readily adaptable to other systems.

7.8.6 SUMMARY

The FMEA does not replace the need for sound engineering judgment at the design level. This systems analysis is, however, practical in determining many of the significant details which may not otherwise be determined by separate, individual studies. Like other design tools, the FMEA has limitations such as those discussed below.

(1) It is not a substitute for good design. If used for its intended purpose it can be an aid to better design.

(2) It will not solve item problems which may exist as a limitation to effective systems design. It should define and focus attention on such problems and indicate the need for a design solution.

(3) It will not, in itself, guarantee a system design. It is nothing more than a logical way of establishing "bookkeeping" which can be systematically analyzed for design reliability.

7.9 FAULT TREE ANALYSIS

The "fault tree" analysis (FTA) technique is a method for block diagramming constituent lower level elements. It determines, in a logical way, which failure modes at one level produce critical failures at a higher level in the system. The technique is useful in safety analysis where the discipline of block diagramming helps prevent an oversight in the basic FMEA discussed in the previous subsection.

As was previously mentioned, FMEA is considered a "bottoms up" analysis, whereas an FTA is considered a "top down" analysis. FMEAs and FTAs are compatible and basically equivalent methods of risk analysis, with the choice of method dependent on the nature of the risk to be evaluated. There are some differences, however, because FTA is a top down analysis there is a higher probability of misinterpretation at the lowest level. On the other hand, FMEA starts at the lowest level, therefore will probably result in a better method of risk analysis (assuming lowest level data is available). In general, FTA requires a greater skill level than FMEA.

Fault tree methods of analysis are particularly useful in functional paths of high complexity in which the outcome of one or more combinations of noncritical events may produce an undesirable critical event. Typical candidates for fault tree analysis are functional paths or interfaces which could have critical impact on flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. The fault tree provides a concise and orderly description of the various combinations of possible occurrences within the system which

can result in a predetermined critical output event. However, performance of the fault tree analysis does require considerable engineering time and even then the quality of results is only as good as the validity of input data and accuracy of the fault tree logic.

Fault tree methods can be applied beginning in the early design phase, and progressively refined and updated to track the probability of an undesirable event as the design evolves. Initial fault tree diagrams might represent functional blocks (e.g., units, equipments, etc.), becoming more definitive at lower levels as the design materializes in the form of specific parts and materials. Results of the analysis are useful in the following applications:

(1) Allocation of critical failure mode probabilities among lower levels of the system breakdown

(2) Comparison of alternative design configurations from a safety point of view

(3) Identification of critical fault paths and design weaknesses for corrective action

(4) Evaluation of alternative corrective action approaches

(5) Development of operational, test, and maintenance procedures to recognize and accommodate unavoidable critical failure modes

Symbols commonly used in diagramming a fault tree analysis are shown in Figure 7.9-1. The basic relationships between functional reliability (success) block diagrams and the equivalent fault tree diagrams, using some of these symbols, are illustrated in Figures 7.9-2 and 7.9-3.

Success of the simple two element series system comprised of blocks A and B is given by $R = AB$; and the probability of system failure (i.e., unsuccessful or unsafe performance) is given by $\bar{R} = (1 - R) = 1 - AB$. When individual element unreliability ($\bar{R}_i$) is less than 0.1, the following approximations may be used to simplify computations in the fault tree logic diagram, with little (10%) error:

$$\bar{R} = 1 - AB = 1 - (1 - \bar{A})(1 - \bar{B})$$
$$= \bar{A} + \bar{B} - \bar{A}\bar{B} \approx \bar{A} + \bar{B}$$

The two element block diagrams of Figure 7.9-2 is reconfigured as a simple parallel redundant system in Figure 7.9-3 to illustrate the treatment of parallel redundant elements in the fault tree logic diagram. Note that "AND" gates for the combination of successes (Rs) become "OR" gates for the combination of failures ($\bar{R}$s); and "OR" gates for Rs become "AND" gates for $\bar{R}$s. This is illustrated in the series parallel network of Figure 7.9-3.

The fault tree analysis of critical failure modes should proceed as illustrated in the following steps.

"A"
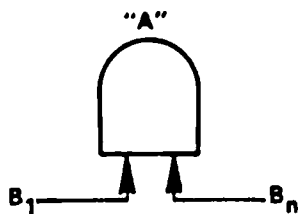
A logical "AND" gate – "A" exists if and only if all of B_1, B_2, ... B_n exist simultaneously.

B_1 — — B_n

"A"
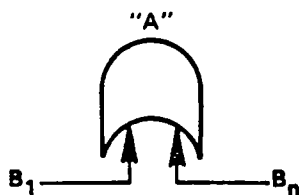
A logical inclusive "OR" gate – "A" exists if any of B_1, B_2, ...B_n or any combination thereof exists.

B_1 — — B_n
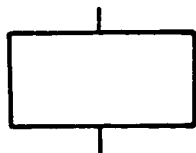
An event--usually the output of (or input to) an "AND" or an "OR" gate.

X_i
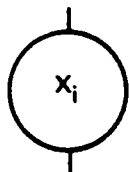
A failure or malfunction event--in terms of a specific circuit or component, represented by the symbol X with a numerical subscript.

W_i
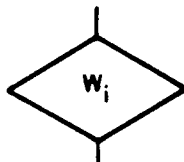
An event not developed further because of lack of information or because of lack of sufficient consequence. Represented by the symbol W with a numerical subscript.

A connecting symbol to another part of the fault tree within the same major branch.

An "inhibit" gate, used to describe the relationship between one fault and another. The input fault directly produces the output fault if the indicated condition is satisfied.

FIGURE 7.9-1: FAULT TREE ANALYSIS SYMBOLS

$$R = AB$$
$$\bar{R} = 1 - AB = \bar{A} + \bar{B} - \bar{A}\bar{B}$$

SUCCESSFUL
EVENT
$R = AB$

UNSUCCESSFUL
EVENT
$\bar{R} = \bar{A} + \bar{B} - \bar{A}\bar{B}$

AND

OR

A   B

$\bar{A}$ $\bar{B}$

AB

$\bar{A} + \bar{B} - \bar{A}\bar{B}$
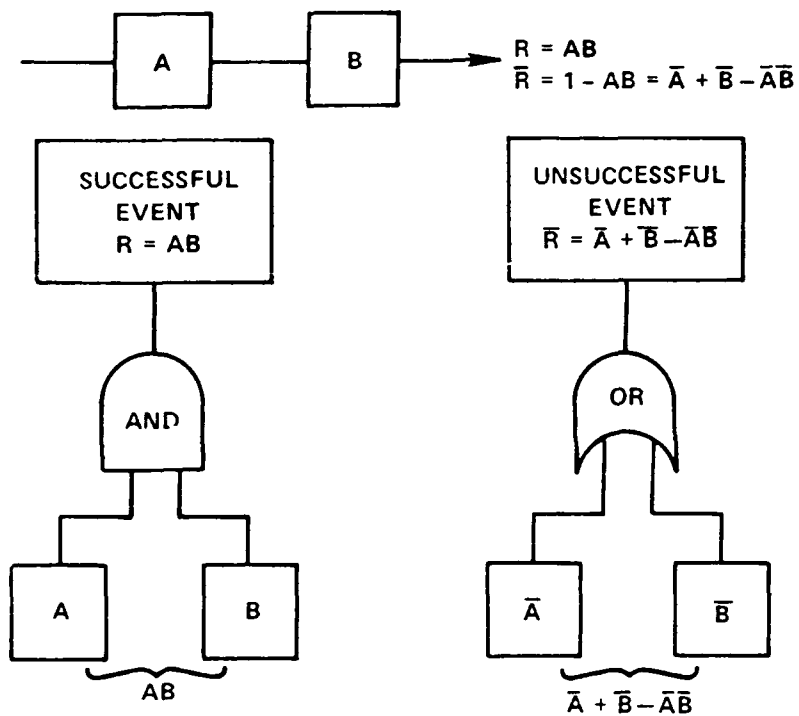
FIGURE 7.9-2:   <u>TRANSFORMATION OF TWO-ELEMENT SERIES RELIABILITY BLOCK DIAGRAM TO "FAULT TREE" LOGIC DIAGRAMS</u>

$$R = CD(1 - \overline{A}\,\overline{B}) = CD(A + B - AB)$$

$$\overline{R} = 1 - CD(1 - \overline{A}\,\overline{B})$$
$$= \overline{C} + \overline{D} + \overline{A}\overline{B} - (\overline{C}\overline{D} + \overline{A}B\overline{C} + \overline{A}B\overline{D} - \overline{A}B\overline{C}\overline{D})$$

SUCCESS
$$R = CD(A + B - AB)$$

FAILURE
$$\overline{R} = \overline{C} + \overline{D} + \overline{A}\overline{B}$$
$$- (\overline{C}\overline{D} + \overline{A}B\overline{C} + \overline{A}B\overline{D} - \overline{A}B\overline{C}\overline{D})$$

CD

$$A + B \cdot AB$$

$$\overline{C} + \overline{D} - \overline{C}\overline{D}$$

$$\overline{A}\overline{B}$$
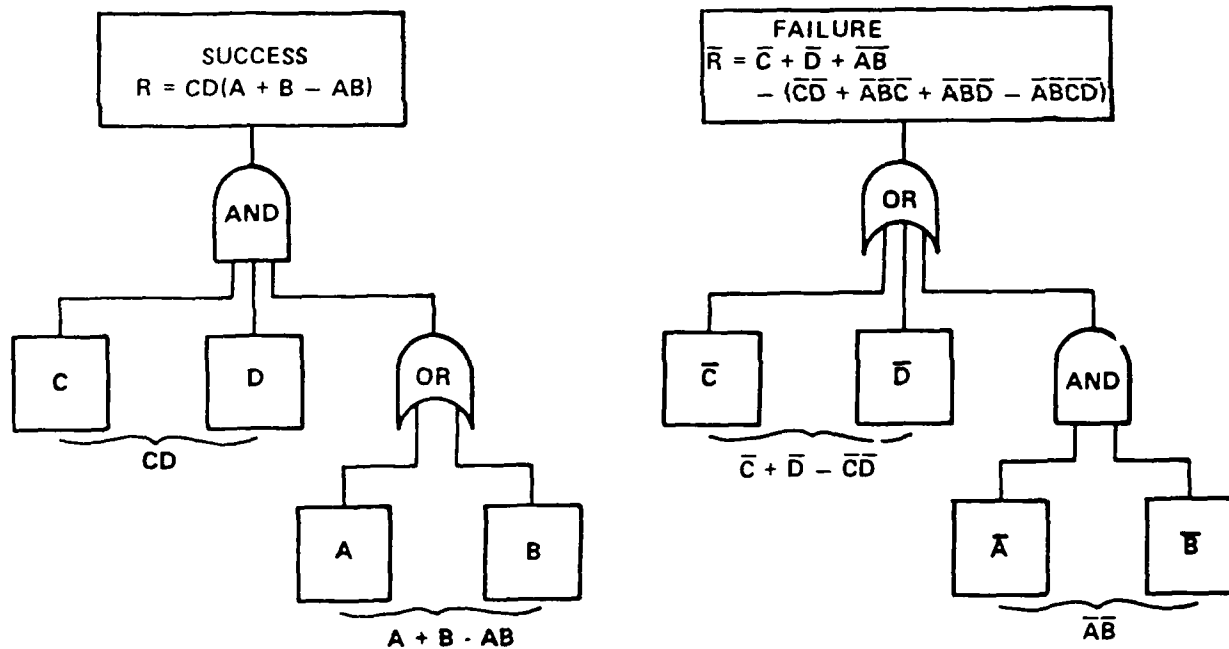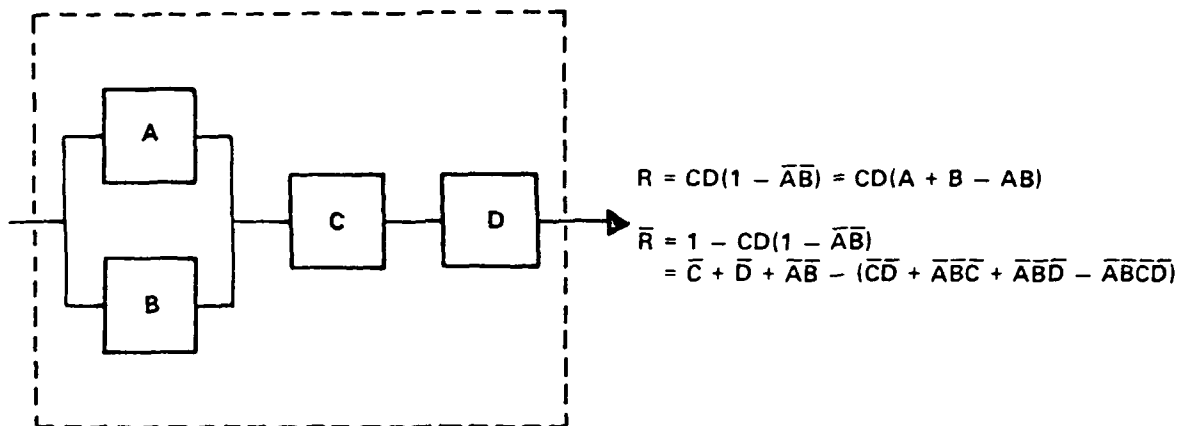
FIGURE 7.9-3: TRANSFORMATION OF SERIES/PARALLEL BLOCK DIAGRAM TO EQUIVALENT FAULT TREE LOGIC DIAGRAMS

Step 1: Develop Function Reliability Block Diagram. Develop reliability block diagram for the system/equipment functional paths in which the critical failure mode is to be circumvented or eliminated. Define the critical failure mode in terms of the system level malperformance symptom to be avoided. For example, the hypothetical firing circuit of Figure 7.9-4 is designed to ignite a proposed rocket motor in the following sequence:

(1) Shorting switch S_1 is opened to enable launcher release and firing

(2) Firing switch S_2 is closed by the pilot to apply power to relay R_1

(3) Relay R_1 activates the guidance and control (G&C) section

(4) Relay R_2 is activated by signal from the G&C section, closing the igniter firing circuit which starts the rocket motor

The rocket motor can be inadvertently fired by premature ignition due to electronic failure, electromagnetic interference (EMI), or by external factors such as shock, elevated temperature, etc. These are the events to be studied in the fault tree analysis.

Step 2: Construct the Fault Tree. Develop the fault tree logic diagram relating all possible sequences of events whose occurrence would produce the undesired events identified in Step 1, e.g., inadvertent firing of the missile rocket motor. The fault tree should depict the paths that lead to each succeeding higher level in the functional configuration. Figure 7.9-5 illustrates the construction of one branch of the fault tree for the ignition circuit.

In constructing the fault tree for each functional path or interface within the reliability model, consideration must be given to the time sequencing of events and functions during the specified mission profile. Very often the operational sequence involves one or more changes in hardware configuration, functional paths, critical interfaces, or application stresses. When such conditions are found to apply, it is necessary to develop a separate fault tree for each operating mode, function, or mission event in the mission sequence.

Step 3: Develop Failure Probability Model. Develop the mathematical model of the fault tree for manual (or computer) computation of the probability of critical event occurrence on the basis of failure modes identified in the diagram. For example, the undesired system level critical failure mode identified in Figure 7.9-5 is "accidental rocket motor firing," given by the top level model as follows:

$$\bar{A} = \bar{B} + \bar{C} - \bar{B}\bar{C}$$
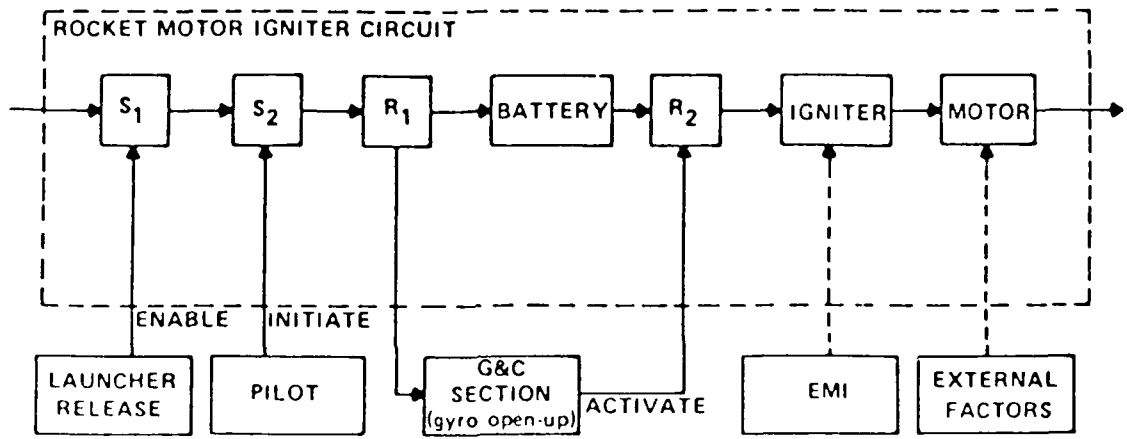
FIGURE 7.9-4: <u>RELIABILITY BLOCK DIAGRAM OF HYPOTHETICAL ROCKET MOTOR FIRING CIRCUIT</u>
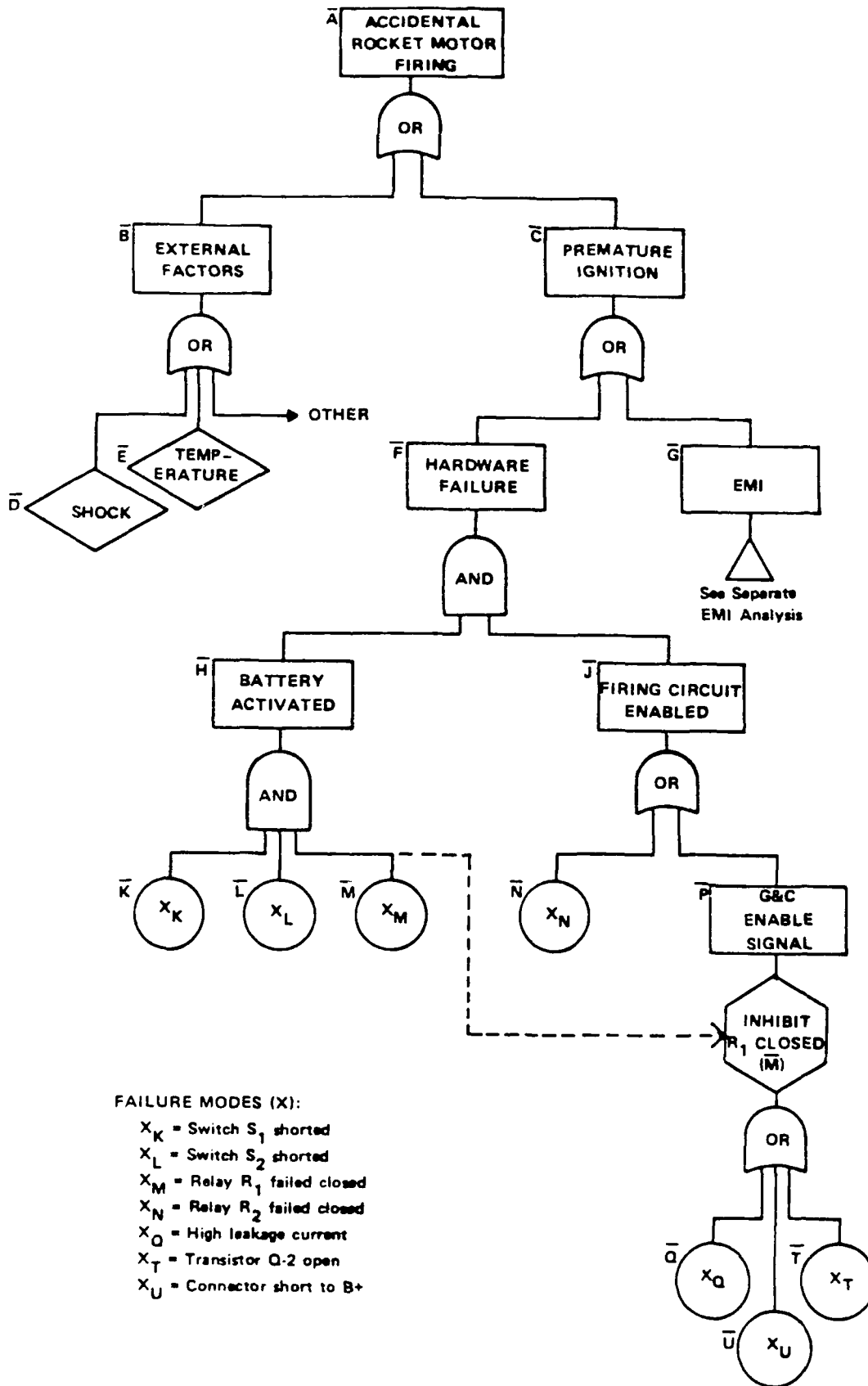
FIGURE 7.9-5: FAULT TREE FOR SIMPLIFIED ROCKET MOTOR FIRING CIRCUIT

FAILURE MODES (X):

X_K = Switch S_1 shorted

X_L = Switch S_2 shorted

X_M = Relay R_1 failed closed

X_N = Relay R_2 failed closed

X_Q = High leakage current

X_T = Transistor Q-2 open

X_U = Connector short to B+

As indicated in the figure, C represents the probability of accidental rocket motor firing due to premature ignition via the firing circuit either due to hardware failure (F) or electromagnetic interference (G), i.e.:

$$\bar{C} = \bar{F} + \bar{G} - \bar{F}\bar{G}$$

Considering hardware failures only, the probability of premature ignition due to hardware failure is given by:

$$\bar{F} = \bar{H}\bar{J}$$

where

$$\bar{H} = \overline{KLM}$$
$$\bar{J} = \bar{N} + \bar{P} - \bar{N}\bar{P}$$
$$\bar{P} = \bar{Q} + \bar{T} + \bar{U} - (\overline{QT} + \overline{QU} + \overline{TU} - \overline{QTU})$$

Step 4: Determine Failure Probabilities or Identified Failure Modes. Determine probability of occurrence (i.e., probability of failure) in each event or failure mode identified in the model. Compute safety parameters at the system level by applying the failure data in the models derived in Step 3.

Assume, for example, the following failure probabilities in the premature ignition branch of the fault tree:

$$\bar{K} = 50 \times 10^{-3}$$
$$\bar{L} = 100 \times 10^{-3}$$
$$\bar{M} = 40 \times 10^{-3}$$
$$\bar{N} = 5 \times 10^{-3}$$
$$\bar{Q} = 2 \times 10^{-3}$$
$$\bar{T} = 1 \times 10^{-3}$$
$$\bar{U} = 0.5 \times 10^{-3}$$

Using the bottom up approach, combine these data in the failure probability models developed in Step 3, and estimate the system level probability as follows:

$$\bar{P} = \bar{Q} + \bar{T} + \bar{U} - (\overline{QT} + \overline{QU} + \overline{TU} - \overline{QTU})$$
$$= (2 + 1 + 0.5)10^{-3} - [(2 + 1 + 0.5)10^{-6} - (1)10^{-9}]$$
$$\approx 3.5 \times 10^{-3}$$

Higher order (product) terms in the model can be dropped in the P model since the values of individual terms are much less than 0.10.

Combining $\bar{P}$ with $\bar{N}$ to find $\bar{J}$ yields:

$$\bar{J} = \bar{N} + \bar{P} - \bar{N}\bar{P}$$
$$= 5 \times 10^{-3} + 3.5 \times 10^{-3} - 17.5 \times 10^{-6}$$
$$\approx 8.5 \times 10^{-3}$$

This is the probability of accidental firing circuit operational conditional on relay R_1 having failed in the closed position (i.e., M) in the battery branch of the fault tree. In the battery branch, the battery can be accidentally activated only if switches S_1 and S_2 fail in the short mode, and if relay R_1 fails in the closed position, given by:

$$\bar{H} = \overline{KLM}$$
$$= (50 \times 10^{-3})\ (100 \times 10^{-3})\ (40 \times 10^{-3})$$
$$= 200 \times 10^{-6}$$

Probability of premature ignition because of hardware failure is then estimated from:

$$\bar{F} = \overline{HJ} = (200 \times 10^{-6})\ (8.5 \times 10^{-3})$$
$$= 1.70 \times 10^{-6}$$

Assume that the EMI analysis discloses a probability of accidental ignition ($\bar{G} = 5 \times 10^{-6}$) due to exposure to specified level of RF radiation in the operating environment. The probability of premature ignition to either cause (hardware failure or EMI exposure) is given by:

$$\bar{C} = \bar{F} + \bar{G} - \bar{F}\bar{G}$$
$$\approx (1.70 \times 10^{-6}) + (5 \times 10^{-6}) - (1.70 \times 10^{-6})\ (5 \times 10^{-6})$$
$$\approx 6.70 \times 10^{-6}$$

Assume that failure data accrued during rocket motor qualification tests indicates $\bar{D} = 2.5 \times 10^{-6}$ and $\bar{E} = 12.5 \times 10^{-6}$ under specified conditions and levels of exposure. Under these circumstances,

$$\bar{B} = \bar{D} + \bar{E} - \bar{D}\bar{E}$$
$$= (2.5 \times 10^{-6}) + (12.5 \times 10^{-6}) - (2.5 \times 10^{-6})\ (12.5 \times 10^{-6})$$
$$\bar{B} = 15 \times 10^{-6}$$

Probability of accidental rocket motor firing during the handling and loading sequence is then:

$$\bar{A} = \bar{B} + \bar{C} - \bar{B}\bar{C}$$
$$\approx (15 \times 10^{-6}) + (6.70 \times 10^{-6}) - (15 \times 10^{-6})\ (6.75 \times 10^{-6})$$
$$\approx 21.7 \times 10^{-6}$$

That is, approximately 22 premature rocket motor firings per million missile load/launch attempts.

Failure rate values for most standard electronic and electromechanical parts are available in MIL-HDBK-217. The most recent document for failure rate values for mechanical parts is Reference 4. Failure rate data for new parts and more recently developed "high reliability" parts may not be available in these sources, however. In such cases, it becomes necessary to draw on vendor certified data or special tests.

In the absence of complete and validated failure rate/failure mode data for all inputs, a preliminary fault tree analysis can be performed using conservative estimates of failure rates in the critical failure modes. This preliminary analysis will identify those input values which have little effect, as well as those having a critical effect on system performance. The latter can then be investigated in depth by testing.

Evaluation of the fault tree model may reveal that the conservatively estimated values are sufficient to satisfy the performance goal. Other values will warrant further study. In some cases, it may even be more expedient to change the design than to validate a data value.

Step 5: Identify Critical Fault Paths. When the probability of an unsafe failure mode at the system level exceeds specification tolerances, identify the critical paths which contribute most significantly to the problem. For example, both paths in the preceding analysis contribute about equally to the total problem because of environmental sensitivity -- ignition circuit to EMI, and propellant insulation to high ambient temperature.

7.9.1 DISCUSSION OF FTA METHODS

There are basically three methods for solving fault trees: (1) direct simulation (Ref. 65), (2) Monte Carlo (Ref. 66), and (3) direct analysis (Ref. 67).

Direct simulation basically uses Boolean logic hardware (similar to that in digital computers) in a one-to-one correspondence with the fault tree Boolean logic to form an analog circuit. This method usually is prohibitively expensive. A hybrid method obtains parts of the solution using the analog technique and parts from a digital calculation, in an effort to be cost competitive. Because of the expense involved, this method rarely is used.

Monte Carlo methods are perhaps the most simple in principle but in practice can be expensive. Since Monte Carlo is not practical without the use of a digital computer, it is discussed in that framework. The most easily understood Monte Carlo technique is called "direct simulation." The term "simulation" frequently is used in conjunction with Monte Carlo methods, because Monte Carlo is a form of mathematical simulation. (This simulation should not be confused with direct analog simulation.) Probability data are provided as input, and the simulation program represents the fault tree on a computer to provide quantitative results. In this manner, thousands or millions of trials can be simulated. A typical simulation program involves the following steps.

(1) Assign failure data to input fault events within the tree and, if desired, repair data.

(2) Represent the fault tree on a computer to provide quantitative results for the overall system performance, subsystem performance, and the basic input event performance.

(3) List the failure that leads to the undesired event and identify minimal cut sets contributing to the failure.

(4) Compute and rank basic input failure and availability performance results.

In performing these steps, the computer program simulates the fault tree and, using the input data, randomly selects the various parameter data from assigned statistical distributions; and then tests whether or not the TOP event occurred within the specified time period. Each test is a trial, and a sufficient number of trials is run to obtain the desired quantitative resolution. Each time the TOP event occurs, the contributing effects of input events and the logical gates causing the specified TOP event are stored and listed as computer output. The output provides a detailed perspective of the system under simulated operating conditions and provides a quantitative basis to support objective decisions.

A number of computer programs have been developed for fault tree analysis. They are classified and listed in Figure 7.9.1-1. Also, Reference 68 is one of the most comprehensive documents available on fault tree analysis; it contains a more detailed description of most of the computer programs shown in Figure 7.9.1-1.

In practice, the methods used for fault tree analysis will depend on which ones are available for the computer being used. It will rarely, if ever, be worthwhile generating a computer program especially for a particular problem.

7.10 SNEAK CIRCUIT ANALYSIS (SCA)

7.10.1 INTRODUCTION AND GENERAL DESCRIPTION

A relatively new designers' analysis tool which has become increasingly popular during the past decade is that of sneak circuit analysis.

A sneak circuit is an unexpected path or logic flow within a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. The path may consist of hardware, software, operator actions, or combinations of these elements. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system or coded into the software program, which can cause it to malfunction under certain conditions. Categories of sneak circuits are:

(1) Sneak paths which cause current, energy, or logical sequence to flow along an unexpected path or in an unintended direction.

(2) Sneak timing in which events occur in an unexpected or conflicting sequence.

(3) Sneak indications which cause an ambiguous or false display of system operating conditions and thus may result in an undesired action taken by an operator.
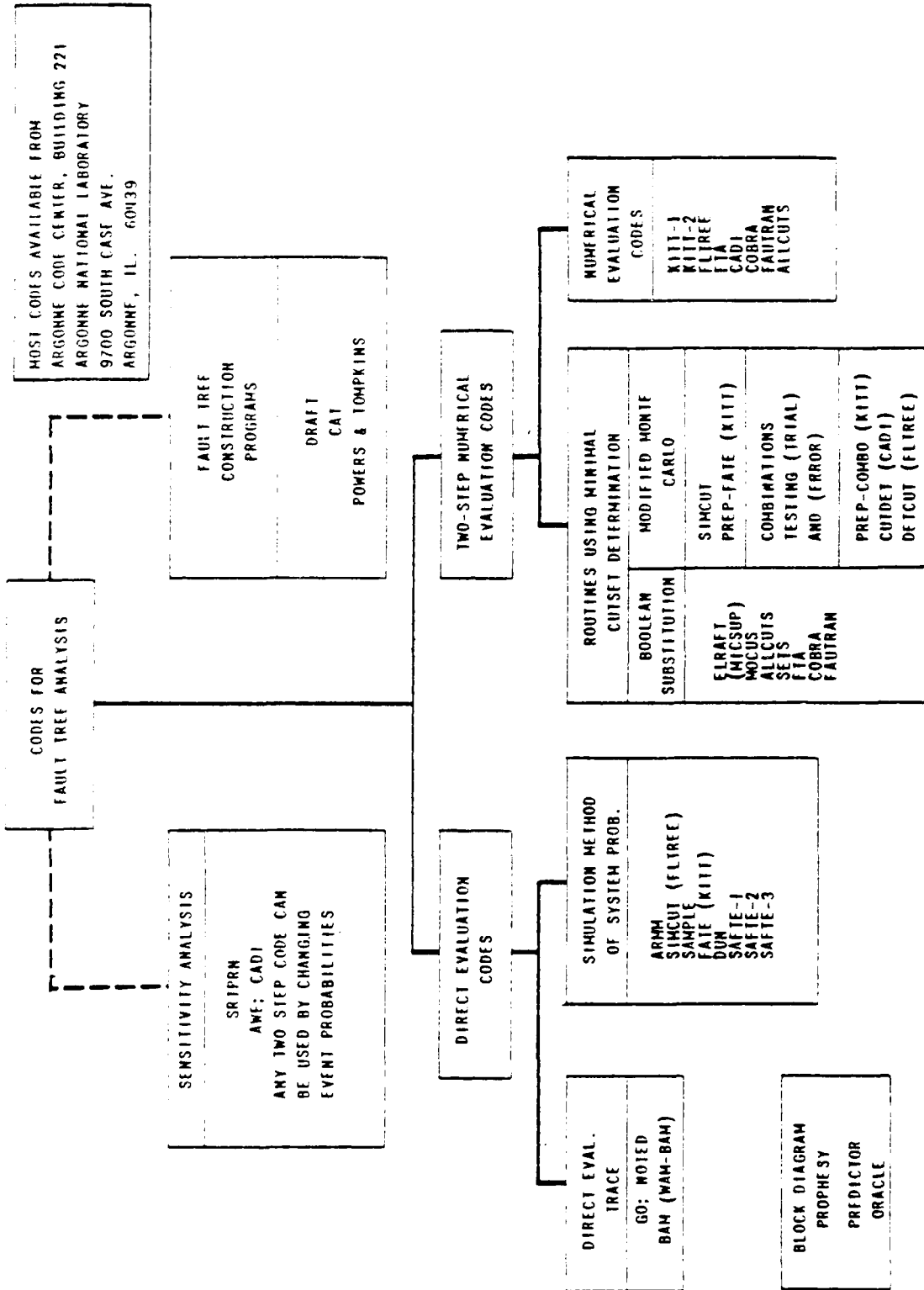
FIGURE 7.9.1-1: PROGRAMS FOR FAULT TREE ANALYSIS

(4) Sneak labels which incorrectly or imprecisely label system functions, e.g., system inputs, controls, displays, buses, etc., and thus may mislead an operator into applying an incorrect stimulus to the system.

Figure 7.10.1-1 depicts a simple sneak circuit example. With the ignition off, the radio turned to the on position, the brake pedal depressed, and the hazard switch engaged, the radio will power on with the flash of the brake lights.

Sneak circuit analysis is the term that has been applied to a group of analytical techniques which are intended to methodically identify sneak circuits in systems. SCA techniques may be either manual or computer assisted, depending on system complexity. Current SCA techniques which have proven useful in identifying sneak circuits in system include:

(1) Sneak Path Analysis. A methodical investigation of all possible electrical paths in a hardware system. Sneak path analysis is a technique used for detecting sneak circuits in hardware systems, primarily power distribution, control, switching networks, and analog circuits. The technique is based on known topological similarities of sneak circuits in these types of hardware systems.

(2) Digital Sneak Circuit Analysis. An analysis of digital hardware networks for sneak conditions, operating modes, timing races, logical errors, and inconsistencies. Depending on system complexity, digital SCA may involve the use of sneak path analysis techniques, manual or graphical analysis, computerized logic simulators or computer aided design (CAD) circuit analysis.

(3) Software Sneak Path Analysis. An adaption of sneak path analysis to computer program logical flows. The technique is used to analyze software logical flows by comparing their topologies to those with known sneak path conditions in them.

(4) Other Sneak Circuit Analysis Techniques. Because the technology of hardware and software systems is evolving at a rapid rate, new SCA techniques will undoubtedly evolve as well. The technique will also find use in analysis of other than electrical, or electronic systems (such as mechanical, hydraulic, pneumatic, etc.), where analogous situations of energy flow, logic timing, etc. are encountered.

7.10.2 EXAMPLES OF CATEGORIES OF SNEAK CIRCUITS

The broad categories of sneak circuits were described in the previous section; following are some specific examples of each of the categories.
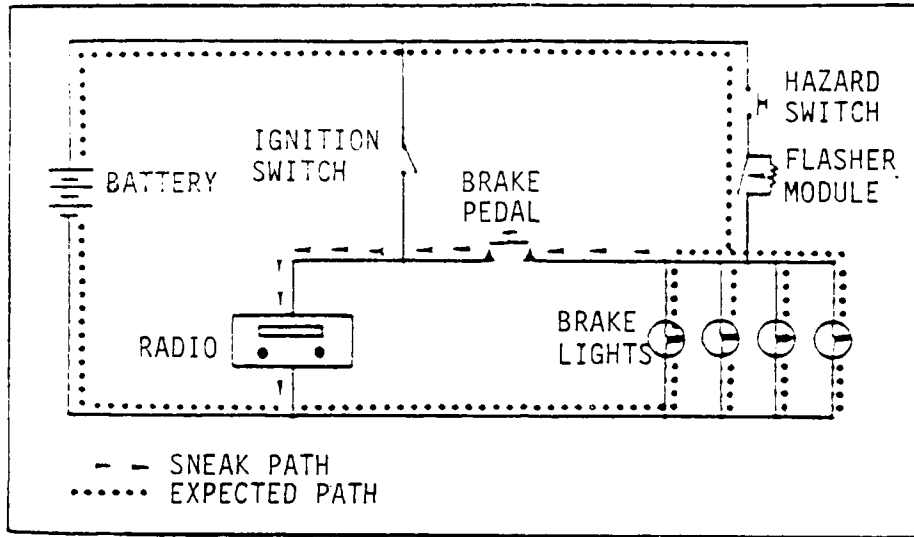
FIGURE 7.10.1-1: <u>AUTOMOTIVE SNEAK CIRCUIT</u>

Sneak Path. A sneak path is one which allows current or energy to flow along an unsuspected path or in an unintended direction. There are two distinct subsets of this category. They are:

Sneak Path, Enable occurs when the sneak path initiates an undesired function or result under certain conditions, but not all conditions. An example of this class is shown in Figure 7.10.2-1.

The electrical power regulator output circuits shown in Figure 7.10.2-1 represent a portion of the power ditribution system in an air vehicle instrument. The sneak path is identified by the arrows along the connection between terminal E6 and pin A of connector J16. This sneak path connects the +4VDC output of regulator VR1 to the +12VDC output of regulator VR2. This path would permit excessive current to flow from the +12VDC output into the +4VDC loads. The result could be failure of either or both regulators (VR1, VR2) and possible catastrophic burnout of the +4VDC loads. Any of these failures would result in the loss of the instrument. If immediate failure did not occur, out-of-tolerance operation of the +4VDC loads would occur due to the 3-times normal voltage being applied. The recommended correction was to remove the wire connection between terminal E6 and pin A of connector J16.

Sneak Path, Inhibit occurs when the sneak path prevents a desired function or results under certain conditions, but not all conditions. An example of this is shown in Figure 7.10.2-2.

The circuit shown in Figure 7.10.2-2 was used in a satellite to provide isolation of the power circuits in a double redundant subsystem. The technique removes both power and power ground from the nonoperating backup circuit. The sneak paths which bypass the Q3 grounding switches are identified in Figure 7.10.2-2 by the arrows placed along each path. When the hardware was wired as shown, total isolation no longer existed and the design intent was violated. The recommended correction was to remove the wire in cable W62 connecting pin 27 of connector P12 to terminal E5 of the single point ground (SPG). When wired as recommended, the power ground switching can be performed by either channel's Q3 and the SPG at E4.

Other basic categories of sneak paths are:

Sneak Timing. A sneak timing condition is one which causes functions to be inhibited or to occur at an unexpected or undesired time. The example in Figure 7.10.2-3a illustrates a sneak that occurred in the digital control circuitry of a mine. The enable logic for U4 and U5 allows them, briefly, to be enabled simultaneously. Being CMOS devices in a "wired or" configuration, this allows a potential power-to-ground short through the two devices, damaging or destroying them during operation.

VR2
+12 VDC
REGULATOR

VR1
+4 VDC
REGULATOR

P1-C

P1-A

E4   E6

E7

J16-A

TO OTHER
CARDS

TO OTHER
CARDS

TO OTHER
CARDS

▷ Connection to frequency
discriminator
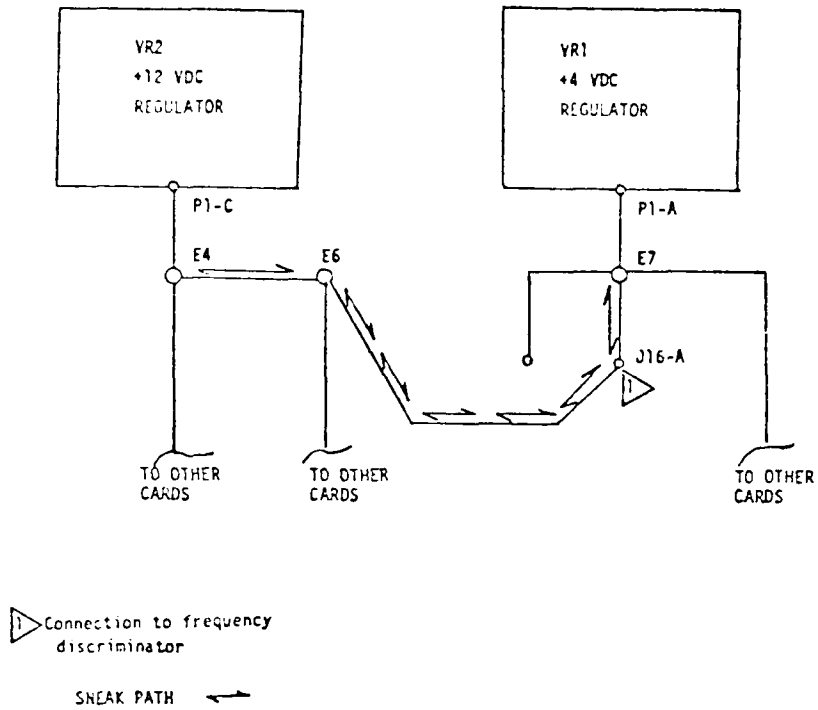
SNEAK PATH ⟵

FIGURE 7.10.2-1:   SNEAK PATH ENABLE
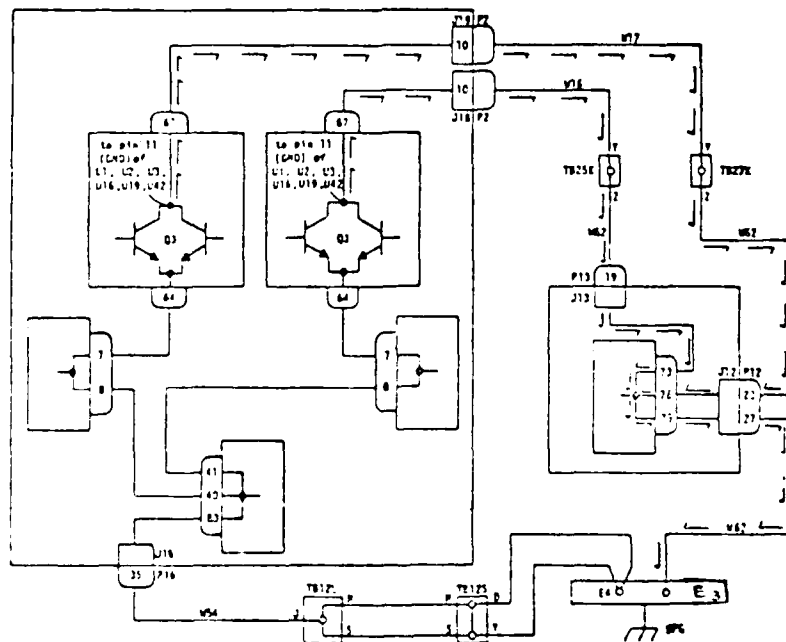
FIGURE 7.10.2-2:   REDUNDANT CIRCUIT SWITCHED GROUND
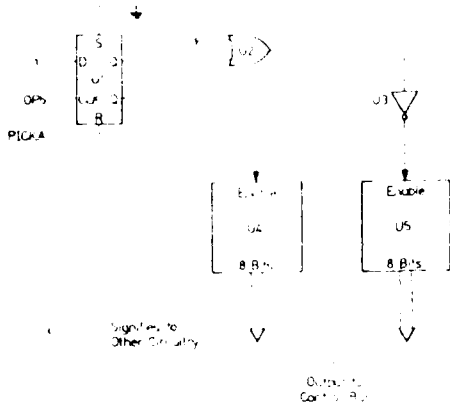
(a) SNEAK TIMING
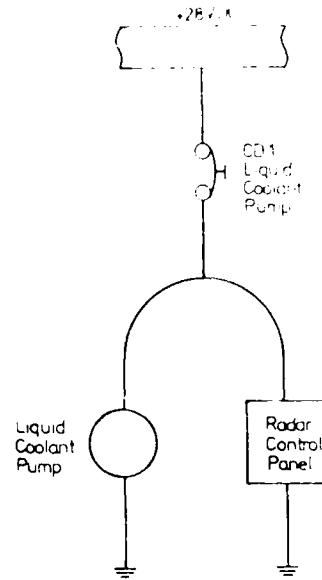
(b) SNEAK LABEL
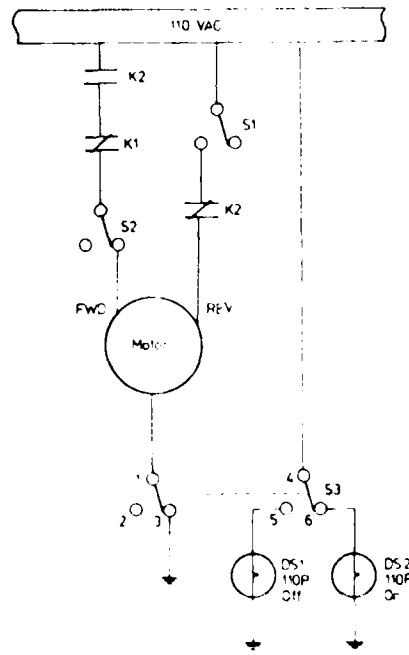
(c) SNEAK INDICATOR

FIGURE 7.10.2-3: EXAMPLES OF CATEGORIES OF SNEAK CIRCUITS

Sneak Label. A label on a switch or control device which would cause incorrect actions to be taken by operators. The example in Figure 7.10.2-3b taken from an aircraft radar system, involves a circuit breaker which provides power to two disparate systems, only one of which is reflected in its label. An operator attempting to remove power from the liquid coolant pump would inadvertently deactivate the entire radar.

Sneak Indication. An indication which causes ambiguous or incorrect displays. Figure 7.10.2-3c illustrates a sneak indication which occurred in a sonar power supply system. The MOP (Motor Operated Potentiometer) OFF and ON indicators do not, in fact, monitor the status of the MOP motor. Switch S3 could be in the position shown, providing an MOP ON indication even through switches S1 or S2 or relay contacts K1 or K2 could be open, inhibiting the motor.

7.10.3   SNEAK CIRCUIT METHODOLOGY

7.10.3.1 NETWORK TREE PRODUCTION

The first major consideration that must be satisfied to identifying sneak circuit conditions is to insure that the data being used for the analysis represent the actual "as built" circuitry of the system. Functional, integrated, and system level schematics do not always represent the actual constructed hardware. Detail manufacturing and installation schematics must be used, because these drawings specify exactly what was built, contingent on quality control checks, tests, and inspection. However, manufacturing and installation schematics rarely show complete circuits. The schematics are laid out to facilitate hookup by technicians without regard to circuit or segment function. As a result, analysis from detail schematics is extremely difficult. So many details and unapparent continuities exist in these drawings that an analyst becomes entangled and lost in the maze. Yet, these schematics are the data that must be used if analytical results are to be based on true electrical continuity. The first task of the sneak analyst is, therefore, to convert this detailed, accurate information into a form usable for analytical work. The magnitude of data manipulation required for this conversion necessitates the use of computer automation in most cases.

Automation has been used in sneak circuit analysis since 1970 as the basic method for tree production from manufacturing detail data. Computer programs have been developed to allow encoding of simple continuities in discrete "from-to" segments extracted from detail schematics and wire lists. The encoding can be accomplished without knowledge of circuit function. The computer connects associated points into paths and collects the paths into node sets. The node sets represent interconnected nodes that make up each circuit. Plotter output of node sets and other reports are generated by the computer to enable the analyst to easily sketch accurate topological trees. The computer reports also provide complete indexing of every component and data point to its associated tree. This feature is especially useful in cross indexing functionally related or interdependent trees, in incorporating changes, and in troubleshooting during operational support.

7.10.3.2 TOPOLOGICAL PATTERN IDENTIFICATION

Once the network trees have been produced, the next task of the analyst is to identify the basic topological patterns that appear in each tree. Five basic patterns exist for hardware SCA: (1) single line (no-node) topograph, (2) ground dome, (3) power dome, (4) combination dome, and (5) "H" pattern. These patterns are illustrated in Figure 7.10.3.2-1. One of these patterns or several in combination will characterize the circuitry shown in any given network tree. Although, at first glance, a given circuit may appear more complex than these basic patterns, closer inspection reveals that the circuit is actually composed of these basic patterns in combination. As the sneak circuit analyst examines each node in the network tree, he must identify the topographical pattern or patterns incorporating the node and apply the basic clues that have been found to typify sneak circuits involving that particular pattern.

7.10.3.3 CLUE APPLICATION

Associated with each pattern is a list of clues to help the analyst identify sneak circuit conditions. These lists were first generated during the original study of historical sneak circuits. The lists were updated and revised during the first several years of applied sneak circuit analysis. Now, the list of clues provides a guide to all possible design flaws that can occur in a circuit containing one or more of the five basic topological configurations, subject to the addition of new clues associated with new technological developments. The lists consist of a series of questions that the analyst must answer about the circuit to ensure that it is sneak free.

As an example, the single line topograph (Figure 7.10.3.2-1) would have clues such as: (a) Is switch S open when load L is desired? (b) Is switch S closed when load L is not desired?

Obviously, sneak circuits are rarely encountered in this topograph because of its simplicity. Of course, this is an elementary example and is given primarily as the default case which covers circuitry not included by the other topographs.

With each successive topograph, the clue list becomes longer and more complicated. The clue list for the "H" pattern includes over 100 clues. This pattern, because of its complexity, is associated with more sneak circuits than any of the previous patterns. Almost half of the critical sneak circuits identified to date can be attributed to the "H" patterns. Such a design configuration should be avoided whenever possible. The possibility of current reversal through the "H" crossbar is the most commonly used clue associated with "H" pattern sneak circuits.

7.10.4 SOFTWARE SNEAK ANALYSIS

Since SCA seemed to work for hardware, why not try it for software? This was done in 1975 when a feasibility study was performed which resulted in the development of a formal technique involving the use of
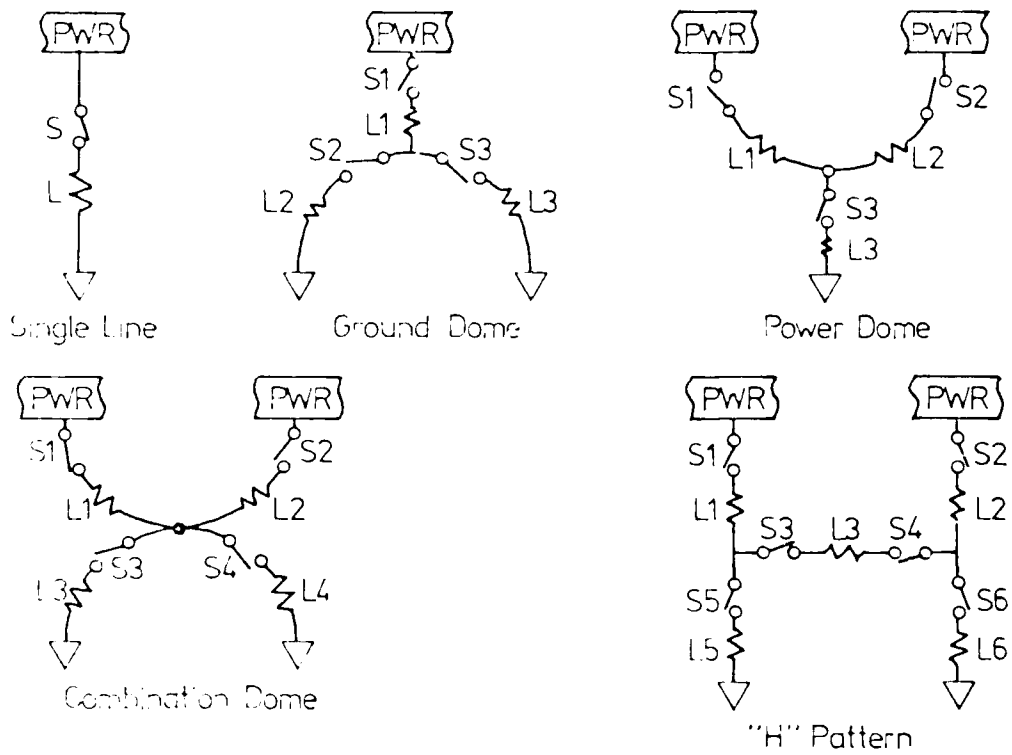
FIGURE 7.10.3.2-1: <u>BASIC TOPOGRAPHS</u>

mathematical graph theory, electrical sneak theory, and computerized search algorithms which are applied to a software package to identify software sneaks. A software sneak is defined as a logic control path which causes an unwanted operation to occur or which bypasses a desired operation, without regard to failures of the hardware system to respond as programmed.

The feasibility study concluded that:

(1) Software Sneak Analysis is a viable means of identifying certain classes of software problems

(2) Software Sneak Analysis works equally well on different software languages

(3) Software Sneak Analysis does not require execution of the software to detect problems

The Software Sneak Analysis technique has evolved along lines very similar to hardware Sneak Circuit Analysis. Topological network trees are used with electrical symbology representing the software commands to allow easy cross analysis between hardware and software trees and to allow the use of a single standardized analysis procedure.

Since topological pattern recognition is the keystone of both Sneak Circuit Analysis and Software Sneak Analysis, the overall methodologies are quite similar. The software package to be analyzed must be encoded, processed, and reduced to a standardized topographical format, the basic topological patterns identified and the appropriate problem clues applied to each pattern. For software, it has been found that six basic patterns exist: the Single Line, the Return Dome, the Iteration/Loop Circuit, the Parallel Line, the Entry Dome, and the Trap Circuit, as shown in Figure 7.10.4-1 below:

SINGLE LINE

RETURN
DOME

ITERATION/LOOP
CIRCUIT

PARALLEL
LINE

ENTRY DOME

TRAP CIRCUIT
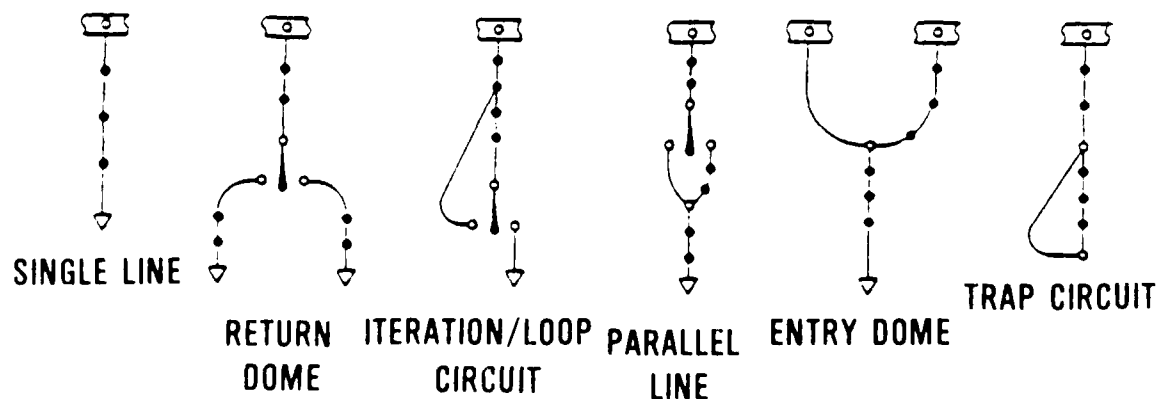
SOFTWARE TOPOGRAPHS

FIGURE 7.10.4-1

Although at first glance, a given software tree may appear to be more complex than these basic patterns, closer inspection will reveal that the code is actually composed of these basic structures in combination. As each node in the tree is examined, the analyst must identify which pattern or patterns include that node. The analyst then applies the basic clues that have been found to typify the sneaks involved with that particular structure. These clues are in the form of questions that the analyst must answer about the use and interrelationships of the instructions that are elements of the structure. These questions are designed to aid in the identification of the sneak conditions in the instruction set which could produce undesired program outputs.

Software sneaks are classified into four basic types:

(1) Sneak Output. The occurrence of an undesired output.

(2) Sneak Inhibit. The undesired inhibition of an output.

(3) Sneak Timing. The occurrence of an undesired output by virtue of its timing or mismatched input timing

(4) Sneak Message. The program message does not adequately reflect the condition.

Figure 7.10.4-2 illustrates a software sneak which occurred in the operating software of a military aircraft. Figure 7.10.4-2a illustrates the design intent of the section of software with the sneak. When the actual code was produced, however, the two tests were inadvertently interchanged. The network tree of the actual software code (see Figure 7.10.4-2b) makes the sneak readily apparent. This historical problem was uncovered only during the software system integrated testing when it was found that the instructions represented by LOAD 1 could never be executed.

7.10.5   INTEGRATION OF HARDWARE/SOFTWARE ANALYSIS

After a sneak circuit analysis and a software sneak analysis have been performed on a system, the interactions of the hardware with the system software can readily be determined. The analyst has at his disposal diagramatic representations of these two elements of the system in a single standardized format. The effect of a control operation that is initiated by some hardware element can be traced through the hardware trees until it impacts the system software. The logic flow can then be traced through the software trees to determine its ultimate impact on the system. Similarly, the logic sequence of a software initiated action can be followed through the software and electrical network trees until its eventual total system impact can be assessed.

The joint analysis of a system's software and hardware circuitry previously described is termed simply Sneak Analysis. This system safety tool helps provide visibility of the interactions of a system's hardware and software and hence will help reduce the difficulties involved in the
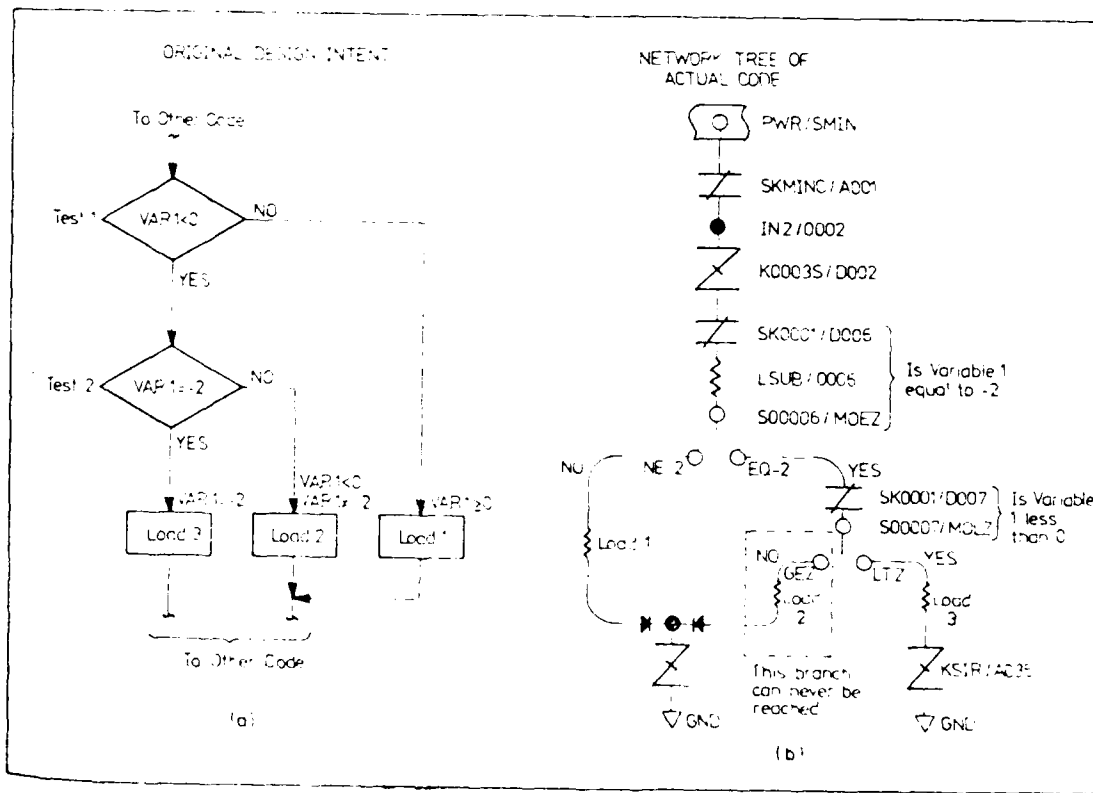
FIGURE 7.10.4-2: SOFTWARE SNEAK EXAMPLE

proper integration of two such diverse, complex systems designs. As hardware and software systems increase in complexity, the use of interface bridging analysis tools, such as Sneak Analysis, becomes imperative to help provide assurance of safety of the total system.

7.10.6   SUMMARY

SCA is contrasted to other analyses commonly performed in a reliability program in a number of important ways. SCA generally concentrates on the interconnections, interrelationships, and interactions of system components rather than on the components themselves. SCA concentrates more on what might go wrong in a system rather than on verifying that it works right under some set of test conditions. The SCA technique is based on a comparison with other systems which have "gone wrong", not because of part failures, but because of design oversight or because a human operator made a mistake. The consequence of this subtly different perspective may be very important, because it tends to concentrate on and find problems which may be hidden from the perspectives of other analytical techniques.

For example FMEA/FMECA differs from SCA in that it predicts and quantifies the response of a system to failures of individual parts or subsystems. An FMECA is an analysis of all expected failure modes and their effect on system performance. FMECA results are often used in maintainability predictions, in the preparation of maintenance dependency charts, and to establish sparing requirements. On the other hand SCA considers possible human error in providing system inputs while FMECA does not. In this regard the two types of analysis tend to complement one another.

Fault Tree Analysis is a deductive method in which a catastrophic, hazardous end result is postulated and the possible events, faults, and occurrences which might lead to that end event are determined. FTA, thus overlaps SCA because the FTA is concerned with all possible faults, including component failures as well as operator errors.

Concerning availability of SCA computer programs, the original SCA computer programs developed under government contract with (NASA), Johnson Spacecraft Center, Houston, Texas, on the Apollo program are available to all industry and government agencies. They can be purchased from Computer Software Management and Information Center (COSMIC), University of Georgia, 112 Barrow Hall, Athens, Georgia 30602. These programs may not be current. However, several companies have purchased these programs and spent development funds to update them. The improved programs and the accompanying analysis techniques are considered proprietary by most companies.

References 19 and 69-74 provide more details on SCA. References 73 and 74 are recent military documents dealing with SCA procedures and management.

7.11 DESIGN REVIEWS

7.11.1 INTRODUCTION AND GENERAL INFORMATION

Design reviews are an essential element of reliability design process. The general purpose of a design review is to assure the procuring activity and the contractor(s) that each design has been studied to identify possible problems. Its purpose is to improve the item where necessary and to provide assurance that the most satisfactory design has been selected to meet the specified requirements. Design reviews are critical audits of all pertinent aspects of the design and are conducted at critical milestones in the acquisition program. They are an essential activity of reliability engineering. The scope of the design review program is normally defined in the Reliability Program Plan. However, this does not imply that it is purely a reliability function. The design review program for an item is a subject of contractual agreement between the procuring activity and the contractor.

The formal review of equipment design concepts and design documentation for both hardware and software is an essential activity in any development program. Standard procedures ought to be established to conduct a review of all drawings, specifications, and other design information by the contractor's technical groups such as equipment, engineering, reliability engineering, and manufacturing engineering. This review should be accomplished prior to the release of design information for manufacturing operations. Such a review is an integral part of the design-checking reviews. Responsible members of each reviewing department meet to consider all design documents, resolve any problem areas uncovered, and signify their acceptance of the design documentation by approving the documents for their departments.

Reliability engineering in conjunction with the equipment engineering groups, ought to conduct an intensive review of the system during initial design. The design review includes the following major tasks:

(1) Analysis of environment and specifications

(2) Formal design review of engineering information

(3) Reliability participation in all checking reviews

Prior to the formal review, the requirements defined in applicable military and equipment specifications are reviewed. The expected environmental extremes of the system are studied to determine suspected detrimental effects on equipment performance. Checklists, based on these studies, are prepared to assure that the objectives of formal design reviews are fulfilled.

The formal design review, which is instituted prior to the release of drawings, is intended to do the following:

(1)   Detect any conditions that could degrade equipment reliability

(2)   Provide assurance of equipment conformance to applicable specifications

(3)   Assure the use of preferred or standard parts as far as practical

(4)   Assure the use of preferred circuitry as far as possible

(5)   Evaluate the electrical, mechanical, and thermal aspects of the design

(6)   Provide stress analysis to assure adequate part derating

(7)   Assure accessibility of all parts that are subject to adjustment

(8)   Assure interchangeability of similar subsystems, circuits, modules, and subassemblies

(9)   Assure that adequate attention is given to all human factors aspects of the design

(10) Assure that the quality control effort will be effective

Reviews should be made at appropriate stages of the design process to evaluate achievement of the reliability requirements. The planned reviews should include, to the extent applicable but not necessarily limited to: current reliability estimates and achievements for each mode of operation, as derived from reliability analyses or test(s); potential design or production (derived from reliability analyses) problem areas, and control measures necessary to preserve the inherent reliability; failure mode(s) and effect(s) and criticality analyses; corrective action on reliability critical items; effects of engineering decisions, changes and tradeoffs upon reliability achievements, potential and growth, within the functional model framework; status of subcontractor and supplier reliability programs; and status of previously approved design review actions. The results of reliability reviews should be documented.

In order to satisfy the objectives of the design review, the review team must have sufficient breadth to handle aspects of the items under review, such as performance, reliability, etc., and the interfaces and interactions with adjacent items. Technical competency for reliability in a design review team is provided by reliability engineering. The design is primarily oriented toward seeing that the design will work, whereas Reliability Engineering must find out those areas which would cause the design not to operate, the indication of its unreliability. By systematic approaches of the mathematical model, FMEAs, FTAs and criticality lists, the designer can be assisted in arriving at theportions of design that he must concentrate on in order to arrive at a balanced and reliable design. In a complex system, it is a difficult

assessment for the designer to make without assistance of the
reliability engineering organization. Since the mathematical model is a
systematic functional diagramming of components as they fit into
subsystems and systems, this model can materially aid the designer in
having an overall feel for the complete system. This, in turn, will
help him in providing designs that will provide reliability for the
total system rather than overdesign a particular portion of it and
thereby not improve the total reliability.

7.11.2 INFORMAL RELIABILITY DESIGN VERIFICATION

The design verification review depicted in Figure 7.11.2-1 is a part of
the design formulation process. These reviews, conducted for the
benefit of the equipment designer and systems engineer, help achieve the
appropriate degree of design maturity the first time around. The
reliability verification review is thus conducted for the purpose of
evaluating and guiding specified reliability characteristics and
maintenance features "in process." That is, it is conducted while the
design is in the evolutionary or formative stage and still amenable to
major conceptual and configuration changes. Reviews are conducted on an
unscheduled, "as required," informal basis. They are usually conducted
at the request of the designer or the systems engineer to verify
conformance throughout the team effort, to allocate requirements and
design constraints, to verify the solution of problems identified in
earlier design iterations, or to provide the basis for selection of
design alternatives.

Much of the reliability design engineer's activity in the design support
role is devoted to these reviews. He must work closely with the
hardware and software designer in developing the analytical and
diagrammatic models which best represent the configuration to be
verified. He must also perform a real world design assessment. Even
though the verification review is an informal "shirt sleeve" working
session involving only a few selected reviewers from within the
contractor's own project organization, results of each review should be
documented in the design report as a step in the scientific "analyze,
then cut and try" process by which the final design configuration is
evolved. The five alternatives for further design iteration are shown
in Figure 7.11.2-1.

(1) Reverify Design Adequacy to provide additional analytical or
    empirical proof of design adequacy to facilitate design review
    approval decision with more confidence than current data will
    substantiate

(2) Redesign to correct design discrepancies and marginal
    characteristics disclosed by the review.

(3) Reallocate Design Requirements to rectify allocation errors identi-
    fied in the review, or reallocate subsystem requirements on the
    basis of updated estimates of design feasibility or changes in
    relative criticality disclosed during the review.
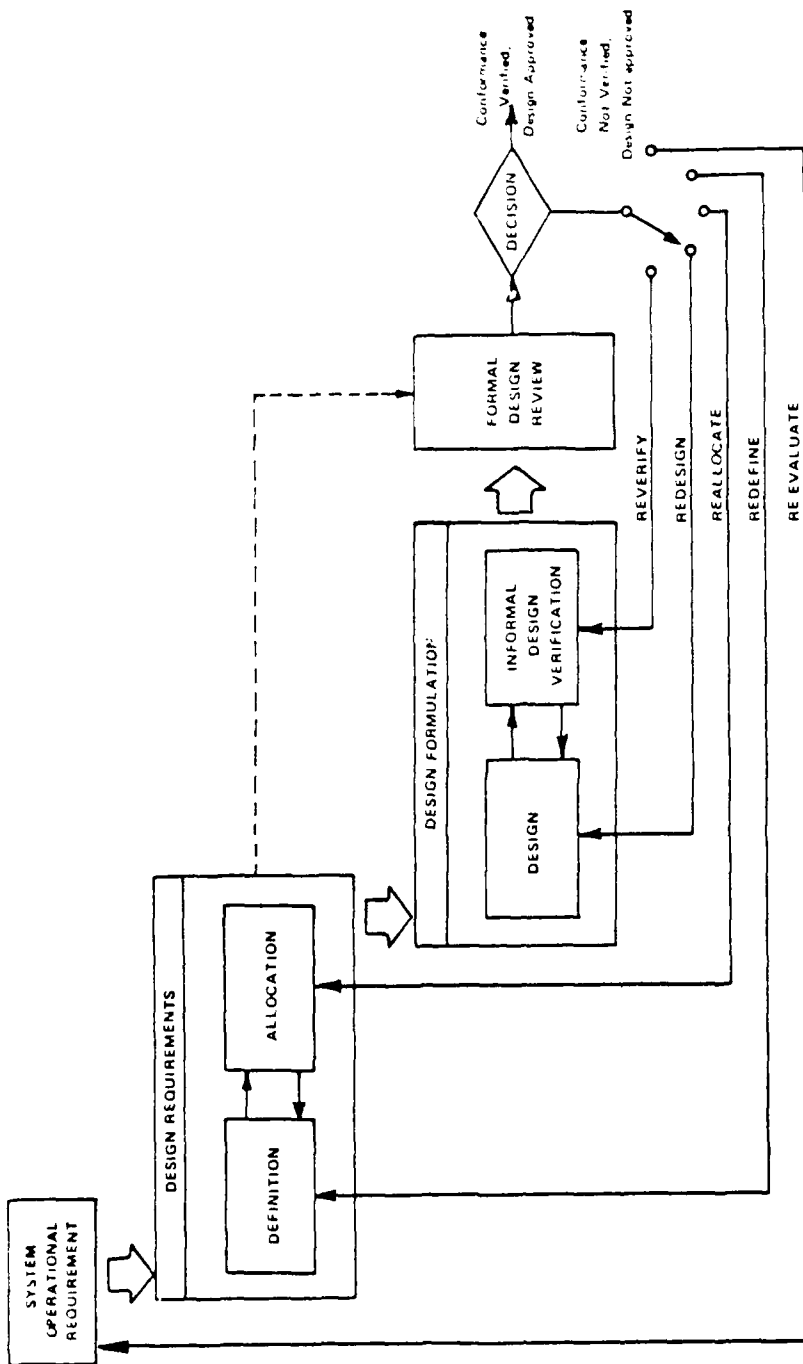
FIGURE 7.11.2-1: DESIGN REVIEW AS A CHECK VALVE IN THE SYSTEM ENGINEERING CYCLE

(4) <u>Redefine Design Requirements</u> to restudy previous requirements analyses and tradeoff studies, and redefine or refine baseline design and configuration requirements more nearly consistent with state-of-art and program constraints revealed during the design review. Such redefinition must necessarily remain within the limits of feasibility allowed in the Operational Requirement document unless Government approval is obtained for the proposed changes in accordance with the next alternative.

(5) <u>Re-evaluate System Operational Requirements</u> to provide basis for Government approval of either of two alternatives: (a) to redefine system operational requirements consistent with current design state-of-art and program constraints; or (b) to redefine program constraints, such as delivery schedule and funds, to rectify earlier estimating errors.

The recommended design review team membership, and functions of each member, are briefly summarized in Table 7.11.2-1. For these early stage, informal, design reviews, Government or customer participation is usually optional. These are internal reviews, primarily for members of the contractor's design team. Government people are usually invited to attend as observers. During formal design reviews (discussed in the next subsection), Government specialists play a more participative role.

7.11.3 FORMAL DESIGN REVIEWS

Formal design review programs for specific equipment/systems are usually the subject of contractual agreement between the Government and the contractor. Some examples of formal reviews are discussed below.

<u>Preliminary Design Review (PDR)</u>. The PDR, conducted prior to the detail design process, should evaluate the progress and technical adequacy of the selected design approach, determine its compatibility with the performance requirements of the specification; and establish the existence and the physical and functional interfaces between the item and other items of equipment or facilities. The basic design reliability tasks shown in Figure 7.11.3-2 should be accomplished for the PDR.

Eight suggested basic steps pertinent to the PDR are shown in Figure 7.11.3-1. The basic design reliability tasks shown in Figure 7.11.3-2 should be accomplished for the PDR.

<u>Critical Design Review (CDR)</u>. The CDR date is usually shown on the master schedule; it requires final approval by the cognizant Government manager/engineer.

The CDR is conducted when detail design is essentially complete and fabrication drawings are ready for release. It should determine that the detail design satisfies the design requirements established in the specification, and establish the exact interface relationships between the item and other items of equipment ships between the item and other items of equipment and facilities.

TABLE 7.11.2-1: DESIGN REVIEW GROUP, RESPONSIBILITIES AND
MEMBERSHIP SCHEDULE

Group Member	Responsibilities
Chairman	Calls, conducts meetings of group, and issues interim and final reports
Design Engineer(s) (of product)	Prepares and presents design and substantiates decisions with data from tests or calculations
*Reliability Manager or Engineer	Evaluates design for optimum reliability, consistent with goals
Quality Control Manager or Engineer	Ensures that the functions of inspection, control, and test can be efficiently carried out
Manufacturing Engineer	Ensures that the design is producible at minimum cost and schedule
Field Engineer	Ensures that installation, maintenance, and operator considerations were included in the design
Procurement Representative	Assures that acceptable parts and materials are available to meet cost and delivery schedules
Materials Engineer	Ensures that materials selected will perform as required
Tooling Engineer	Evaluates design in terms of the tooling costs required to satisfy tolerance and functional requirements
Packaging and Shipping Engineer	Assures that the product is capable of being handled without damage, etc.
Design Engineers (not associated with unit under review)	Constructively review adequacy of design to meet all requirements of customer
Customer Representative (optional)	Generally voices opinion to acceptability of design and may request further investigation on specific items

*Similar support functions performed by maintainability, human factors, value engineering, etc.

① PREPARE
DESIGN REVIEW
SCHEDULE

② PREPARE
DESIGN REVIEW
AGENDA
(RELIABILITY)

③ DEFINE DATA
REQUIREMENTS
& TASKS

④ DESIGNER
PREPARE FOR
REVIEW

COORDINATE

⑤ REVIEWER
PREPARE FOR
REVIEW

⑥ CONDUCT
DESIGN
REVIEW

⑦ DECISION — NO →

⑧ ASSIGN
ACTION ITEMS
FOR FOLLOW-UP
REVIEW

YES

PRELIMINARY
DESIGN
APPROVED
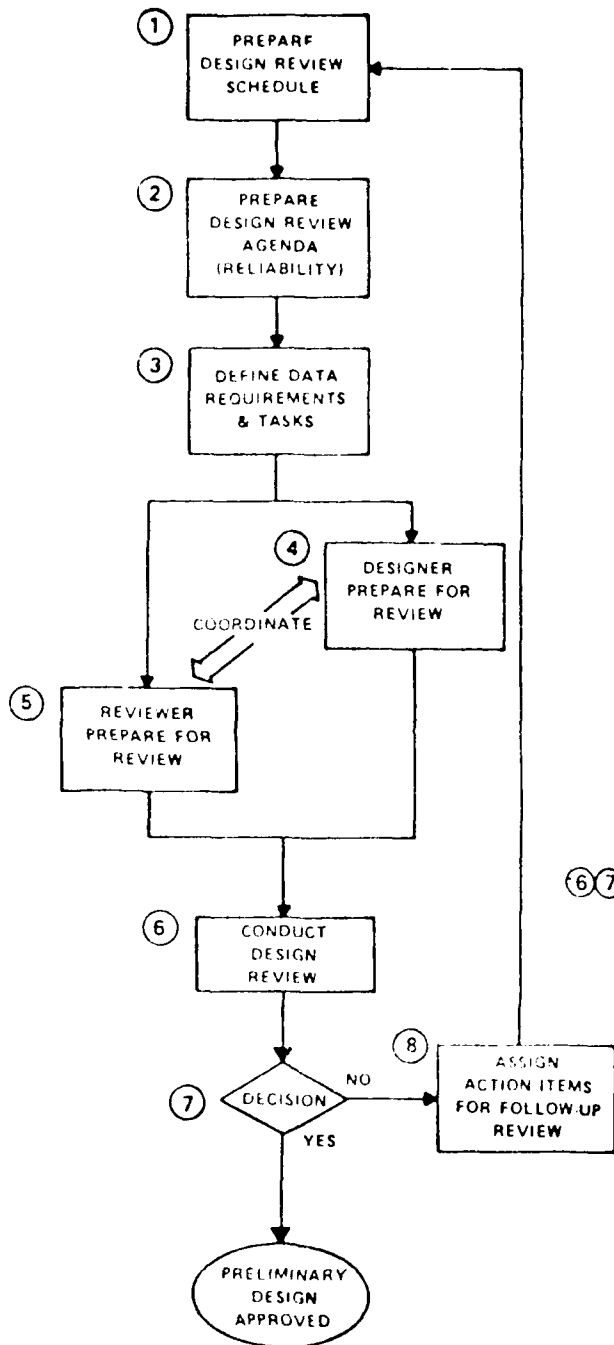
① GOV'T. contractually establishes design review requirements. Contractor prepares preliminary design review schedule compatible with master program milestone schedule.

② Contractor prepares and distributes agenda in advance of each review, defining: purpose and scope of review; specific items to be reviewed; date, time, and place for the review.

③ Contractor defines applicable data, to assist designer and reviewer in preparation for the design review.

④ Designer prepares for review, to include answers to questions accompanying the agenda, description of design concept, analyses, test results, problems, requirements, etc.

⑤ Review committee members prepare for review; formulate questions and suggestions.

⑥⑦⑧ Review committee members approve or disapprove preliminary design

FIGURE 7.11.3-1: BASIC STEPS IN THE PRELIMINARY DESIGN REVIEW (PDR) CYCLE

1. Identify the quantitative reliability requirements and compare preliminary predictions with specified requirements.

2. Review failure rate sources, derating policies, and prediction methods.

3. Identify planned actions when predictions are less then specified requirements.

4. Identify and review parts or items which have a critical life or require special consideration, and general plan for handling.

5. Identify applications of redundant elements. Evaluate the basis for their use and provisions for redundancy with switching.

6. Review critical signal paths to determine that a fail-safe/fail-soft design has been provided.

7. Review margins of safety between functional requirements and design provisions for elements, such as: power supplies, transmitter modules, motors, and hydraulic pumps. Similarly, review structural elements, i.e., antenna pedestals, dishes, and radomes to determine that adequate margins of safety are provided between operational stresses and design strengths.

8. Review Reliability Design Guidelines to insure that design reliability concepts shall be available and used by equipment designers. Reliability Design Guidelines shall include, as a minimum, part application guidelines (electrical derating, thermal derating, part parameter tolerances), part selection order of preference, prohibited parts/materials, reliability allocations/predictions, and management procedures to ensure compliance with the guidelines.

9. Review preliminary reliability demonstration plan: failure counting ground rules, accept-reject criteria, number of test articles, test location and environment, planned starting date, and test duration.

10. Review elements of reliability program plan to determine that each task has been initiated toward achieving specified requirements.

11. Review subcontractor/supplier reliability controls.

FIGURE 7.11.3-2: DESIGN RELIABILITY TASKS FOR THE PDR

The basic design reliability tasks shown in Figure 7.11.3-3 should be accomplished for the CDR. Suggested steps for a CDR are shown in Figure 7.11.3-4.

Preproduction Reliability Design Review (PRDR). The PRDR is a formal technical review conducted to determine if the achieved reliability of a weapon system at a particular point in time is acceptable to justify commencement of production. Details for the PRDR are usually provided in the individual Service documents or instructions, e.g., NAVAIR INST. 13070.5.

The PRDR is conducted after completion of IOT&E and prior to production to ensure the adequacy of the design from a reliability standpoint. The level of achieved reliability and adequacy of design will be evaluated primarily on the initial Procuring Activity's technical and operational testing, e.g., test results, failure reports, failure analyses reports, reports of corrective action, and other documents which could be used as necessary for back-up or to provide a test history.

7.11.4   DESIGN REVIEW CHECKLISTS

A design review checklist delineates specific items to be considered for the item under review. In order to ensure that every consideration has been appropriately taken into account, a checklist for design should be prepared. The technical checklist should be prepared by reliability engineering and furnished to the designer in the very early stages of design. They should be devised for convenient use by the designer for completion along with the design, analyses and other documentation. Figure 7.11.4-1 is a typical list of items to be considered in various stages of a design review (not to be considered all inclusive). Table 7.11.4-1 is a typical example of a Reliability Actions Checklist.

Technical checklists can be oriented in a question format to ensure that critical factors will not be overlooked. Figure 7.11.4-2 illustrates typical questions which could be asked at various stages of the design review.

Appendix C is an example of a checklist which may be used.

1. Review the most recent predictions of quantitative reliability and compare against specified requirements and substantiate predictions by review of parts application stress data.

2. Review applications of parts or items with minimum life, or those which require special consideration to insure their effect on system performance is minimized.

3. Review completed Reliability Design Review Checklist to insure principles have been satisfactorily reflected in the design.

4. Review applications of redundant elements to establish that expectations have materialized since the PDR.

5. Review detailed reliability demonstration plan for compatibility with specified test requirements. Review the number of test articles, schedules, location, test conditions, and personnel involved to insure a mutual understanding of the plan and to provide overall planning information to activities concerned.

FIGURE 7.11.3-3: DESIGN RELIABILITY TASKS FOR THE CRITICAL DESIGN REVIEW (CDR)

① ② Government Aquisition Manager establishes design review requirements. Contractor prepares and distributes agenda in advance of Critical Design Review (CDR) defining: purpose and scope of review; specific items to be reviewed; date, time and place for the review.

③ Contractor defines applicable data, to assist designer and reviewer in preparation for the design review.

④ Designer prepares for pre-critical design review, to include answers to questions accompanying the agenda, description of design concept, analyses, test results, problems, requirements, etc.

⑤ Review committee members prepare for review; formulate questions and suggestions.

Designer notifies Government Acquisition Manager that preparations for critical design review are complete.

⑥ Government Acquisition Manager conducts the critical design review meeting with contractor support.

⑦ Government makes decision either to approve the design or to withhold approval pending correction of deficiencies.

⑧ Government Acquisition Manager and contractor assign action items agreed upon for correction of deficiencies and establish schedule for follow-up review.

FIGURE 7.11.3-4: BASIC STEPS IN THE CDR CYCLE

1. System concept/alternative approaches

2. System performance and stability

3. Design documentation

4. Design changes

5. Tradeoff studies

6. Materials and Processes

7. Construction, Fabrication, Maintenance and Service

8. Analyses (Failure Mode, Effects and Criticality, Tolerance, etc.)

9. Equipment compatibility

10. Environmental effects

11. Test data

12. Reliability allocation/prediction/assessment

13. Redundancy

14. Cost and procurement considerations

15. Life and controls

16. Interchangeability, spares and repair parts

17. Weight

18. Supplier design

19. Safety

20. Critical functions

FIGURE 7.11.4-1: <u>TYPICAL ITEMS TO BE COVERED IN A DESIGN REVIEW</u>

TABLE 7.11.4-1:   RELIABILITY ACTIONS CHECKLIST

DESIGN TITLE			NUMBER		Responsibility		Notes & Comments
No.	Item			Completed	Design	Reliability	
1.	System Constraints				D	X	
	a. Success Criteria				D	X	
	b. Environmental Stresses				D	X	
	c. Compatibility Factors				D	X	
	d. User Skill Levels				D	X	
2.	Feasibility Study				D	X	
3.	Reliability Apportionment					R	
4.	Preliminary Reliability Review				D	R	
5.	Trade-Off Studies				D	X	
6.	Functional Schematics				D	X	
7.	Block Diagram				D	X	
8.	Cause and Effect Analysis				D	X	
9.	Worst Case Analysis				D	X	
10.	Subsystem and Equipment Reliability Prediction						
	a. Part Failure Rate Method				D	X	
	b. Safety Margin Method				D	X	
	c. Drift Rate and Tolerance Method				D	X	
11.	Intermediate Design Review				D	R	
12.	Time/Cycle Recording Requirements				D	X	
13.	Failure Reporting Requirements				D	X	
14.	Serialization Requirements				D	X	
15.	Procurement Specification Review					R	
16.	Vendor Proposal Review					R	
17.	Source Selection Review					R	
18.	Parts Selection and Application Review				D	X	
19.	Reliability Signoff - Topp Assy. & Inst. Dwgs.					R	
20.	Vendor Design Review					R	

CODE

D - Prime Action by Designer - check off, sign and date as completed.

R - Prime Action by Reliability Engineer - check off, sign and date as completed.

X - Check by Reliability Engineer - sign and date.

TABLE 7.11.4-1: RELIABILITY ACTIONS CHECKLIST (Cont'd)

DESIGN TITLE _____

No.	Item	NUMBER Completed	Responsibility Design	Responsibility Reliability	Notes & Comments
21.	Critical Design Review		D	R	
22.	Process Controls		D	X	
23.	Manufacturing Procedure Controls		D	X	
24.	Qualification Test Review		D	X	
25.	Acceptance Test Review		D	X	
26.	Integration Test Review		D	X	
27.	Reliability Demonstration Test Review		D	X	
28.	System Test:				
	a. Test Requirements Review		D	X	
	b. Test Plans Review		D	X	
	c. Reliability Tests			R	
29.	Reliability Summary Sheet			R	

CODE

D - Prime Action by the Designer - check off, sign and date as completed.

R - Prime Action by Reliability Engineer - check off, sign and date as completed.

X - Check by Reliability Engineer - Initial and date.

1.   Is design simple? Minimum number of parts?

2.   Is it designed into a unified overall system rather than as an accumulation of parts, etc.?

3.   Is the item compatible with system in which it is used?

4.   Is the item properly integrated and installed in the system?

5.   Are there adequate indicators to verify critical functions?

6.   Has reliability for spares and repair parts been considered?

7.   Are reliability requirements established for critical items? For each part?

8.   Is there specific reliability design criteria for each item?

9.   Have reliability tests been established?

10. Are standard high-reliability parts being used?

11. Are unreliable parts identified?

12. Has the failure rate for each part or part class been established?

13. Have parts been selected to meet reliability requirements?

14. Have below-state-of-the-art parts or problems been identified?

15. Has shelf life of parts been determined?

16. Have limited-life parts been identified, and inspection, and replacement requirements specified?

17. Have critical parts which required special procurement, testing, and handling been identified?

18. Have stress analyses been accomplished?

19. Have derating factors been used in the application of parts?

20. Have safety factors and safety margin been used in the application of parts?

21. Are circuit safety margins ample?

22. Have standard and proven circuits been utilized?

23. Has the need for the selection of parts (matching) been eliminated?

24. Have circuit studies been made considering variability and degradation of electrical parameters of parts?

25. Have solid-state devices been used where practicable?

FIGURE 7.11.4-2: TYPICAL QUESTIONS CHECKLIST FOR THE DESIGN REVIEW (SHEET 1 of 2)

26. Is the reliability or MTBF of the item based on actual application of the parts?

    a.   Comparison made with reliability goal?

    b.   Provision for necessary design adjustments?

27. Are the best available methods for reducing the adverse effects of operational environments on critical parts being utilized?

28. Has provision been made for the use of electronic failure prediction techniques, including marginal testing?

29. Is there provision for improvements to eliminate design inadquacies observed in tests?

30. Have normal modes of failure and the magnitude of each mode for each item or critical part been identified?

31. In the application of failure rates of items to reliability equations, have the following effects been considered?

    a.   External effects on the next higher level which the item is located.

    b.   Internal effects on the item.

    c.   Common effects, or direct effect of one item on another item, because of mechanical or electro-mechanical linkage.

32. Has redundancy been provided where needed to meet specified reliability?

33. Has failure mode and effects analyses been adequately covered by design?

34. Have the risks associated with critical item failures been identified? Accepted? Has design action been taken?

35. Does the design account for early failure, useful life and wear-out?

FIGURE 7.11.4-2: <u>TYPICAL QUESTIONS CHECKLIST FOR THE DESIGN REVIEW (SHEET 2 of 2)</u>

REFERENCES

1. NAVSEA 0967-LP-597-1011, Parts Application and Reliability Information Manual for Navy Electronic Equipment, Naval Sea Systems Command, Department of the Navy, Washington DC, 20362 September 1980.

2. Lipson, C., et al., Reliability Prediction -- Mechanical Stress/Strength Interference Models, RADC-TR-68-403, March 1967.

3. Lipson, C., et al., Reliability Prediction -- Mechanical Stress/Strength Interference (nonferrous), RADC-TR-68-403, December 1968.

4. Yurkowsky, W., Nonelectronic Reliability Notebook, RADC-TR-69-458, March 1970.

5. Fink, D.G. and D. Christiansen, ed., Electronic Engineers' Handbook, McGraw Hill Book Co., NY, 1982.

6. AMCP706-124, Engineering Design Handbook: Reliable Military Electronics, Headquarters U.S. Army Materiel Command, 5001 Eisenhower Ave, Alexandria, VA 22333, AD#A025665.

7. NASA CR-1126, Practical Reliability, Vol. 1 - Parameter Variations Analysis, Research Triangle Institute, Research Triangle Park, North Carolina, 27709, July 1968.

8. AMCP706-196, Engineering Design Handbook: Design for Reliability, AD#A027370, January 1976.

9. Jensen, R.W., and L.P. McNamee, Handbook of Circuit Analysis Languages and Techniques, Prentice Hall, Inc., Englewood Cliffs, New Jersey 07632.

10. Deger, E., and T.C. Jobe, "A Design Factor in Reliability," Electronics, August 30, 1973, pp. 83-89.

11. Klion, J., A Redundancy Notebook, RADC-TR-77-287, December 1977, AD#A050837.

12. Shooman, M., Probabilistic Reliability: An Engineering Approach, McGraw-Hill Book Co., New York, 1968.

13. Barrett, L.S., "Reliability Design and Application Considerations for Classical and Current Redundancy Schemes," Lockheed Missiles and Space Co., Inc., Sunnyvale, CA, September 30, 1973.

14. AMCP 706-115, Engineering Design Handbook: Environmental Series, Part One, Basic Environmental Concepts, AD#784999.

15. AMCP 706-116, Engineering Design Handbook: Environmental Series, Part Two, Natural Environmental Factors, AD#A012648.

16. AMCP 706-117, Engineering Design Handbook: Environmental Series, Part Three, Induced Environmental Factors, AD#A023512.

17. AMCP 706-118, Engineering Design Handbook: Environmental Series, Part Four, Life Cycle Environments, AD#A015179.

18. AMCP 706-119, Engineering Design Handbook: Environmental Series, Part Five, Glossary of Environmental Terms.

19. Arsenault, J.E., and J.A. Roberts, Reliability and Maintainability of Electronic Systems, Computer Science Press, 9125 Fall River Lane, Potomac, MD 20854, 1980.

20. Pavia, R.V., An Investigation into Engine Wear Caused by Dirt, Aeronautical Research Committee Report ACA-50, July 1950.

21. AMCP 706-335 (SRD), Engineering Design Handbook: Design Engineers' Nuclear Effects Manual, Vol. I, Munitions and Weapon Systems (U).

22. AMCP 706-336 (SRD), Engineering Design Handbook: Design Engineers' Nuclear Effects Manual, Vol. II, Electronic Systems and Logistical Systems (U).

23. AMCP 706-336 (SRD), Engineering Design Handbook: Design Engineers' Nuclear Effects Manual, Vol. III, Nuclear Environment (U).

24. AMCP 706-338 (SRD), Engineering Design Handbook: Design Engineers' Nuclear Effects Manual, Vol. IV, Nuclear Effects (U).

25. Meister, D., "A Critical Review of Human Performance Reliability Prediction Methods," IEEE Trans. Reliability R-22, August 1973, pp. 116-123.

26. Meister, D., "Comparative Analysis of Human Reliability Models," Final Report Contract N00024-71-C-1257, Bunker-Ramo Corp., Nov. 1971, AD#734432.

27. McCormis, E.J., Human Engineering, McGraw Hill Publishing Co., New York, NY, 1967.

28. Leuba, H.R., "The Impact of Policy on System Reliability," IEEE Trans. on Reliability R-18, August 1969, pp. 137-140.

29. Woodson, W.E., and D.W. Conover, Human Engineering Guide For Equipment Designers, University of California Press, Berkeley, California, 1966.

30. Davis, B.P., and C.N. Cordoni, "People Subsystem Measurement for Total Reliability," Proceedings of the 1970 Annual Symposium on Reliability, 1970, p. 394.

31. Miller, G.E., et al., Human Factors Aspects of Reliability, Publication No. U2296, Philco Corp., Newport Beach, California, 1964.

32. Kraft, J.A., "Mitigation of Human Error through Human Factors Design Engineering," Annals of the 7th Reliability and Maintainability Conference, 7,300, 1968.

33. Inaba, K., and R. Matson, "Measurement of Human Errors with Existing Data," Annals of the 7th Reliability and Maintainability Conference, 7,301, 1968.

34. Rabideau, G.F., "Prediction of Personnel Subsystem Reliability Early in System Development Cycle," Proceedings of the National Aerospace System Reliability Symposium, Institute of Aerospace Sciences, New York, NY, 1962.

35. O'Connell, R.D., Handbook of Human Performance Measures, Space Biology Laboratory, University of California, Los Angeles, July 1972.

36. Simon, C.W., Economical Multifactor Designs for Human Factors Engineering Experiments, Hughes Aircraft Company, Report No. HAC-P73-326, Culver City, California, June 1973.

37. Chaikin, G., Human Factors/Human Engineering, report of Ground Equipment and Materials Command, Army Missile Command, Redstone Arsenal, Alabama, June 1973, AD#763168.

38. Little, I.J., The Design of Analysis of a Human Body Motion Measurement System, Report of Guidance and Control Directorate, Army Missile Command, Redstone Arsenal, Alabama, September 1972, AD#751134.

39. Chapanis, A., Relevance of Physiological and Psychological Criteria to Man-Machine Systems - The Present State of the Art, Report TR-24, Dept. of Psychology, Johns Hopkins University, MD, 1970.

40. Regulinski, T.L., "Systems Maintainability Modeling," Proceedings 1970 Annual Reliability Symposium, 1970, pp. 449-457.

41. Regulinski, T.L., and W.B. Askren, _Mathematical Modeling of Human Performance Errors for Reliability Analysis of Systems_, Report of Aerospace Medical Research Laboratory No. AMRL-TR-68-93, Wright-Patterson AFB, Ohio 45433, January 1969.

42. Meister, D., et al., _The Effect of Operator Performance Variables on Airborne Electronic Equipment Reliability_, Report RADC-TR-70-140, Rome Air Development Center, Griffiss AFB, NY, July 1970.

43. Hanifa, D.T., _Human Performance Quantification in System Development: Recent Advances_, Report No. 70-M-0733 of Dunlap Associates, Inc., Santa Monica, CA, July 1970.

44. Siegel, A.I., and J.J. Wolf, _Man-Machine Simulation Models_, John Wiley and Sons Publishing Co., New York, NY, 1969.

45. Siegel, A.I., and J.J. Wolf, "A Model for Digital Simulation of Two-Operator Man-Machine Systems," _Ergonomics_, 5:4, 1962.

46. Siegel, A.I., and J.J. Wolf, "A Technique for Evaluating Man-Machine Systems Design," _Human Factors_, 3:1, 1961.

47. Swain, A.D., "Shortcuts in Human Reliability Analysis," NATO Advanced Study Institute on Generic Techniques in Systems Reliability Assessment, Nordhoff Publishing Company, Holland, 1975.

48. Regulinski, T.L., and W.B. Askren, "Stochastic Modeling of Human Performance Effectiveness Functions," _Proceedings, 1972 Annual Reliability and Maintainability Symposium_, 1972, pp. 407-416.

49. Regulinski, T.L., ed., _Special Issue on Human Performance Reliability: IEEE Transactions on Reliability R-22, No. 3_, August 1973.

50. Chaikin, G., et al., _Engineering Practice Study-Human Engineering_, Report No. RC-S-65-1, U.S. Army Missile Command, Redstone Arsenal, AL, 1965.

51. Davis, Faulkner, and Miller, "Work Physiology," _Human Factors 11, No. 2_, April 1969, p. 157.

52. Swain, Alan, "The Human Element in System Development," _Proceedings of the 1970 Annual Symposium on Reliability_, 1970, pp. 20-28.

53. Keenan, J.J., "Interactionist Models of the Varieties of Human Performance," _Annals of 6th Reliability and Maintainability Conference 6_, 76, 1967.

54. Meister, D., and D.E. Farr, _The Utilization of Human Factors Information by Designers_, System Effectiveness Laboratory, The Bunker-Ramo Corp., California, 1967.

55. Meister, D., et al., A Further Study of the Use of Human Factors Information by Designers, System Effectiveness Laboratory, The Bunker-Ramo Corp., California, 1967.

56. Pew, R.W., Human Information-Processing Concepts for System Engineers, Univ. of Michigan, Michigan, 1965.

57. AR 70-8, Human Resources Research Program.

58. Malmberg, A.F., "NET-1 Network Analysis Program," Proceedings of the Eleventh National Symposium on Reliability and Quality Control, 1965, pp. 510-517.

59. Tyson, H.N., Jr., et al., "The IBM Electronic Circuit Analysis Program (ECAP)," Proceedings of the 1966 Annual Symposium on Reliability, 1966, pp. 45-65.

60. Hausrath, D.A., and R. Ranalli, "Computer Studies of Abnormally Operating Circuits," Proceedings of the 1966 Annual Symposium on Reliability, 1966, pp. 66-86.

61. Brown, K.R., Failure Mode Analysis Program (IM-045), Report No. 63-C5G-043-20-36, North American Aviation, Inc., Downey, California, September 1963.

62. Bond, K.L., and D.S. Kordell, Ground Support Equipment Mode Analysis Program (IM-063), Report No. 64-CT-043-14-41, North American Aviation, Inc., Downey, California, March 1964.

63. Kordell, D.S., Airborne Failure Mode Analysis Program (IM-066), Report No. 64-CT-043-14-14, North American Aviation, Inc., Downey, California, January 1964, AD#459212.

64. Failure Mode and Effects Analysis Program, Computer Software Management and Information Center, 112 Barrow Hall, University of Georgia, Athens, GA 30602.

65. Michels, J.M., "Computer Evaluation of the Safety Fault Tree Model," System Safety Symposium, Proceedings, 1965, available from University of Washington Library, Seattle, Washington.

66. Crosetti, P.A., Computer Program for Fault Tree Analysis, DUN-5508, April 1969.

67. Vesely, W.E., "A Time-Dependent Methodology for Fault Tree Evaluation," Nuclear Engineering and Design, 13, 2 August 1970.

68. Fault Tree Handbook, NUREG-0492, available from Division of Technical Information and Document Control, U.S. Nuclear Regulatory Commission, Washington, DC 20555.

69. Clardy, R.C., "Sneak Circuit Analysis Development and Application," 1976 Region V IEEE Conference Digest, 1976, pp. 112-116.

70. Hill, E.J., and L.J. Bose, "Sneak Circuit Analysis of Military Systems," Proceedings of the 2nd International System Safety Conference, July 1975, pp. 351-372.

71. Buratti, D.L., and Goday, S.G., Sneak Analysis Application Guidelines, RADC-TR-82-179, Rome Air Development Center, Griffiss Air Force Base, N.Y., 13441, June 1982.

72. Godoy, S.G., and G.J. Engels, "Sneak Circuit and Software Sneak Analysis," Journal of Aircraft, Vol. 15, August 1978, pp. 509-513.

73. NAVSEA TE001-AA-GYD-010/SCA, Contracting and Management Guide for Sneak Circuit Analysis (SCA), Naval Sea Systems Command, SEA 6151, Washington DC 20362, September 1980.

74. MIL-HDBK-XXX, Sneak Circuit Analysis, May 1979, Naval Sea Systems Command (SEA 5523) Washington, DC 20362.

75. NAVAIR 16-1-519 Handbook, Preferred Circuits, Navy Aeronautical Electronic Equipment.

APPENDIX A: REDUNDANCY CONSIDERATIONS IN DESIGN

INTRODUCTION

Under certain circumstances during system design, it may become necessary to consider the use of redundancy to reduce the probability of system failure -- to enhance system reliability -- by providing more than one functional path or operating element in areas that are critically important to system success. The use of redundancy is not a panacea to solve all reliability problems, nor is it a substitute for good design in the first place. By its very nature, redundancy implies increased complexity, increased weight and space, increased power consumption, and usually a more complicated system checkout and monitoring procedure. On the other hand, redundancy is the only solution to many of the problems confronting the designer of today's complex weapon systems.

It is the purpose of this appendix to present a brief description of the more common types of redundant configurations available to the designer, with the applicable block diagrams, mathematical formulae, and reliability functions to facilitate the computation of reliability gain to be expected in each case.

LEVELS OF REDUNDANCY

Redundancy may be applied at the system level (essentially two systems in parallel) or at the subsystem, component, or part level within a system. Figure A-1 is a simplified reliability block diagram drawn to illustrate the several levels at which redundancy can be applied. System D is shown with its redundant alternate, D', at the system level. D' is in turn built up of redundant subsystems or components (C_1 and C_2) and redundant parts within components (b_1 and b_2 within Component B).

From the reliability block diagram and a definition of block or system success, the paths which result in successful system operation can be determined. For example, the possible paths for I to O are:

(1) A, a, b_1, C_1

(2) A, a, b_1, C_2

(3) A, a, b_2, C_1

(4) A, a, b_2, C_2

(5) D

The success of each path may be computed by determining an assignable reliability value for each term and applying the multiplicative theorem. The computation of system success (all paths combined) requires a knowledge of the type of redundancy to be used in each case and an estimate of individual element reliability (or unreliability).
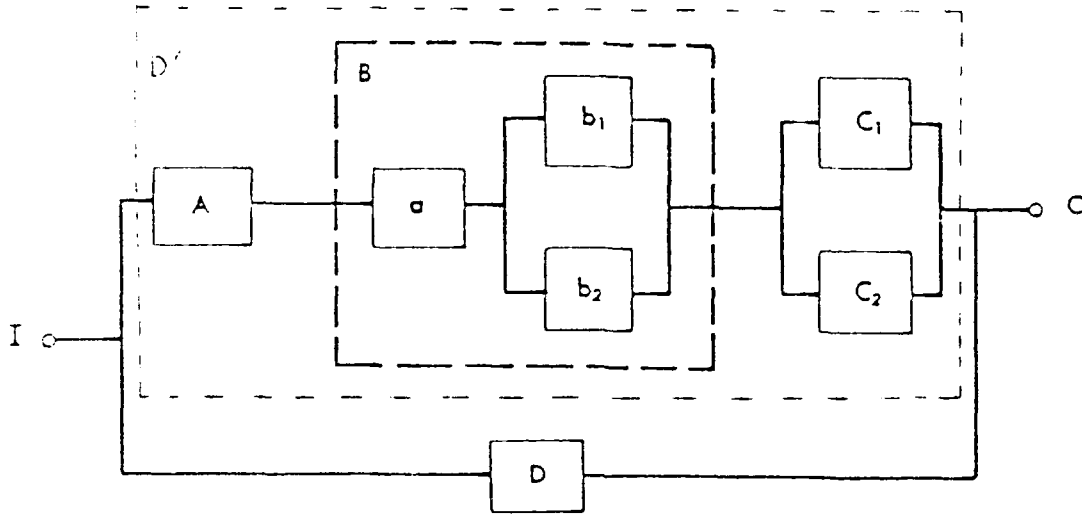
FIGURE A-1: <u>RELIABILITY BLOCK DIAGRAM DEPICTING REDUNDANCY AT THE SYSTEM, SUBSYSTEM, AND COMPONENT LEVELS</u>.

PROBABILITY NOTATION FOR REDUNDANCY COMPUTATIONS

Reliability of redundancy combinations is expressed in probabilistic terms of success or failure -- for a given mission period, a given number of operating cycles, or a given number of time independent "events," as appropriate. The "MTBF" measure of reliability is not readily usable because of the nonexponentiality of the reliability function produced by redundancy. Reliability of redundancy combinations which are "time dependent" is therefore computed at a discrete point in time, as a probability of success for this discrete time period. The following notation is applicable to all cases and is used throughout this appendix:

R probability of success or reliability of a unit or block

$\bar{R}$ probability of failure or unreliability of a unit or block

p = probability of success or reliability of an element

q = probability of failure or unreliability of an element

For probability statements concerning an event:

$P(A)$ = probability of A occurs

$P(\bar{A})$ = probability that A does not occur

For the above probabilities:

$R + \bar{R}$ = 1

$p + q = 1$

$P(A) + P(\bar{A}) = 1$

REDUNDANCY COMBINATIONS

The method of handling redundancy combinations can be generalized as follows:

    (1)   If the elements are in parallel and the units in series (Figure A-2), first evaluate the redundant elements to get the unit reliability. Then find the product of all unit reliabilities to obtain the block reliability.

    (2)   If the elements are in series and the units or paths are in parallel (Figure A-3), first obtain the path reliability by calculating the product of the reliabilities of all elements in each path. Then consider each path as a redundant unit to obtain the block reliability.

UNIT A　　　　UNIT B　　　UNIT C
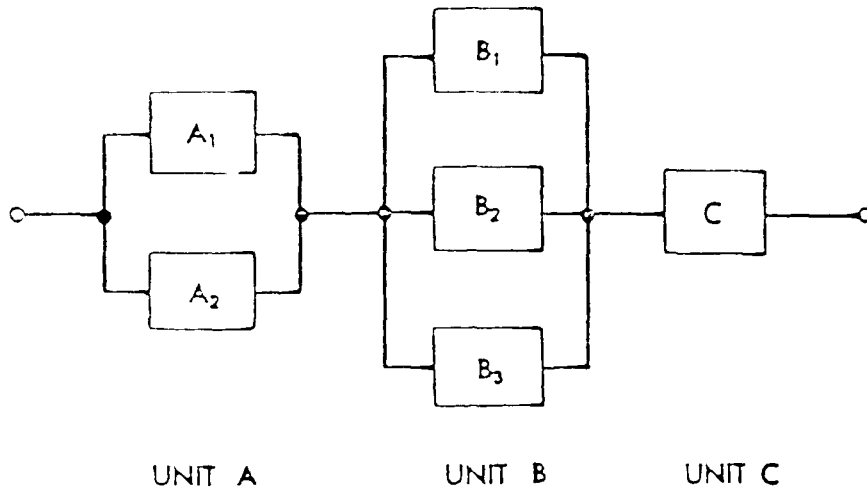
FIGURE A-2:　SERIES-PARALLEL CONFIGURATION

(a)　　　　　　　　　　　　(b)
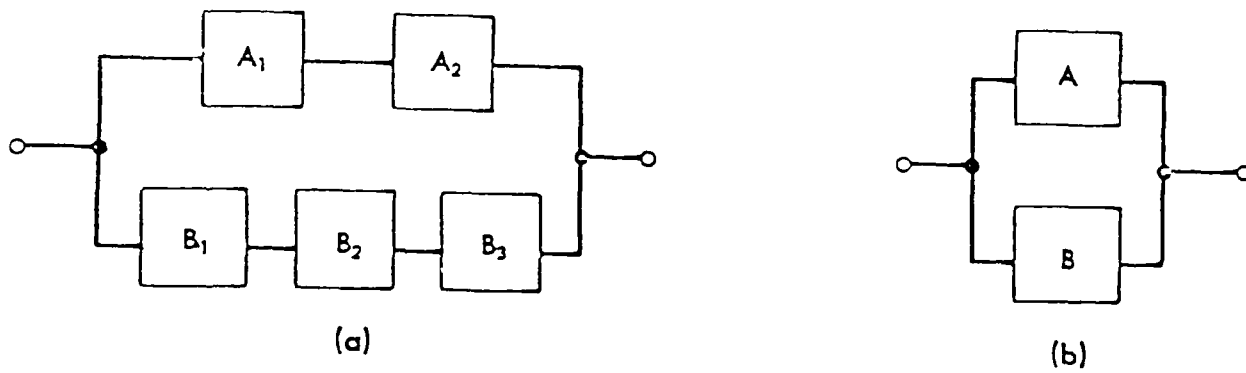
FIGURE A-3:　PARALLEL-SERIES CONFIGURATION

In the redundancy combination shown in Figure A-2, Unit A has two parallel redundant elements, Unit B has three parallel redundant elements, and Unit C has only one element. Assume that all elements are independent. For Unit A to be successful, A_1 or A_2 must operate; for Unit B success, B_1, B_2, B_3 must operate; and C must always be operating for block success. Translated into probability terms, the reliability of Figure A-2 becomes:

$$R = [1 - P(\bar{A}_1) P(\bar{A}_2)] [1 - P(\bar{B}_1) P(\bar{B}_2) P(\bar{B}_3)] P(C)$$

If the probability of success p, is the same for each element in a unit,

$$R = [1 - (1 - p_A)^2] [1 - (1 - p_B)^3] p_C$$

$$= (1 - q_A^2) (1 - q_B^3) p_C$$

where

$$q_i = 1 - p_i$$

Often there is a combination of series and parallel redundancy in a block as shown in Figure A-3a. This arrangement can be converted into the simple parallel form shown in Figure A-3b by first evaluating the series reliability of each path:

$$p_A = p_{a_1} p_{a_2}$$

$$p_B = p_{b_1} p_{b_2} p_{b_3}$$

where the terms on the right hand side represent element reliability. Then block reliability can be found from

$$R = 1 - (1 - p_A) (1 - p_B)$$

$$= 1 - q_A q_B$$

TIME DEPENDENT CONSIDERATIONS

The reliability of elements used in redundant configurations is usually time dependent. If the relation between element reliability and time is known, inclusion of the time factor does not change the basic notation and approach to redundancy computation outlined above. As as example, assume two active independent elements in parallel. System reliability is given by:

$$R = p_a + p_b - p_a p_b$$

This equation is applicable for one time interval. To express reliability over a segment of time, the reliability of each element must be expressed as a function of time.

Hence,

$$R(t) = p_a(t) + p_b(t) - p_a(t)p_b(t)$$

where

$R(t)$ = system reliability at time t, t > 0

$p_a(t)$, $p_b(t)$ = element reliabilities at time t

The failure pattern of most components is described by the exponential distribution, i.e.:

$$R = e^{-\lambda t} = e^{-t/\theta}$$

where λ is the constant failure rate; t is the time interval over which reliability, R, is measured; and θ is the mean-time-between-failure.

For two elements in series with constant failure rates λ_a and λ_b, using the product rule of reliability gives:

$$R(t) = p_a(t)p_b(t)$$
$$= e^{-(\lambda_a)t} e^{-(\lambda_b)t}$$
$$= e^{-(\lambda_a + \lambda_b)t}$$

The system reliability, $R(t)$, function is also exponential. With redundant elements present in the system, however, the system reliability function is not itself exponential. This is illustrated by two operative parallel elements whose failure rates are constant. From

$$R(t) = p_a + p_b - p_a p_b$$
$$R(t) = e^{-(\lambda_a)t} + e^{-(\lambda_b)t} - e^{-(\lambda_a + \lambda_b)t}$$

which is not of the simple exponential form $e^{-\lambda t}$. Element failure rates cannot, therefore, be combined in the usual manner to obtain the system failure rate if considerable redundancy is inherent in the design.

Although a single failure rate cannot be used for redundant systems, the mean-time-to-failure of such systems can be evaluated. The mean life of a redundant "pair" whose failure rates are λ_a and λ_b, respectively, can be determined from

$$MTBF = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} - \frac{1}{\lambda_a + \lambda_b} = \int_0^\infty R(t)dt$$

If the failure rates of both elements are equal, then,

$$R(t) = 2e^{-\lambda t} - e^{-2\lambda t}$$

and

$$MTBF = \frac{3}{2\lambda} = \frac{3}{2}\theta$$

For three independent elements in parallel, the reliability function is

$$R(t) = 1 - [(1 - e^{-(\lambda_a)t})(1 - e^{-(\lambda_b)t})(1 - e^{-(\lambda_c)t})]$$

$$MTBF = \frac{1}{\lambda_a} + \frac{1}{\lambda_b} + \frac{1}{\lambda_c} - \frac{1}{\lambda_a + \lambda_b} - \frac{1}{\lambda_a + \lambda_c}$$

$$- \frac{1}{\lambda_b + \lambda_c} + \frac{1}{\lambda_a + \lambda_b + \lambda_c}$$

If

$$\lambda_a = \lambda_b = \lambda_c = \lambda$$

$$R(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$$

$$MTBF = \frac{3}{\lambda} - \frac{3}{2\lambda} + \frac{1}{3\lambda} = \frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{1}{3\lambda} = \frac{11}{6\lambda} = \frac{11}{6}\theta$$

In general, for n active parallel elements, each element having the same constant failure rate, λ,

$$R(t) = 1 - [1 - e^{-\lambda t}]^n$$

and

$$MTBF = \sum_{i=1}^{n} \frac{1}{i\lambda} = \sum_{i=1}^{n} \frac{\theta}{i}$$

TYPES AND CLASSIFICATIONS OF REDUNDANCY

The following types of parallel redundancy most commonly used in equipment design are described in this appendix.

   (1) Operative Redundancy - redundancy units (or elements), all of which are fully energized during the system operational cycle. Operative redundancy may be further classified as described below.

      (a) Load-Sharing Redundancy - redundant units are connected in such a manner that, upon failure of one unit, the remaining redundant unit(s) will continue to perform the system function. It is not necessary to switch out the failed unit nor to switch in the redundant unit. Failure of the one may or may not change the probability of failure of the remaining units, depending upon the nature of the "load" being shared.

      (b) Switching Redundancy - operative redundant units are connected by a switching mechanism to disconnect a failed unit, and to connect one of the remaining operative redundant units into the system.

(2) <u>Standby Redundancy</u> - redundant units (or elements) that are non operative (i.e., have no power applied) until they are switched into the system upon failure of the primary unit. Switching is therefore always required.

(3) <u>Voting Redundancy</u> - the outputs of three or more operating redundant units are compared, and one of the outputs that agrees with the majority of outputs is selected. In most cases, units delivering outputs that fall in the minority group are classed as "unit failures."

(4) <u>Redundancy-with-Repair</u> - if a redundant element fails during a mission and can be repaired essentially "on line" (without aborting the mission), then redundancy-with-repair can be achieved. The reliability of dual or multiple redundant elements can be substantially increased by use of this design concept.

Diagrams, formulae, charts, and reliability functions are presented in the following pages for the above types and classes of redundancy.

OPERATIVE OR ACTIVE REDUNDANT CONFIGURATIONS

Formulae and graphs presented in this section do not account for any change in failure rates which survivors in a redundant "load sharing" configuration might experience as a result of increased operating stresses. This aspect of redundancy design is discussed in page 7A-22 of this appendix, under "Dependent Failure Probabilities." Also, it is assumed in the operative case that switching devices are either not required, or are relatively simple and failure free.

MULTIPLE REDUNDANCY

Figure A-4 shows a block diagram representing duplicate parallel components. There are two parallel paths for successful operation -- A_1 or A_2. If the probability of each component operating successfully is p_i, the probability of circuit success can be found by either the addition theorem or the multiplication theorem of probability.

By the multiplicative theorem, the circuit can fail only if both components fail. Since A_1 and A_2 are independent, the probability of success is equal to one minus the probability that both components fail, or

$$R = 1 - q_1 q_2$$

For example; if $p_1 = p_2 = 0.9$

$$R = 1 - (0.1)^2 = 0.99$$

More than two redundant elements are represented by the reliability block diagram shown in Figure A-5. There are m paths (or elements), at least one of which must be operating for system success. The probability of system success is therefore the probability that not all of the elements will fail during the mission period, shown as

$$R = 1 - q_1 q_2 \ldots q_m$$

where

$$q_1 = 1 - p_1, \text{ etc.}$$

If parallel elements are identical, then

$$R = 1 - q^m$$

Figure A-6 summarizes the information on simple parallel redundancy. Figure A-7 is a chart relating system reliability to the ratio $t/\theta = \lambda t$ of individual elements making up the redundant system. Curves for n elements (from n = 1 to n = 5) are shown. One element in n must remain operative for the prescribed time interval t, to achieve the probability of system failure shown.

Example

The inverter function for an airborne system has been allocated a reliability requirement of R(t) = .99 for a five hour mission. Current predictions of the MTBF feasibility by conventional design is 50 hours. Entering the chart at t/θ = 5/50 = 0.1, proceed vertically to .99, the required reliability for the inverter function. n = 2 is the number of inverters that are required in active parallel, to obtain a 99% probability of survival for the inverter function.

PARTIAL REDUNDANCY

In the previous example, the system was successful if at least one of n parallel paths was successful. There may be cases where at least k out of n elements must be successful. In such cases, the reliability of the redundant group is given by a series of additive terms (binomial) in the form of

$$P(k, n \mid p) = \binom{n}{k} p^k (1 - p)^{n-k}$$

Example

Figure A-8 illustrates three channels of a receiver. The receiver will operate if at least two channels are successful, that is, if k = 2 or k = 3. The probability of each channel being successful is equal to p; then

$$R = P(2, 3 \mid p) + P(3, 3 \mid p)$$

$$R = \binom{3}{2} p^2 (1 - p) + \binom{3}{3} p^3 (1 - p)^0$$

$$R = [3p^2(1 - p)] + p^3$$

$$R = 3p^2 - 2p^3$$
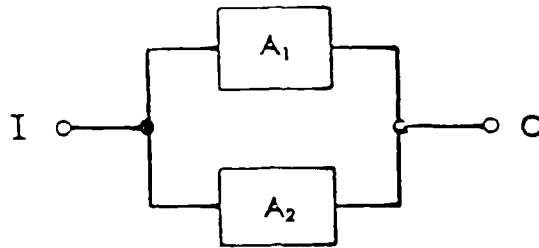
FIGURE A-4: DUPLICATE PARALLEL REDUNDANCY (OPERATIVE CASE)
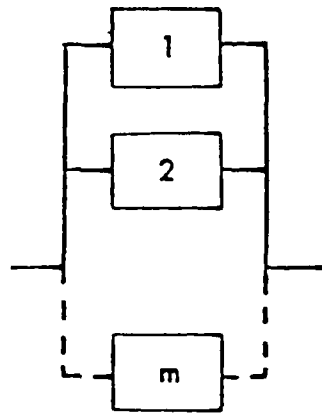
FIGURE A-5: MULTIPLE REDUNDANT ARRAY OF m ELEMENTS
WITH k = 1 REQUIRED FOR SUCCESS
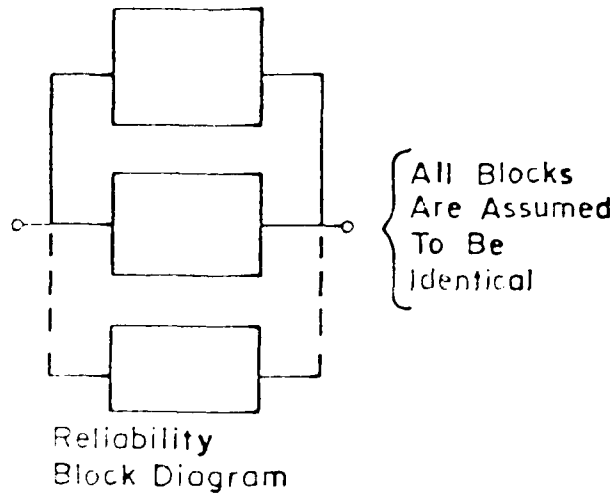
APPLICATION

Provides protection against irreversible hardware failures for continuously operating equipments.

Reliability Block Diagram

All Blocks Are Assumed To Be Identical

MATHEMATICAL MODEL

$$R = 1-(1-e^{-\lambda t})^n$$

SIMPLIFIED MODEL

$$R = 1-(\lambda t)^n$$

for small $\lambda t \leq 0.1$

where

n = number of parallel elements

λ = failure rate

R = reliability

$M = MTBF = \dfrac{1}{\lambda}$

n=5
n=4
n=3
n=2
Single Element
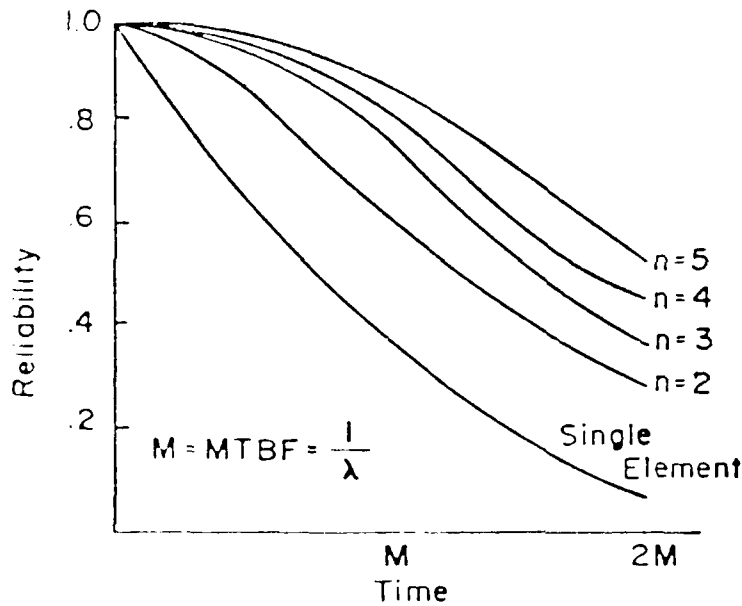
RELIABILITY FUNCTION FOR SIMPLE PARALLEL RELIABILITY

ADVANTAGES

- Simplicity
- Significant gain in Reliability from nonredundant element
- Applicable to both analog and digital circuitry

DISADVANTAGES

- Load sharing must be considered
- Sensitive to voltage division across the elements
- Difficult to prevent failure propagation
- May present circuit design problems

FIGURE A-6: SIMPLE PARALLEL REDUNDANCY

Basic element reliability $P_s = e^{-\lambda t}$

System reliability $R_S = 1 - (1 - e^{-\lambda t})^n$
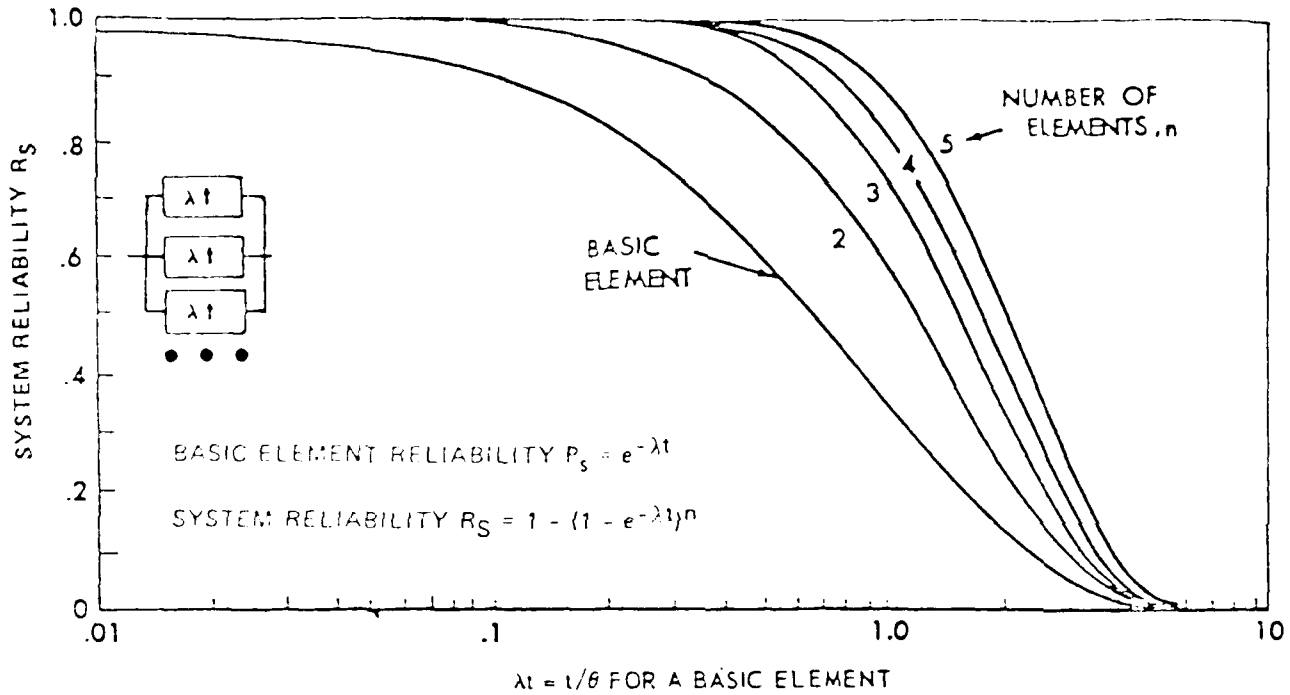
FIGURE A-7: SYSTEM RELIABILITY FOR n ELEMENT OPERATIVE REDUNDANT CONFIGURATIONS
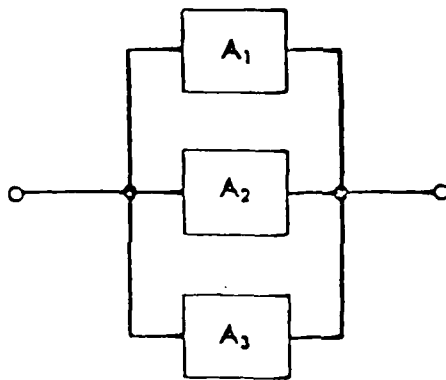
FIGURE A-8   PARTIAL REDUNDANT CONFIGURATION OF n = 3 ELEMENTS,
WITH K = 2 REQUIRED FOR SUCCESS

Use of the binomial formula becomes impractical in multi-element partial redundant configurations when the values of n, k, and r become large[1]. In these cases, the normal approximation to the binomial may be used. The approach can be best illustrated by an example.

Example

A new transmitting array is to be designed using 1000 RF elements to achieve design goal performance for power output and beam width. A design margin has been provided, however, to permit a 10% loss of RF elements before system performance becomes degraded below the acceptable minimum level. Each element is known to have a failure rate of 1000 x 10^{-6} failures per hour. The proposed design is illustrated in Figure A-9, where the total number of elements is n = 1000; the number of elements required for system success is k = 900; and, the number of element failures permitted is r = 100. It is desired to compute and plot the reliability function for the array.

Each discrete point for time (t) on the function is given by the binomial summation as:

$$R_s(t) = \sum_{x=0}^{r} \binom{n}{x} p^x q^{n-x}$$

$$= \sum_{x=0}^{100} \binom{1000}{x} (1 - e^{-\lambda t})^x (e^{-\lambda t})^{n-x}$$

where

$P = 1 - e^{-\lambda t}$

$q = e^{-\lambda t}$

$\lambda = $ element failure rate

This binomial summation can be approximated by the standard normal distribution function using Table A-1 at the end of Section 5 to compute reliability for the normalized statistic Z:

$$R_s(t) = F(Z)$$

and

$$Z = \frac{X-\mu}{\sigma} = \frac{X-np}{\sqrt{npq}}$$

$$= \frac{X-n(1-e^{-\lambda t})}{\sqrt{n(1-e^{-\lambda t})e^{-\lambda t}}}$$

[1] See any good text book on probability and statistics

A-13
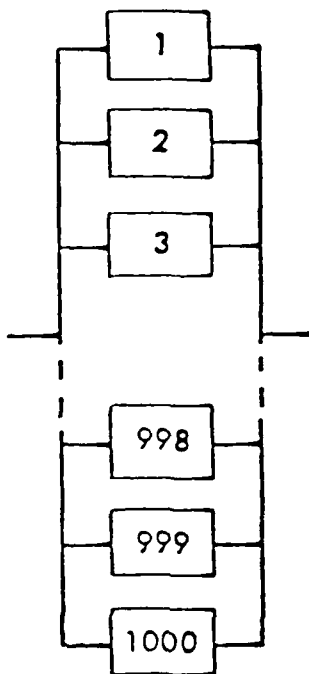
FIGURE A-9: <u>PARTIAL REDUNDANT ARRAY WITH m = 1000 ELEMENTS</u>
<u>r = 0, 50, 100, 150 PERMISSIBLE ELEMENT FAILURES</u>

By observation, it can be reasoned that system MTBF will be approximately 100 hours, since 100 element failures are permitted and one element fails each hour of system operation. A preliminary selection of discrete points at which to compute reliability might then fall in the 80- to 100-hour bracket.

At 80 hours:

$$\mu = np = 1000 \ (1 - e^{-1000 \times 10^{-6} \times 80})$$

$$= 77$$

$$q = e^{-1000 \times 10^{-6} \times 80} = .923$$

$$\sigma = \sqrt{npq} = \sqrt{71.07} = 8.4$$

$$X = 100$$

$$Z_{80} =$$

$$R_s(80) = F(Z_{80}) = F(+2.74)$$

$$= .997, \text{ from standard normal tables}$$

At 100 hours:

$$\mu = np = 1000 \ (1 - e^{-1000 \times 10^{-6} \times 100})$$

$$= 95$$

$$q = e^{-1000 \times 10^{-6} \times 100} = .905$$

$$\sigma = \sqrt{npq} = \sqrt{86} = 9.3$$

$$X = 100$$

$$Z_{100} = \frac{100-95}{9.3} = 0.54$$

$$R_s(100) = F(Z_{100}) = F(+.54) = .705$$

Reliability at other discrete points in time, computed as above, are:

Time, t	Z	$F(Z) = R_s(t)$
90	1.57	.942
95	.989	.8389
105	0	.500
110	-.42	.337
120	-1.30	.097
130	-2.03	.021

These points are then used to plot the reliability function for the array, shown in Figure A-10.

FAILURE MODES IN THE OPERATIVE REDUNDANT CASE

The previous redundant models were based on the assumption of one mode of failure, adequately protected so that failure of an individual element could not affect the operation of a surviving element. Two modes of failure are now considered -- open-circuit and short-circuit -- either of which can affect the surviving element unless proper design precautions are taken. In series redundant circuits, the open-circuit mode prevents surviving elements from functioning. In parallel redundant circuits, the short-circuit mode prevents the surviving elements from functioning.

The probabilities that are necessary to describe element failure can best be illustrated by an example. Assume that 100 randomly selected items are tested for a prescribed time to determine failure probabilities. The results are as follows:

  80 items experienced no failures
  15 items experienced an open failure
   5 items experienced a short-circuit failure

Thus, the estimated probability of success is $80/100 = 0.80$. The estimated probability of an open failure (q_o) is 0.15, and the estimated probability of a short-circuit failure (q_s) is 0.05. The sum of the two failure probabilities (opens and shorts are mutually exclusive events) is the probability of element failure (q), 0.20. This could have been obtained by subtracting the probability of element success (p) from one, i.e.,

$$q = 1 - p = q_o + q_s$$

The conditional probabilities of open and short failures are sometimes used to represent element failure probabilities. The data indicate that 15 of the 20 failures that occurred were due to opens. Therefore, the conditional probability of an open failure -- i.e., the probability that if a failure occurs, it is an open failure -- is $15/20 = 0.75$. Similarly, the conditional probability of a short-circuit is $5/20 = 0.25$. If

q'_o = conditional probability of an open

   $= q_o/q$

q'_s = conditional probability of a short

   $= q_s/q$

then the following relationship holds true:

$$q'_o + q'_s = 1$$
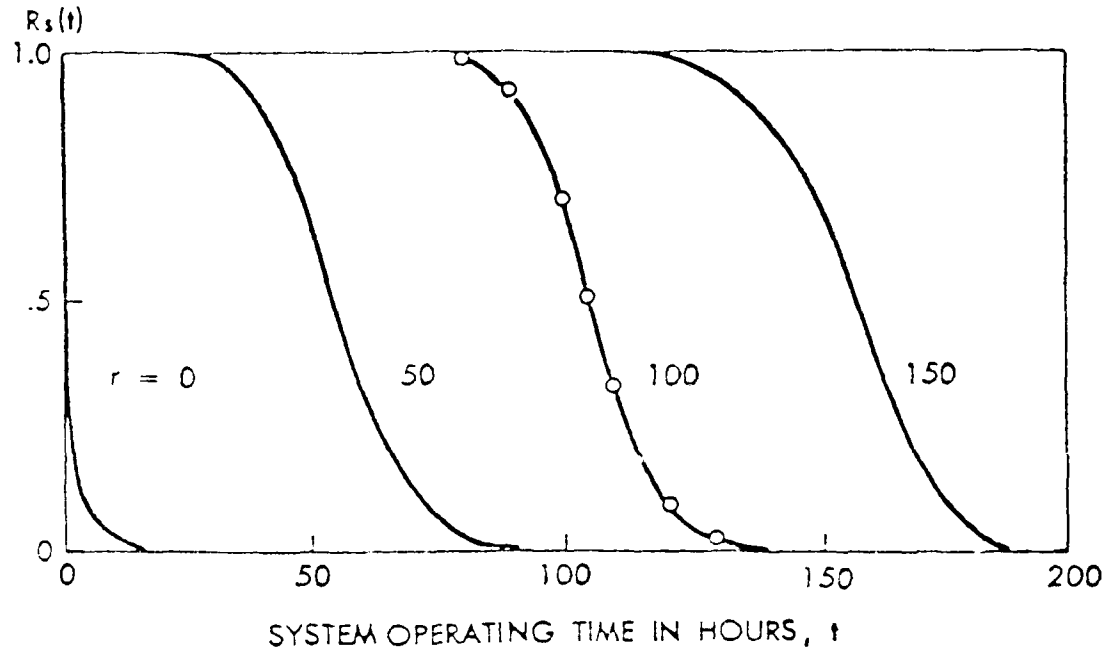
FIGURE A-10: RELIABILITY FUNCTIONS FOR PARTIAL REDUNDANT ARRAY OF FIGURE A-9

PARALLEL ELEMENTS

For two elements, A and B in an operative parallel redundant configuration, the unit will fail if either A or B shorts (a. below), or both A and B open (b. below). The probabilities of these two event are:

a. $P_1(S) = P_a(S) + P_b(S) - P_a(S)P_b(S)$

$$= 1 - \big([1 - P_a(S)][1 - P_b(S)]\big)$$

$$= 1 - \big([1 - q_{sa}][1 - q_{sb}]\big)$$

b. $P_2(0) = P_a(0)P_b(0)$

$$= q_{oa}q_{ob}$$

where $P_i(0)$ is the probability that Element i opens and $P_i(S)$ is the probability that Element i shorts. Since Events a. and b. are mutually exclusive, the probability of unit failure is the sum of the two event probabilities, or

$$P(F) = \bar{R} = P_1(S) + P_2(0)$$

$$= 1 - \big((1 - q_{sa})(1 - q_{sb})\big) + q_{oa}q_{ob}$$

In general, if there are m parallel elements,

$$\bar{R} = 1 - \prod_{i=1}^{m} (1 - q_{si}) + \prod_{i=1}^{m} q_{oi}$$

The reliability is equal to 1 - R, or

$$R = \prod_{i=1}^{m} (1 - q_{si}) - \prod_{i=1}^{m} q_{oi}$$

If all elements are equal, unit reliability is then

$$R = (1 0 q_s)^m - q_o m$$

OPTIMUM NUMBER OF PARALLEL ELEMENTS

By introducing the possibility of short circuit failures, unit reliability may be decreased by adding parallel elements. As an example, if $q_o = 0.10$, the reliability for several values of m and q_s is as shown in Table A-1. For Cases (a) and (b), adding one parallel element (m = 2) increases unit reliability. For (a), the reliability increases as m increases, and approaches 1 as m approaches infinity. However, for (b), increasing m from 2 to 3 decreases reliability. In fact, the reliability continues to decrease as m gets larger.

Therefore, for Case (b), the optimum number of parallel elements for maximum reliability is 2. For Case (c), R is the same for $m = 1$ and 2, but is less for $m = 3$. For Case (d), the maximum reliability occurs for $m = 1$, the nonredundant configuration.

For any range of q_0 and q_s, the optimum number of parallel elements is 1 if $q_s \geq q_0$. For most practical values of q_s and q_0, the optimum number is 2.

Figure A-11 gives the optimum number of parallel elements for values of q_0 ranging from 0.001 to 0.5 and for the ratio q_s/q_0 ranging from 0.001 to 1.0 (use the left hand and bottom axes). Knowing the general range of element failure probabilities and possibly knowing the ratio of short to open possibilities, the figure can be used to determine the optimum number of parallel elements. For example, if it is believed that overall element reliability is somewhere between 0.8 and 0.9 and that opens are likely to occur about twice as often as shorts, then

$$0.1 \leq q \leq 0.2, \text{ and } q_S/q_O \doteq 0.5$$

Since $q_0 + q_s = q$,

$$0.1 \leq 3/2q_0 \leq 0.2 \text{ or } 0.07 \leq q_0 \leq 0.13$$

TABLE A-1: VALUES OF R FOR $q_0 = 0.10$

	Case (a) $q_s = 0$	Case (b) $q_s = 0.05$	Case (c) $q_s = 0.10$	Case (d) $q_s = 0.20$
$m = 1$	0.900	0.85	0.80	0.70
$m = 2$	0.990	0.89	0.80	0.63
$m = 3$	0.999	0.86	0.73	0.51

For each of the values of q_0 between 0.07 and 0.13, the optimum number is determined at $q_0/q_s = 0.5$. If this number is the same for all or nearly all possible values of q_0, then the optimum design is fairly well established. In this case, Figure A-11 shows that 2 is the optimum number of parallel elements. If an optimum number boundary line is crossed somewhere in the interval of possible values of q_0, then it will be necessary to narrow the length of this interval by a thorough reappraisal of existing failure data or by tests specifically designed to yield more precise information.
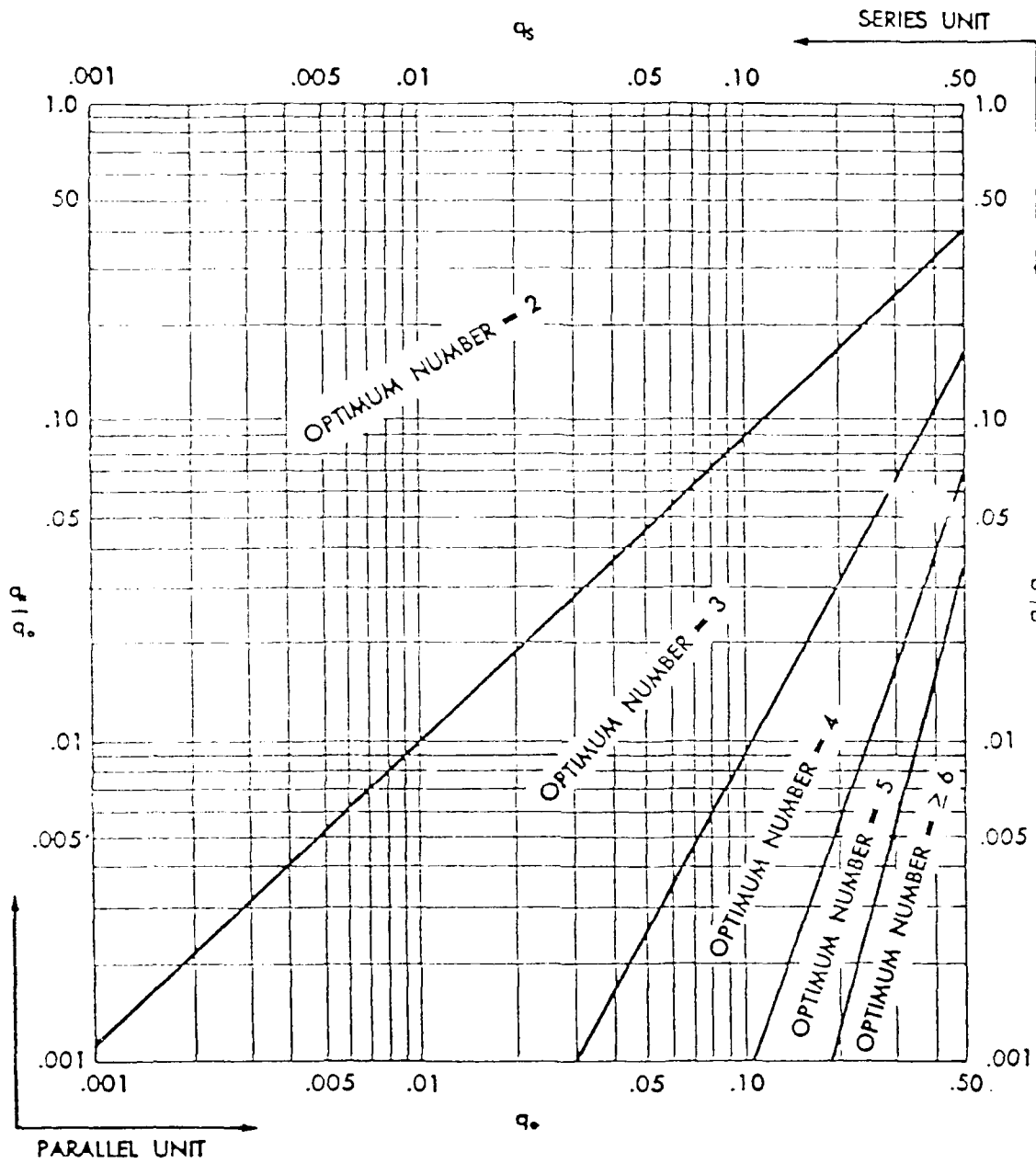
FIGURE A-11: OPTIMUM NUMBER OF PARALLEL ELEMENTS AS A FUNCTION OF FAILURE-MODE PROBABILITIES

SERIES ELEMENTS

The results given above show that if $q_s \geq q_0$, the optimum number of parallel paths is 1. However, adding an element in series with another element will result in an increase in reliability if q_s is much greater than q_0. Assume we have a system made up of two series elements, A and B, in which both short circuit and open failures are possible. The unit will fail if both A and B short (a. below), or either A or B open (b. below). The probabilities of Events a. and b. are:

a. $\quad P_1(S) = P_a(S)P_b(S)$

$\qquad\qquad = q_{sa}q_{sb}$

b. $\quad P_2(0) = P_a(0) + P_b(0) - P_a(0)P_b(0)$

$\qquad\qquad = 1 - \Big([1 - P_a(0)] \, [1 - P_b(0)]\Big)$

$\qquad\qquad = 1 - \Big([1 - q_{0a}] \, [1 - q_{0b}]\Big)$

Since Events a. and b. are mutually exclusive, the probability of unit failure is the sum of two events, or

$$P(F) = \bar{R} = P_1(S) + P_2(0)$$

$$= q_{sa}q_{sb} + 1 - \Big((1 - q_{0a})(1 - q_{0b})\Big)$$

In general, if there are n series elements,

$$\bar{R} = 1 - \prod_{i=1}^{n}(1 - q_{0i}) + \prod_{i=1}^{n} q_{si}$$

and

$$R = \prod_{i=1}^{n}(1 - q_{0i}) - \prod_{i=1}^{n} q_{si}$$

If all elements are identical, then the reliability of an n-element series unit is

$$R = (1 - q_0)^n - q_s n$$

Note that n replaces m in the equation for a parallel unit and the positions of q_0 and q_s are reversed.

Figure A-11 can be used to determine the optimum number of series elements by using the upper and right hand axes. As in parallel systems, if $q_0 \geq q_s$, the optimum number of series elements is 1.

SERIES-PARALLEL ELEMENTS

A four-element series-parallel configuration is shown in Figure A-12. Each element performs the same function.

Block success is defined as an output for at least one element. Therefore, the block is successful if either unit has less than two opens (a. below), and at least one unit has no short (b. below).

a. $P_1(0)$ = probability that at least one unit has 2 opens

= 1 - probability that both units have at least 1 "no open"

= $1 - [1 - P_{a_1}(0)P_{a_2}(0)] [1 - P_{b_1}(0)P_{b_2}(0)]$

b. $P_2(S)$ = probability that at least 1 element in each unit shorts

= $1 - [(1 - P_{a_1}(S)) (1 - P_{a_2}(S))]$

$[1 - [(1-P_{b1}(S))(1-P_{b2}(S))]]$

Then

$P_1(0) + P_2(S)$ = probability of block failure

$1 - [P_1(0) + P_2(S)]$ = reliability of block
= R_{sp}

Since

$P_i(0) = q_{oi}$

and

$P_i(S) = q_{si}$

Then

R_{sp} = $[1 - q_{oa_1} q_{oa_2}] [1 - q_{ob_1} q_{ob_2}]$

- $[1 - (1 - q_{sa_1}) (1 - q_{sa_2})][1 - (1 - q_{sb_1}) (1 - q_{sb_2})]$

A-22
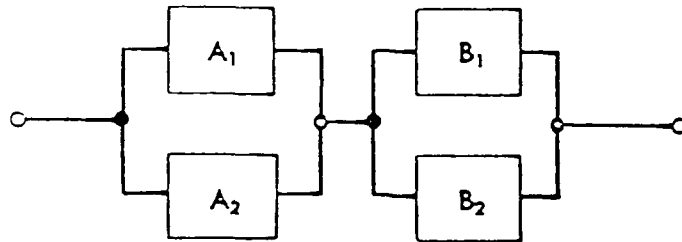
FIGURE A-12: SERIES-PARALLEL CONFIGURATION

When the units are identical ($A_1 = B_1$ and $A_2 = B_2$) and all components perform the same function, then

$$R_{sp} = [1 - q_{oa}q_{ob}]^2$$
$$- [1 - (1 - q_{sa})(1 - q_{sb})]^2$$

For n identical units each containing m elements,

$$R_{sp} = [1 - \prod_{i=1}^{m} q_{oi}]^n - [1 - \prod_{i=1}^{m}(1 - q_{si})]^n$$

and if all elements are identical,

$$R_{sp} = [1 - q_o^m]^n - [1 - (1-q_s)^m]^n$$

If q_s and q_o are small, then

$$R_{sp} = 1 - nq_o^m - (mq_s)^n$$

PARALLEL-SERIES ELEMENTS

A 4-element parallel-series configuration is shown in Figure A-13. Each element performs the same function. Success is defined as an output from at least one element. Therefore, the block is successful if at least one path has no opens (a. below), and both paths have less than two shorts (b. below).

a. $P_1(0)$ = probability that at least one element in each path has opened

$$= [1 - (1 - P_{a1}(0))(1 - P_{a2}(0))]$$
$$[1 - (1 - P_{b1}(0))(1 - P_{b2}(0))]$$

b. $P_2(S)$ = probability that at least one path has two shorts

= one minus the probability that both paths have at least one "no short"

$$= 1 - [1 - P_{a1}(S) P_{a2}(S)][1 - P_{b1}(S) P_{b2}(S)]$$

Then

$$P_1(0) + P_2(S) = \text{probability of block failure}$$

$$1 - [P_1(0) + P_2(S)] = \text{reliability of block}$$

$$= R_{ps}$$

Since

$$P_i(0) = q_{oi}$$

and

$$P_i(S) = q_{si}$$

then

$$R_{ps} = [1 - q_{sa_1} q_{sa_2}] [1 - q_{sb_1} q_{sb_2}]$$
$$- [1 - (1 - q_{oa_1})(1 - q_{oa_2})]$$
$$[1 - (1 - q_{ob_1})(1 - q_{ob_2})]$$

If all paths are identical $(A_1 = B_1$ and $A_2 = B_2)$ and all components perform the same function

$$R_{ps} = [1 - q_{sa} q_{sb}]^2$$
$$- [1 - (1 - q_{oa})(1 - q_{ob})]^2$$

For m identical paths each containing n elements,

$$R_{ps} = [1 - \prod_{i=1}^{n} q_{si}]^m - [1 - \prod_{i=1}^{n}(1 - q_{oi})]^m$$

If all elements are identical

$$R_{ps} = [1 - q_s^n]^m - [1 - (1 - q_o)^n]^m$$

If q_o and q_s are small

$$R_{ps} = 1 - m q_s^n - (n q_o)^m$$

Information on series/parallel and parallel series configurations is summarized in Figure A-14.

OPERATIVE REDUNDANCY, SWITCHING REQUIRED

Until now we have dealt with circuits where it was assumed that switching devices were either absent or failure free. We now deal with circuits whose redundant elements are continuously energized but do not become part of the circuit until switched in after a primary element fails. We will consider two modes of failure that can be associated with the switching mechanism:

a. Type (1). The switch may fail to operate when it is supposed to.

b. Type (2). The switch may operate without command (prematurely).

A-25
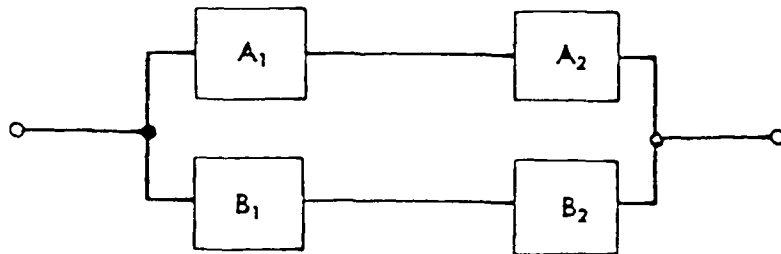
FIGURE A-13:   PARALLEL-SERIES CONFIGURATION

Reliability Block Diagram

(a)

(b)

{ All Elements
Shown In
The Block
Diagram Are
Assumed Identical
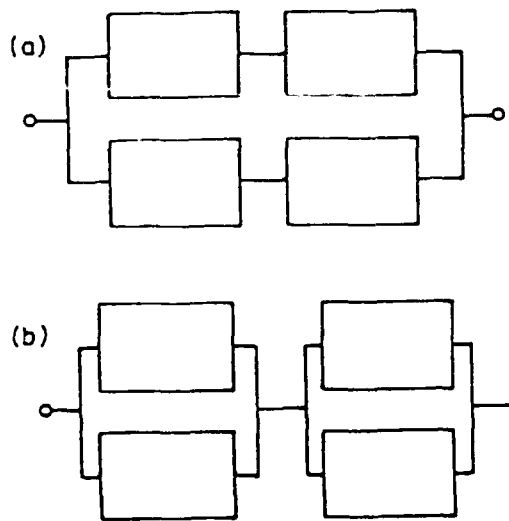
APPLICATION

Applicable primarily at the part level where short and open protection is required.

a) Protects primarily against the short failure mode.

b) Protects primarily against the open failure mode.
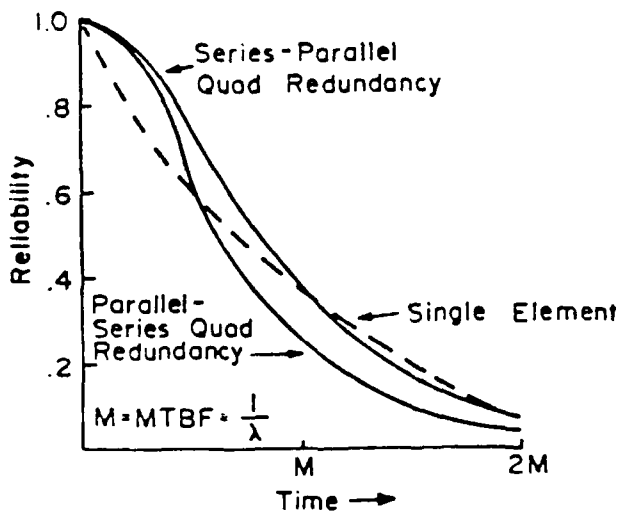
MATHEMATICAL MODEL

a) $R = 2e^{-2\lambda t} - e^{-4\lambda t}$

b) $R = 4e^{-2\lambda t} - 4e^{-3\lambda t} + e^{-4\lambda t}$

Reliability graph:

- Series-Parallel Quad Redundancy
- Parallel-Series Quad Redundancy
- Single Element
- $M = MTBF = \frac{1}{\lambda}$

Vertical axis: Reliability (1.0, .8, .6, .4, .2)
Horizontal axis: Time → (M, 2M)

RELIABILITY FUNCTION FOR
BIMODAL CONFIGURATIONS

ADVANTAGES

• Provides significant gain in reliability at the part or stage level for short mission times.

DISADVANTAGES

• Difficult to design.

• Restricted to part and/or stage applications.

FIGURE A-14: BIMODAL REDUNDANCY

In the following discussion

q_s = probability of a Type (1) failure

q'_s = probability of a Type (2) failure

TWO PARALLEL ELEMENTS

Consider the system in Figure A-15. There are three possible states that could lead to system failure:

a. A succeeds, B fails, switch fails (Type 2)

b. A fails, B succeeds, switch fails (Type 1)

c. A fails, B fails

The unreliability of the system, $\overline{R}$, is found from

$$\overline{R} = p_a q_b q'_s + q_a p_b q_s + q_a q_b$$

If we are not concerned with Type (2) failures,

$$q'_s = 0$$

and the unreliability is

$$\overline{R}_D = q_a p_b q_s + q_a q_b$$

As an example, assume

$$q_a = q_b = 0.2$$

and

$$q_s = q'_s = 0.1$$

Then

$$
\begin{aligned}
\overline{R} &= p_a q_b q'_s + q_a p_b q_s + q_a q_b \\
&= (0.8)(0.2)(0.1) + (0.2)(0.8)(0.1) + (0.2)(0.2) \\
&= 0.072 \\
R &= 1 - \overline{R} \\
&= 1 - 0.072 \\
&= 0.928
\end{aligned}
$$
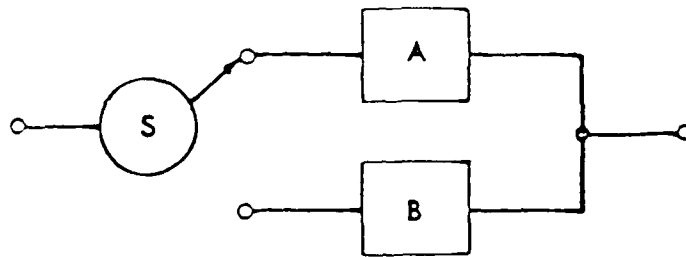
FIGURE A-15: REDUNDANCY WITH SWITCHING

If $q'_s = 0$,

$$R_D = q_a p_b q_s + q_a q_b$$

$$= (0.2)(0.8)(0.1) + (0.2)(0.2)$$

$$= 0.056$$

$$R_D = 1 - 0.056$$

$$= 0.944$$

THREE PARALLEL ELEMENTS

Figure A-16 illustrates this type circuit. It operates as follows: If A fails, S switches to B. If B then fails, S switches to C. Enumerating all possible switching failures shows two kinds of Type (1) failure and four kinds of Type (2) failure:

a. Type (1) Switching Failures:

    1. q_{s_1} - A fails, S does not switch to B

    2. q_{s_2} - A fails, S switches to B, B fails, S fails to switch to C

b. Type (2) Switching Failures:

    1. q'_{s_3} - A succeeds, but S switches to B

    2. q'_{s_4} - A succeeds, S switches to B, B fails, S does not switch to C

    3. q'_{s_5} - A succeeds, S switches to B, B succeeds, S switches to C

    4. q'_{s_6} - A fails, S switches to B, B succeeds, S switches to C

The possible states of operation of elements A, B, and C and also switching failures that will cause system failure for each state are shown in Table A-2.

The probability of system failure can be found by summing up the probabilities of individual combinations or operating states which result in system success, each multiplied by the probability of a switching failure which would produce system failure in each state, i.e.:

$$\bar{R} = \sum_{i=1}^{8} P_i q_{s_i}$$

MIL-HDBK-338-1A
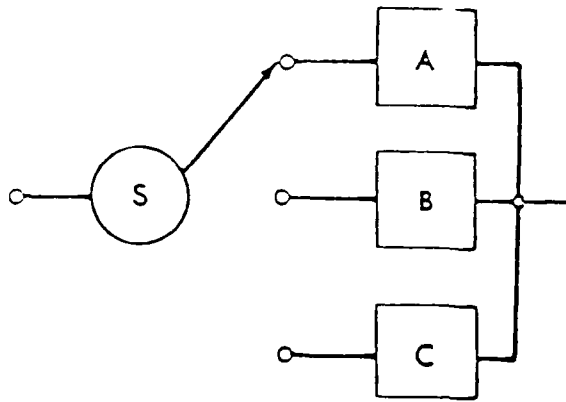
FIGURE A-16:   THREE-ELEMENT REDUNDANT CONFIGURATIONS WITH SWITCHING

TABLE A-2:
STATES OF OPERATION OF A THREE PARALLEL ELEMENT

| Operating State (i) | Operating Condition | | Switching Failure Resulting in System Failure | $\overline{R} = \sum\limits_{i=1}^{8} p_i q_s$ |
	Succeed	Fail		
1	A	$\overline{BC}$	s_3	$\overline{ABC}\overline{s_3}$
2	B	$\overline{AC}$	s_1 or s_6	$\overline{ABC}(\overline{s_1} + \overline{s_6})$
3	C	$\overline{AB}$	s_1 or s_2	$\overline{ABC}(\overline{s_1} + \overline{s_2})$
4	AB	$\overline{C}$	s_5	$\overline{ABC}(\overline{s_5})$
5	AC	$\overline{B}$	s_4	$\overline{ABC}(\overline{s_4})$
6	BC	$\overline{A}$	s_1	$\overline{ABC}(\overline{s_1})$
7	ABC	-	Cannot fail	ABC
8	-	$\overline{ABC}$	Always fails	-

or, as shown in Table A-2,

$$\overline{R} = p_a q_b q_c q'_{s_3} + p_b q_a q_c (q_{s_1} + q'_{s_6})$$
$$+ p_c q_a q_b (q_{s_1} + q_{s_2})$$
$$+ p_a p_b q_c q'_{s_5} + p_a p_c q_b q'_{s_4}$$
$$+ p_b p_c q_a q_{s_1} + q_a q_b q_c$$

(Primes denote "static" or Type (2) switch failures)

If the probability of Type (2) switching faiures is very small (q'_{s_i} = 0), and $q_{s1} = q_{s2} = q_s$, $\overline{R}$ can be found directly from the following equation:

$$\overline{R} = q_a q_s + q_a p_s q_b q_s + q_a p_s q_b p_s q_c$$

VOTING REDUNDANCY

Figure A-17 shows three elements, A, B, and C, and the associated switching and comparator circuit which make up a voting redundant system. The circuit function will always be performed by an element whose output agrees with the output of at least one or the other
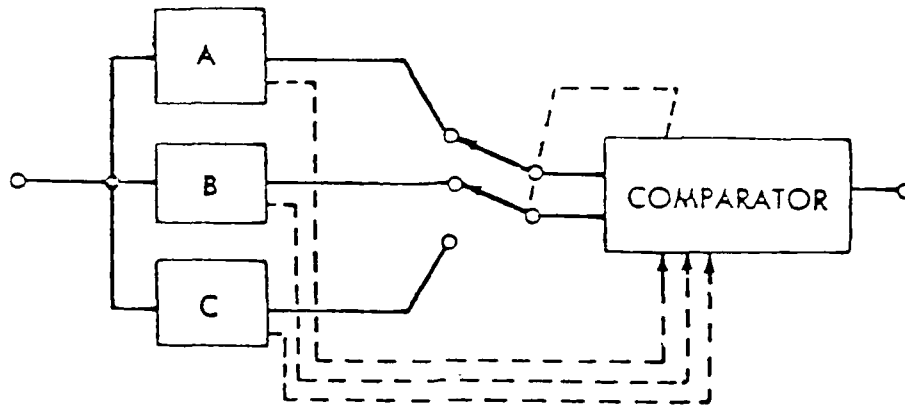
FIGURE A-17: THREE-ELEMENT VOTING REDUNDANCY

elements. At least two good elements are required for successful operation of the circuit. Two switches are provided so that a comparison of any two outputs of the three elements can be made. A comparator circuit is required that will operate the two switches so that a position is located where the outputs again agree after one element fails.

If comparison and switching are failure free, the system will be successful as long as two or three elements are successful. In this case,

$$R = p_a p_b + p_a p_c + p_b p_c - 2p_a p_b p_c$$

If failure free switching cannot be assumed, conditional probabilities of switching operation have to be considered. To simplify the discussion, consider the probability of the comparator and switches failing in such a manner that the switches remain in their original positions. If this probability is q_s, then

$$R = p_a p_b + (p_a p_c + p_b p_c - 2p_a p_b p_c)(1 - q_s)$$

Example: Let all three elements have the same probability of success, 0.9, i.e., $p_a = p_b = p_c = 0.9$. Assume that the comparator switch has a probability of failing (q_s) of 0.01:

$$R = .9^2 + (.9)^2 + (.9)^2 - 2(.9)^3 [1 - .01]$$

$$R = .970$$

Information and expressions for the general majority voting case are given in Figure A-18.

STANDBY REDUNDANCY

In a system with redundant elements on a completely standby basis (not energized), no time is accumulated on a secondary element until a primary element fails. For a two-element system (Figure A-19) the reliability function can be found directly as follows. The system will be successful at time t if either of the following two conditions hold (let A be the primary element):

a. A is successful up to time t

b. A fails at time $t_1 < t$, and B operates form t_1 to t

For the exponential case where the element failure rates are λ_a and λ_b, reliability of the standby pair is given by

$$R(t) = \frac{\lambda_b}{\lambda_b - \lambda_a} e^{-(\lambda_a)t} - \frac{\lambda_a}{\lambda_b - \lambda_a} e^{-(\lambda_b)t}$$

This is a form of the mixed exponential and it does not matter whether the more reliable element is used as the primary or as the standby element.

Reliability Function For Majority
Voting Redundancy

Reliability For Mission Time Less
Than One MTBF
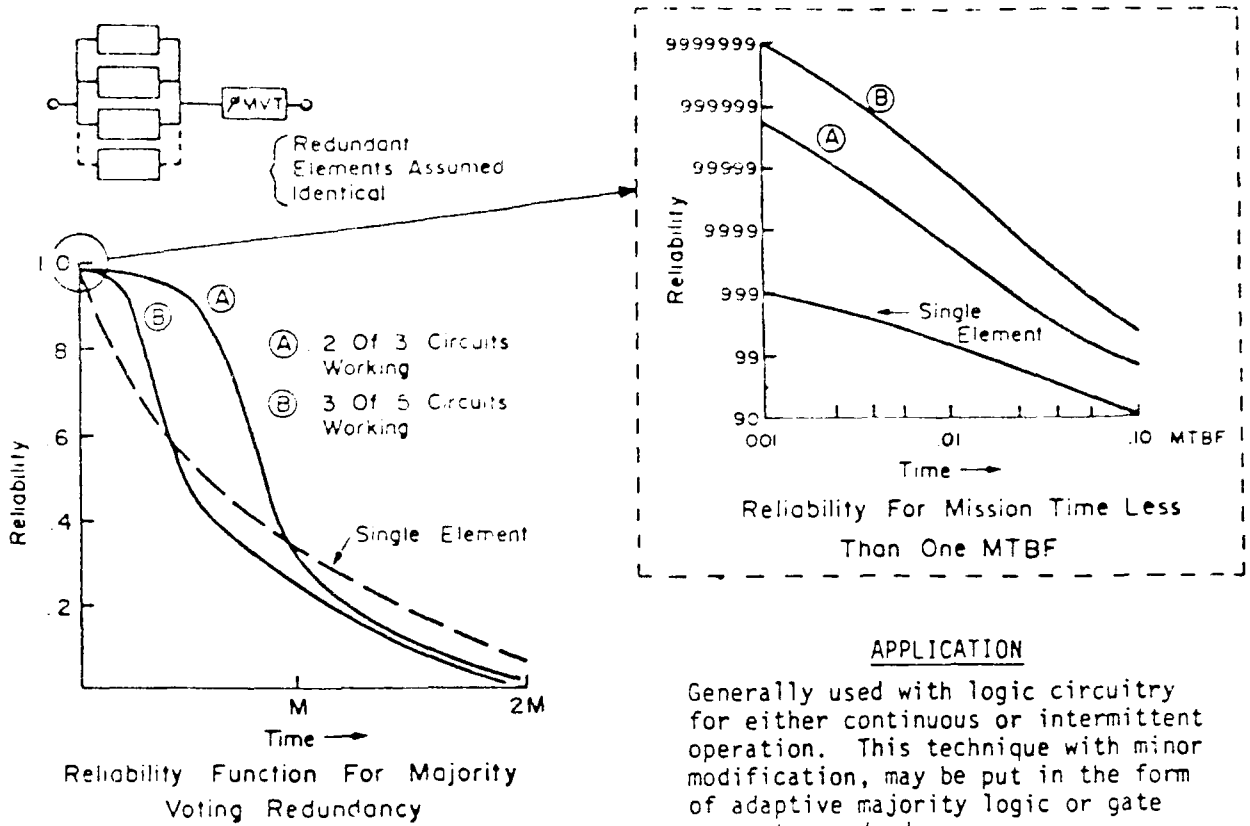
APPLICATION

Generally used with logic circuitry
for either continuous or intermittent
operation. This technique with minor
modification, may be put in the form
of adaptive majority logic or gate
connector redundancy.

ADVANTAGES

- Can be implemented to provide
  indication of defective elements

- Can provide a significant gain in
  reliability for short mission
  times (less than one MTBF)

DISADVANTAGES

- Requires voter reliability
  significantly better than
  element reliability

- Lower reliability for long
  mission time (greater than
  one MTBF)

MATHEMATICAL MODEL

$$R = \left[\sum_{i=0}^{n} \binom{2n+1}{i}(1-e^{-\lambda t}) \, e^{-\lambda t (2n+1-i)} \right] e^{-\lambda_m t}$$

SIMPLIFIED MODEL

$$R = e^{\lambda_m t} - \binom{2n+1}{n+1}(\lambda t)^{n+1}$$

for small λt

where

n = number of redundant elements
minus minimum number of
elements required

λ = failure rate

R = reliability

λ_m = failure rate of Majority Vote
Comparator (MVT)

FIGURE A-18: MAJORITY VOTING REDUNDANCY

The mean-time-to-failure of the system is

$$MTBF = \frac{\lambda_a + \lambda_b}{\lambda_a \lambda_b}$$

$$= \theta_a + \theta_b \text{ when } \theta_a \neq \theta_b$$

$$= 2\theta \text{ when } \theta_a = \theta_b = \theta$$

For n elements of equal reliability, it can be shown that,

$$R(t) = e^{-\lambda t} \sum_{r=0}^{n-1} \frac{(\lambda t)^r}{r!}$$

$$MTBF = \frac{n}{\lambda} = n\theta$$

Figure A-20 is a chart relating system reliability to the reliability of individual standby redundant parallel elements as a function of mission time, t/θ. By entering the chart at the time period of interest and proceeding vertically to the allocated reliability requirement, the required number of standby elements can be determined.

Example: A critical element within a system has a demonstrated MTBF, θ = 100 hours. A design requirement has been allocated to the function performed by this element of R_s = .98 at 100 hours. This corresponds to a 30-to-1 reduction in unreliability below that which can be achieved by a single element. In this case, n = 4 will satisfy the design requirement at t/θ = 1. In other words, a four-element standby redundant configuration would satisfy the requirement. Failure rates of switching devices must next be taken into account.

Figure A-21 summarizes information for the general case of standby redundancy (operating and nonoperating) with a switch.

DEPENDENT FAILURE PROBABILITIES

Up to this point, it has been assumed that the failure of an operative redundant element has no effect on the failure rates of the remaining elements. This might occur, for example, with a system having two elements in parallel where both elements share the full load.

An example of conditional or dependent events is illustrated by Figure A-22. A and B are both fully energized, and normally share or carry half the load, L/2. If either A or B fails, the survivor must carry the full load, L. Hence, the probability that one fails is dependent on the state of the other, if failure probability is related to load or stress. The system is operating satisfactorily at time t if either A or B or both are operating successfully.
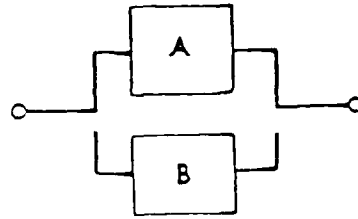
FIGURE A-19: <u>DIAGRAM DEPICTING A STANDBY REDUNDANT PAIR</u>

BASIC ELEMENT RELIABILITY $\quad R_s = e^{-\lambda t}$

SYSTEM RELIABILITY $\quad R_s = e^{-\lambda t} + \lambda t e^{-\lambda t} \cdots + \dfrac{(\lambda t)^{n-1}}{n-1} e^{-\lambda t}$

$\lambda t = t/\theta$ FOR A BASIC ELEMENT
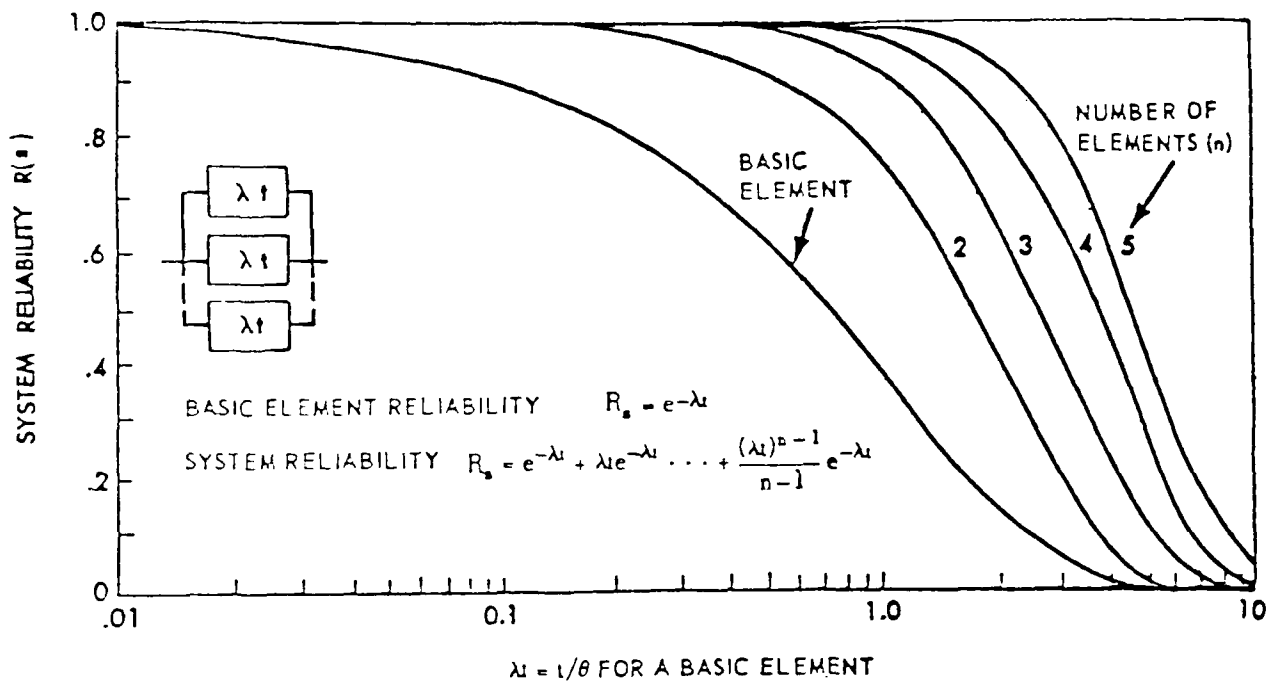
FIGURE A-20: <u>SYSTEM RELIABILITY FOR n STANDBY REDUNDANT ELEMENTS</u>

Reliability Block Diagram

Redundant
Elements $(A_1,....A_n)$
Are Identical
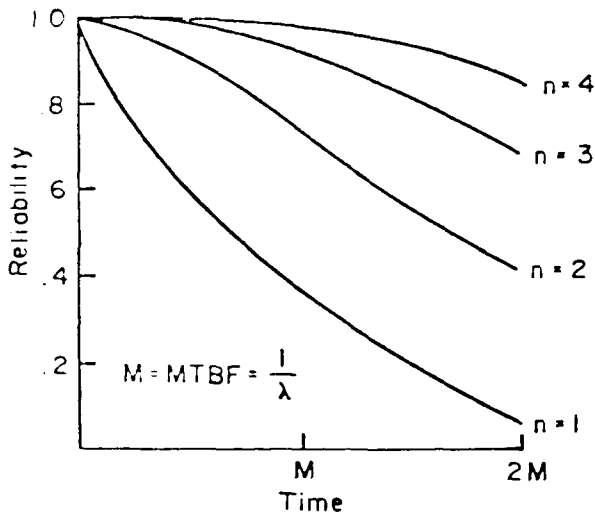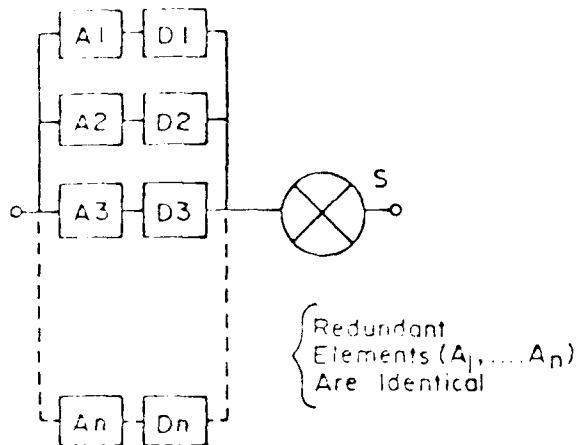
RELIABILITY FUNCTION FOR OPERATING
REDUNDANCY WITH UNIT SELECTION

This configuration uses single mode redundancy with a sensor (Dn) on each unit possessing switching capability when a failure is detected. It is used when long starting time must be avoided and only single output can be tolerated. This technique may be reconfigured to a standby redundancy technique by altering the switching arrangement to activate the elements as they are switched into the circuit.

MATHEMATICAL MODEL
(Operating Redundancy)

$$R = e^{-\lambda t}\left[\sum_{r=0}^{n-1} \frac{(\lambda t)^r}{r!}\right]$$

Assuming error detector and switching reliability is 1.0.

where

n = number of parallel elements

λ = failure rate $(A_n + D_n)$

R = reliability

MATHEMATICAL MODEL
(Standby Redundancy)

$$R = e^{-\lambda t}\left[1 + \frac{\lambda}{\lambda_s}(1 - e^{-\lambda_s t})\right]$$

where

λ = element failure rate

λ_s = failure rate of switching function

R = reliability

ADVANTAGES

- Applicable to analog and digital circuitry

- Effective for intermittent failure modes

DISADVANTAGES

- Delay due to sensing and switching

- Redundancy gains are limited by failure modes of sensing and switching devices

- Increased complexity due to sensing and switching

FIGURE A-21: STANDBY REDUNDANCY

Figure A-23 illustrates the three possible ways the system can be successful. The bar above a letter represents a failure of that element. A primed letter represents operation of that element under full load; absence of a prime represents operation under half load. If the elements' failure times are exponentially distributed and each has a mean life of θ under load L/2 and $\theta' = \theta/k$ under load L where $k > \theta$, block reliability is given below without derivation:

$$R(t) = \frac{2\theta'}{2\theta' - \theta} e^{-t/\theta'} - \frac{\theta}{2\theta' - \theta} e^{-2t/\theta}$$

System mean life is equal to

$$\theta_s = \theta/k + \theta/2$$

When $k = 1$, the system is one in which load sharing is not present or an increased load does not affect the element failure probability. Thus, for this case, θ_s is equal to $3\theta/2$. If there were only one element it would be operating under full load, so system mean life would be $\theta' = \theta/k$. Hence, the addition of a load sharing element increases the system mean life by $\theta/2$. This increase in mean life is equivalent to that gained when the elements are independent, but the overall system reliability is usually less because θ' is usually less than $\theta(k > 1)$.

OPTIMUM ALLOCATION OF REDUNDANCY

Decision and switching devices may fail to switch when required or may operate inadvertently. However, these devices are usually necessary for redundancy, and increasing the number of redundant elements increases the number of switching devices. If such devices are completely reliable, redundancy is most effective at lower system levels. If switching devices are not failure free, the problem of increasing system reliability through redundancy becomes one of choosing an optimum level at which to replicate elements.

Since cost, weight, and complexity factors are always involved, the minimum amount of redundancy that will produce the desired reliability should be used. Thus efforts should be concentrated on those parts of the system which are the major causes of system unreliability.

As an example, assume that we have two elements, A and B, with reliabilities over a certain time period of 0.95 and 0.50, respectively. If A and B are joined to form a series nonredundant circuit, its reliability is

$$R = (0.95)(0.50) = 0.475$$

If we duplicate each element, as in Figure A-24a,

$$R_1 = [1 - (0.50)^2][1 - (0.05)^2]$$

$$= 0.748$$
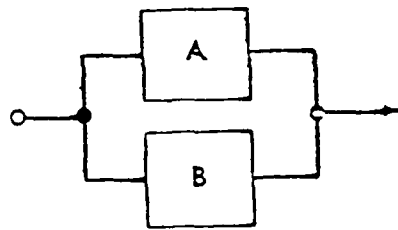
FIGURE A-22: LOAD-SHARING REDUNDANT CONFIGURATION
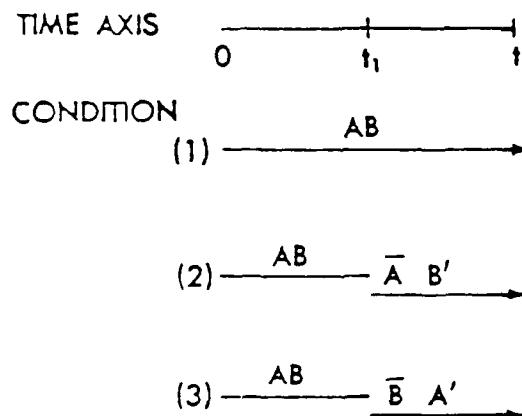
FIGURE A-23: SUCCESS COMBINATIONS IN TWO-ELEMENT LOAD-SHARING CASE
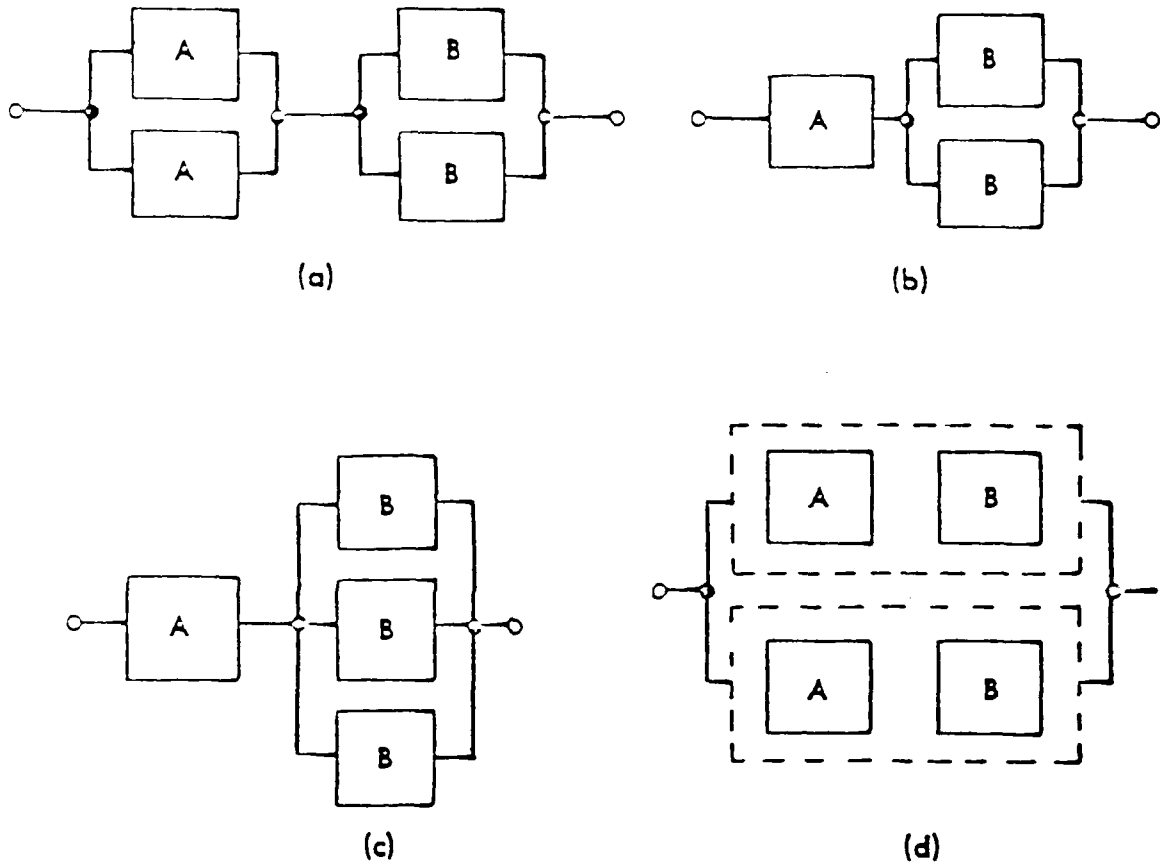
FIGURE A-24: POSSIBLE REDUNDANT CONFIGURATIONS RESULTING FROM ALLOCATION STUDY

Duplicating Element B only, as in Figure A-24b,

$$R_2 = 0.95 \, [1 - (0.50)^2]$$

$$= 0.712$$

Obviously, duplicating Element A contributes little to increasing reliability.

Triplication of B gives the configuration shown in Figure A-24c and

$$R_3 = 0.95 \, [1 - (0.5)^3]$$

$$= 0.831$$

R_3 gives a 75% increase in original circuit reliability as compared to the 58% increase of R_1.

If complexity is the limiting factor, duplicating systems is generally preferred to duplicating elements, especially if switching devices are necessary. If another series path is added in parallel, we have the configuration in Figure A-24d, and

$$R_4 = 1 - (1 - .475)^2$$

$$= 0.724$$

R_4 is only slightly less than R_1. If switches are necessary for each redundant element, R_4 may be the best configuration. A careful analysis of the effect of each element and switch on system reliability is a necessary prerequisite for proper redundancy application.

REDUNDANCY-WITH-REPAIR

In certain instances it may be more practical to design a system with built-in "on line" maintenance features to overcome a serious reliability problem than to concentrate on improving reliability of the components giving rise to the problem. Redundancy with repair can be made to approach the upper limit of reliability (unity), contingent on the rate with which element failures can be detected and repaired or replaced. The system thus continues on operational status while its redundant elements are being repaired or replaced, as long as these repairs are completed before their respective redundant counterparts also fail.

There are, in general, two types of monitoring that may be used for failure detection in systems employing redundant elements.

(1) Continuous Monitoring. Element failures are recognized at the instant they occur and repair or replacement action begins immediately. It is assumed that repairs can be made at the rate of μ per hour, where μ is the mean of an exponential distribution of repair times.

(2) Interval Monitoring. The system is checked for element failures every T hours. Failed elements are replaced with operable elements. Here it is assumed that the time required to monitor the elements and make replacements are negligible.

CONTINUOUS MONITORING

The reliability equation for two redundant elements is:

$$R(t) = \frac{s_1 e^{s_2 t} - s_2 e^{s_1 t}}{s_1 - s_2}$$

In the case of operative redundancy

$$s_1 = -\frac{1}{2}\left[(3\lambda + \mu) + \sqrt{\mu^2 + 6\mu\lambda + \lambda^2}\right]$$

$$s_2 = -\frac{1}{2}\left[(3\lambda + \mu) - \sqrt{\mu^2 + 6\mu\lambda + \lambda^2}\right]$$

For standby redundancy

$$s_1 = -\frac{1}{2}\left[(2\lambda + \mu) + \sqrt{\mu^2 + 4\mu\lambda}\right]$$

$$s_2 = -\frac{1}{2}\left[(2\lambda + \mu) - \sqrt{\mu^2 + 4\mu\lambda}\right]$$

The reliability equations for these two cases are plotted in Figure A-25 and A-26.

Example: Two similar elements with MTBFs of 100 hours are to be used as a redundant pair. The mean-time-to-repair for each element is 10 hours. Determine the reliability of the pair for a 23-hour mission when used as (1) an operative redundant pair, and (2) a standby redundant pair.

The graphs of the reliability equations, Figures A-25 and A-26, are given in term of λt and μ/λ. From the information given, $\lambda = 1/MTBF = 10^{-2}$, t = 23 hours, and $\mu = 1/(\text{repair time}) = 10^{-1}$. Hence, $\lambda t = .23$ and $\mu/\lambda = 10$. By means of the graphs, the reliability for the two cases is found to be:

Operative redundancy: R(23 hours) = .9760

Standby redundancy: R(23 hours) = .9874

When comparing the reliability of two situations that exceed .90, as above, it is more meaningful to compare the unreliabilities. In this case, a comparison of .0240 versus .0126 shows about a 2-to-1 difference
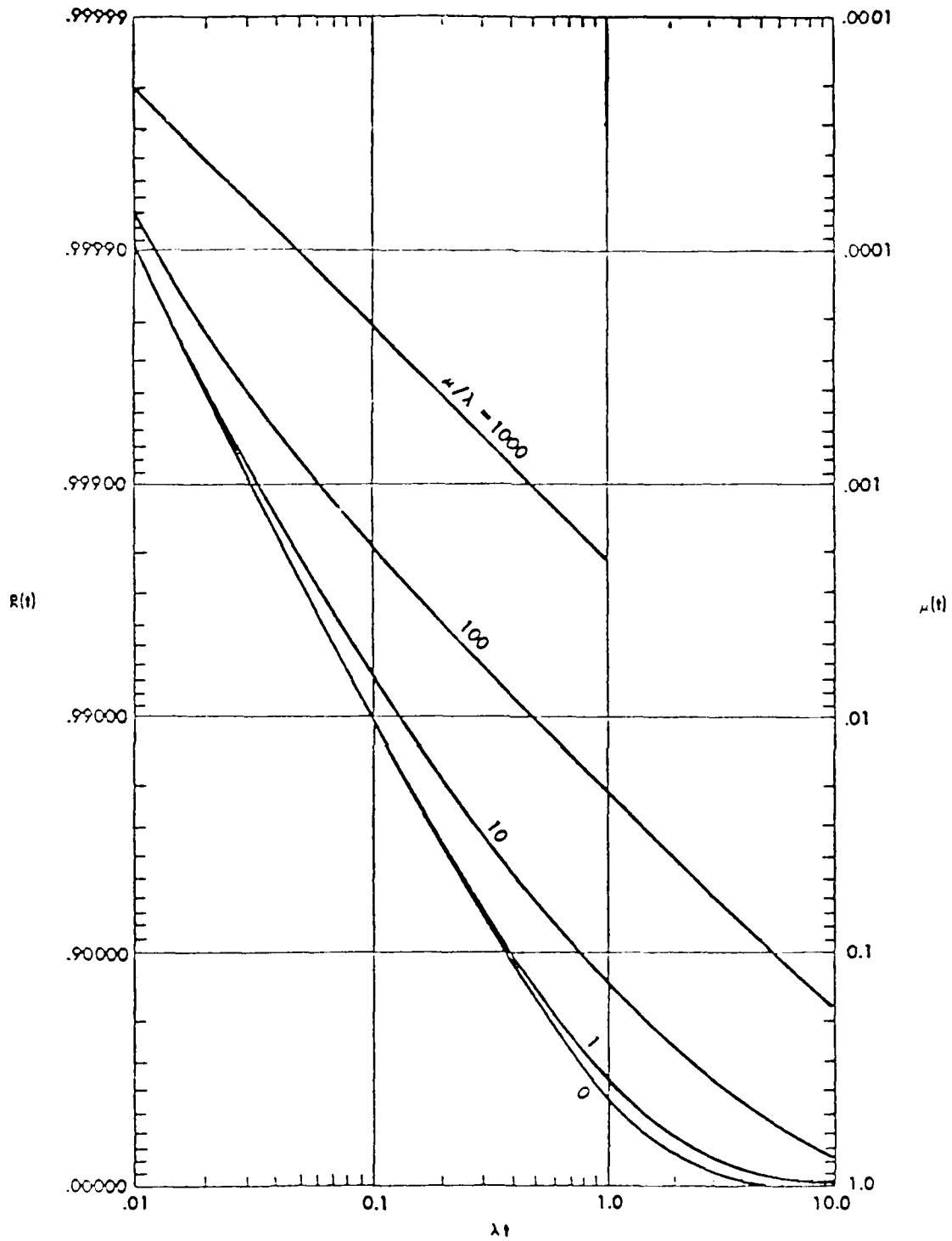
FIGURE A-25: OPERATIVE REDUNDANCY-WITH-REPAIR (CONTINUOUS MONITORING)
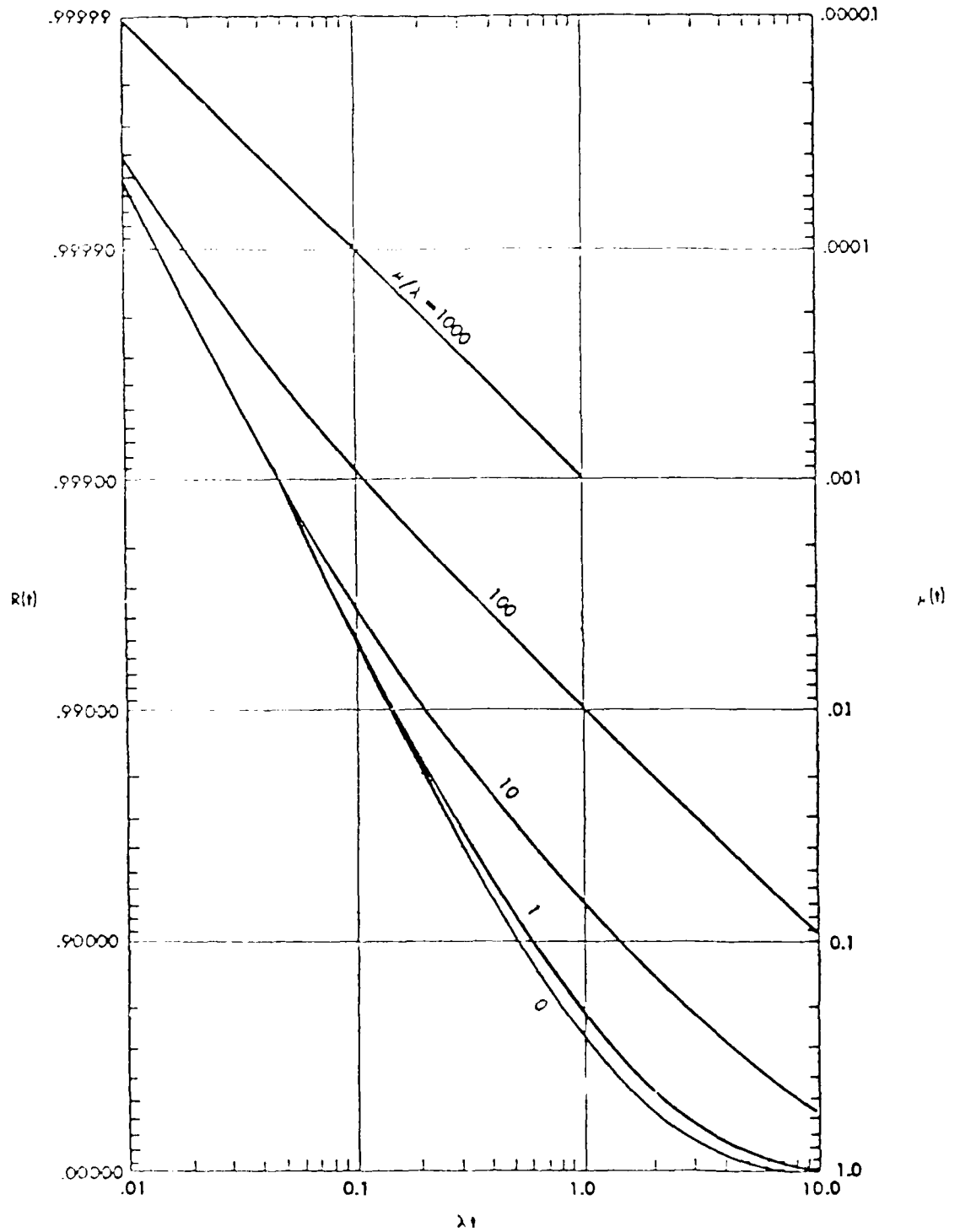
FIGURE A-26:   STANDBY REDUNDANCY-WITH-REPAIR (CONTINUOUS MONITORING)

in unreliability between the operative and the standby case, in favor of the latter.

INTERVAL MONITORING

The reliability equations for interval monitoring require that the mission time be expressed as two components, $t = nT + d$. The number of times the elements will be monitored during the mission (t) is given by n; T is the time interval between monitoring points; and d is the time between the last monitoring point and the end of the mission. Module replacement or switching time is assumed to be zero.

For operative redundancy:

$$R(t) = (2e^{-\lambda d} - e^{-2\lambda d})(2e^{-\lambda T} - e^{-2\lambda T})^n$$

For standby redundancy:

$$R(t) = (1 + \lambda T)^n (1 + \lambda d)e^{-\lambda t}$$

Example: Two similar elements with MTBFs of 100 hours are to be used as a redundant pair. The pair will be monitored every three hours. When a defective element is found, it will be replaced by an operable element immediately. We wish to determine the reliability of the pair for a 23-hour mission when used as an operative redundant pair. From the above, it is determined that $t = 23$ hours, $n = 7$, $nT = 21$, and $d = 2$ hours. As in the previous example, $\lambda = 10^{-2}$.

$$R(23 \text{ hours}) = (2e^{-.02} - e^{-.04})(2e^{-.03} - e^{-.06})^7$$

$$= .9935$$

Figure A-27 presents reliability functions normalized with respect to operating time t/θ, for five cases of T/θ monitoring intervals. This illustrates the reliability potential of designs which provide this redundancy with interval monitoring and on line repair capability.
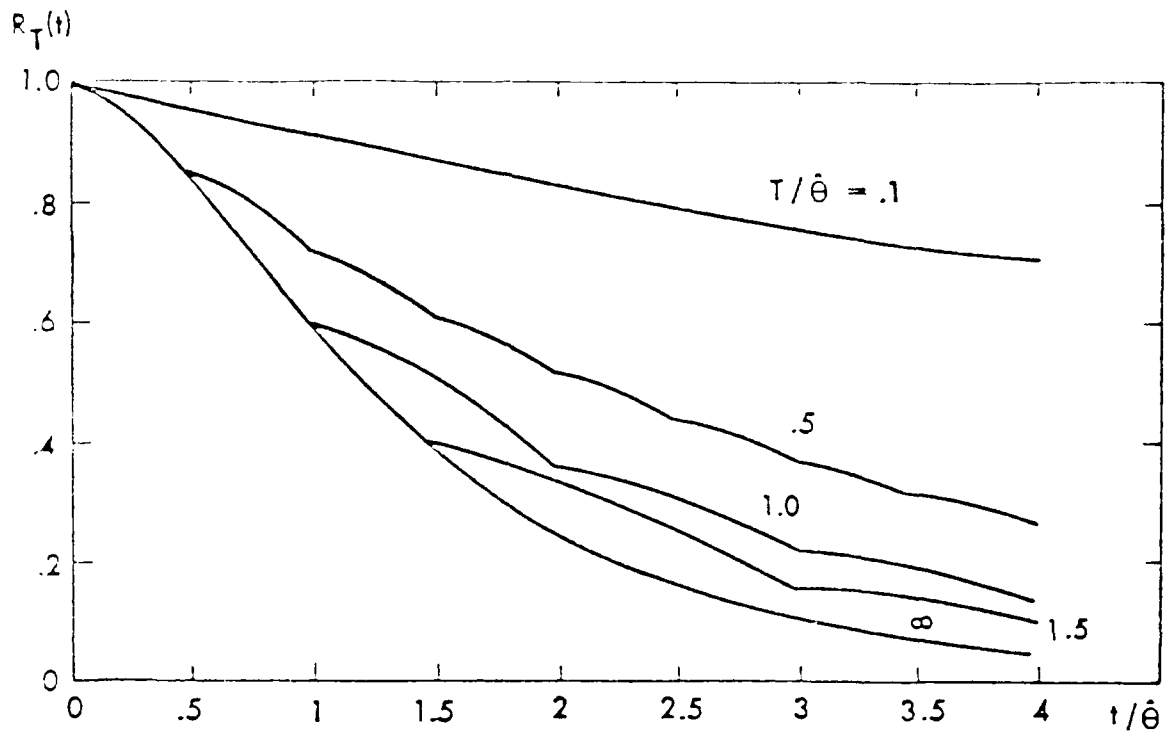
FIGURE A-27: RELIABILITY FUNCTIONS FOR SEVERAL CASES OF INTERVAL MONITORING AND REPAIR

APPENDIX B: ENVIRONMENTAL CONSIDERATIONS IN DESIGN

ENVIRONMENTAL STRENGTH

In order to fully realize the benefits of a reliability oriented design, consideration must be given early in the design process to the required environmental strength of the equipment being designed. The environmental strength, both intrinsic, and that provided by specifically directed design features, will singularly determine the ability of the equipment to withstand the harmful stresses imposed by the environment in which the equipment will be operated. The first step for determining the required environmental strength is the identification and detailed description of the environments in which the equipment must operate. The next step is to determine the performance of the parts and materials that comprise the equipment when exposed to the degrading stresses of the identified environments. When performance is inadequate/marginal with regard to the equipment reliability goals, corrective measures such as derating, redundancy, protection from adverse environments, or selection of more resistant materials and parts are necessary. This fulfills the reliability requirements of the equipment.

To design inherently reliable equipment, the design engineer must take into account the environment in which the equipment is to operate, with relation to the ideal operating conditions for the elements which make up the equipment. Each item in a system has its own failure rate based upon the conditions under which it operates.

MIL-STD-210 (Climatic Extremes for Military Equipment) establishes climatic design criteria for material intended for worldwide usage. It provides design conditions for land, sea, and air in which equipment will be required to operate (or be stored). The standard breaks down climate extremes into three categories -- ground, naval surface and air, and worldwide air. For these three categories, the climatic conditions for which values and factors are presented include temperature, humidity, precipitation, atmospheric pressure, and many others. MIL-STD-210 is the baseline document from which climatic environmental conditions are derived. Operating conditions may vary considerably from climatic conditions due to changes caused by system operation, e.g., equipment heating. The designer may have to overcome climatic problems experienced with parts by using special parts. These parts will operate at low temperature, incorporate pre-heating arrangements, utilize temperature tolerant lubricants or other methods of adjusting for climatic conditions.

ENVIRONMENTAL FACTORS

Since reliability is strongly dependent upon the operating conditions that are encountered during the entire life of the equipment, it is important that such conditions are accurately identified at the beginning of the design process. Environmental factors which exert a strong influence on equipment reliability are included in Table B-1, which provides a checklist for environmental coverage.

Concurrent (combined) environments may be more detrimental to reliability than the effects of a single environment. In characterizing the design process, the developed design/test criteria must consider both the single and/or combined environments in anticipation of providing hardware capability to withstand the hazards of the system profile. Figure B-1 illustrates the effects of combined environments (typical) in a matrix relationship. It shows the combinations where the total effect is more damaging than the cumulative effect of each environment acting independently. The exposure of an item to concurrent environments whose effects are more damaging than the cumulative effect of environments acting singly, may include a combination such as temperature, humidity, altitude, shock, and vibration while an item is being transported. The item's acceptance to its end-of-life sequence must be examined for these effects. Table B-2 provides reliability considerations for pairs of environmental factors.

TABLE B-1: ENVIRONMENTAL COVERAGE CHECKLIST (TYPICAL)

Natural	Induced
Clouds	Acceleration
Fog	Electromagnetic, Laser
Freezing Rain	Electrostatic, Lightning
Frost	Explosion
Fungus	Icing
Geomagnetism	Radiation, Electromagnetic
Gravity, Low	Radiation, Nuclear
Hail	Shock
Humidity, High	Temperature, High, Aero. Heating
Humidity, Low	Temperature, Low, Aero. Cooling
Ice	Turbulence
Ionized Gases	Vapor Trails
Lightning	Vibration, Mechanical
Meteoroids	Vibration, Acoustic
Pollution, Air	
Pressure, High	
Pressure, Low	
Radiation, Cosmic, Solar	
Radiation, Electromagnetic	
Rain	
Salt Spray	
Sand and Dust	
Sleet	
Snow	
Temperature, High	
Temperature, Low	
Wind	

MIL-HDBK-338-1A

FIGURE B-1: EFFECTS OF COMBINED ENVIRONMENTS

B-3

TABLE B-2: VARIOUS ENVIRONMENTAL PAIRS

High Temperature and Humidity	High Temperature and Low Pressure	High Temperature and Salt Spray
High temperature tends to increase the rate of moisture penetration. The general deterioration effects of humidity are increased by high temperatures.	Each of these environments depends on the other. For example, as pressure decreases, outgassing of constituents of materials increases, and as temperature increases, the rate of outgassing increases. Hence, each tends to intensify the effects of the other.	High temperature tends to increase the rate of corrosion caused by salt spray.
High Temperature and Solar Radiation	**High Temperature and Fungus**	**High Temperature and Sand and Dust**
This is a man-independent combination that causes increasing effects on organic materials.	A certain degree of high temperature is necessary to permit fungus and microorganisms to grow. But, above 160F (71ºC) fungus and microorganisms cannot develop.	The erosion rate of sand may be accelerated by high temperature. However, high temperatures reduce sand and dust penetration.
High Temperature and Shock and Vibration	**High Temperature and Acceleration**	**High Temperature and Explosive Atmosphere**
Since both of these environments affect common material properties, they will intensify each other's effects. The amount that the effects are intensified depends on the magnitude of each environment in the combination. Plastics and polymers are more susceptible to this combination than metals, unless extremely high temperatures are involved.	This combination produces the same effect as high temperature and shock and vibration.	Temperature has very little effect on the ignition of an explosive atmosphere, but it does affect the air-vapor ratio which is an important consideration.
Low Temperature and Humidity	**High Temperature and Ozone**	
Humidity decreases with temperature, but low temperature induces moisture condensation, and, if the temperature is low enough, frost or ice.	Starting at about 300ºF (150ºC), temperature starts to reduce ozone. Above about 520ºF (270ºC) ozone cannot exist at pressures normally encountered.	
Low Temperature and Solar Radiation	**Low Temperature and Low Pressure**	**Low Temperature and Salt Spray**
Low temperature tends to reduce the effects of solar radiation, and vice versa.	This combination can accelerate leakage through seals, etc.	Low temperature reduces the corrosion rate of salt spray.
	Low Temperature and Sand and Dust	**Low Temperature and Fungus**
	Low temperature increases dust penetration.	Low temperature reduces fungus growth. At sub-zero temperatures, fungi remain in suspended animation.

TABLE B-2: VARIOUS ENVIRONMENTAL PAIRS (Cont'd)

Environmental Pair	Description
Low Temperature and Shock and Vibration	Low temperature tends to intensify the effects of shock and vibration. It is, however, a consideration only at very low temperatures.
Low Temperature and Acceleration	This combination produces the same effect as low temperature and shock and vibration.
Low Temperature and Explosive Atmosphere	Temperature has very little effect on the ignition of an explosive atmosphere. It does however, affect the air-vapor ratio which is an important consideration.
Low Temperature and Ozone	Ozone effects are reduced at lower temperatures, but ozone concentration increases with lower temperatures.
Humidity and Low Pressure	Humidity increases the effects of low pressure, particularly in relation to electronic or electrical equipment. However, the actual effectiveness of this combination is determined largely by the temperature.
Humidity and Salt Spray	High humidity may dilute the salt concentration, but it has no bearing on the corrosive action of the salt.
Humidity and Fungus	Humidity helps the growth of fungus and microorganisms but adds nothing to their effects.
Humidity and Sand and Dust	Sand and dust have a natural affinity for water and this combination increases deterioration.
Humidity and Solar Radiation	Humidity intensifies the deteriorating effects of solar radiation on organic materials.
Humidity and Vibration	This combination tends to increase the rate of breakdown of electrical material.
Humidity and Shock and Acceleration	The periods of shock and acceleration are considered too short for these environments to be affected by humidity.
Humidity and Explosive Atmosphere	Humidity has no effect on the ignition of an explosive atmosphere, but a high humidity will reduce the pressure of an explosion.
Humidity and Ozone	Ozone meets with moisture to form hydrogen peroxide, which has a greater deteriorating effect on plastics and elastomers than the additive effects of moisture and ozone.
Low Pressure and Salt Spray	This combination is not expected to occur.
Low Pressure and Solar Radiation	This combination adds nothing to the overall effects.
Low Pressure and Fungus	This combination adds nothing to the overall effects.
Low Pressure and Sand and Dust	This combination only occurs in extreme storms during which small dust particles are carried to high altitudes.
Low Pressure and Vibration	This combination intensifies effects in all equipment categories but mostly with electronic and electrical equipment.
Low Pressure and Shock or Acceleration	These combinations only become important at the hyperenvironmental levels, in combination with high temperature.

TABLE B-2: VARIOUS ENVIRONMENTAL PAIRS (Cont'd)

Environmental Pair	Effect
Low Pressure and Explosive Atmosphere	At low pressures, an electrical discharge is easier to develop, but the explosive atmosphere is harder to ignite.
Salt Spray and Fungus	This is considered an incompatible combination.
Salt Spray and Dust	This will have the same combined effect as humidity and sand and dust.
Salt Spray and Vibration	This will have the same combined effect as humidity and vibration.
Salt Spray and Shock or Acceleration	These combinations will produce no added effects.
Salt Spray and Explosive Atmosphere	This is considered an incompatible combination.
Salt Spray and Ozone	These environments have the same combined effect as humidity and ozone.
Solar Radiation and Fungus	Because of the resulting heat from solar radiation, this combination probably produces the same combined effect as high temperature and fungus. Further, the ultraviolet in unfiltered radiation is an effective fungicide.
Solar Radiation and Sand and Dust	It is suspected that this combination will produce high temperatures.
Solar Radiation and Ozone	This combination increases the rate of oxidation of materials.
Fungus and Ozone	Fungus is destroyed by ozone.
Solar Radiation and Shock or Acceleration	Thses combinations produce no additional effects.
Solar Radiation and Vibration	Under vibration conditions, solar radiation deteriorates plastics, elastomers, oils, etc., at a higher rate.
Vibration and Acceleration	This combination produces increased effects when encountered with high temperatures and low pressures in the hyperenvironmental ranges.
Sand and Dust and Vibration	Vibration might possibly increase the wearing effects of sand and dust.
Shock and Vibration	This combination produces no added effects.
Solar Radiation and Explosive Atmosphere	This combination produces no added effects.

Each of the environmental factors, if present, requires determination of its impact on the operational and reliability characteristics of the materials and parts comprising the equipment being designed. It also requires the identification of packaging techniques that afford the necessary protection against such degrading factors.

In the environmental stress identification process that precedes the selection of environmental strength techniques, it is essential that stresses associated with all life intervals of the equipment be considered. This includes not only the operational and maintenance environments, but also the pre-operational environments, when stresses imposed on the parts during manufacturing assembly, inspection, testing, shipping, and installation may have significant impact on the eventual reliability of the equipment. Stresses imposed during the pre-operational phase are often overlooked. They may, however, represent a particularly harsh environment which the equipment must withstand. Often, the environments to which systems are exposed during shipping and installation are more severe than those it will encounter under normal operating conditions. It is also probable that some of the environmental strength features that are contained in a system design pertain to conditions that are encountered in the pre-operational phase, and not in conditions that the equipment experiences after being put into operation.

Environmental stresses affect parts in different ways. Table B-3 illustrates the principal effects of typical environments on system parts and materials.

High temperatures impose a severe stress on most electronic items since they can cause not only catastrophic failure such as melting of solder joints and burnout of solid state devices, but also slow progressive deterioration of performance levels due primarily to chemical degradation effects. It is often stated that excessive temperature is the primary cause of poor reliability in electronic equipment.

In electronic systems design, great emphasis is placed on small size and high part densities. This generally requires a cooling system to provide a path of low thermal resistance from heat producing elements to an ultimate heat sink of reasonably low temperature.

Solid state parts are generally rated in terms of maximum junction temperatures. The thermal resistance from this point to either the case or to free air are usually specified. The specification of maximum ambient temperature for which a part is suitable is generally not a sufficient method for part selection, since the surface temperatures of a particular part can be greatly influenced by heat radiation or heat conduction effects from nearby parts. These effects can lead to overheating, even though an ambient temperature rating appears not to be exceeded. It is preferable to specify thermal environment ratings such as equipment surface temperatures, thermal resistance paths associated

TABLE B-3: ENVIRONMENTAL EFFECTS (SHEET 1 OF 3)

ENVIRONMENT	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED

High temperature	Thermal aging:
	  Oxidation
	  Structural change
	  Chemical reaction
	Softening, melting, and sublimation
	Viscosity reduction and evaporation
	Physical expansion
		Insulation failure;
		Alteration of electrical properties.
		
		Structural failure.
		Loss of lubrication properties.
		Structural failure;
		Increased mechanical stress;
		Increased wear on moving parts.

Low temperature	Increased viscosity and solidification Ice formation Embrittlement Physical contraction	Loss of lubrication properties. Alteration of electrical properties. Loss of mechanical strength; Cracking, fracture. Structural failure; Increased wear on moving parts.

High relative humidity	Moisture absorption
	
	Chemical reaction
	  Corrosion
	  Electrolysis
		Swelling, rupture of container;
		Physical breakdown;
		Loss of electrical strength.
		Loss of mechanical strength;
		Interference with function;
		Loss of electrical properties;
		Increased conductivity of insulators.

Low relative humidity	Desiccation
	  Embrittlement
	  Granulation
		Loss of mechanical strength;
		Structural collapse;
		Alteration of electrical properties,
		  "dusting".

High pressure	Compression	Structural collapse; Penetration of sealing; Interference with function.
Low pressure	Expansion Outgassing Reduced dielectric strength of air	Fracture of container; Explosive expansion. Alteration of electrical properties; Loss of mechanical strength. Insulation breakdown and arc-over; Corona and ozone formation.

TABLE B-3: ENVIRONMENTAL EFFECTS (SHEET 2 OF 3)

ENVIRONMENT	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED
Solar radiation	Actinic and physiochemical reactions: Embrittlement	Surface deterioration; Alteration of electrical properties; Discoloration of materials; Ozone formation.
Sand and dust	Abrasion Clogging	Increased wear. Interference with function; Alteration of electrical properties.
Salt spray	Chemical reactions: Corrosion Electrolysis	Increased wear; Loss of mechanical strength; Alteration of electrical properties; Interference with function. Surface deterioration; Structural weakening; Increased conductivity.
Wind	Force application Deposition of materials Heat loss (low velocity) Heat gain (high velocity)	Structural collapse; Interference with function; Loss of mechanical strength. Mechanical interference and clogging; Abrasion accelerated. Accelerates low-temperature effects. Accelerates high-temperature effects.
Rain	Physical stress Water absorption and immersion Erosion Corrosion	Structural collapse. Increase in weight; Aids heat removal; Electrical failure; Structural weakening. Removes protective coatings; Structural weakening; Surface deterioration. Enhances chemical reactions.
Temperature shock	Mechanical stress	Structural collapse or weakening; Seal damage.

TABLE B-3: ENVIRONMENTAL EFFECTS (SHEET 3 OF 3)

ENVIRONMENT	PRINCIPAL EFFECTS	TYPICAL FAILURES INDUCED
High-speed particles (nuclear Irradiation)	Heating Transmutation and ionization	Thermal aging; Oxidation. Alteration of chemical, physical, and electrical properties; Production of gases and secondary particles.
Zero gravity	Mechanical stress Absence of convection cooling	Interruption of gravity-dependent functions. Aggravation of high-temperature effects.

Ozone	Chemical reactions:
	  Crazing, cracking
	  Embrittlement
	  Granulation
	  Reduced dielectric strength of air
		Rapid oxidation;
		Alteration of electrical properties;
		Loss of mechanical strength;
		Interference with function.
		Insulation breakdown and arc-over.

Explosive decompression	Severe mechanical stress	Rupture and cracking; Structural collapse.

Dissociated gases	Chemical reactions:
	
	  Contamination
	  Reduced dielectric strength
		Alteration of physical and electrical properties.
		
		Insulation breakdown and arc-over.

Acceleration	Mechanical stress	Structural collapse.
Vibration	Mechanical stress Fatigue	Loss of mechanical strength; Interference with function; Increased wear. Structural collapse.
Magnetic fields	Induced magnetization	Interference with function; Alteration of electrical properties; Induced heating.

with conduction, convection and radiation effects, and cooling provisions such as air temperature, pressure and velocity. In this manner, the true thermal state of the temperature sensitive internal elements can be determined. Reliability improvement techniques for high temperature stress include the use of heat dissipation devices, cooling systems, thermal insulation, and heat withstanding materials.

Low temperatures experienced by electronic equipment can also cause reliability problems. These problems are usually associated with mechanical elements of the system. They include mechanical stresses produced by differences in the coefficients of expansion(contraction) of metallic and nonmetallic materials, embrittlement of nonmetallic components, mechanical forces caused by freezing of entrapped moisture, stiffening of liquid constituents, etc. Typical examples include cracking of seams, binding of mechanical linkages, and excessive viscosity of lubricants. Reliability improvement techniques for low temperature stress include the use of heating devices, thermal insulation and cold withstanding materials.

Additional stresses are produced when electronic equipment is exposed to sudden changes of temperature or rapidly changing temperature cycling conditions. These conditions generate large internal mechanical stresses in structural elements, particularly when dissimilar materials are involved. Effects of the thermal shock induced stresses include cracking of seams, delamination, loss of hermeticity, leakage of fill gases, separation of encapsulating components from components and enclosure surface leading to the creation of voids, and distortion of support members.

A thermal shock test is generally specified to determine the integrity of solder joints since such a test creates large internal forces due to differential expansion effects. Such a test has also been found to be instrumental in creating segregation effects in solder alloys leading to the formulation of lead-rich zones which are susceptible to cracking effects.

Electronic equipment is often subjected to environmental shock and vibration both during normal use and testing. Such environments can cause physical damage to parts and structural members when deflections produced cause mechanical stresses which exceed the allowable working stress of the constituent parts.

The natural frequencies of items comprising the equipment are important parameters which must be considered in the design process since a resonant condition can be produced if a natural frequency is within the vibration frequency range. The resonance condition will greatly amplify the deflection of the subsystem and may increase stresses beyond the safe limit.

The vibration environment can be particularly severe for electrical connectors, since it may cause relative motion between members of the connector. This motion, in combination with other environmental stresses, can produce fret corrosion. This generates wear debris and causes large variations in contact resistance. Reliability improvement techniques for vibration stress include the use of stiffening, control of resonance, and reduced freedom of movement.

Humidity and salt air environments can cause degradation of equipment performance since they promote corrosion effects in metallic components. They can also foster the creation of galvanic cells, particularly when dissimilar metals are in contact. Another deleterious effect of humidity and salt air atmospheres is the formation of surface films on nonmetallic parts. These films cause leakage paths and degrade the insulation and dielectric properties of these materials. Absorption of moisture by insulating materials can also cause a significant increase in volume conductivity and the dissipation factor of materials so affected. Reliability improvement techniques for humidity and salt environments include the usage of hermetic sealing, moisture resistant material, dehumidifiers, protective coatings, protective covers, and reduced use of dissimilar metals.

Electromagnetic and nuclear radiation can cause disruption of performance levels and, in some cases, permanent damage to exposed equipment. It is important, therefore, that such effects be considered in determining tne required environmental strength for electronic equipment that must achieve a specified reliability goal.

Electromagnetic radiation often produces interference and noise effects within electronic circuitry which can impair the functional performance of the system. Sources of these effects include corona discharges, lightning discharges, spaiking, and arcing phenomena. These may be associated with high voltage transmission lines, ignition systems, brush type motors, and even the equipment itself. Generally, the reduction of interference effects requires incorporation of filtering and shielding features, or the specification of less susceptible components and circuitry.

Nuclear radiation can cause permanent damage by alteration of the atomic or molecular structure of dielectric and semiconductor materials. High energy radiation can also cause ionization effects which degrade the insulation levels of dielectric materials. The mitigation of nuclear radiation effects typically involves the use of materials and parts possessing a higher degree of radiation resistance, and the incorportion of shielding and hardening techniques.

Each of the environmental factors experienced by an item in its total life cycle requires consideration in the design process. This assures that adequate environmental strength is incorporated into the design for reliability.

SYSTEM USE CONDITIONS AND ENVIRONMENT

Each event and situation in the life cycle of an item can be related to environmental factors. These events and situations in the pre-operational, operational, and maintenance environments can be related to stresses, which the equipment must withstand to perform reliably. Table B-4 provides a typical system use conditions checklist. This list provides an aid to determine if environments have been adequately considered in the design for events and situations of an item's life cycle.

Table B-5 shows some effects of natural and induced environments during the various phases of the lifetime of an item. Table B-6 rates the importance of the environmental factors for the various regions of the environment.

MIL-STD-1670 ENVIRONMENTAL CRITERIA AND GUIDELINES FOR AIR LAUNCHED WEAPONS

(1) Provides guidelines for determining the environmental conditions to which air launched weapons will be subjected during the factory to target sequence (acceptance to end of useful life profile)

(2) Describes the tasks involved in applying the essential environmental design criteria in all phases of weapon development

(3) Provides the developer with background data on which to base environmental design and test requirements.

Starting with program initiation, the standard defines the requirements necessary for the development of information leading to full scale development. Usage information needed for delineation and examination of all probable environments that could affect reliability or operational capability of an air launched weapon includes the aircraft profile (launch to landing subphases), combat use tactics, store mix, etc., of the same nature as items shown in Table B-4. For reference, MIL-STD-1670 includes a method of presenting environmental criteria. This method is presented in Table B-7. It illustrates the major events, corresponding environments, and weapon status in a factory to target sequence. The air launched weapon must perform as required in this sequence subsequent to or while being subjected to the established environments.

For more detailed information on environments, see References 14-18.

TABLE B-4: <u>SYSTEM USE CONDITIONS CHECKLIST (TYPICAL) (SHEET 1 OF 2)</u>

HANDLING/TRANSFER	TRANSPORTATION
— CONUS	— CONUS
— Oversea Global Locality	— Oversea Global Locality
— Shore Station	— Truck Transport
— NWS	Flatbed truck, exposed
— Depot	Van, Truck
— Commercial Rework	Trailer
— Truck Transport	Containerized
— Rail Transport	— Rail Transport
— Air Transport	Boxcar
— Marine Transport	Flatcar
— Carrier Onboard Delivery (COD)	Containerized
Aviation spares airlift	— Air Transport
— Underway Replenishment (UNREP)	Turboprop
Vertical (Rotary Wing Aircraft)	Propeller
Cargo aircraft	Jet
Ram tensioned high line (RTHL)	— Marine Transport
High line transfer	Ammunition Ship (AE)
UNREP ship	Fast Combat Support Ship
— Launch Platform	(AOE)
Aircraft carrier	Cargo Ship (AK)
Expeditionary airfield	Other auxiliary ship (AKL,...)
Short Airfield for Tactical Support (SATS)	Ship hold
Non-aviation ship	Ship deck exposure
(AGC, AK, CA, DE, DLGN,...)	— NWS
— Operational	— Shore station
A/C handling, weapons handling	— Depot
Shipboard tie down	— Commercial rework
Land based tie down	— Packaging
Land based apron tie down	
Towing, Spotting	
Handling equipment	
Maintenance test	
Maintenance shop	
Avionics maintenance van	
A/C elevator vertical transit	
A/C cyclic turnaround	
Hangar/flight deck	
Mobile maintenance facility	
Flight deck to storage, storage to	
flight deck	

TABLE B-4: SYSTEM USE CONDITIONS CHECKLIST (TYPICAL) (SHEET 2 OF 2)

STORAGE	OPERATIONAL
— CONUS	— Natural environment
— Oversea global locality	— Induced environment
— Shore station	— Combined environment
— NWS	— Catapult launch
— Depot	— Arrested landing
— Commercial rework	— Store separation
— Igloo magazine	— Weapon release
— Uninsulated building	— Weapon delivery
— Roofed Structure — no sidewalls	— Weapon exhaust impingement
— Dump storage, exposed	— Weapon to weapon
— Dump storage, revetment	— Weapon to A/C
— Railroad siding	— A/C to weapon
— Store item	— A/C taxi
— Weapons item	— Jet exhaust backflow
— Explosives item	— Helicopter In-flight Refueling (HIFR)
— Aircraft carrier	— Probe/drogue refueling
— Expeditionary airfield	— Buddy tanker
— SATS	— Jet blast (other aircraft)
— Non-aviation ship	— Jet blast (VTOL)
— Long term	— Mission mix
— Short term	— Store mix
— Interim	— Combat tactics
— Maintenance shop	— Operational deployment
— Avonics maintenance van	— A/C /weapons maneuvers
— Mobile maintenance facility	— Equipment location
— Containerization	— Flight line operations
— Packaging	— Chance of environment encounter
	— Launch platform

MISSION REGIME	STORAGE	TRANSPORT-ATION	STAND BY (IDLE)	STAND BY (ACTIVE)	USE	MAINTE-NANCE
Aridity	x				o	
Asteroids						
Birds	o				❷	❷
Clouds				o	o	
Cosmic Radiation					x	
Density, Air					o	
Dust, Interplanetary						
Dust, Lunar						
Dust, Terrestrial	❷	x	x	o		❷
Electricity, Atmospheric					❷	
Fog	x		x	o		o
Frost	x		x	o		x
Fungi	x					x
Geomagnetism					o	
Gravity				.	o	
Heat	x	x	x	❷	❷	x
Humidity	x	x	x	❷	❷	x
Icing	x	x	❷	❷	❷	❷
Ionized Gases					❷	
Insects	❷	❷	❷	❷	❷	❷
Lightening	x	x	x	❷	❷	❷
Meteroids						
Ozone					x	
Pollution, Air	x	x	x			❷
Pressure, Air				o	❷	o
Rain	x	x	x	❷	❷	❷
Salt Atmosphere	x	x	❷	❷		❷
Snow and Sleet	x	x	❷	❷	❷	
Solar Flares						
Solar Radiation	x					x
Temperature	x	x	x	o	o	❷
Temperature Shock		x		x	x	x
Terrain		x				❷
Trapped Radiation (Van Allen)						
Turbulance				❷	❷	❷
Wind, Gust, Sheer	x	x	x	❷	❷	❷

(Left vertical label: MAN-INDEPENDENT ENVIRONMENTS)

Table B-5: ENVIRONMENTAL ANALYSIS

TABLE 3-5: <u>ENVIRONMENTAL ANALYSIS (CONTINUED)</u>

MISSION REGIME		STORAGE	TRANSPORT-ATION	STAND BY (IDLE)	STAND BY (ACTIVE)	USE	MAINTE-NANCE
INDUCED ENVIRONMENTS	Acceleration				⊜	⊜	
	Acoustic Vibration			⊜	⊜	⊜	
	Countermeasures					⊜	
	Enemy Action	x	x	x	⊜	⊜	
	Explosive Atmosphere						
	Flutter					⊜	
	Ionized Gases					x	
	Magnetic Fields				o	o	o
	Moisture	x		x	⊜	⊜	⊜
	Nuclear Radiation				x	⊜	⊜
	Pressure					⊜	
	Shock		x		x	⊜	x
	Temperature			⊜	⊜	⊜	
	Temperature Shock			⊜	⊜	⊜	
	Vibration		x		x	x	x

EFFECTS:

o - Operational

x - Mechanical/Physical

⊜ - Either or both

Operational effects: Function, mission, etc., influenced, rather than direct physical alteration of item. Example: Reduced visibility caused by fog.

Mechanical/Physical effect: Direct physical alteration of item. Examples: Corrusion, fracture, puncture, melting.

TABLE B-6: ASSOCIATION OF FACTOR IMPORTANCE WITH REGION OF ENVIRONMENT

Environmental factor

Region of the environment	Terrain	Temperature	Humidity	Pressure	Solar radiation	Rain	Solar precipitation	Fog	Wing	Salt	Ozone	Macrobiological organism	Microbiological organism	Atmospheric pollutants	Sand and dust	Vibration	Shock	Acceleration	Acoustics	Electromagnetic radiation	Nuclear radiation
Storage	O	A	A	C	O	O	O	O	O	C	C	B	B	C	C	C	B	O	O	O	O
Transportation																					
Highway	A	B	B	O	C	B	B	B	C	O	O	O	O	O	C	A	A	C	O	O	O
Rail	A	B	B	O	C	C	B	C	C	O	O	O	O	O	C	A	A	C	O	O	O
Ship	O	C	B	O	C	C	O	B	C	B	O	C	O	O	O	B	C	C	O	O	O
Air	O	B	O	C	O	C	C	A	B	O	O	O	O	O	C	B	B	B	O	O	O
Operational use																					
Cold regions	A	A	A	O	B	A	A	B	B	C	O	C	O	C	C	B	B	O	C	B	C
Hot-wet	A	A	A	C	B	A	O	O	B	B	O	C	A	O	O	B	B	O	C	B	C
Hot-dry	A	A	O	C	A	O	O	O	B	B	O	O	O	O	A	B	B	O	C	B	C
Temperate	A	A	A	C	B	A	B	B	B	B	C	C	B	C	B	B	B	O	O	B	O
Indoor use	O	B	B	O	O	O	O	O	O	O	O	C	C	C	B	C	O	O	O	B	O
Operational storage	O	A	A	O	B	B	B	O	C	B	C	B	B	C	C	O	C	O	O	C	C

A - Major importance
B - Important
C - Minor
O - Absent

TABLE B-7: AIR-LAUNCHED WEAPON SAMPLE ENVIRONMENTAL CRITERIA (SHEET 1 OF 4)

ENVIRONMENT/EVENT	TRANSPORTATION			
	TRUCK	RAIL	SHIP	AIR (FLIGHT)
Air Temp/Time (high)	Fig. 1*	Fig. 1*	Fig. 3*	Fig. 5*
Air Temp/Time (low)	Fig. 2*	Fig. 2*	40^OF for 24 hrs	Fig. 1*
Relative humidity	Fig. 12*	Fig. 12*	Fig. 12*	Fig. 12*
Rain	50 mm/hr for 1 hr	50 mm/hr for 1 hr	50 mm/hr for 1 hr	NA
Ice and hail	25 mm/hr 50 mm build-up	25 mm/hr 50 mm build-up	25 mm/hr 50 mm buildup	NA
Snow	250 mm/hr for 1/2 hr	250 mm/hr for 1/2 hr	250 mm/hr for 1/2 hr	NA
Corrosion rates	Negligible (time dependent)	Negligible (time dependent)	Negligible (time dependent)	Negligible (time dependent)
Sand and dust	45 knot wind .015 to 3.2 mm dia particle size	45 knot wind .015 to 3.2 mm dia particle size	NA	NA
Shock	3.5 g for 25-50 ms half sine wave	25 g for 25 ms half sine wave	80 g, 4 ms vert	Negligible
Vibration (peak values)	Fig. 8*	Fig. 9*	Fig. 10*	Fig. 11*
Electromagnetic environment	To be determined			
Acoustic	Negligible	Negligible	Negligible	Negligible
Altitude	Sea level to 10,000 ft	Sea level to 10,000 ft	Sea level	10,000 ft
Fungus	Use non-nutrient materials only			

←————————MISSILE IS IN SHIPPING CONTAINER————————→

*Figures are contained MIL-STD-1670

TABLE B-7: AIR-LAUNCHED WEAPON SAMPLE ENVIRONMENTAL CRITERIA (SHEET 2 OF 4)

ENVIRONMENT/EVENT	STORAGE			AT SEA TRANSFER
	IGLOO	COVERED	DUMP	
Air Temp/Time (high)	100°F for 24 hrs	Fig. 1*	Fig. 6*	Fig. 7*
Air Temp/Time (low)	0°F for 72 hrs	-10°F for 72 hrs	-40°F for 72 hrs	30°F for 24 hrs
Relative humidity	Fig. 12*	Fig. 12*	Fig. 12*	Fig. 12*
Rain	NA	Negligible	50 mm/hr for 1 hr	50 mm/hr for 1 hr
Ice and hail	NA	Negligible	25 mm/hr for 1 hr	Negligible
Snow	NA	Negligible	250 mm/hr for 1/2 hr	Negligible
Corrosive rates	0.1 in. of HRS/yr	0.1 in. of HRS/yr	0.1 in. of HRS/yr	Negligible (time dependent)
Sand and dust	Negligible	45-knot wind .015 to 3.2 mm dia particle size	45-knot wind .015 to 3.2 mm dia particle size	NA
Shock	NA	NA	NA	10 ft/sec impact velocity
Vibration	NA	NA	NA	Negligible
Electromagnetic environment	To be determined			
Acoustic	Negligible	Negligible	Negligible	Negligible
Fungus	Use non-nutrient materials only			
Immersion	NA	NA		
	←————— MISSILE IS IN SHIPPING CONTAINER —————→			

*Figures are contained in MIL-STD-1670

TABLE B-7: AIR-LAUNCHED WEAPON SAMPLE ENVIRONMENTAL CRITERIA (SHEET 3 OF 4)

ENVIRONMENT/EVENT	AIRFIELD		AIRCRAFT CARRIER	
	STORAGE	HANDLING	STORAGE	HANDLING
Air Temp/Time (high)	Fig. 6*	140°F for 2 hrs	Fig. 3*	110°F for 2 hrs
Air Temp/Time (low)	-40°F for 72 hrs	-40°F for 72 hrs	40°F for 24 hrs	30°F for 24 hrs
Relative humidity	Fig. 12*	Fig. 12*	Fig. 12*	Fig. 12*
Rain	50 mm/hr for 1 hr	50 mm/hr for 1 hr	NA	50 mm/hr for 1 hr
Ice and hail	25 mm/hr for 1 hr	25 mm/hr for 1 hr	NA	None
Snow	250 mm/hr for 1/2 hr	250 mm/hr for 1/2 hr	NA	None
Corrosion rates	0.1 in. of HRS/yr	Negligible (time dependent)	0.1 in. of HRS/yr	Negligible (time dependent)
Sand and dust	45-knot wind .015 to 3.2 mm dia particle size	45-knot wind .015 to 3.2 mm dia particle size	NA	NA
Acceleration loads	NA	NA	NA	NA
Shock	NA	15 g for 11-18 ms half sine wave	80 g, 4 ms vert	15 g for 11-18 ms half sine wave
Vibration	NA	Negligible	Refer to Fig. 10*	Negligible
Electromagnetic environment	To be determined			
Acoustic	Negligible	Negligible	Negligible	Negligible
Fungus	Use non-nutrient materials			
	Missile In Shipping Container	Missile Out of Container	Missile In Container	Missile Out of Container

*Figures are contained in MIL-STD-1670

TABLE B-7: AIR-LAUNCHED WEAPON SAMPLE ENVIRONMENTAL CRITERIA (SHEET 4 OF 4)

ENVIRONMENT/EVENT	ABOARD AIRCRAFT	LAUNCH TO TARGET
	VA	
Skin Temp/Time (high)	150°F for 10 min 120°F for 1 hr	Up to 187°F for 4 min
Skin Temp/Time (low)	-62°F for 4 hr	-3°F for 5 min
Relative humidity	Fig. 12*	Fig. 12*
Rain	Aircraft flight limitations	Aircraft flight limitations
Ice and hail	Aircraft flight limitations	Aircraft flight limitations
Snow	Aircraft flight limitations	Aircraft flight limitations
Corrosion	Negligible	NA
Sand and dust	.015 to 3.2 mm dia particle size, 100-knot relative velocity	NA
Acceleration	Fig. 27 and 28*	
Shock	15 g for 20 ms ±long. + vert	Fig. 13 & 14*
Vibration	Fig. 15 through 25*	Fig. 15 through 25*
Electromagnetic environment		
Acoustic	Fig. 26*	Fig. 26*
Gun blast	2 psi, plane wave 1 ms duration	NA
Ignition shock	NA	Half sine
Altitude	Refer to XAS-2070	
	←——————Missile Out Of Container——————→	

*Figures are contained in MIL-STD-1670.

APPENDIX C: RELIABILITY DESIGN CHECKLIST

Example taken from:

Reliability (R) and Maintainability (M)

Design Checklist

NAVSEA S0300-AC-MMA-010-R&M

October 1977

Obtainable from:

Naval Publications and Forms Center
5801 Tabor Ave
Philadelphia, Pennsylvania 19120

Attn: Code F01G

PRODUCTION FOLLOW ON

R/M PROGRAM ELEMENTS	TYPE OF CONTRACT					
	NEW DEVELOPMENT			MODIFIED DEVELOPMENT		
	A	B	C	A	B	C
PROGRAM PLAN	X	X	X	X	X	X
ORGANIZATION	X	X	X	X	X	X
SUBCONTRACTOR & SUPPLIER CONTROL	X			X		
PROGRAM REVIEW						
R ANALYSIS						
MODEL	X			X		
THERMAL ANALYSIS	X	X		X	X	
ALLOCATION	X			X		
PREDICTION						
SIMILARITY			X			X
AVERAGE STRESS		X			X	
DETAILED STRESS	X			X		
PART CONTROL	X	X		X	X	
FM&EA/FAULT TREE	X	X		X	X	
CRITICAL ITEM CONTROL	X	X		X	X	
STORAGE EFFECTS	X			X		
DESIGN REVIEW	X	X		X	X	

NOTE: See next page for explanation of A, B, and C, above.

R&M LEVELS

LEVEL A

- HIGH LEVEL OF SAFETY
- CRITICAL SYSTEM
- DOWNTIME CRITICAL, MAINTENANCE DIFFICULT AND EXPENSIVE

LEVEL B

- SAFETY FACTOR IN DESIGN
- MODERATELY CRITICAL SYSTEM
- MAINTENANCE MODERATELY DIFFICULT AND EXPENSIVE

LEVEL C

- SAFETY OF MINIMUM CONCERN
- LOW SYSTEM CRITICALITY
- DOWNTIME NOT CRITICAL

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
2.	**Management**			
(a)	Does contractor have a permanent in-house R staff?	—	—	
(b)	Is staff composed of experienced R engineers?	—	—	
(c)	Does program R engineer report directly to program manager?	—	—	
(d)	Does R group have the facility/authority to interface directly with other engineering groups:			
	(1) Design?	—	—	
	(2) Systems engineering?	—	—	
	(3) Quality Control?	—	—	
	(4) Integrated Logistics support?	—	—	
	(5) Procurement?	—	—	
	(6) Test and Evaluation?	—	—	
(e)	Is R group representative(s) member(s) of design review team?	—	—	
(f)	Does R group review all drawings and specifications for adequacy of R requirements?	—	—	
(g)	Does R program engineer have sign-off authority on all drawings and specifications?	—	—	
(h)	Does R engineer/group review Purchase Orders and Purchase specifications to assure all parts and subassemblies are procured with adequate R requirements?	—	—	
(i)	Does R group have membership and a voice in decisions for the following:			
	(1) Material Review Board?	—	—	
	(2) Failure Review Board?	—	—	
	(3) Engineering Change Review Board?	—	—	
(j)	Is R group represented on surveys and quality audits of potential subcontractors?	—	—	
(k)	Is R group represented at subcontractor design reviews and meetings where R is a topic of discussion?	—	—	
(l)	Does an R group member(s) monitor/witness subcontractor R tests?	—	—	
(m)	Does R group contain experts in the fields of components/failure analyses?	—	—	

RELIABILITY (R) DESIGN CHECKLIST

No	Item Description	Yes	No	Remarks
22	Design for R			

THERMAL REQUIREMENTS:

No	Item Description	Yes	No	Remarks
(a)	Have detailed thermal analysis been performed to determine component/module ambient operating temperature?	—	—	
(b)	Has a unit similar to final configuration (e.g., brassboard, preproduction unit, etc.), been instrumented to develop a thermal mapping of the design?	—	—	
(c)	Have anemometer probes been used to measure coolant air flow patterns?	—	—	
(d)	Are equipment internal cooling considerations sufficient to limit internal temperature rises to 20°C maximum?	—	—	
(e)	Are high power dissipation components (e.g., large power resistors, diodes, transformers, etc.) heat sinked?	—	—	
(f)	Where chilled water or chilled air is used for cooling have hermetically sealed components been selected due to possible moisture condensation?	—	—	
(g)	Where chilled water or chilled air is used for cooling are components shielded or otherwise protected from moisture condensation?	—	—	
(h)	Where chilled water or chilled air is used for cooling has consideration been given to removal of condensation to avoid accumulation of moisture and possible fungus growth or corrosion within the equipment?	—	—	
(i)	Are all printed circuit boards conformally coated?	—	—	
(j)	Have circuit performance tests been conducted at high and low temperature extremes to assure circuit stability over the required operating temperature range?	—	—	
(k)	Do heat conducting surfaces make good contact (no air gaps) and have low thermal resistances?	—	—	
(l)	Do surface coatings and paints provide good conduction, convection and radiation coefficients for heat transfer?	—	—	
(m)	Do adhesives where used for fastening components to PCB's or chassis have good thermal conductive properties?	—	—	
(n)	Do potting, encapsulation and conformal coating materials where used have good thermal conducting properties?	—	—	
(o)	Have differences in thermal expansion of interfacing materials been taken into account?	—	—	
(p)	Are high power dissipation components mounted directly to the chassis for better heat sinking rather than encapsulated or thermally insulated?	—	—	
(q)	Is thermal contact area between components and heat sinks kept to a maximum?	—	—	
(r)	Are components sensitive to heat located away from heat flow paths, power supplies and other high power dissipation components?	—	—	
(s)	Are air gaps or thermal insulation provided where necessary to avoid heat flow to temperature sensitive components?	—	—	
(t)	Are temperature overload devices/alarms used to prevent damage due to loss of cooling apparatus?	—	—	
(u)	Do inlet temperature ducts have filters to prevent accumulation of dirt on assemblies which would result in reduction of heat transfer?	—	—	
(v)	Do components mounted on PCB's have adequate lead lengths and are the leads formed to relieve lead stresses during thermal expansion and contraction?	—	—	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks

VIBRATION/SHOCK/STRUCTURAL REQUIREMENTS:

(w)   Has analysis been performed to determine resonant frequencies to be experienced in the equipment environment?   ___ ___

(x)   Have detailed vibration/shock/structural analyses been performed to validate structural integrity of the design?   ___ ___

(y)   Have critical/unique assemblies been instrumented with accelerometers and tested to verify design adequacy with respect to vibration and shock transmissibility factors?   ___ ___

(z)   Have structural mountings been designed to resonate away from resonant frequencies and their harmonics?   ___ ___

(aa) Have damping considerations been applied to sub-assemblies and components mounting where natural frequencies are close to expected environmental frequencies?   ___ ___

(bb) Are large components (over 1/2 oz.) being clamped or tied down to the chassis or printed circuit boards to prevent high stresses or fatigue failure of electrical leads?   ___ ___

(cc) Heavy components are mounted near corners of the chassis near mounting points for direct structural support rather than between supports?   ___ ___

(dd) Centers of gravity of heavy components are kept low close to the plane of the mounts?   ___ ___

(ee) Are cables/harnesses clamped close to terminal connections to avoid resonances and prevent stress and failure at the point of connection?   ___ ___

(ff) Do cables/wires have sufficient slack to prevent stresses during thermal changes and mechanical vibration/shock?   ___ ___

(gg) Stranded wire is used when cabling might be susceptible to fatigue failure?   ___ ___

(hh) Components and subassemblies have adequate sway space to avoid collision during vibration and shock?   ___ ___

(ii) Welding (not spot welding) and/or riveting is used for permanently attached structural members rather than nuts and bolts?   ___ ___

(jj) All component leads have minimum bend radii to avoid overstressing?   ___ ___

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
	MISCELLANEOUS REQUIREMENTS:			
(kk)	Has consideration been given to avoid the use of dissimilar metals?	—	—	
(ll)	Have the PCB's been designed for the following considerations:			
	(1) PCB material is compatible with storage and operating temperature (plus operating temperature rises) with respect to:			
	(1) PCB material?	—	—	
	(2) Metal cladding/bonding strengths?	—	—	
	(3) Board warping?	—	—	
	(2) PCB resistivity is sufficiently high to meet circuit leakage current requirements even under high humidity?	—	—	
	(3) PCB arc resistance is sufficiently high where high voltages are present?	—	—	
	(4) PCB dielectric constraint is sufficiently low to prevent building up of unwanted capacitances?	—	—	
	(5) PCB flexural strengths (function of board material and dimensions) is sufficient to meet structural and vibration requirements?	—	—	
	(6) PCB conductors width is sufficient to handle maximum current flow without harmful heat generation or resistance drop?	—	—	
	(7) PCB's have plated through holes to aid in soldering of lead electrical connections?	—	—	
	(8) PCB conductor spacings have a minimum spacing based upon voltage between conductor (e.g., .025" per 150 volts peak)?	—	—	
	(9) PCB conductor paths are spaced and designed to keep capacitance between conductors to a minimum?	—	—	
	(10) Are PCB's conformally coated?	—	—	
(mm)	Where encapsulation, embedding and potting used, does the material have:			
	(1) Good thermal conductivity for heat transfer?	—	—	
	(2) Good electrical isolation/dielectric?	—	—	
	(3) Provide dampening for shock and vibration?	—	—	
	(4) Thermal expansion coefficients which match those of items encapsulated?	—	—	
	(5) Will not crack or shatter under vibration and mechanical and thermal shock?	—	—	
	(6) Has good chemical stability under anticipated use environments?	—	—	
(nn)	Have worst case analyses or statistical variation of parameters been conducted to determine required component electrical tolerances considering:			
	(1) Manufacturing tolerances?	—	—	
	(2) Tolerances due to temperature changes?	—	—	
	(3) Tolerances due to aging?	—	—	
	(4) Tolerances due to humidity?	—	—	
	(5) Tolerances due to high frequency or other operating constraints?	—	—	
(oo)	Has redundancy been considered for critical functions where practical?	—	—	
(pp)	Where redundancy is used, has considerations been given to avoid common mode failure situations which could disable all redundant circuits?	—	—	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks

(qq) Has design practices been applied to obtain RFI suppression such as:

(1) Use alternating current non-commutating machinery rather than direct current machinery when feasible? ___ ___

(2) Provide optimum interference suppression with two twisted wires in a common shield whenever wire pairs can be used? ___ ___

(3) Use short wires in preference to long wires? ___ ___

(4) Filter power lines to remove harmonics and other types of inherent interference? ___ ___

(5) Mount filters as close to interference sources as possible without altering the effectiveness of the filter? ___ ___

(6) Use bonding techniques to insure that good electrical contact is made between chassis, conduit, shielding, connectors, structural and housing metal parts? ___ ___

(7) Remove non-conducting coatings from bolts, nuts, and tapped holes? ___ ___

(8) Internally shield individual sections of equipment which are either highly susceptible to interference or which generate interference. For example, the r-f input stages and local oscillators should be shielded individually? ___ ___

(9) Use a bandwidth consistent with the minimum possible value for the received signal. This often improves the signal-to-noise ratio? ___ ___

(10) Use direct current filament sources where practicable? ___ ___

(11) Ground center tap of filament transformer secondary winding to reduce hum? ___ ___

(12) Avoid the use of gaseous lighting devices in the vicinity of sensitive wiring or electronic equipment? ___ ___

(13) Do not cable noisy and clean leads together? ___ ___

(14) Never route cables near known interference sources? ___ ___

(15) Do not use shields or metal structures for return current paths? ___ ___

(16) Avoid the use of corrosion preventive compounds with high insulating qualities at bond joints? ___ ___

(rr) Have considerations been given to preclude damage due to:

(1) Installation? ___ ___
(2) Handling? ___ ___
(3) Transportation? ___ ___
(4) Storage? ___ ___
(5) Shelf Life? ___ ___
(6) Packaging? ___ ___
(7) Maintenance environment? ___ ___

(8) Other environments:
(a) Humidity? ___ ___
(b) Fungus? ___ ___
(c) Sand and dust? ___ ___
(d) Salt atmosphere? ___ ___

(ss) Has reliability been considered as a factor in all tradeoff studies affecting equipment reliability? ___ ___

RELIABILITY (R) DESIGN CHECKLIST

No	Item Description	Yes	No	Remarks
23	**Parts Program**			
(a)	Does contractor have a Parts Control Board (PCB) to promote proper selection and application of parts used in the design?	—	—	
(b)	Has contractor established and maintained an up-to-date Preferred Parts List (PPL) to be used by designers?	—	—	
(c)	Has contractor established derating guidelines for derating of electrical/electronic parts electrical stresses?	—	—	
(d)	Do derating guidelines correspond to specification requirements?	—	—	
(e)	Has contractor developed part application guidelines for proper selection of part types for circuit use?	—	—	
(f)	Are military grade parts used in the design?	—	—	
(g)	Are non-standard parts used only when a military equivalent part cannot be obtained?	—	—	
(h)	Where non-standard parts are used do they have adequate qualification/test data and a history of high reliability?	—	—	
(i)	Where non-standard parts are used are they procured via specification control drawing which specifies:			
	(1) Reliability requirements?	—	—	
	(2) Environmental requirements?	—	—	
	(3) Test requirements?	—	—	
(j)	Has contractor submitted non-standard part data for approval per applicable specification (e.g., MIL-STD-749/965)?	—	—	
(k)	Do parts used in the design meet the environmental requirements to which they will be subjected during use with respect to:			
	(1) Operating temperature (plus worst case internal case temperature rises)?	—	—	
	(2) Non-operating/storage temperature?	—	—	
	(3) Humidity?	—	—	
	(4) Vibration?	—	—	
	(5) Shock?	—	—	
(l)	Have parts been reviewed for proper application, have part stresses been calculated ( ) or measured ( ) and do they meet:			
	(1) Derating guidelines?	—	—	
	(2) Application guidelines?	—	—	
(m)	Are established reliability (ER) components and JAN semiconductors and microcircuit devices used in the design?	—	—	
(n)	Where ER components are used, is the most representative level of all ER components used:			
	(1) L ?	—	—	
	(2) M ?	—	—	
	(3) P ?	—	—	
	(4) R ?	—	—	
	(5) S ?	—	—	
	(6) T ?	—	—	
(o)	Where JAN semiconductors (MIL-S-19500) are used, the most representative level of all such devices used are:			
	(1) JAN ?	—	—	
	(2) JANTX ?	—	—	
	(3) JANTXV ?	—	—	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
(p)	Where JAN microcircuits (MIL-M-38510) or high quality microcircuits are used the most representative level of all such devices used are:			
	(1) MIL-M-38510 Class S ?	—	—	
	(2) MIL-M-38510 Class B ?	—	—	
	(3) MIL-M-38510 Class C ?	—	—	
	(4) MIL-STD-883 Class S ?	—	—	
	(5) MIL-STD-883 Class B ?	—	—	
	(6) MIL-STD-883 Class C ?	—	—	
	(7) Vendor equivalent to _____ ?	—	—	
(q)	Do parts meet the interchangeability requirements of MIL-STD-454 Requirement 7?	—	—	
(r)	Do all parts selected meet the life requirements of the equipment?	—	—	
(s)	Are handling requirements specified for critical and delicate parts susceptible to damage, degradation, contamination from shock, vibration, static electric discharge, uncleanliness, etc. ?	—	—	
(t)	Are assembly and cleaning procedures specified to prevent damage to components during assembly on PCB's, chassis, etc. ?	—	—	
(u)	Have dominant failure modes of a particular part type been considered in the selection of that part?	—	—	
(v)	Are fixed rather than variable components (such as resistors, capacitors, inductors, etc.) used in the design wherever possible?	—	—	
(w)	Are all relays, motors, dynamotors, rotary power converters, etc. suppressed so as not to produce excessive spikes or transients during operation ?	—	—	
(x)	Are all semiconductor devices silicon rather than Germanium ?	—	—	
(y)	Plastic coated and/or encapsulated semiconductor devices are not used?	—	—	
(z)	Do all microcircuits have hermetically sealed ceramic cases rather than plastic cases?	—	—	
(aa)	Do all microcircuits used have at least two potential suppliers?	—	—	
(bb)	Do all unused gates of a digital microcircuit have inputs grounded?	—	—	
(cc)	Are the number of expandable gates limited to no more than 75% of allowable number of expandables?	—	—	
(dd)	Where humidity is not controlled are hermetically sealed resistors, capacitors, relays, etc., used?	—	—	
(ee)	Are all power supplies designed and manufactured in-house ?	—	—	
(ff)	Are parts, even MIL-M-38510, JANTX, Established Reliability (ER) parts screened at incoming inspection:			
	(1) 100%?	—	—	
	(2) Sampling plan per _____ ?	—	—	
	(3) Environmentally _____ ?	—	—	

RELIABILITY (R) DESIGN CHECKLIST

No	Item Description	Yes	No	Remarks
24	Developmental Test Program			
(a)	Is contractor conducting a developmental test program?	—	—	
(b)	Does developmental test program include:			
	(1) All critical assemblies?	—	—	
	(2) Each assembly with a unique form factor?	—	—	
	(3) Critical non-standard parts?	—	—	
(c)	Does developmental testing include environmental testing at or above the levels specified for qualification:			
	(1) High and low temperature?	—	—	
	(2) Vibration?	—	—	
	(3) Shock?	—	—	
	(4) Humidity?	—	—	
(d)	Are performance requirements checked over required operating temperature levels?	—	—	
(e)	Are life tests or reliability tests of critical components/subassemblies being or have they been conducted?	—	—	
(f)	Is "Step Stress" testing being performed on sub-assemblies. etc., to determine design margins?	—	—	
(g)	Is developmental test program monitored by the reliability group or does the reliability group provide inputs to developmental testing?	—	—	
(h)	Are failure data and maintenance data collected during developmental testing for determining need for reliability improvement?	—	—	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
25	**Reliability Analyses**			
(a)	Have the following reliability analyses been performed:			
	(1) Reliability Mathematical Models?			
	(2) Reliability Apportionments?	—	—	
	(3) Reliability Predictions?	—	—	
	(4) Failure Modes and Effects Analyses?	—	—	
	(5) Criticality Analyses?	—	—	
	(6) Circuit Analysis (nominal and worst cases)?	—	—	
	(7) Thermal Analysis?	—	—	
	(8) Sneak Circuit Analysis?	—	—	
(b)	Do predictions meet apportioned values?	—	—	
(c)	Do predictions meet numerical reliability specification requirements?	—	—	
(d)	Have the results of the predictions been used to increase equipment reliability by:			
	(1) Reduction of circuit complexity?	—	—	
	(2) Reduction of ambient temperature conditions?	—	—	
	(3) Reduction of internal temperature rises?	—	—	
	(4) Reduction of part stresses by further derating?	—	—	
	(5) Increase of part quality levels?	—	—	
	(6) Addition of redundancy?	—	—	
(e)	Has a numerical approach for Criticality Analysis been used?	—	—	
(f)	Does the numerical criticality analysis consider:			
	(1) Frequency of failure?	—	—	
	(2) Degree of effect on system performance?	—	—	
	(3) Difficulty to diagnose and/or repair?	—	—	
	(4) Personnel or equipment safety?	—	—	
(g)	Have all critical modes of system failure been identified?	—	—	
(h)	Have critical items been ranked as to criticality?	—	—	
(k)	Has the use of limited life items been kept to a minimum?	—	—	
(l)	Have the analyses considered the effects of storage, transportation and handling on failure modes, effects and failure rates?	—	—	
(m)	Has the use of circuit analysis provided a stable, design over the worst case conditions?	—	—	
(n)	Has protective circuitry been utilized in the equipment design?	—	—	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks

26   Burn-in Program

(a)   Does the contractor impose burn-in at:
(1) Component level?   —— ——
(2) Subassembly/module level?   —— ——
(3) Equipment/system level?   —— ——

(b)   Is burn-in performed under:
(1) Temperature (elevated)?   —— ——
(2) Temperature cycling?   —— ——
(3) Vibration?   —— ——

(c)   Are lengths of burn-in adequate for each level?   —— ——

(d)   Do spares receive same burn-in as modules/subassembly level?   —— ——

(e)   Do all equipments/systems receive the same amount of burn-in?   —— ——

(f)   Does contractor have a failure free burn-in requirement prior to acceptance of the equipment?   —— ——

(g)   Is random vibration performed?   —— ——
(1) Equipment level? _____
(2) "g" level? _____
(3) Frequency range? _____
(4) Time duration? _____

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
27	Failure Reporting Analysis and Corrective Action (FRACA) Program			
(a)	Has contractor implemented a FRACA program?	___	___	
(b)	Does FRACA program cover failures during:			
	(1) Source inspection at subcontractor's plant?	___	___	
	(2) Incoming inspection?	___	___	
	(3) In-process inspection?	___	___	
	(4) Development tests?	___	___	
	(5) Subassembly/module test?	___	___	
	(6) Equipment integration and checkout?	___	___	
	(7) Equipment burn-in?	___	___	
	(8) Equipment formal tests:			
	(a) Acceptance tests?	___	___	
	(b) Environmental/qualification tests?	___	___	
	(c) Reliability/Maintainability tests?	___	___	
(c)	Does contractor have in-house facilities for performing detailed failure analysis?	___	___	
(d)	Is failure analysis conducted for all failures?	___	___	
(e)	Are failures summarized by part number and failure type to determine trends and patterns?	___	___	
(f)	Has contractor established thresholds (percent defective or failure rate) for determining need for corrective action?	___	___	
(g)	Does failure report form contain the necessary information with regards to:			
	(1) Identification of failed part subassembly, assembly, etc.?	___	___	
	(2) Elapsed time meters (for failure at equipment level)?	___	___	
	(3) Failure symptoms?	___	___	
(g)	(4) Effect of failure on system/equipment?	___	___	
	(5) Test and environmental conditions at time of failure?	___	___	
	(6) Suspected cause of failure?	___	___	
(h)	Is the same type of FRACA program imposed upon subcontractors of critical subassemblies?	___	___	
(i)	Are subcontractor failure reports included in contractor failure summaries?	___	___	
(j)	Are all failure reports, analyses and corrective actions reviewed by the reliability group?	___	___	
(k)	Are failure trends monitored by the reliability group?	___	___	
(l)	Are corrective actions involving design changes tested in the equipment for an adequate period of time prior to their formalization?	___	___	
(m)	Are corrective action investigations reopened upon a recurrence of the same type of failure?	___	___	
(n)	Are proposed corrective actions referred to the Procuring Activity for concurrence?	___	___	

RELIABILITY (R) DESIGN CHECKLIST

No.	Item Description	Yes	No	Remarks
28	Reliability Demonstration Test Planning			
(a)	Will test simulate operating profile that will be seen aboard ship?	—	—	
(b)	Will all modes of equipment operation be tested?	—	—	
(c)	Is definition of failure in accordance with contract specification requirements?	—	—	
(d)	Are relevant and non-relevant failure definitions adequately defined?	—	—	
(e)	Will test be performed under environmental levels specified by the contract specifications?	—	—	
(f)	Will burn-in to be performed on reliability test units be no more or no less than that specified for production units?	—	—	
(g)	Non-operating and equipment standby time will be discounted from applicable test time for validating reliability, true?	—	—	
(h)	No Preventive Maintenance other than that contained in technical manuals and approved by the Navy will be performed during the test, true?	—	—	
(i)	Performance checks capable of checking the complete equipment failure rate, performed no less frequently than daily have been defined for the test, true?	—	—	
(j)	Test will be performed per agreed schedule, true?	—	—	
(k)	Procuring Activity will be notified of the exact test date at least 30 days prior to the test, true?	—	—	
(l)	All interfaces are simulated or stimulated?	—	—	
(m)	All interfaces are real?	—	—	
(n)	If interfaces are real, is GFE required?	—	—	
(o)	If GFE is required, has a request been made to obtain GFE?	—	—	
(p)	Is test DD 1423 documentation on schedule?	—	—	

8.0 RELIABILITY DATA COLLECTION AND ANALYSIS, DEMONSTRATION, AND GROWTH

8.1 INTRODUCTION

Successful or satisfactory operation - the goal of all design efforts - yields little information on which to base improvements. Failures, on the other hand, contribute a wealth of data on "what to improve" or "what to design against" in subsequent efforts. The feedback of information obtained from the analysis of failures is one of the principal stepping stones of progress.

The prediction or assessment of reliability is actually an evaluation of unreliability -- the rate at which failures occur. The nature and underlying cause of failures must be identified and corrected to improve reliability. Reliability data consist of reports of failures and reports of duration of successful operation of the monitored equipment/system.

Reliability data is used for three main purposes:

(1) To verify that the equipment is meeting its reliability requirements.

(2) To discover deficiencies in the equipment to provide bases for corrective action.

(3) To establish failure histories for comparison and for use in prediction.

Reliability data can also be useful in providing information about logistics, maintenance, and operations. The data can provide a good estimate of the degradation and wearout characteristics of parts and components and how spare parts requirements are affected.

From this information, not only can effective preventive maintenance routines to control frequent trouble areas be developed, but also an estimate can be obtained of the number of maintenance manhours required to assure a desired level of reliability.

It is important that the data be factual so that a high degree of credence may be placed in the conclusions derived from it. Incomplete and inaccurate reporting will inevitably lead to either complete loss of confidence in the data or to incorrect conclusions and, hence, incorrect decisions and actions based on the conclusions.

Reliability/failure data can be obtained from a number of sources:

(1) an in plant failure reporting, analysis, and corrective action system (FRACAS)

(2) reliability test data

(3) subcontractor or vendor data

(4) field data

(5) reliability data banks

The most useful of the above sources are (1) and (2), and possibly (5). The other sources are not as reliable since they are, in most cases, incomplete. For example, the military maintenance collection systems for collecting field data (e.g., the Army's TAMMS, the Navy's 3M, and the Air Force's 66-1) are primarily maintenance oriented (see Section 11). Thus, field reliability cannot be assessed by these systems alone.

The following section provides more details on a FRACAS system. The sections on Reliability Testing and Growth discuss the collection and analysis of reliability test data.

8.2 FAILURE REPORTING, ANALYSIS, AND CORRECTIVE ACTION SYSTEM (FRACAS)

MIL-STD-785, Task 104 calls for the establishment of a FRACAS program. The purpose of this task is to establish a closed loop failure reporting system, procedures to determine cause, and documentation for recording corrective action taken. It requires the contractor to have a system that collects, analyzes and records failures that occur for specified levels of assembly prior to acceptance of the hardware by the procuring activity.

The purpose of an in plant FRACAS is to determine the basic cause of failure resulting from design or manufacture, and to provide a closed-loop method of implementing corrective action. The system should emphasize investigation and analysis of all failures regardless of their apparent magnitude, and classification of failures according to categories of design/part procurement, manufacture, or assembly and inspection. It is well known that the most economical repair of a failure occurs at the component part level. A conditional rule of thumb is that a repair action at the subassembly level costs an order of magnitude more than at the part level, and a repair at the product level costs an order of magnitude more than a repair at the subassembly level.

Essentially the FRACAS system must provide information on:

(1) What failed
(2) How it failed
(3) Why it failed
(4) How future failures can be eliminated

Figure 8.2-1 indicates the main steps in a closed loop FRACAS. Figure 8.2-2 is an example of a typical failure report form used in a FRACAS system.

There are several "keys" that make the failure reporting and corrective action cycle effective. These are outlined below.

(1) The discipline of the report writing itself must be maintained so that an accurate description of failure occurrence and proper identification of the failed items are assured.
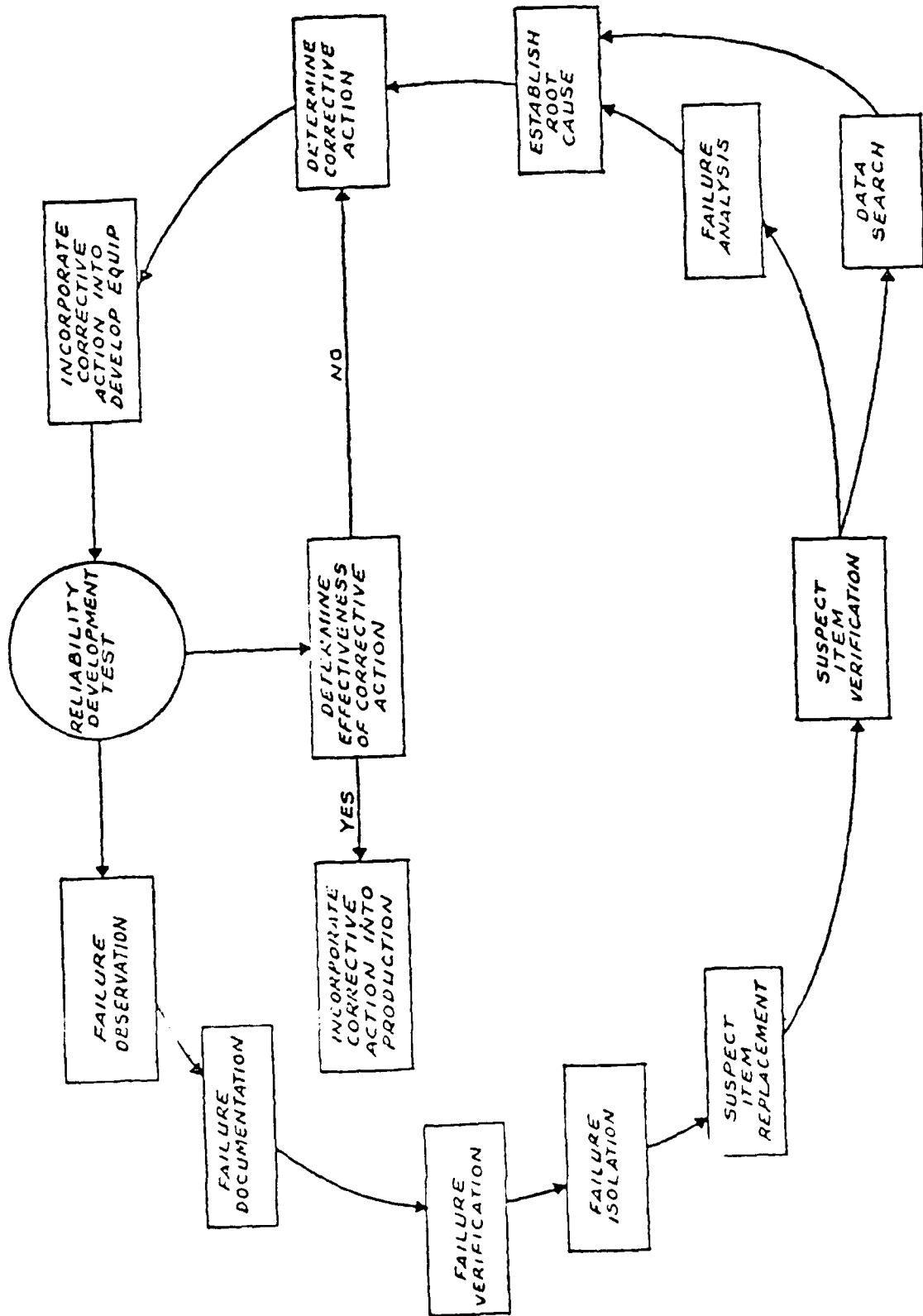
FIGURE 8.2-1: CLOSED LOOP FAILURE REPORTING AND
CORRECTIVE ACTION SYSTEM

'ORIGINATOR UNLESS HE IS COG. ENGR. TO COMPLETE SECTION I ONLY

I.E., STC-1, LCE-2, ETC.

ENTER ACTUAL PROBLEM/FAILURE DATE

I.E., BUREAU NUMBER ETC.

CHECK APPLICABLE BLOCK

CHECK OFF "FLIGHT" OR "OSE"

PROVIDED AS A CONVENIENCE FOR ORIGINATOR'S INTERNAL CONTROL REFERENCES

IDENTIFY PERTINENT PROJECT TO SUBJECT PROBLEM/FAILURE

IF ACTUAL TIME IS NOT KNOWN, ENTER APPROXIMATE TIME AND SO INDICATE

FILL OUT COMPLETELY

LOCATION OF PROBLEM/FAILURE SHOULD BE REPORTED

FOR RELIABILITY P/FR STAFF USE ONLY

ORIGINATOR SPECIFIES THE RESPONSIBLE COGNIZANT ENGINEER'S NAME(S)

TESTING CONDITIONS AND ENVIRONMENT SHALL BE NOTED

DESCRIBE PROBLEM/ FAILURE COMPLETELY AND ACCURATELY INCLUDING APPLICABLE INFORMATION, I.E., SPECS AND/OR DRAWINGS

INDICATE CAUSE OR PROBLEM/FAILURE AND THE RESULTS OF P/FR ANALYSIS

CHECK APPLICABLE BLOCKS TO INDICATE IF PERTINENT PART(S) ARE OF PRIMARY OR SECONDARY CAUSE OF PROBLEM/FAILURE

CHECK APPLICABLE BLOCK

NORMALLY COMPLETED BY COG. ENGR. BUT QA MAY MAKE RECOMMENDATIONS

APPLICABLE TO PART OR PARTS INVOLVED

DOCUMENT EXPLICITLY ACTION INITIATED OR COMPLETED TO PRECLUDE RECURRENCE OF SUBJECT PROBLEM/ FAILURE

RECORD "CORRECTIVE ACTION TAKEN" COMPLETELY

ENTER ECR NO. IF CORRECTIVE ACTION HAS REQUIRED ISSUANCE OF AN ENGINEERING CHANGE REQUIREMENT (ECR)

INDICATE "DISPOSITION" AS DETERMINED BY "CORRECTIVE ACTION"

EFFECTIVITY POINT OR SCOPE OF "CORRECTIVE ACTION"

DETERMINED BY PROJECT ENGINEER

STANDARD DISTRIBUTION LISTS BY RELIABILITY P/FR GROUP "SPECIALS" BY QA GROUP

ENTER NAME(S) OF PERSONNEL NOT ON STANDARD DISTRIBUTION LIST WHO SHOULD RECEIVE COPY/COPIES OF A CERTAIN REPORT

Form fields:

□ FLIGHT (A/C SER. NO. ____) □ OSE (COMPLEX SER. NO. ____)

□ PROBLEM/ □ FAILURE REPORT   NO. ____

1. PROJECT   2. PROBLEM/FAILURE DATE   3. LOG NO.

	A. REFERENCE DESIGNATIONS	B. NOMENCLATURE	C. SERIAL NUMBERS	D. OPERATING TIME
4. SUBSYSTEM				
5. ASSEMBLY				
6. SUBASSEMBLY				

7. REPORTING LOCATION
□ ORIG   □ VENDOR   □ SAF   □ ETR   □ OTHER

8. PROBLEM/FAILURE NOTED DURING   INITIAL DISTRIBUTION DATE
□ BENCH TESTING □ IN-PROCESS TESTING □ TA TESTING □ PA TESTING □ SYSTEMS TESTING
□ SPECIFIC ENVIRONMENT ____ □ OTHER

9. DESCRIPTION OF PROBLEM/FAILURE

ORIGINATOR ____ DATE ____ COGNIZANT ENGINEER ____

10. VERIFICATION & ANALYSIS

11. CAUSE OF PROBLEM/FAILURE
□ DESIGN □ PIECE PART FAILURE □ OPERATOR ERROR □ DAMAGE (MISHANDLING) □ ADJUSTMENT
□ WORKMANSHIP □ MANUFACTURING □ OSE FAILURE □ OTHER

12. FOLLOWUP ASSIGNMENT
□ COGNIZANT ENGINEER □ DESIGN REVIEW □ VENDOR ____ □ COMPONENTS EVALUATION GROUP
□ MATERIAL REVIEW BOARD □ QUALITY ASSURANCE □ OTHER

13. P.O.A.R.T.A	A. PIECE PART NAME & NUMBER	B. SERIAL NO.	C. CIRCUIT DESIG	D. MANUFACTURER	E. DEFECT	F. PRI	G. SEC

PERSON COMPLETING SECTION II SIGNATURE ____ DATE ____

14. CORRECTIVE ACTION TAKEN

15. DISPOSITION
□ REWORKED □ SUPERSEDED □ READJUSTED □ SCRAPPED □ OTHER

16. EFFECTIVITY
□ TH. UNIT □ ALL UNIT □ OTHER ____   ECR NO. ____

SIGNATURE COGNIZANT ENGINEER ____ BY ____ DATE ____ SIGNATURE COGNIZANT SEC CHIEF ____

17. REVIEW CONCURRENCE
RELIABILITY COORDINATOR ____ DATE ____
COGNIZANT PROJECT ENGINEER ____ DATE ____

18. CLASSIFICATION
□ CRITICAL
□ NON-CRITICAL

19. STANDARD & SPECIAL DISTRIBUTION

P/FR RELIABILITY STAFF

DISTRIBUTION

COPIES OF ALL PROBLEM FAILURE REPORTS WILL BE DISTRIBUTED TO ALL CONCERNED PERSONNEL

STANDARD DISTRIBUTIONS, BY PROJECTS, WILL BE ESTABLISHED BY RELIABILITY AND CONCERNED EXECUTIVE PERSONNEL

USAGE

USE SYMBOL "N/A" ON SUBJECT P/FR FORM WHENEVER REQUESTED INFORMATION IN ANY BLOCK IS NON-APPLICABLE

FIGURE 8.2-2:   EXAMPLE OF FAILURE REPORT FORM

(2) The proper assignment of priority and the decision for failure analysis must be made with the aid of cognizant design engineers and systems engineers.

(3) The status of all failure analyses must be known. It is of prime importance that failure analyses be expedited as priority demands and that corrective action be implemented as soon as possible.

(4) The root cause of every failure must be understood. Without this understanding, no logically derived corrective actions can follow.

(5) There must be a means of tabulating failure information for determining failure trends and the mean times between failures of system elements.   There should also be a means for management visibility into the status of failure report dispositions and corrective actions.

(6) The system must provide for a high level technical management approval; concurring in the results of failure analysis, the soundness of corrective action, and the completion of formal actions in the correction and recurrence prevention loop.

(7) An extremely valuable assurance mechanism is to have active Government involvement in the surveillance of the adequacy of the failure reporting, analysis, and corrective action effort.

References 1 and 2 provide additional details on FRACAS systems. Also, relative to failure analysis of integrated circuits - by far the largest part population of electronic systems - Ref. 3, is the most recent and comprehensive document available.

8.3 RELIABILITY DATA ANALYSIS

From a reliability assessment viewpoint, failure data is used to:

(1) determine the underlying probability distribution of time to failure and estimate its parameters (if not already known).

(2) determine a point estimate of a specific reliability parameter, e.g., MTBF

(3) determine a confidence interval that is believed to contain the true value of the parameter.

Two methods are used to analyze failure data:

(1) graphical methods
(2) statistical analysis

In many practical cases, graphical methods are simple to apply and produce adequate results for estimating the underlying distribution.

They are virtually always a useful preliminary to more detailed statistical analysis. The two methods will be discussed in more detail in the following subsections.

8.3.1 GRAPHICAL METHODS

The basic idea of graphical methods is the use of special probability plotting papers in which the cumulative distribution function (cdf) or the cumulative hazard can be plotted as a straight line for the particular distribution being studied. Since a straight line has two parameters (slope and intercept), two parameters of the distribution can be determined. Thus, reliability data can be evaluated quickly, without a detailed knowledge of the statistical mathematics being necessary. This facilitates analysis and presentation of data.

Graphical curve fitting techniques and special probability plotting papers have been developed for all of the distributions commonly associated with reliability analysis (Refs. 4, 5).

Ranking of Data

Probability graph papers are based upon plots of the variable of interest against the cumulative percentage probability. The data therefore need to be ordered, and the cumulative probability calculated. For reliability work, the data is ordered from the smallest to largest; this is referred to as order statistics. For example, consider the data on times to failure of 20 items (Table 8.3.1-1). For the first failure, the cumulative proportion is 1/20 or 5%. For the second, the cumulative proportion is 2/20 or 10%, and so on to 20/20 or 100% for the 20th failure. However, for probability plotting, it is better to make an adjustment to allow for the fact that each failure represents a point on a distribution. Thus, considering that the whole population of 20 items represent a sample, the times by which 5, 10 ... 100% will have failed in several samples of 20 will be randomly distributed. However, the data in Table 8.3.1-1 show a bias, in that the first failure is shown much further from the zero cumulative percentage point than is the last from 100% (in fact it coincides). To overcome this, and thus to improve the accuracy of the estimation, mean or median ranking of cumulative percentages is used for probability plotting. Mean ranking is used for symmetrical distributions, e.g., normal; median ranking is used for skewed distributions, e.g., Weibull.

The usual method for mean ranking is to use (n + 1) in the denominator, instead of n, when calculating the cumulative percentage position. Thus in Table 8.3.1-1 the cumulative percentages (mean ranks) would be:

$$\frac{100}{20 + 1} = 5$$

$$\frac{200}{20 + 1} = 10$$

.

.

.

$$\frac{2000}{20 + 1}$$

TABLE 8.3.1-1: <u>DATA ON TIMES TO FAILURE OF 20 ITEMS</u>

Order No.	Time to Failure (hrs.)	Cumulative % (Cdf)	Mean Rank (%) (Cdf)
1	175	5 (1/20)	5
2	695	10 (2/20)	10
3	872	15 (3/20)	14
4	1250	20 (4/20)	19
5	1291	25 (5/20)	24
6	1402	30 (6/20)	29
7	1404	35 (7/20)	33
8	1713	40 (8/20)	38
9	1741	45 (9/20)	43
10	1893	50 (10/20)	48
11	2025	55 (11/20)	52
12	2115	60 (12/20)	57
13	2172	65 (13/20)	62
14	2418	70 (14/20)	67
15	2583	75 (15/20)	71
16	2725	80 (16/20)	76
17	2844	85 (17/20)	81
18	2980	90 (18/20)	86
19	3268	95 (19/20)	90
20	3538	100 (20/20)	95

These data are shown plotted on normal probability paper in Figure 8.3.1-1 (circles). The plotted points show a reasonably close fit to the straight line drawn 'by eye.' Therefore, we can say that the data appear to fit the cumulative normal distribution represented by the line.

Median ranking, as was previously stated, is used for skewed distributions such as the Weibull because it provides a better correction. The most common approximation for median ranking (Ref. 4) is given by

$$r_i = \frac{i - 0.3}{n + 0.4}$$

where r_i is the the ith order value and n is the sample size. Median ranking is the method most used in probability plotting, particularly if the data is known not to be normally distributed. Also, to save calculations, tables of median ranks are available for use. These are included in Table 8.3.1-2 and will be used in the the examples to be described later.
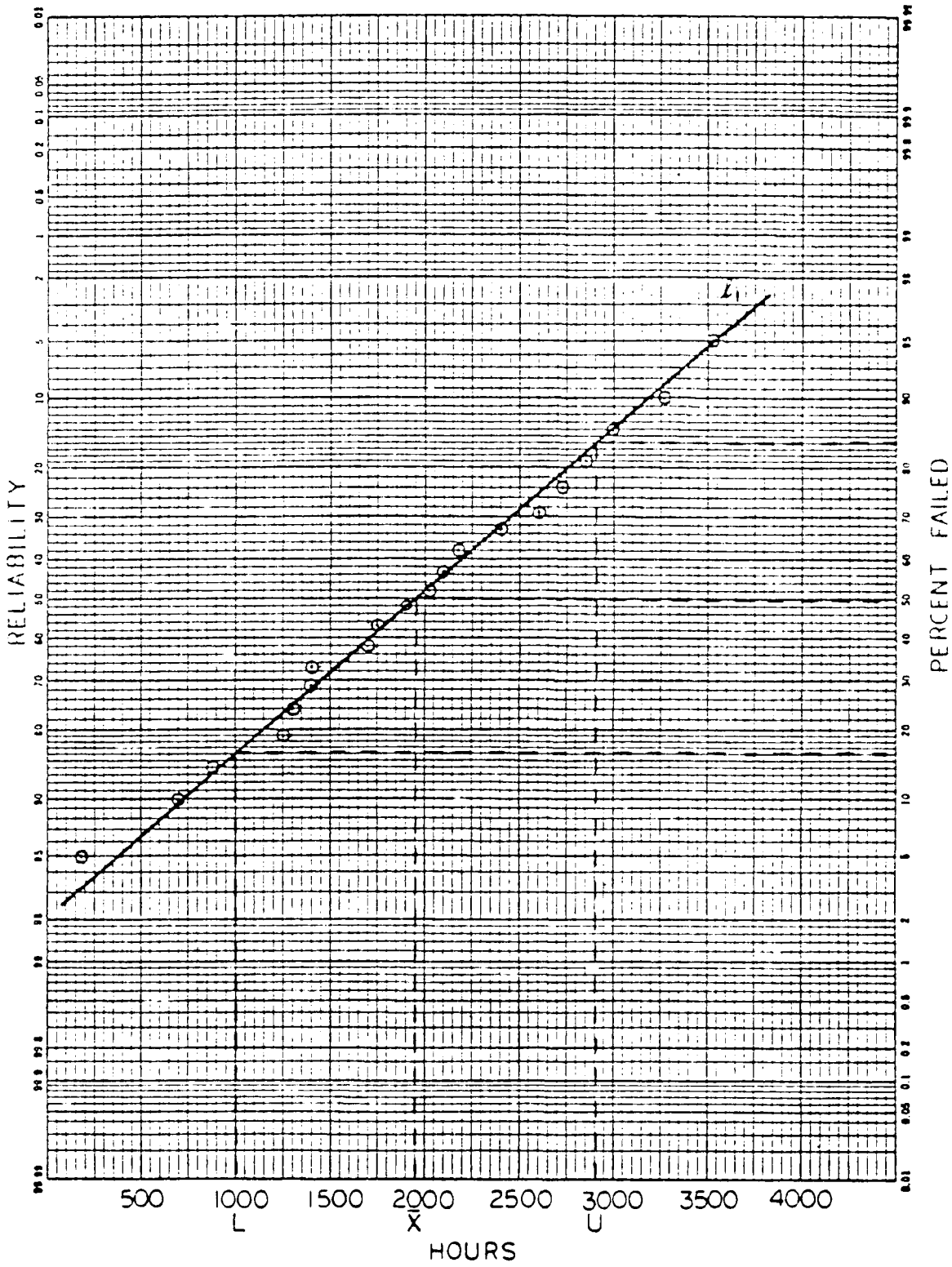
FIGURE 8.3.1-1: GRAPHICAL POINT ESTIMATION FOR THE NORMAL DISTRIBUTION

TABLE 8.3.1-2: <u>MEDIAN RANKS</u>

j	1	2	3	4	5	6	7	8	9	10
1	.5000	.2929	.2063	.1591	.1294	.1091	.0943	.0830	.0741	.0670
2		.7071	.5000	.3864	.3147	.2655	.2295	.2021	.1806	.1632
3			.7937	.6136	.5000	.4218	.3648	.3213	.2871	.2594
4				.8409	.6853	.5782	.5000	.4404	.3935	.3557
5					.8706	.7345	.6352	.5596	.5000	.4519
6						.8909	.7705	.6787	.6065	.5481
7							.9057	.7979	.7129	.6443
8								.9170	.8194	.7406
9									.9259	.8368
10										.9330

sample size = n
failure rank = j

j	11	12	13	14	15	16	17	18	19	20
1	.0611	.0561	.0519	.0483	.0452	.0424	.0400	.0378	.0358	.0341
2	.1489	.1368	.1266	.1788	.1101	.1034	.0975	.0922	.0874	.0831
3	.2366	.2175	.2013	.1873	.1751	.1644	.1550	.1465	.1390	.1322
4	.3244	.2932	.2760	.2568	.2401	.2254	.2125	.2009	.1905	.1812
5	.4122	.3789	.3506	.3263	.3051	.2865	.2700	.2553	.2421	.2302
6	.5000	.4596	.4253	.3958	.3700	.3475	.3275	.3097	.2937	.2793
7	.5878	.5404	.5000	.4653	.4350	.4085	.3850	.3641	.3453	.3283
8	.6756	.6211	.5747	.5347	.5000	.4695	.4425	.4184	.3968	.3774
9	.7634	.7018	.6494	.6042	.5650	.5305	.5000	.4728	.4484	.4264
10	.8511	.7825	.7240	.6737	.6300	.5915	.5575	.5272	.5000	.4755
11	.9389	.8632	.7987	.7432	.6949	.6525	.6150	.5816	.5516	.5245
12		.9439	.8734	.8127	.7599	.7135	.6725	.6359	.6032	.5736
13			.9481	.8822	.8249	.7746	.7300	.6903	.6547	.6226
14				.9517	.8899	.8356	.7875	.7447	.7063	.6717
15					.9548	.8966	.8450	.7991	.7579	.7207
16						.9576	.9025	.8535	.8095	.7698
17							.9600	.9078	.8610	.8188
18								.9622	.9126	.8678
19									.9642	.9169
20										.9659

8.3.1.1 SOME POINTERS ON GRAPHICAL METHODS

Reference 5, provides an excellent discussion of caveats that must be considered in graphical estimation. Now, let us turn to some examples.

8.3.1.2 EXAMPLES OF GRAPHICAL METHODS

Example #1: Normal Distribution

1. **When to Use**

This method estimates u and σ, the mean and standard deviation when failure times are normally distributed. This method yields a less accurate estimate than statistical analysis but requires very minimal calculations.

2. **Conditions for Use**

   a. Failure times must be collected, but may be censored; censored data is discussed in the next section.

   b. Normal probability paper is required.

3. **Method**   **Example**

   a. On normal probability paper   a. The sample data used in
       plot the ith failure time   Table 8.3.1-1 is repeated
       in a sample of n ordered   here, with the necessary
       failure times on the lower   plotting positions (mean
                                                 ranks).
       axis vs. $\frac{i}{n+1}$ on the right
       hand axis.

Failure Time	Plotting Position $\frac{i}{n+1}$
175 hours	.05
695 hours	.10
872 hours	.14
1250 hours	.19
1291 hours	.24
1402 hours	.29
1404 hours	.33
1713 hours	.38
1741 hours	.43

Failure Time	Plotting Position $\frac{i}{n+1}$
1893 hours	.48
2025 hours	.52
2115 hours	.57
2172 hours	.62
2418 hours	.67
2583 hours	.71
2725 hours	.76
2844 hours	.81
2980 hours	.86
3268 hours	.90
3538 hours	.95

b. Draw the Normal line of best fit through the plotted points by using the last point plotted as a reference point for a straight edge and dividing the rest of the points into two equal groups above and below the line.

b. Figure 8.3.1-1 is the plot of this data on normal paper. The normal line has been labeled ℓ_1.

c. The mean, μ, is estimated by projecting the 50% probability of failure point on the right hand axis to the normal line and then projecting that intersection point down to the lower axis. The estimate of μ, $\bar{x}$, is read off there.

c. The value of $\bar{x}$ is read off as 1950 hours.

d. The estimate of σ is obtained by projecting the intersection of the 84% probability of failure point on the right hand axis with the normal line to the lower axis. Call that point on the lower axis U.

d. U = 2900 hours

e. Repeat step d. with the 16% point. Call the point L.

e. L = 1000 hours

f. The estimate of σ is

$$s = \frac{U-L}{2}$$

f. The sample standard deviation, s, is

$$\frac{U-L}{2} = \frac{2900-1000}{2} = 950 \text{ hours}$$

g. The 95% confidence limits around the mean are given by

$$\bar{x} \pm t\, s/\sqrt{n}$$

where t is shown below for various sample sizes n.

g. $1950 \pm (2.09)(950)/\sqrt{20}$

$$1950 \pm 444 \text{ hrs.}$$

n	t
5	2.57
10	2.23
20	2.09
30	2.04
50	2.00
∞	1.96

Example #2: Weibull Distribution

1. When to Use

Estimates of the Weibull shape and scale parameters may be obtained graphically by using specially prepared Weibull probability paper. The decision to use this method should be based wholly on the accuracy desired. This method is less accurate than statistical analysis but can be done quickly and easily.

2. Conditions for Use

a. Failure times must be collected.

b. Median rank tables are required. They are provided in Table 8.3.1-2.

c. Weibull probability paper is required. See Figure 8.3.1.2-1.

3. Method   Example

a. To plot the ith failure
    time in a set of n ordered
    failure times, find the median
    rank plotting position on the
    left hand ordinate by consult-
    ing the table of median ranks
    at n, i. To obtain median
    ranks for n greater than
    twenty, the following formula
    may be used:

    Median rank (n, i) = $\dfrac{i - 0.3}{n + 0.4}$

    where   i = order no. of failures
            n = number of failures

a. As an example of plotting
    failure times on Weibull
    probability paper, consider
    a case in which 20 items are
    all tested to failure; the
    20 failure times, in ascend-
    ing order, are given below
    in the left hand column.
    In the right hand column are
    the median rank plotting
    positions for each failure
    time, obtained from the
    table of median ranks for
    n = 20 in Table 8.3.1-2.

Failure Times (Hours)	Median Ranks
92	.0341
130	.0831
233	.1322
260	.1812
320	.2302
325	.2793
420	.3283
430	.3774
465	.4264
518	.4755
640	.5245
700	.5736
710	.6226
770	.6717
830	.7207
1010	.7698
1020	.8188
1280	.8678
1330	.9169
1690	.9659

Before plotting the data, it
is necessary to perform a
transformation on the bottom
scale of Figure 8.3.1.2-1 to
accommodate the large fail-
ure times. The axis must be
multiplied by 10^2 in order
for the failure data to fit
on the paper. So, the bottom
scale is properly labeled
HOURS X 10^2.

8-13

b. The Weibull line is drawn through the plotted data by using the last point plotted as a reference point for a straight edge and dividing the rest of the points into two equal groups above and below the line.

b. The Weibull line, labeled ℓ_1 in Figure **8.3.1.2-1** is drawn as described.

c. To estimate β, parallel to the Weibull line draw a line passing through the small circled point on the paper.

c. The shape parameter β is estimated by drawing the line, labeled ℓ_2, parallel to ℓ_1 and passing through point A.

d. Horizontal projection of the point where this line intersects the principal ordinate to the right hand scale gives -β. The principal ordinate terminates in 0.0 on the upper scale. Note that the Weibull paper illustrated in Figure 8.3.1.2-1 has a small beta estimator in the top left hand corner of the paper. To use it, draw a line parallel to the Weibull line and passing through the point marked ORIGIN. The intersection of this line with the farthest left scale gives - βdirectly.

d. The point where ℓ_2 intersects ℓ_3, the principal ordinate, is projected horizontally to the right hand axis and - β read off as -1.45. So, β = 1.45.

e. Sometimes in order to plot the failure data it is necessary to convert the bottom scale to handle larger numbers. The scales used on this axis are selected for the purpose of convenience in presenting the data on the graph. If the bottom scale has been multiplied by K, then read -ln α_K at the horizontal projection to the right hand axis of the intersection of the Weibull line and the principal ordinate.

e. To find α, the intersection of ℓ_1 and ℓ_3 is projected horizontally to the right hand axis. The value read off the axis, -2.9, is -ln α_K, and must be converted.
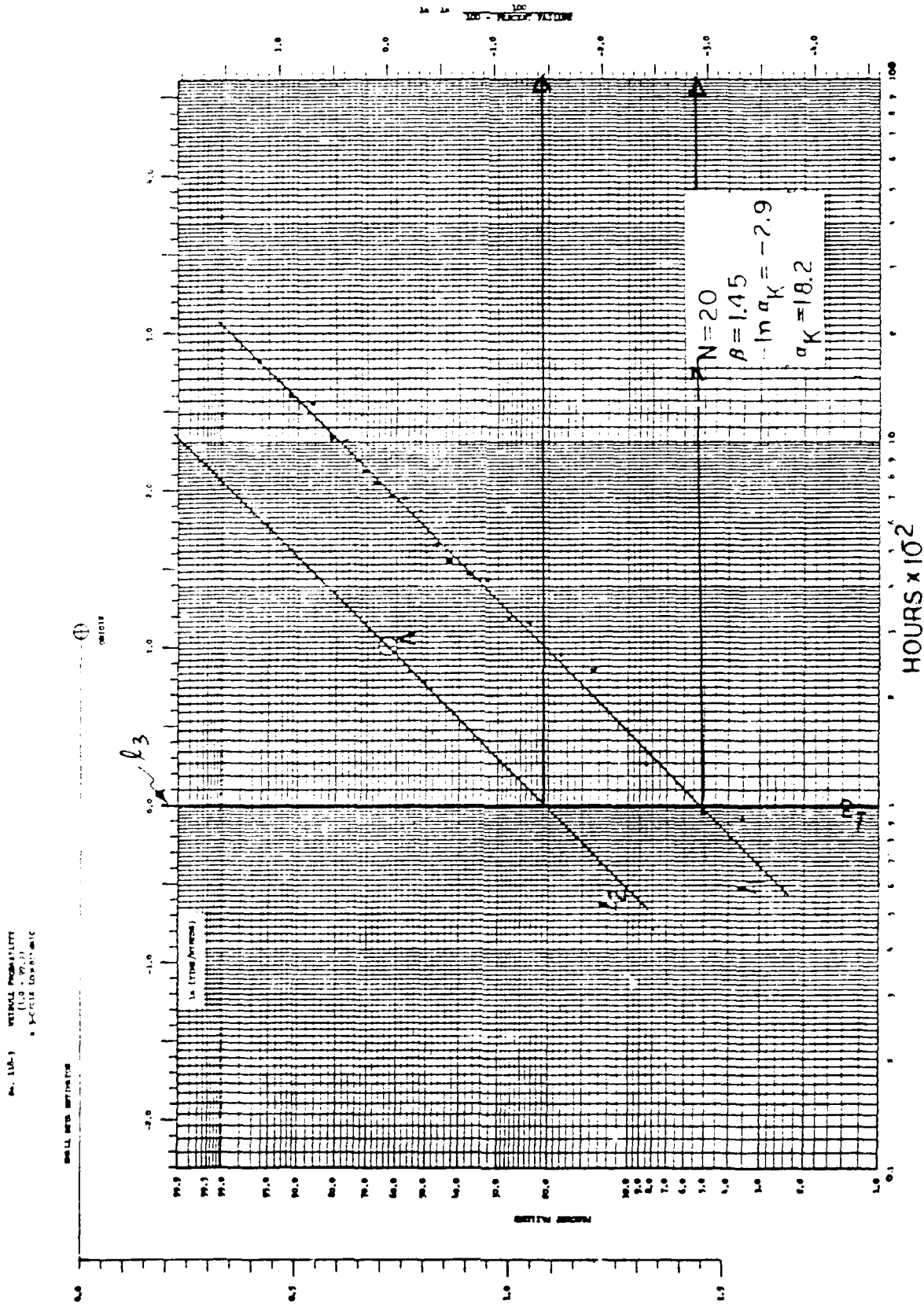
FIGURE 8.3.1.2-1: GRAPHICAL POINT ESTIMATION FOR THE WEIBULL DISTRIBUTION

f. Find the value of α_K by using a table of natural logarithms. The computed α_K is a coded value which is dependent on the time scale used.

f. The value of α_K is found to be 18.2 by looking for the antilog of 2.9 in a table of natural logarithms.

g. To convert α_K to an uncoded state that is independent of the time scale used on the probability paper, divide α_K by $K\beta$, where β is the previously obtained shape parameter.

g. α_K is converted to an uncoded state by dividing by $K\beta$. So, divide 18.2 by $(10^2 \ (1.5))$ giving

$$\alpha = 18.2/10^{-2\beta} = 18.2 \times 10^{(2)(1.5)}$$

$$= 1.82 \times 10^4$$

h. Find the reliability at t = 1000 hrs.

h. At the 1000 hr. point on the lower abscissa project vertically to line ℓ_1, and horizontally to the left ordinate. The reliability is 100 minus the intersection of the horizontal line and left ordinate; e.g., R(1000) = 100 - 80 = 20% = 0.2.

Example #3: Exponential Distribution

A simple graphical procedure to test the validity of the exponential distribution is to plot the cumulative test or operating time against the cumulative number of failures as shown in Figure 8.3.1.2-2.

8.3.2   STATISTICAL ANALYSIS

8.3.2.1 INTRODUCTION

Since the available data usually only constitutes a sample from the total population, statistical methods are used to estimate the reliability parameters of interest, e.g., MTBF, failure rate, probability of survival, etc.

The main advantage of statistics is that it can provide a good measure of the uncertainty involved in a numerical analysis. The secondary advantage is that it does provide methods for estimating effects that might otherwise be lost in the random variations in the data.

It is important to keep in mind the fact that data constitutes a sample from the total population, that random sampling peculiarities must be smoothed out, that population density parameters must be estimated, that the estimation errors must themselves be estimated, and -- what is even more difficult -- that the very nature of the population density must be
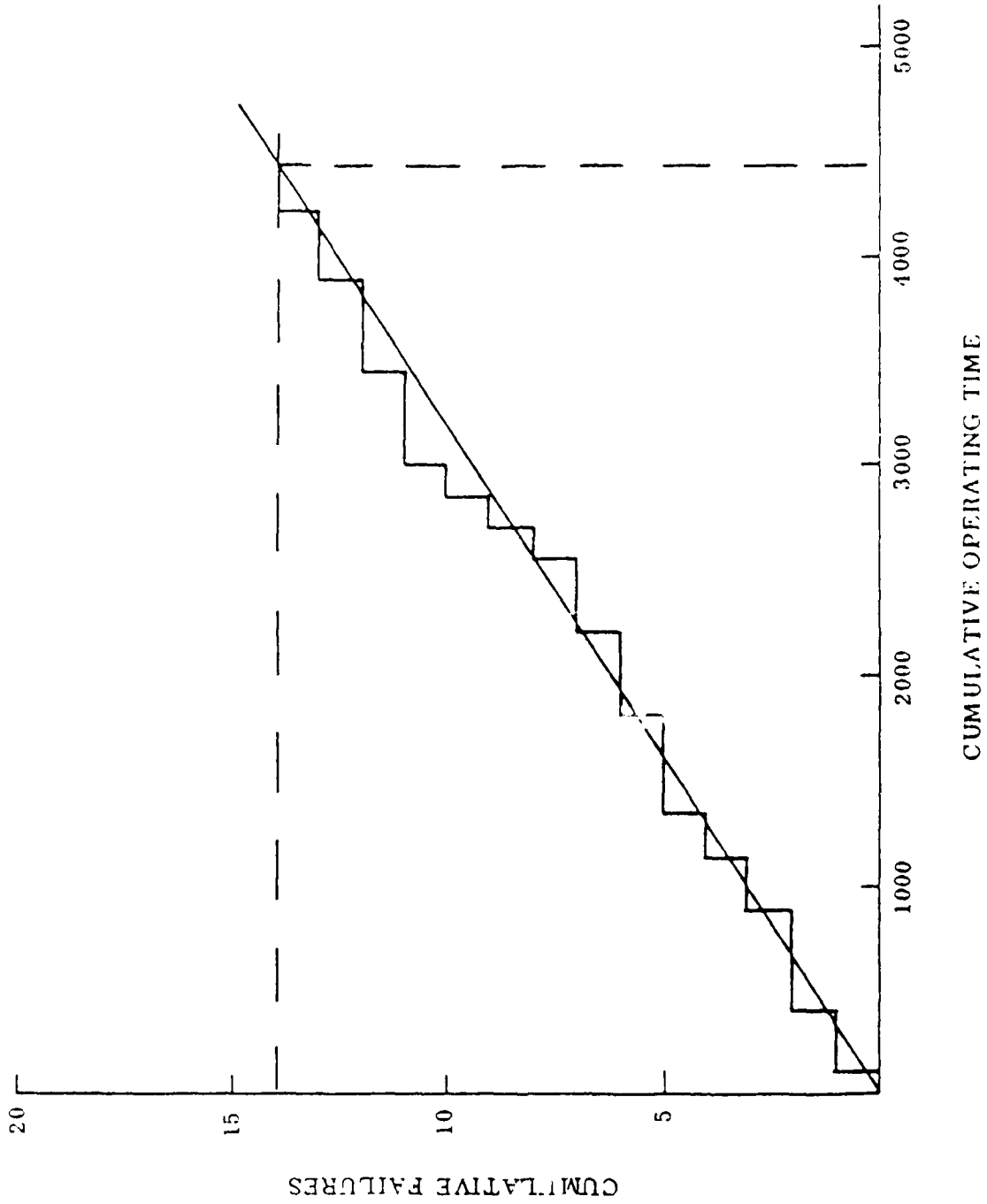
FIGURE 8.3.1.2-2: DISTRIBUTION GRAPHICAL EVALUATION

estimated. To achieve these ends, it is necessary to learn as much as one can about the possible population density functions, and especially what kind of results we can expect when samples are drawn, the data are studied, and we attempt to go from data backward to the population itself. It is also important to know what types of population densities are produced from any given set of engineering conditions. This implies the necessity for developing probability models, or going from a set of assumed engineering characteristics to a population density.

It is customary, even necessary, in statistical analysis to develop, from the physical engineering principles, the nature of the underlying distribution. The sample of data is then compared against the assumed distribution.

The usual parameter of interest in reliability is the distribution of times to failure, called the probability distribution function or failure density function. The failure density function may be discrete, that is, only certain (integral) values may occur, as in tests of an explosive squib. Success or failure will occur on any trial, time not being considered. Or it may be continuous, any value of time to failure being possible.

Typically histograms are plotted (e.g., time to failure plots) and statistical techniques used to first test the data to determine the applicable form of the probability distribution, and then identify and evaluate the relationship between the reliability parameter(s), such as failure rate, and the critical hardware characteristics/attributes which impact reliability (such as technology, complexity, application factors, etc.) as defined by the data.

8.3.2.2 TREATMENT OF FAILURE DATA

Failure data is usually obtained from a) test results or b) field failure reports. Experience has shown that a good way to present these data is to compute and plot either the failure density function, f(t), or the hazard rate, h(t), as a function of time.

Remember from Section 5 that f(t) is given by the ratio of the number of failures occurring in the time interval to the size of the original population, divided by the length of the time interval. The hazard rate, h(t), on the other hand, is given by the ratio of the number of failures occurring in the time interval to the number of survivors at the beginning of the time interval, divided by the length of the time interval.

Although f(t) and h(t) are defined as continuous functions, what is done is to compute piecewise continuous functions of f(t) and h(t), look at the graphed results, and choose a continuous model which best fits the data.

Once having found f(t) and h(t) from the data, F(t) (the cumulative distribution of time to failure) and R(t) = 1-F(t), the reliability function or survival probability, can be readily determined from the relationships.

$$F(t) = \int_{\infty}^{t} f(t) dT \tag{8.1}$$

$$R(t) = 1 - F(t) \tag{8.2}$$

Some examples follow

Example #1

TABLE 8.3.2.2-1: FAILURE DATA FOR TEN HYPOTHETICAL ELECTRONIC COMPONENTS

Failure Number	Operating Time, Hr
1	8
2	20
3	34
4	46
5	63
6	86
7	111
8	141
9	186
10	266

From Table 8.3.2.2-2 and Eq. (8.1) and (8.2) one can calculate and plot F(t) and R(t). The data plots for the various function of interest are shown in Figure 8.3.2.2-1.

Note that from the dashed lines of Figure 8.3.2.2-1 (a) and (b), that the exponential distribution of time to failure represents a rather good approximation to the data.

Example #2

In this case, we show data for a single B-52 performing 1000 missions of 2 to 24 hours, or the equivalent of 1000 B-52s performing a single mission of 2 to 24 hours (Ref. 6). (Tables 8.3.2.2-3 and 8.3.2.2-4, Figure 8.3.2.2-2).

8.3.2.3 RELIABILITY FUNCTION (SURVIVAL CURVES)

A survival curve or reliability function, R(t), is a graphic representation of the relationship between the probability of survival and time. Here, probability of survival is synonomous with probability of nonfailure or probability of satisfactory performance. Three types of survival curves are of primary interest. The first is a discrete or point-type curve derived from observed data by nonparametric or distribution free methods. The second type is a continuous curve based on an assumption as to the form of the distribution (Gaussian,

TABLE 8.3.2.2-2: <u>COMPUTATION OF DATA FAILURE DENSITY AND DATA HAZARD RATE</u>

Time interval, hr	Failure density per hr $f(t)$ $(x\ 10^{-2})$	Hazard rate per hr $h(t)$ $(x\ 10^{-2})$
0-8	$\dfrac{1}{10 \times 8} = 1.25$	$\dfrac{1}{10 \times 8} = 1.25$
8-20	$\dfrac{1}{10 \times 12} = 0.84$	$\dfrac{1}{9 \times 12} = 0.93$
20-34	$\dfrac{1}{10 \times 14} = 0.72$	$\dfrac{1}{8 \times 14} = 0.96$
34-46	$\dfrac{1}{10 \times 12} = 0.84$	$\dfrac{1}{7 \times 12} = 1.19$
46-63	$\dfrac{1}{10 \times 17} = 0.59$	$\dfrac{1}{6 \times 17} = 0.98$
63-86	$\dfrac{1}{10 \times 23} = 0.44$	$\dfrac{1}{5 \times 23} = 0.87$
86-111	$\dfrac{1}{10 \times 25} = 0.40$	$\dfrac{1}{4 \times 25} = 1.00$
111-141	$\dfrac{1}{10 \times 30} = 0.33$	$\dfrac{1}{3 \times 30} = 1.11$
141-186	$\dfrac{1}{10 \times 45} = 0.22$	$\dfrac{1}{2 \times 45} = 1.11$
186-266	$\dfrac{1}{10 \times 80} = 0.13$	$\dfrac{1}{1 \times 80} = 1.25$
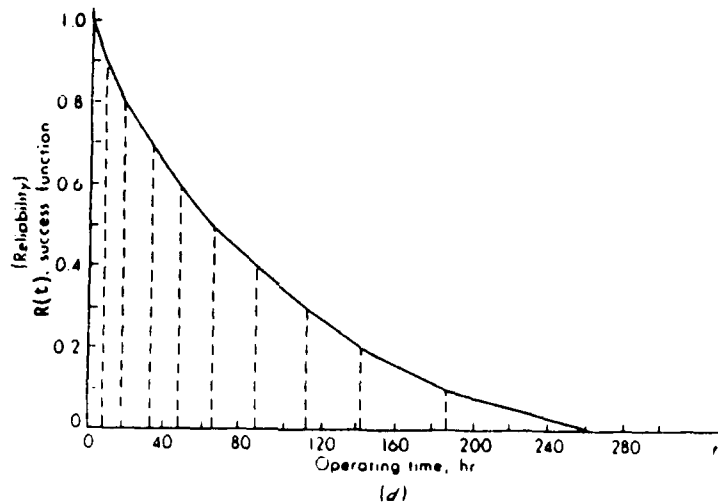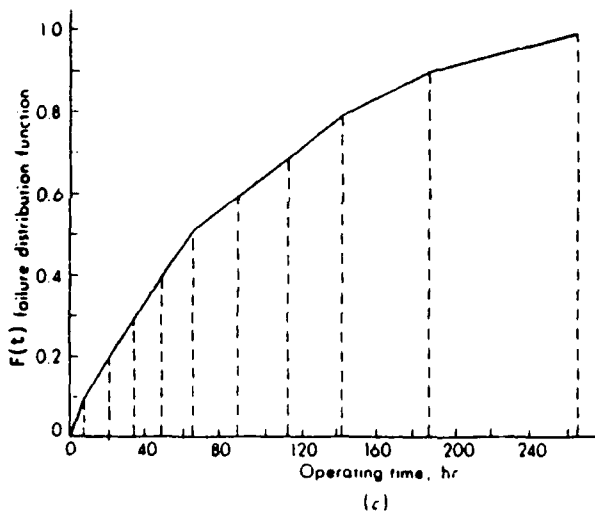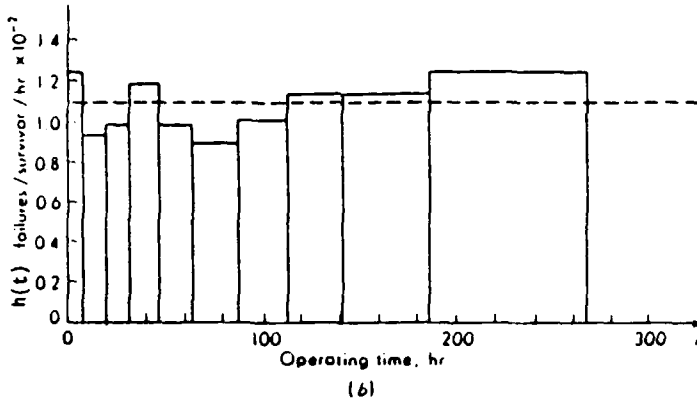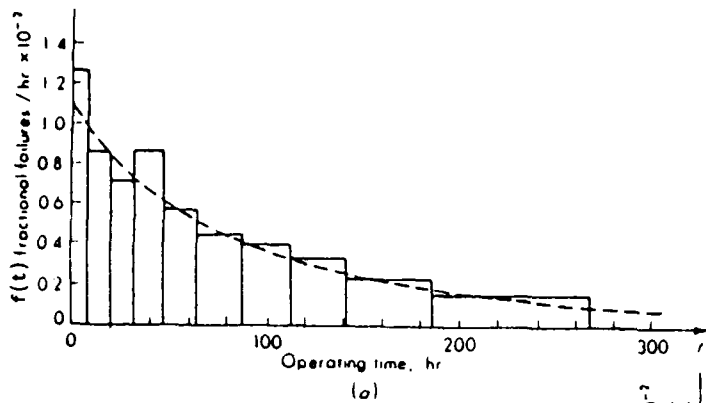
FIGURE 8.3.2.2-1: HAZARD AND DENSITY FUNCTIONS FOR TABLE 8.3.2.2-1

TABLE 8.3.2.2-3: FAILURE DATA FOR 1,000 B-52 AIRCRAFT

Time till failure, hr	Number of failures in interval	Failure density/hr $f(t)$	Hazard rate/hr $h(t)$
0–2	222	$\dfrac{222}{1,000 \times 2} = 0.1110$	$\dfrac{222}{1,000 \times 2} = 0.1110$
2–4	45	$\dfrac{45}{1,000 \times 2} = 0.0225$	$\dfrac{45}{778 \times 2} = 0.0289$
4–6	32	$\dfrac{32}{1,000 \times 2} = 0.0160$	$\dfrac{32}{733 \times 2} = 0.0218$
6–8	27	$\dfrac{27}{1,000 \times 2} = 0.0135$	$\dfrac{27}{701 \times 2} = 0.0192$
8–10	21	$\dfrac{21}{1,000 \times 2} = 0.0105$	$\dfrac{21}{674 \times 2} = 0.0156$
10–12	15	$\dfrac{15}{1,000 \times 2} = 0.0075$	$\dfrac{15}{653 \times 2} = 0.0113$
12–14	17	$\dfrac{17}{1,000 \times 2} = 0.0085$	$\dfrac{17}{638 \times 2} = 0.0133$
14–16	7	$\dfrac{7}{1,000 \times 2} = 0.0035$	$\dfrac{7}{621 \times 2} = 0.0056$
16–18	14	$\dfrac{14}{1,000 \times 2} = 0.0070$	$\dfrac{14}{614 \times 2} = 0.0114$
18–20	9	$\dfrac{9}{1,000 \times 2} = 0.0045$	$\dfrac{9}{600 \times 2} = 0.0075$
20–22	8	$\dfrac{8}{1,000 \times 2} = 0.0040$	$\dfrac{8}{591 \times 2} = 0.0068$
22–24	Total $\dfrac{3}{420}$	$\dfrac{3}{1,000 \times 2} = 0.0015$	$\dfrac{3}{583 \times 2} = 0.0026$

TABLE 8.3.2.2-4: TIME-TILL-FAILURE DATA FOR S = 1,000 MISSIONS/HR

TIME-TILL-FAILURE (HRS.)	CUMULATIVE FAILURES=F	$R\dfrac{S-F}{S}$
2	222	.778
4	267	.733
6	299	.701
8	326	.674
10	347	.653
12	362	.638
14	379	.621
16	386	.614
18	400	.600
20	409	.591
22	417	.583
24	420	.580
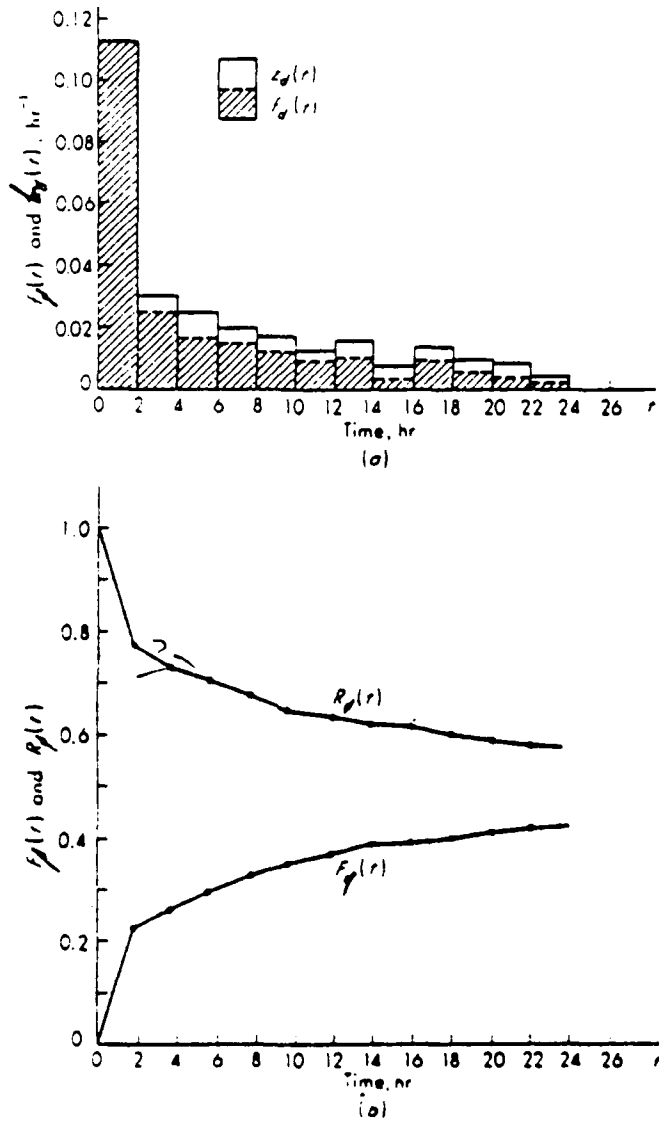
FIGURE 8.3.2.2-2: RELIABILITY FUNCTIONS FOR THE EXAMPLE GIVEN IN TABLE 8.3.2.2-3.

exponential, etc.) and on values of the distribution parameters estimated from the observed data. The third type of curve is the true reliability function of the population from which the sample observations were drawn. This last function can only be estimated (i.e., not determined precisely), although the limits within which it will fall a given percentage of the time can be defined.

Figure 8.3.2.2-3 presents a frequency distribution of failures in a fixed population of 90 items, over a 6-hour period. To obtain a survival curve from these data, the following simplified method is used.

During the first period of observation, from 0 to 1 hour, 4 of the original 90 items failed. The failure rate during this period was 4/90, or 0.0445, which is equivalent to a survival rate of 1 - 0.0445, or 0.9555. In the second period of observation, 21 of the 86 remaining items failed. The failure rate was 21/86, or 0.244, and the survival rate was 1 - 0.244, or 0.756. The tabulation above Figure 8.3.2.2-4 gives the failure rates and survival rates for the remaining periods of observation. It will be noted that the failure rate increases with time; also that the terms failure rate and hazard rate are not used synonymously.

To obtain a survival curve, which is the cumulative probability of survival with time, the probabiliy of survival in each time period is multiplied by the survival rate in the succeeding time period. Thus, 0.9555 x 0.756 = 0.723; 0.723 x 0.538 = 0.388, etc. The probability values are plotted versus the centers of the time periods as shown at the bottom of 8.3.2.2-4.

Figure 8.3.2.2-5 presents a frequency distribution of failures for a population in which the removal rate is constant with time. The approach described in connection with the normal curve yields the tabulation and exponential survival curve shown in Figure 8.3.2.2-6.

Survival curves for most electronic equipment/systems are of the exponential form. Survival curves for mechanical parts, on the other hand, are frequently of the normal or Weibull form. As parts wear out, their failure rate increases and their probability of survival decreases. A large number of such parts, all having normal or Weibull survival curves but each having a different mean life and variance, will produce a system malfunction rate which is essentially constant, since the mean lives of the parts will be randomly distributed.

To determine what type of population gives rise to a particular survival curve, the theoretical reliability function most closely resembling the curve is computed from sample parameters. The theoretical function is then matched to the observed curve by statistical techniques. If this procedure establishes that there is no significant difference between the observed and theoretical curves, the theoretical curve is usually employed for all additional calculations.

HOURS	NO. OF FAILURES
0 - 1	30
1 - 2	20
2 - 3	14
3 - 4	9
4 - 5	6
5 - 6	4

FIGURE 8.3.2.2-5:
EXPONENTIAL DISTRIBUTION OF FAILURES IN TIME

TIME	FAILURE RATE	SURVIVAL RATE	PROBABILITY OF SURVIVAL
0 - 1	0.333	0.667	0.667
1 - 2	0.333	0.667	0.444
2 - 3	0.350	0.650	0.289
3 - 4	0.346	0.654	0.189
4 - 5	0.353	0.647	0.122
5 - 6	0.364	0.636	0.078
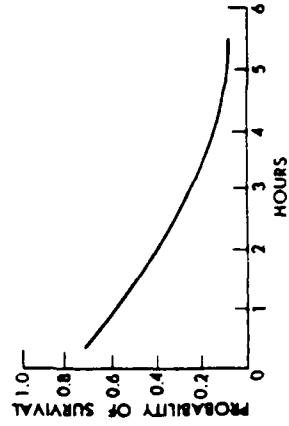
FIGURE 8.3.2.2-6:
CALCULATION AND PRESENTATION OF AN
EXPONENTIAL SURVIVAL CURVE

HOURS	NO. OF FAILURES
0 - 1	4
1 - 2	21
2 - 3	30
3 - 4	25
4 - 5	8
5 - 6	2

FIGURE 8.3.2.2-3:
NORMAL DISTRIBUTION OF FAILURES IN TIME

TIME	FAILURE RATE	SURVIVAL RATE	PROBABILITY OF SURVIVAL
0 - 1	0.0445	0.9555	0.9555
1 - 2	0.2440	0.7560	0.7230
2 - 3	0.4620	0.5380	0.3880
3 - 4	0.7140	0.2860	0.1110
4 - 5	0.8000	0.2000	0.0220
5 - 6	1.0000	0.0000	---

FIGURE 8.3.2.2-4:
CALCULATION AND PRESENTATION OF
A NORMAL SURVIVAL CURVE

Figures 8.3.2.2-7 and 8.3.2.2-8 portray observed and theoretical probability of survival, R(t), curves for the case of normal and exponential distributions of time to failure. Note that the mean life for the exponential case is 0.368 value of R(t), whereas for the normal case it is 0.5 of R(t). This is due to the symmetrical characteristic of the normal distribution, versus the skewed characteristic of the exponential.

Thus, if one can develop a mathematical expression for R(t), it can be shown that the mean time to failure is given by:

$$MTTF = \int_0^\infty R(t)dt \qquad (8.3)$$

8.3.2.3.1 COMPUTATION OF THEORETICAL EXPONENTIAL RELIABILITY FUNCTION

When the form of the distribution is sufficiently well defined, it is possible to estimate the reliability function in terms of the parameters of the distribution. This method has the advantage of permitting utilization of all the accumulated knowledge concerning the items in the population. In addition, the reliability function can be summarized by specifying the values of the parameters, and can be compared with other reliability functions merely by comparing the values of the summarized data.

For the case of an equipment/system which is repaired upon failure, the reliability function is given by:

$$R(t) = e^{-t/MTBF} \qquad (8.4)$$

where

t = time at which R(t) is calculated
MTBF = mean time between failures, given by

$$MTBF = \frac{nt}{r} \qquad (8.5)$$

where

n = the number of equipments operated to time t
r = the number of failures, with the last failure occurring at time t

For example, assume that in a sample of twenty equipments operated for 773 hours, we observed 10 failures (each of which was repaired), with the last failure occurring at 773 hours.

Then

$$MTBF = \frac{nt}{r} = \frac{(20)(773)}{10} = 1546 \text{ hrs}.$$

$$R(t) = e^{-t/1546}$$

SAMPLE MEAN LIFE $\cong$ 3230 HOURS

95% CONFIDENCE LIMITS = 2395 - 4615 HOURS

——— OBSERVED
– – – THEORETICAL
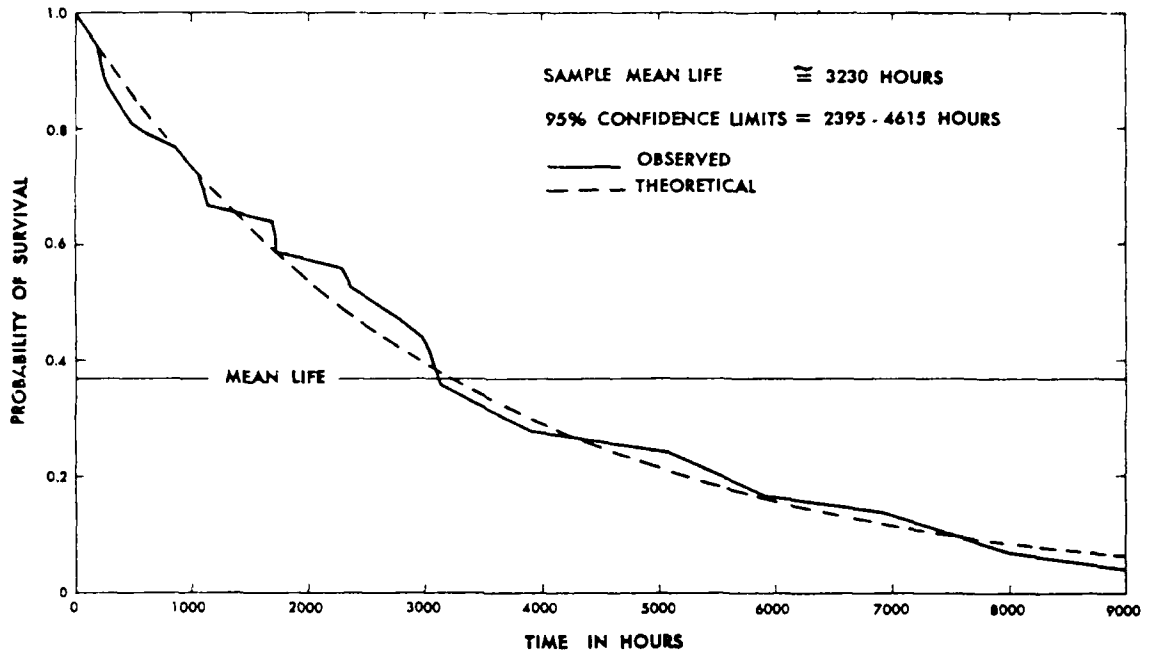
FIGURE 8.3.2.2-7:

OBSERVED AND THEORETICAL EXPONENTIAL SURVIVAL CURVES

SAMPLE MEAN LIFE $\cong$ 2950 HOURS

STANDARD DEVIATION $\cong$ 1000 HOURS

95% CONFIDENCE LIMITS = 2711 - 3189 HOURS

——— OBSERVED
– – – THEORETICAL
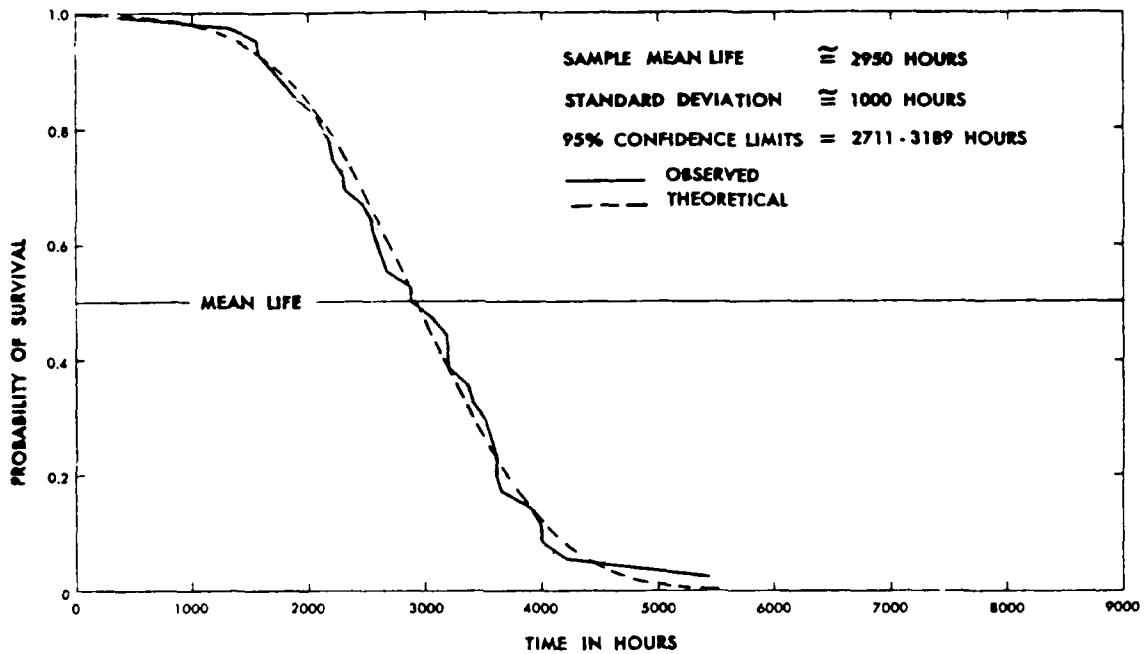
FIGURE 8.3.2.2-8:

OBSERVED AND THEORETICAL NORMAL SURVIVAL CURVES

Table 8.3.2.3.1-1 shows the computations for R(t) for selected values of
t. Figure 8.3.2.3.1-1 shows the actual reliability function (solid
line) plotted from the data versus the theoretical exponential function
from column 3 of Table 8.3.2.3.1-1. Determination of confidence
intervals is discussed briefly in the next section.

8.3.2.3.2 COMPUTATION FOR NORMAL RELIABILITY FUNCTION

Table 8.3.2.3.2-1 presents some observed failure data for a sample of
twenty units tested to failure, and the failure times observed. The
units were known to follow a normal distribution of time to failure.

The sample mean, $\bar{x}$, an estimate of μ, is given by:

$$\bar{x} = \sum_{i=1}^{20} x_{i/n} = \frac{39104}{20} = 1955.2 \text{ hrs}$$

The sample standard deviation, s, an estimate of σ is given by:

$$s = \left[\frac{\sum_{i=1}^{20} (x_i - \bar{x})^2}{n - 1} \right]^{1/2} = 886.6 \text{ hrs.}$$

where

x_i = i^{th} failure time
n = sample size
$\bar{x}$ = sample mean

Figure 8.3.2.3.2-1 shows the actual or nonparametric reliability
function plotted from the data versus the theoretical function
calculated using the estimates of μ and σ. The thecretical values were
obtained from the expression

$$R(x) = P\left(Z > \frac{x - \mu}{\sigma} \right)$$

where the value of Z was obtained from a table of the normal standard
distribution (Table A-1 of Section 5).

8.3.2.4 CENSORED DATA

If a sample contains both complete and incomplete lifetimes, the incom-
plete lifetimes are referred to as "censored" observations. These
consist primarily of lifetimes which are too long to be observed
completely ("terminated" observations) and lifetimes in which the item
being observed is lost before completion of observation ("lost"
observation). In the case of terminated observations, the length of
observation time is controlled; in the case of lost observations, the
length of observation time is not controlled. In either case, the
investigator knows that the lifetime of the item exceeds the period of
time during which the item was being observed. Terminated observations

TABLE 8.3.2.3.1-1: <u>COMPUTATION OF THEORETICAL EXPONENTIAL</u>
<u>RELIABILITY FUNCTION FOR MTBF = 1546 HOURS</u>

(1) t	(2) t/MTBF	(3) $e^{-t/MTBF}$
0	0	1.000
96	0.0621	0.9398
216	0.1397	0.8696
312	0.2018	0.8173
456	0.2950	0.7445
552	0.3571	0.6997
696	0.4502	0.6375
792	0.5123	0.5991
888	0.5744	0.5630
960	0.6210	0.5374
1200	0.7762	0.4602
1416	0.9159	0.4002
1546	1.0000	0.3679
1896	1.2264	0.2933
2064	1.3351	0.2631
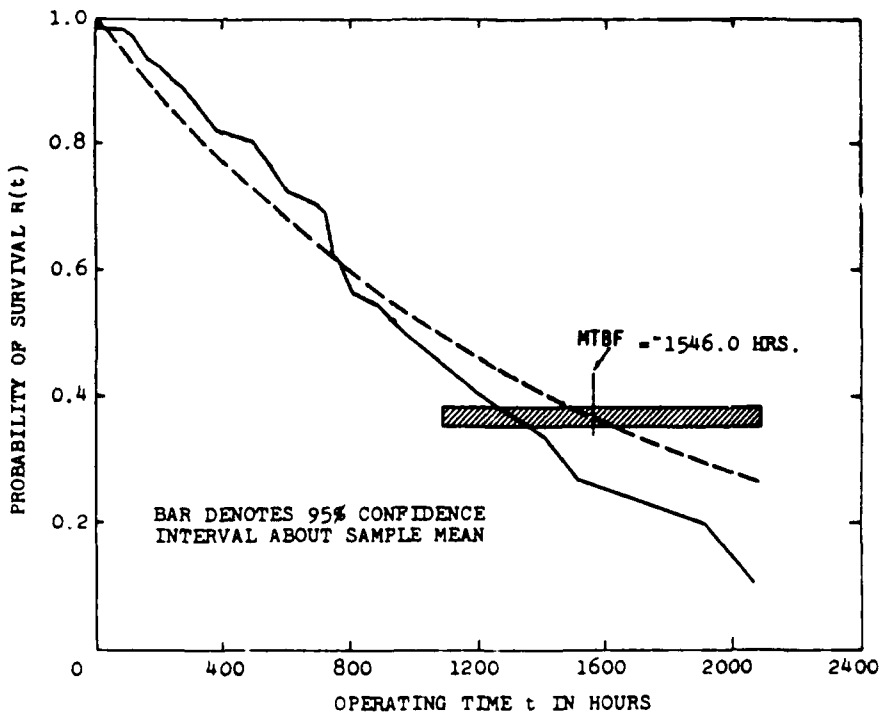
FIGURE 8.3.2.3.1-1: <u>ACTUAL RELIABILITY FUNCTION AND THEORETICAL</u>
<u>EXPONENTIAL RELIABILITY FUNCTION</u>

TIME TO FAILURE, t, IN HRS (10^2)
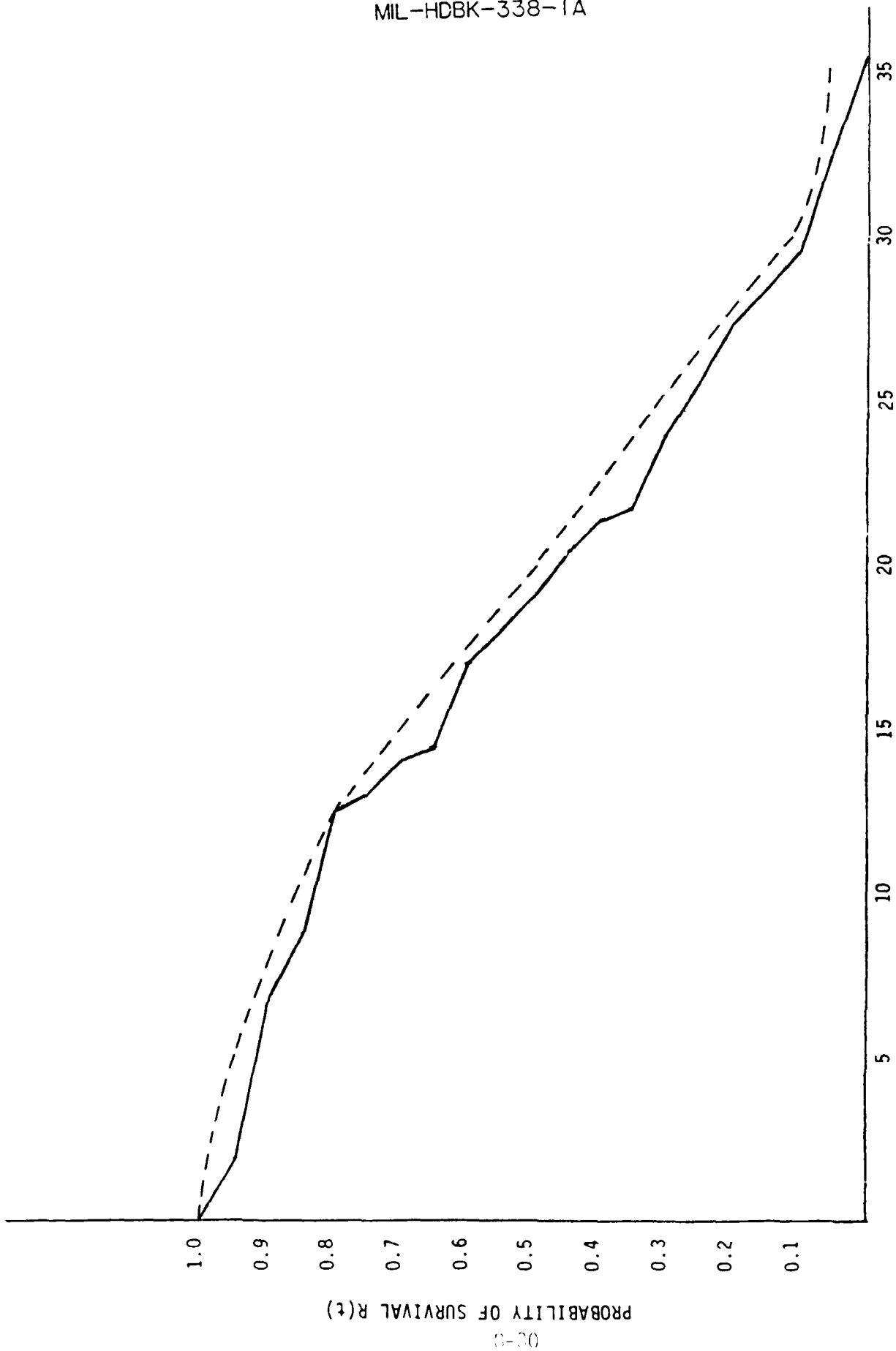
FIGURE 8.3.2.3.2-1:   NON-PARAMETRIC AND THEORETICAL NORMAL RELIABILITY FUNCTIONS

PROBABILITY OF SURVIVAL R(t)

TABLE 8.3.2.3.2-1: OBSERVED FAILURE DATA

Time	Probability of Survival, R =
175	0.95
695	0.9
872	0.85
1250	0.8
1291	0.75
1402	0.7
1404	0.65
1713	0.6
1741	0.55
1893	0.5
2025	0.45
2115	0.4
2172	0.35
2418	0.3
2583	0.25
2725	0.2
2844	0.15
2980	0.1
3268	0.05
3538	0

do not present a problem to the investigator other than to increase the complexity of his calculations, but lost observations may constitute a real problem because they may be associated with only a portion of the population.

For example, for the case of the exponential distribution in which n items are put on test, r of them fail at time t_1, t_2 ... t_r, with the test discontinued at t_r when the rth failure occurs, the MTBF is given by:

$$MTBF = \sum_{i=1}^{r} t_i + (n - r) t_r \tag{8.6}$$

where t_i is the time of each failure and (n - r) represents the number of surviving items at time t_r. In this nonreplacement case, the failed items are not repaired or replaced upon failure.

For the case where k components were withdrawn even though they may not have caused an equipment failure, the expression is given by:

$$MTBF = \frac{\sum_{i=1}^{r} t_i + (n - r) t_r}{r - k} \tag{8.7}$$

where the sum Σt_i is the operating time accumulated by the failed and withdrawn, or censored, components and r is the sum of the failed and withdrawn components.

The mathematics become somewhat more difficult when analyzing censored data where distributions other than the exponential are involved, or when using nonparametric methods. These cases are treated in detail in References 5, 7, 8 and 9.

8.3.2.5 CONFIDENCE LIMITS AND INTERVALS

Previously, we discussed methods of obtaining point estimates of reliability parameters, e.g., R(t), λ , MTBF, etc. For most practical applications, we are interested in the accuracy of the point estimate and the confidence which we can attach to it. We know that statistical estimates are more likely to be closer to the true value as the sample size increases. Only the impossible situation of having an infinitely large number of samples to test could give us 100 percent confidence or certainty that a measured value of a parameter coincides with the true value. For any practical situation, therefore, we must establish confidence intervals or ranges of values between which we know, with a probability determined by the finite sample size, that the true value of the parameter lies.

Confidence intervals around point estimates are defined in terms of a lower confidence limit L and an upper confidence limit U. If, for example, we calculate the confidence limits for a probability of, say,

95 percent, this means that in 95 percent of the cases we can be sure the true value of the reliability parameter will lie within the calculated limits, or in 5 percent of the cases it will lie outside these limits. If we want to be 99 percent sure that the true value lies within certain limits for a given sample size, we must widen the interval or test a larger number of samples if we wish to maintain the same interval. The problem, then, is reduced to one of either determining the interval within which the true parametric value lies with a given probability for a given sample size, or determining the sample size required to assure us with a specified probability that true parametric value lies within a specific interval.

Thus, we would like to be able to make assertions such as:

$$P\left[\left(\hat{\theta}_{lower} < \theta < \hat{\theta}_{upper}\right)\right] = \eta \qquad (8.8)$$

where θ is some unknown population parameter, $\hat{\theta}_{lower}$ and $\hat{\theta}_{upper}$ are estimators associated with a random sample and η is a probability value such as 0.99, 0.95, 0.90, etc. If, for instance, $\eta = 0.95$ we refer to the interval

$$\left(\theta_L < \theta < \theta_U\right) \qquad (8.9)$$

for particular values of $\hat{\theta}_{lower}$ and $\hat{\theta}_{upper}$ as a 95% confidence interval. In this case we are willing to accept a 5% probability (risk) that our assertion is not, in fact, true.

Or, we may also want to make statements such as:

$$P\left[\theta > \hat{\theta}_{lower}\right] = \eta \qquad (8.10)$$

in which case we make statements like, "we are 90% confident that the true MTBF is greater than some lower confidence limit (or measured value)." Eq. (8.10) is the case of the one sided confidence limit, versus Eq. (8.9) which is a two sided confidence limit, or confidence interval.

To help clarify the concept of a confidence interval we can look at the situation in a geometrical way. Suppose we draw repeated samples (x_1, x_2) from a population, one of whose parameters, we desire to bracket with a confidence interval. We construct a three dimensional space with the vertical axis corresponding to θ and with the two horizontal axes corresponding to values of x_1 and x_2 (see Figure 8.3.2.5-1). The actual value of the population parameter θ is marked on the vertical axis and a horizontal plane is passed through this point. Now we take a random sample (x_1, x_2) from which we calculate the values θ_U and θ_L at, say, the 95% confidence level. The interval defined by θ_U and θ_L is plotted on the figure.

Next, we take a second sample (x'_1, x'_2) from which we calculate the value θ'_U and θ'_L at the 95% level. This interval is plotted on the figure. A third sample (x''_1, x''_2) yields the values θ''_U and θ''_L, etc.
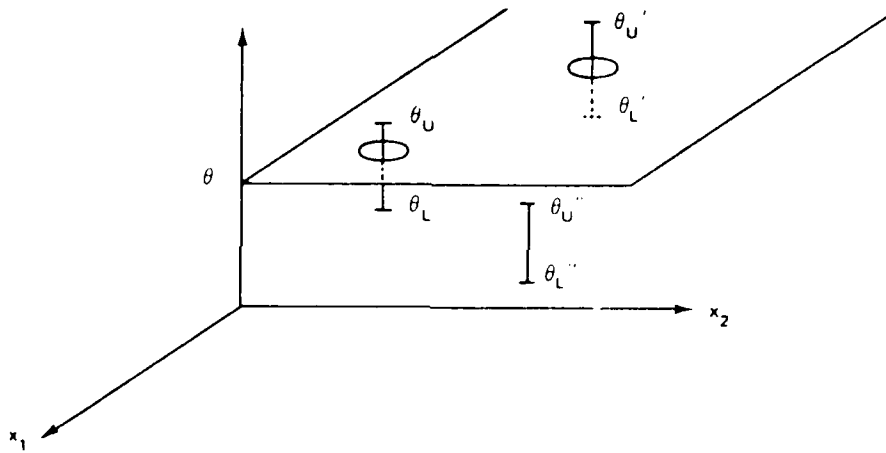
FIGURE 8.3.2.5-1: GEOMETRICAL INTERPRETATION OF THE CONCEPT OF A CONFIDENCE INTERVAL

In this way we can generate a large family of confidence intervals. The confidence intervals depend only on the sample values (x_1, x_2), (x'_1, x'_2), etc., and hence we can calculate these intervals without knowledge of the true value of θ. If the confidence intervals are all calculated on the basis of 95% confidence and if we have a very large family of these intervals, then 95% of them will cut the horizontal plane through θ (and thus include θ) and 5% of them will not.

The process of taking a random sample and computing from it a confidence interval is equivalent to the process of reaching into a bag containing thousands of confidence intervals and grabbing one at random. If they are all 95% intervals, our chance of choosing one that does indeed include θ will be 95%. In constrast, 5% of the time we will be unlucky and select one that does not include θ (like the interval (θ''_U, θ''_L) in Figure 8.3.2.5-1. If a risk of 5% is judged too high, we can go to 99% intervals, for which the risk is only 1%. As we go to higher confidence levels (and lower risks) the lengths of the intervals increase until for 100% confidence levels (and lower risks) the interval includes every conceivable value of θ (I am 100% confident that the number of defective items in a population of 10,000 is somewhere between 0 and 10,000). For this reason 100% confidence intervals are of little interest.

Let us now look at some simple examples of how these concepts are applied to analyze reliability for some of the more commonly used distributions.

8.3.2.5.1 CONFIDENCE LIMITS - NORMAL DISTRIBUTION

When the lives of n components are known from a wearout test and we compute their mean M and their standard deviation s, and when n is large so that we can assume that $s \approx \sigma$, the upper and lower confidence limits can be readily evaluated from Table 8.3.2.5.1-1 for the more commonly used confidence levels:

TABLE 8.3.2.5.1-1: CONFIDENCE LIMITS - NORMAL DISTRUBUTION

$K_{\alpha/2}$	Two-sided confidence intervals $M \pm K_{\alpha/2}\, s/\sqrt{n}$	Confidence levels $100(1-\alpha)\%$
0.84	$\hat{M} \pm 0.84s/\sqrt{n}$	60.0
1.28	$\hat{M} \pm 1.28s/\sqrt{n}$	80.0
1.64	$\hat{M} \pm 1.64s/\sqrt{n}$	90.0
1.96	$\hat{M} \pm 1.96s/\sqrt{n}$	95.0
2.58	$\hat{M} \pm 2.58s/\sqrt{n}$	99.0

Strictly speaking, this procedure of assigning confidence intervals to an estimate is correct only when the true standard deviation σ of component wearout is known and used instead of s in Table 8.3.2.5.1-1. However, it can be applied in reliability work as an approximation whenever the estimate s, of σ, was obtained from a large sample, i.e., when the number of failures is at least 25, and preferably, more. In fact, it can be shown for samples of 20, $K_{\alpha/2}$ (at the 95% confidence level) is 2.09 vs. a value of 1.96 for an infinite number of samples.

Figure 8.3.2.5.1-1 graphically illustrates what is being done. Since the normal distribution is symmetrical, we are computing the confidence interval as the area $(1 - \alpha)$ under the curve, leaving an area $\alpha/2$ in the left and right hand tails which is outside of the confidence interval (CI). For example, using the calculated values of M (or $\bar{x}$) and s obtained from the data in Table 8.3.2.5.1-2, the CI at the 95% level is

$$\hat{M} \pm 1.96 \, s/\sqrt{n} \quad = 1955.2 \pm 1.96 \, (886.6/\sqrt{20})$$

$$= 1955.2 \pm 388.6$$

$$= (2343.8, \, 1566.6)$$

In other words, we can be 95% confident that the true value of the mean life (M) lies between 1566.6 and 2343.8 hours.

Actually in reliability work, we are usually more interested in the lower confidence limit L of the mean wearout life than in the upper limit. Given a measured value of $\hat{M}$, we would like to make some statement about our confidence that the true value of M exceeds some minimum value.

When only the lower confidence limit, L, is of interest, we apply the procedure of so called "one sided" confidence limits, as opposed to the two sided CI of the preceding example. The problem is to assure ourselves (or our customer) that the true mean life, M, is equal to or larger than some specified minimum value with a probability of $(1 - \alpha)$.

Whereas in the case of the two sided confidence limits, we had an area of $\alpha/2$ under the left tail of the normal curve (Figure 8.3.2.5.1-1), we now have an area α to the left of L and an area $(1 - \alpha)$ to the right.

Therefore, the estimate of mean life obtained from the data should be:

$$\hat{M} \geq L + K_\alpha \, \sigma/\sqrt{n} \tag{8.11}$$

If this equation is not satisfied, the requirement that the true M must be at least L at the specified 100 $(1 - \alpha)$ percent confidence level has not been fulfilled.
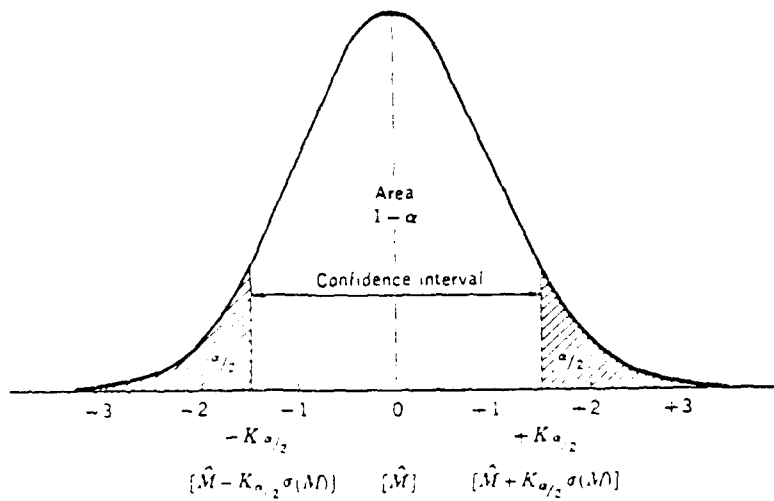
FIGURE 8.3.2.5.1-1: TWO-SIDED CONFIDENCE LEVEL, INTERVAL, AND LIMITS

Table 8.3.2.5.1-2, in which the assumption $s = \sigma$ is made, allows a quick check as to whether an estimate $\hat{M}$ obtained from a sample size n fulfills the requirement that the true M must not be smaller than the specified minimum L. Only the more commonly used confidence levels are given.

TABLE 8.3.2.5.1-2: CONFIDENCE INTERVAL

$K_{\alpha/2}$	The estimate $\hat{M}$ must exceed: $L + K_{\alpha/2}\, s/\sqrt{n}$	Confidence levels $100(1-\alpha)\%$
0.25	$L + 0.25s/\sqrt{n}$	60
0.52	$L + 0.52s/\sqrt{n}$	70
0.84	$L + 0.84s/\sqrt{n}$	80
1.28	$L + 1.28s/\sqrt{n}$	90
1.64	$L + 1.64s/\sqrt{n}$	95
2.33	$L + 2.33s/\sqrt{n}$	99

Once again, using the data and calculated values of $\hat{M}$ and s from Table 8.3.2.5.1-2, assume that we would like to be 95% confident that the true $M \geq 1500$ hours. The equation from Table 8.3.2.5.1-2 is

$$\hat{M} \geq L + 1.64\, s/\sqrt{n}$$

$$1955.2 \geq 1500 + 1.64(886.6)/\sqrt{20}$$

$$1955.2 \geq 1500 + 325$$

$$1955.2 \geq 1825$$

Since the inequality is satisfied, the requirement has been met.

As previously mentioned, the above procedure can be applied if the sample size n is at least 25. However, similar procedures also apply to smaller sample sizes except that now we cannot assume that $s = \sigma$, and we must use another set of equations based on Student's t distribution. Actually, all we do is replace the normal percentage points $K_{\alpha/2}$ and K_α in the above developed equations by the tabulated percentage points $t_{\alpha/2;n-1}$ and $t_{\alpha;n-1}$ of the t distribution, where n-1 is called the degrees of freedom and n is the number of failures. Student's t tables are available in most standard statistical texts.

For example, for the two-side CI example using the data from Table 8.3.2.5.1-2 and calculated values of $\hat{M}$ and s,

$$\hat{M} \pm t_{\alpha/2;n-1}\, s/\sqrt{n} = 1955.2 \pm 2.09(886.6)/\sqrt{20}$$

$$= 1955.2 \pm 414.4$$

$$= (2370,\ 1541.2)$$

which is a slightly wider CI than the case where it was assumed the $s = \sigma$.

8.3.2.5.2 CONFIDENCE LIMITS - EXPONENTIAL DISTRIBUTION

Two situations have to be considered for estimating confidence intervals: one in which the test is run until a preassigned number of failures ($r*$) occurs, and one in which the test is stopped after a preassigned number of test hours ($t*$) is accumulated. The formula for the confidence interval employs the X^2 (chi-square) distribution. A short table of X^2 values are given in Table 8.3.2.5.2-1. The general notation used is

$$X^2 (p, d)$$

where p and d are two constants used to choose the correct value from the table.

The quantity p is a function of the confidence coefficient; d, known as the degrees of freedom, is a function of the number of failures. Equations (8.12) and (8.13) are for one sided or two sided 100 ($1-\alpha$) percent confidence intervals. For nonreplacement tests with a fixed truncation time, the limits are only approximate.

Equations for Confidence Limits on Mean Life

Type of Confidence Limits	Fixed Number of Failures, $r*$	Fixed Truncation† Time $t*$	
One Sided (Lower Limit)	$\left(\dfrac{2T}{\chi^2_{\alpha,2r}}, \infty \right)$	$\left(\dfrac{2T}{\chi^2(\alpha,2r+2)}, \infty \right)$	(8.12)
Two Sided (Upper and Lower Limits)	$\left(\dfrac{2T}{\chi^2(\frac{\alpha}{2},2r)}, \dfrac{2T}{\chi^2(1-\frac{\alpha}{2},2r)} \right)$	$\left(\dfrac{2T}{\chi^2(\frac{\alpha}{2},2r+2)}, \dfrac{2T}{\chi^2(1-\frac{\alpha}{2},2r)} \right)$	(8.13)

†For non-replacement tests, only one-sided intervals are possible
for r = 0. Use 2n degrees of freedom for the lower limit if
r = n.

The terms used are identified as follows:

n = number of items placed on test at time t = 0

$t*$ = time at which the life test is terminated

$\hat{\theta}$ = mean life (or MTBF for the case of replacement or repair upon failure)

$\chi^2(\frac{\alpha}{2}, 2r+2)$, for example, is the $\frac{\alpha}{2}$-percentage point of the chi-square distribution for (2r+2) degrees of freedom

r = number of failures accumulated at time $t*$

$r*$ = preassigned number of failures

α = acceptable risk of error

$1-\alpha$ = confidence level

TABLE 8.3.2.5.2-1

DISTRIBUTION OF x^2 (Chi-Square)

Probability

DF	0.99	0.975	0.95	0.90	0.80	0.75	0.50	0.25	0.20	0.10	0.05	0.025	0.01	0.001
1	0.03157	0.03983	0.00393	0.0158	0.0642	0.10153	0.455	1.323	1.642	2.706	3.841	5.024	6.635	10.827
2	0.0201	0.0506	0.103	0.211	0.446	0.5753	1.386	2.772	3.219	4.605	5.991	7.377	9.210	13.815
3	0.115	0.216	0.352	0.584	1.005	1.2125	2.366	4.108	4.642	6.251	7.815	9.348	11.341	16.268
4	0.297	0.484	0.711	1.064	1.649	1.9225	3.357	5.385	5.989	7.779	9.488	11.143	13.277	18.465
5	0.554	0.831	1.145	1.610	2.343	2.674	4.351	6.625	7.289	9.236	11.070	12.832	15.086	20.517
6	0.872	1.237	1.635	2.204	3.070	3.454	5.348	7.840	8.558	10.645	12.592	14.449	16.812	22.457
7	1.239	1.689	2.167	2.833	3.822	4.254	6.346	9.037	9.803	12.017	14.067	16.013	18.475	24.322
8	1.646	2.179	2.733	3.490	4.594	5.070	7.344	10.218	11.030	13.362	15.507	17.534	20.090	26.125
9	2.088	2.700	3.325	4.168	5.380	5.898	8.343	11.388	12.242	14.684	16.919	19.023	21.666	27.877
10	2.558	3.247	3.940	4.865	6.179	6.737	9.342	12.548	13.442	15.987	18.307	20.483	23.209	29.588
11	3.053	3.816	4.575	5.578	6.989	7.584	10.341	13.701	14.631	17.275	19.675	21.920	24.725	31.264
12	3.571	4.404	5.226	6.304	7.807	8.438	11.340	14.845	15.812	18.549	21.026	23.336	26.217	32.909
13	4.107	5.008	5.892	7.042	8.634	9.299	12.340	15.984	16.985	19.812	22.362	24.735	27.688	34.528
14	4.660	5.629	6.571	7.790	9.467	10.165	13.339	17.117	18.151	21.064	23.685	26.119	29.141	36.123
15	5.229	6.262	7.261	8.547	10.307	11.036	14.339	18.245	19.311	22.307	24.996	27.488	30.578	37.697
16	5.812	6.907	7.962	9.312	11.152	11.912	15.338	19.368	20.465	23.542	26.296	28.845	32.000	39.252
17	6.408	7.564	8.672	10.085	12.002	12.791	16.338	20.488	21.615	24.769	27.587	30.191	33.409	40.790
18	7.015	8.231	9.390	10.865	12.857	13.675	17.338	21.605	22.760	25.989	28.869	31.526	34.805	42.312
19	7.633	8.906	10.117	11.651	13.716	14.562	18.338	22.717	23.900	27.204	30.144	32.852	36.191	43.820
20	8.260	9.591	10.851	12.443	14.578	15.452	19.337	23.827	25.038	28.412	31.410	34.169	37.566	45.315
21	8.897	10.283	11.591	13.240	15.445	16.344	20.337	24.935	26.171	29.615	32.671	35.479	38.932	46.797
22	9.542	10.982	12.338	14.041	16.314	17.239	21.337	26.039	27.301	30.813	33.924	36.780	40.289	48.268
23	10.196	11.688	13.091	14.848	17.187	18.137	22.337	27.141	28.429	32.007	35.172	38.075	41.638	49.728
24	10.856	12.400	13.848	15.659	18.062	19.037	23.337	28.241	29.553	33.196	36.415	39.364	42.980	51.179
25	11.524	13.119	14.611	16.473	18.940	19.939	24.337	29.339	30.675	34.382	37.652	40.646	44.314	52.620
26	12.198	13.844	15.379	17.292	19.820	20.843	25.336	30.434	31.795	35.563	38.885	41.923	45.642	54.052
27	12.879	14.573	16.151	18.114	20.703	21.749	26.336	31.528	32.912	36.741	40.113	43.194	46.963	55.476
28	13.565	15.308	16.928	18.933	21.588	22.657	27.336	32.620	34.027	37.916	41.337	44.460	48.278	56.893
29	14.256	16.047	17.708	19.768	22.475	23.566	28.336	33.711	35.139	39.087	42.557	45.722	49.588	58.302
30	14.953	16.791	18.493	20.599	23.364	24.476	29.336	34.799	36.250	40.256	43.773	46.98	50.892	59.703

Note that T is computed as follows, depending on the type of test procedure:

<u>Replacement Tests</u> (failure replaced or repaired)   (8.14)

$$T = nt*$$

<u>Non-Replacement Tests</u> $T = \left(\sum_{i=1}^{r} t_i \right) + (n - r)t*$ (8.15)

where t_i = time of the ith failure

<u>Censored Items</u> (withdrawal or loss of items which have not failed)

(a) If failures are replaced and censored items are not replaced

$$T = \sum_{j=1}^{r} t_j + (n-c)t*$$ (8.16)

where

t_j = time of censorship
c = number of censored items

(b) If failures are not replaced

$$T = \sum_{i=1}^{r} t_i + \sum_{j=1}^{c} t_j + (n-r-c)t*$$ (8.17)

<u>Example #1.</u> Twenty items undergo a replacement test. Testing continues until ten failures are observed. The tenth failure occurs at 80 hours. Determine (1) the mean life of the items; and (2) the one-sided and two-sided 95% confidence intervals for the MTBF.

(1) From equation (8.4)

$$MTBF = \frac{nt*}{r} = \frac{(20)\,(80)}{10} = 160 \text{ hrs}$$

(2) α = 1 - Confidence Level $=$ 1-0.95 = 0.05

$2r$ = 2 (number of failures) = 2(10) = 20

$$\frac{2T}{\chi^2(\alpha,2r)}, \infty = \frac{2(1600)}{\chi^2(0.05,20)}, \infty = \frac{3200}{31.41}, \infty$$

= <u>101.88 hours</u> for the lower (one-sided) 95% confidence level

Where χ^2 (0.05, 20) = 31.41 is from Table 8.3.2.5.2-1.

In other words, we are 95% confident that the true MTBF exceeds 101.88 hrs.

(3) From Equation (8.13)

$$\left(\frac{2T}{\chi^2\left(\frac{\alpha}{2}, \; 2r\right)}, \; \frac{2T}{\chi^2\left(1-\frac{\alpha}{2}, \; 2r\right)}\right) = \left(\frac{3200}{34.17}, \; \frac{3200}{9.591}\right)$$

= <u>93.65 hours</u> for the lower (two sided) 95% confidence interval

and <u>333.65 hours</u> for the upper (two sided) 95% confidence interval

*Again, using Table 8.3.2.5.2-1 to find χ^2

Or, we are 95% confident that the true MTBF lies between 93.65 and 333.65 hrs.

<u>Example #2</u>. Twenty items undergo a nonreplacement test, which is terminated at 100 hours. Failure times observed were 10, 16, 17, 25, 31, 46, and 63 hours. Calculate (1) the one sided approximate 90% confidence interval (α= 0.10), and (2) the two sided approximate 90% confidence limits of θ(mean life).

(1) From Equations (8.12) and (8.15)

$$\left(\frac{2T}{\chi^2(\alpha, \; 2r + 2)}, \infty\right) = \left(\frac{2\left[\left(\sum_{i=1}^{7} t_i\right) + (20-7)(100)\right]}{\chi^2(.10,16)}, \; \infty\right)$$

$$\in \left(\frac{3020}{23.54}, \infty\right)$$

■ <u>128.3 hours</u> for the lower single-sided 90% confidence interval

(2) From Equation (8.13)

$$\left(\frac{2T}{\chi^2\left(\frac{\alpha}{2}, \; 2r + 2\right)}, \; \frac{2T}{\chi^2\left(1 - \frac{\alpha}{2}, \; 2r\right)}\right) = \left(\frac{3020}{26.30}, \; \frac{3020}{6.57}\right)$$

= <u>114.83 hours</u> for the lower (two-sided) 90% confidence interval

and <u>459.67 hours</u> for the upper (two-sided) 90% confidence interval.

Table 8.3.2.5.2-2 presents the factor $2/\chi^2(p,d)$ for one sided and two sided confidence limits, at six confidence levels for each. Multiplying the appropriate factor by the observed total life T gives a confidence limit on χ^2. Figure 8.3.2.5.2-1 presents a graphical technique for determining upper and lower confidence limits for tests truncated at a fixed time, when the number of failures is known.

TABLE 8.3.2.5.2-2

FACTORS FOR CALCULATION OF MEAN LIFE
CONFIDENCE INTERVALS FROM TEST DATA (FACTORS = $2/\chi^2(p,d)$)

(Assumption of Exponential Distribution)

Confidence level key (Two-Sided / One-Sided):

- 99% Two-Sided / 99-1/2% One-Sided
- 98% Two-Sided / 99% One-Sided
- 95% Two-Sided / 97-1/2% One-Sided
- 90% Two-Sided / 95% One-Sided
- 80% Two-Sided / 90% One-Sided
- 60% Two-Sided / 80% One-Sided

Lower Limit

r	99%	98%	95%	90%	80%	60%
2	.185	.217	.272	.333	.433	.619
4	.134	.151	.180	.210	.257	.334
6	.108	.119	.139	.159	.188	.234
8	.0909	.100	.114	.129	.150	.181
10	.0800	.0857	.0976	.109	.125	.149
12	.0702	.0759	.0856	.0952	.107	.126
14	.0635	.0690	.0765	.0852	.0948	.109
16	.0588	.0625	.0693	.0760	.0848	.0976
18	.0536	.0571	.0633	.0693	.0769	.0878
20	.0500	.0531	.0585	.0635	.0703	.0799
22	.0465	.0495	.0543	.0589	.0648	.0732
24	.0439	.0463	.0507	.0548	.0601	.0676
26	.0417	.0438	.0476	.0513	.0561	.0629
28	.0392	.0413	.0449	.0483	.0527	.0588
30	.0373	.0393	.0425	.0456	.0496	.0551
32	.0355	.0374	.0404	.0433	.0469	.0519
34	.0339	.0357	.0385	.0411	.0445	.0491
36	.0325	.0342	.0367	.0392	.0423	.0466
38	.0311	.0327	.0351	.0375	.0405	.0443
40	.0299	.0314	.0337	.0359	.0385	.0423

Upper Limit

r	99%	98%	95%	90%	80%	60%
2	200.0	100.0	39.58	19.383	9.462	4.47
4	10.00	6.667	4.102	2.826	1.882	1.21
6	3.007	2.3077	1.613	1.221	.909	.652
8	1.481	1.212	.921	0.733	.573	.437
10	.909	.789	.600	.508	.411	.324
12	.645	.555	.454	.383	.317	.256
14	.500	.431	.355	.305	.257	.211
16	.385	.345	.290	.251	.215	.179
18	.322	.286	.243	.213	.184	.156
20	.270	.242	.208	.184	.158	.137
22	.232	.208	.182	.162	.142	.123
24	.200	.185	.161	.144	.128	.111
26	.178	.164	.144	.130	.116	.101
28	.161	.147	.131	.118	.106	.0927
30	.145	.133	.119	.108	.0971	.0856
32	.131	.122	.109	.0997	.0899	.0795
34	.122	.113	.101	.0925	.0834	.0742
36	.111	.104	.0939	.0899	.0781	.0696
38	.103	.0971	.0874	.0804	.0732	.0656
40	.0968	.0901	.0820	.0756	.0689	.0619

To Use: Multiply value shown by total part hours to get MTBF figures in hours.

Note: $d = 2r$, except for the lower limit on tests truncated at a fixed time and where $r < n$. In such cases, use $d = 2(r + 1)$.
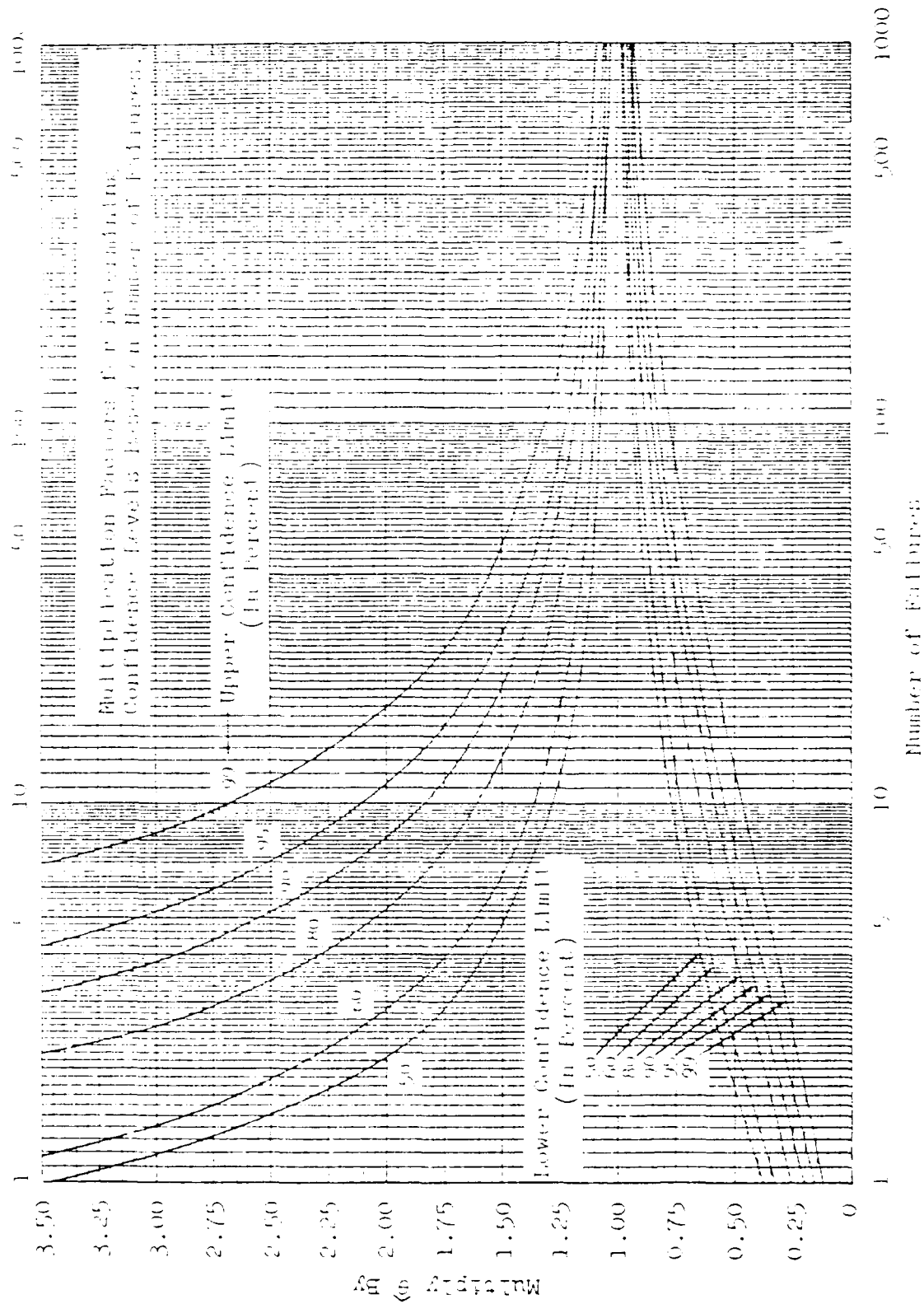
FIGURE 8.3.2.5.2-1

MULTIPLICATION RATIOS FOR DETERMINING UPPER AND LOWER
CONFIDENCE LIMITS VS NUMBER OF FAILURES FOR TESTS TRUNCATED AT A FIXED TIME

Reliability Estimates (Exponential Distribution)

We know the probability of (or proportion of items) surviving t hours is found by:

$$\hat{R}(t) = e^{-t/\theta} \tag{8.18}$$

The confidence interval on R(t) is

$$(e^{-t/\hat{\theta}_L} < R(t) < e^{-t/\hat{\theta}_U})$$

where

$\hat{\theta}_L$ and $\hat{\theta}_U$ are the lower and upper confidence limits on $\hat{\theta}$.

Example #3. Based on the data of Example 1, (1) what is the probability of an item's surviving 100 hours? (2) what are the two sided 95% confidence limits on this probability?

(1) From Equation (8.18)

$$\hat{R}(100) = e^{-100/\hat{\theta}} = e^{-100/160} = 0.535$$

(2) The two-sided confidence limits =

$$(e^{-100/93.65}, e^{-100/333.65})$$

$$= (0.344, 0.741)$$

8.3.2.5.3 CONFIDENCE-INTERVAL ESTIMATES FOR THE BINOMINAL DISTRIBUTION

For situations where reliability is measured as a ratio of the number of successes to the total number of trials, e.g., one shot items, missiles, etc., the confidence interval is determined by consideration of the binominal distribution. Table XI of Hald's Statistical Tables and Formulas (John Wiley and Sons, Inc., New York, 1952) and Ref. 10 gives 95% and 99% confidence limits for a wide range of values. Figure 8.3.2.5.3-1 allows a rough estimate to be made when the number of successes (S) and the number of trials (N) are known.

Example #4. S = 8; N = 10. (a) What is the reliability estimate? (b) What are the two sided upper and lower 95% confidence limits? Answers: (a) 0.80; (b) 0.98 and 0.43.

More detailed analyses of confidence limits and intervals, with many more examples under a variety of circumstances, and for a variety of disitributions, e.g., binominal, gamma, Weibull, etc., are given in Refs. 5, 8, 9 and 10.
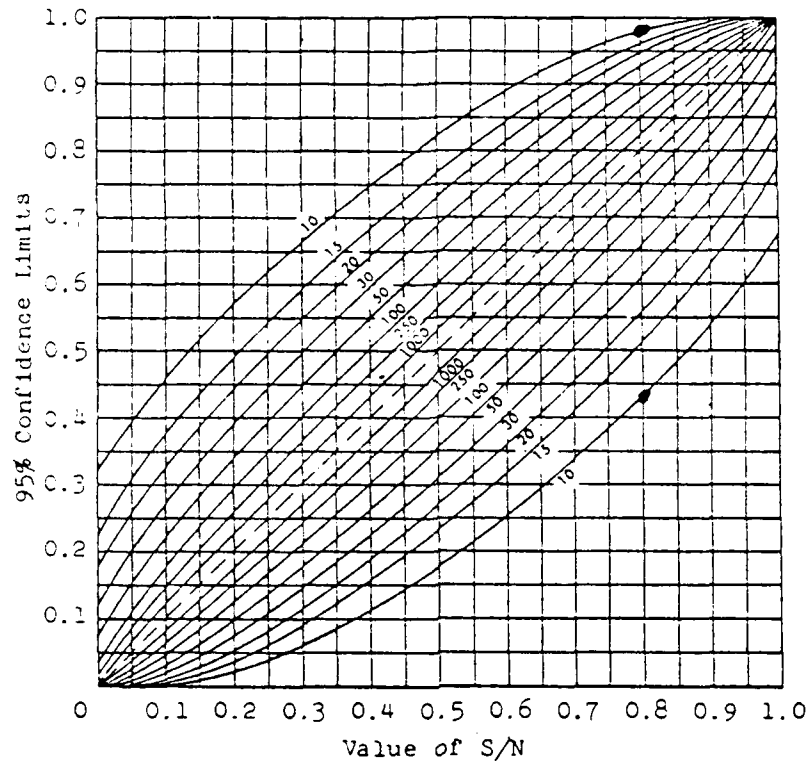
FIGURE 8.3.2.5.3-1

CHART FOR 95% CONFIDENCE LIMITS ON THE PROBABILITY S/N

From Clopper, C.J., and Pearson, E.S., "The Use of Confidence
or Fiducial Limits Illustrated in the Case of the Binomial,"
BIOMETRIKA, Vol. 26 (1934), p. 410. Reprinted with permission.

8.3.2.6   TESTS FOR VALIDITY OF THE ASSUMPTION OF A THEORETICAL
RELIABIITY PARAMETER DISTRIBUTION

The validity of many statistical techniques used in the calculation,
analysis, or prediction of reliability parameters depends on the
distribution of the failure times. Many techniques are based on
specific assumptions about the probability distribution and are often
sensitive to departures from the assumed distributions. That is, if the
actual distribution differs from that assumed, these methods sometimes
yield seriously wrong results. Therefore, in order to determine whether
or not certain techniques are applicable to a particular situation, some
judgment must be made as to the underlying probability distribution of
the failure times.

As was discussed in Section 8.3.1, some theoretical reliability
functions, such as those based on the exponential, normal, lognormal,
and Weibull distributions will plot as straight lines on special types
of graph paper. This is the simplest procedure and should be used as a
"first cut" in determining the underlying distribution. Plot the
failure data on the appropriate graph paper for the assumed underlying
distribution; "eyeball" it, and if it quite closely approximates a
straight line, you're home free.

If it cannot be determined visually that the reliability function
follows a straight line when plotted on special graph paper, then one
must resort to the application of analytical "goodness of fit" tests.

The two goodness of fit tests described in this section make a null
hypothesis, i.e., the sample is from the assumed distribution. Then a
statistic, evaluated from the sample data, is calculated and looked up
in a table that shows how lucky/unlucky you were for the sample. The
luck is determined by the size of the two sided tail area. If that tail
is very small (you were very unlucky if the null hypothesis is true),
the null hypothesis (there is no difference between the actual and the
assumed distributions) is rejected. Otherwise, the null hypothesis is
accepted, i.e., the actual distribution could easily have generated that
set of data (within the range of the data); the test says nothing about
the behavior of the distribution outside the range of the data.

Goodness of fit tests are statistical tests, not engineering tests. No
matter what the distribution or what the test, it is possible to take a
sample small enough so that virtually no distribution will be rejected,
or large enough so that virtually every distribution will be rejected.

Thus, while a method for small sample sizes is presented as well as one
for large sample sizes, it is a fact of life that must be accepted that
tests based on small samples are simply not very powerful. Therefore,
the methodology is presented here for completeness, but very likely a
more logical approach is to first make an assumption regarding the
failure distribution based on engineering judgment or on historical data
or on knowledge of the failure characteristics of similar parts. Once

the failure distribution has been assumed the test can be performed for goodness of fit for that particular distribution. If the hypothesized distribution is shown not to fit, it is quite certain that the assumed distribution was not the one from which the samples were selected. If, however, the goodness of fit test shows that the data could have come from the hypothesized distribution, then it is virtually certain that tests for fit to other distributions would yield like results.

In summary then, it must be realized that the tests presented in the next two sections have limitations. The only cure for these limitations is a larger number of observations. If this proves uneconomical or not feasible from the standpoint of test time required to generate the desired number of failures, then the only alternative is to use the results of small sample size analyses with proper discretion.

8.3.2.6.1 KOLMOGOROV-SMIRNOV (K-S) TEST (also called "d" test)

This test is based upon the fact that the observed cumulative distribution of a sample is expected to be fairly close to the true cumulative distribution. The goodness of fit is measured by finding the point at which the sample and the population are farthest apart and comparing this distance with the entry in a table of critical values, Table 8.3.2.6.1-1, which will then indicate whether such a large distance is likely to occur. If the distance is too large, the chance that the observations actually come from a population with the specified distribution is very small. This is evidence that the specified distribution is not the correct one.

1. When to Use

When failure times from a relatively small sample have been observed and it is desired to determine the underlying distribution of failure times.

2. Conditions for Use

a. Usually historical data or engineering judgment suggests that item failure times of interest are from a given statistical failure distribution. This test then follows the step of assuming a given failure distribution and is useful to determine if empirical data disproves this hypothesis.

b. The Kolmogorov-Smrinov test for goodness of fit is distribution free and can therefore be used regardless of the failure distribution that the data is assumed to follow.

c. The discriminating ability of the statistical test is dependent on sample size so naturally the larger the sample size the more reliable the results. Where large sample sizes are available the χ^2 Test for Goodness of Fit should be used. Where sample sizes are small, the Kolmogorov-Smirnov test provides some assurance.

TABLE 8.3.2.6.1-1 : CRITICAL VALUES d α (N) OF THE MAXIMUM ABSOLUTE DIFFERENCE BETWEEN SAMPLE AND POPULATION RELIABILITY FUNCTIONS

Sample Size (N)	Level of Significance (α)				
	0.20	0.15	0.10	0.05	0.01
3	0.565	0.597	0.642	0.708	0.828
4	0.494	0.525	0.564	0.624	0.733
5	0.446	0.474	0.474	0.565	0.669
10	0.322	0.342	0.368	0.410	0.490
15	0.266	0.283	0.304	0.338	0.404
20	0.231	0.246	0.264	0.294	0.356
25	0.21	0.22	0.24	0.27	0.32
30	0.19	0.20	0.22	0.24	0.29
35	0.18	0.19	0.21	0.23	0.27
40	0.17	0.18	0.19	0.21	0.25
45	0.16	0.17	0.18	0.20	0.24
50	0.15	0.16	0.17	0.19	0.23
over 50	$\dfrac{1.07}{\sqrt{N}}$	$\dfrac{1.14}{\sqrt{N}}$	$\dfrac{1.22}{\sqrt{N}}$	$\dfrac{1.36}{\sqrt{N}}$	$\dfrac{1.63}{\sqrt{N}}$

d.   Strictly speaking, this test method requires prior knowledge of the parameters. If the parameters are estimated from the sample the exact error risks are unknown.

e.   A Kolmogorov-Smirnov table is required (see Table 8.3.2.6.1-1).

3.   Graphic Method (Example Using Exponential Distribution)

Forty-eight samples of an equipment's time to failure are acquired. Based upon the assumption of an exponential distribution of time to failure, the point estimate of MTBF is calculated to be 1546 hours.

We would like to test the hypothesis that the sample came from a population where time to failure followed an exponential distribution with an MTBF of 1546 hours (see Figure 8.3.2.6.1-1).

(a)   Draw the curve (dashed line) for the theoretical distribtuion of R(t) which is assumed to be an exponential with an MTBF = 1546.0 hours.

(b)   Find the value, d, $(1.36/\sqrt{48} = 0.196)$ from Table 8.3.2.6.1-1 which corresponds to sample size, n = 48, and level of significance, α = 0.05.

(c)   Draw curves at a distance d = 0.196 above and below the theoretical curve drawn in step (a), upper and lower boundaries in Figure 8.3.2.6.1-1.

(d)   On the same graph draw the "curve" corresponding to the observed function (solid line).

(e)   If the observed function were to pass outside the band bounded by the two curves above and below the theoretical curve, there would be about a five percent chance that the sample came from an exponential population with a mean life of 1546 hours.

(f)   If the observed function remains inside the band, as it does in the example, this does not prove that the assumed distribution is exactly right, but only that it might be correct and that it is not unreasonable to assume that it is.

This example could have also been solved analytically by calculating the difference between the theoretical cumulative distribution function (CDF) and the actual CDF at each data point, finding the maximum deviation and comparing it with the value derived from Table 8.3.2.6.1-1 (d = 0.196). If the maximum deviation is less than 0.196, we accept the hypothesis (at the .05 significance level) that the time to failure is exponentially distribution with an MTBF of 1546 hours.
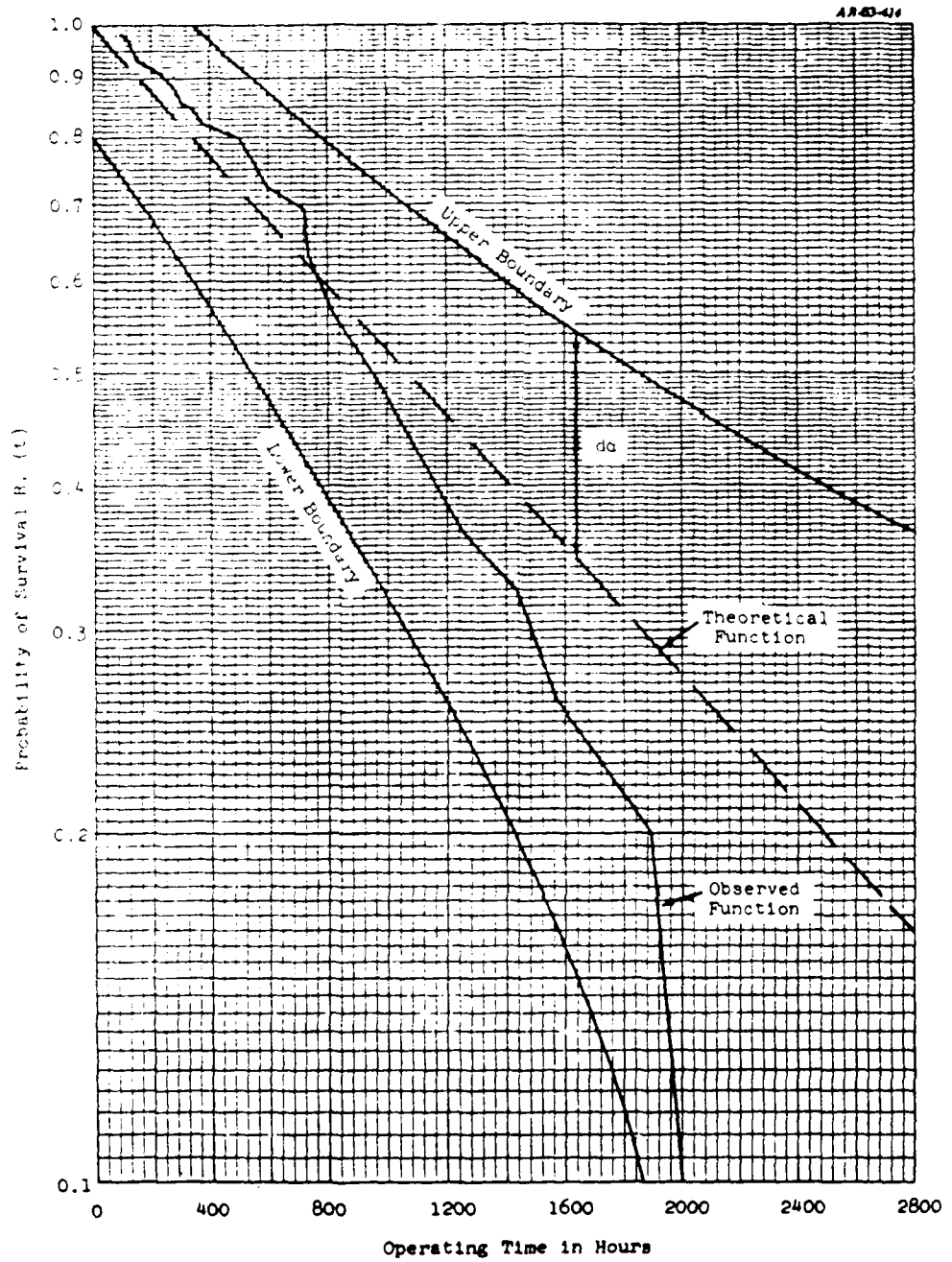
FIGURE 8.3.2.6.1-1 : EXAMPLE OF THE APPLICATION OF THE "d" TEST

4. Analytical Method

Example (Weibull Distribution)

a. Observe and record part failure times

a. Given the following 20 failure times in hours

92	640
130	700
233	710
260	770
320	830
325	1010
420	1020
430	1280
465	1330
518	1690

b. Assume a distribution of failure times based on historical information or on engineering judgment.

b. Assume failure times are distributed according to the two parameter Weibull distribution.

c. Estimate the parameters of the assumed distribution from the observed data.

c. By the graphic method or the method of least squares, find the Weibull parameters. The Weibull shape parameter (β) = 1.50 and the Weibull scale parameter (α) = 28400.

d. Calculate the probability of failure for each observation from the cumulative failure function for the assumed distribution.

d. For the Weibull distribution the cumulative failure function is

$$\hat{F}(x) = 1 - \exp\left(-\frac{x^\beta}{\alpha}\right)$$

where x = observed failure time, β = 1.5 = Weibull shape parameter, α = 28400 = Weibull scale parameter, F(x) = probability of failure at or before time x.

For the 20 observations of this example, the probability of failure at the respective t's is:

x	$\hat{F}(x)$
92	.03
130	.05
233	.12

260	.14
320	.18
325	.19
420	.26
430	.27
465	.30
518	.34
640	.43
700	.48
710	.49
770	.53
830	.57
1010	.68
1020	.68
1280	.80
1330	.82
1690	.91

e. Calculate the percentile for each of (i) failure times by the relationship $F(i) = \frac{1}{n+1}$ and subtract those of step d. above. Record the absolute value of the difference.

e. For n = 20, $\frac{1}{n+1}$ gives the following results:

$\hat{F}(x)$	$\hat{F}(i)$	$\left\lvert \hat{F}(x)-F(i) \right\rvert$
.03	.05	.02
.05	.10	.05
.12	.14	.02
.14	.19	.05
.18	.24	.06
.19	.29	.10
.26	.33	.07
.27	.38	.11
.30	.43	.13
.34	.48	.14
.43	.52	.09
.48	.57	.09
.49	.62	.13
.53	.67	.14
.57	.71	.14
.68	.76	.08
.68	.81	.13
.80	.86	.06
.82	.90	.08
.91	.95	.04

f. Compare the largest difference from step e. with a value at the desired significance level in the Kolmogorov-Smirnov tables to test for goodness of fit. If the tabled value is not exceeded then it is not possible to reject the hypothesis that the failure times are from the assumed distribution.

f. The largest difference in step e. was .14. From the Kolmogorov-Smirnov table for a significance of .05 and for a sample of size 20 a difference of greater than .29 must be observed before it can be said that the data could not have come from a Weibull distribution with β = 1.5, α = 28400.

8.3.2.6.2 CHI-SQUARE (X^2) TEST

The standard chi-square goodness of fit test may be used to test the validity of any assumed distribution, discrete or continuous. The test may be summarized as follows for a continuous distribution.

(a) Determine the underlying distribution to be tested.

(b) Determine a level of significance, α, which is defined as the risk of rejecting the underlying distribution if it is, in fact, the real distribution.

(c) Divide the continuous scale into intervals. For reliability analysis, this scale is usually time.

(d) Determine the number of sample observations falling within each interval.

(e) Using the assumed underlying distribution, determine the expected number of observations in each interval. Combining of intervals may be required because the expected number of observations in an interval must be at least 2.5. This determination may require an estimation of the distribution parameters from the sample data.

(f) Compute

$$X^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i} \tag{8.19}$$

where

O_i = number of sample observations in the ith interval

E_i = expected number of observations in the ith interval

k = number of intervals

(g) If

$$X^2 = \sum_{i}^{k} \frac{(O_i - E_i)^2}{E_i} > X^2(\alpha, k-w-1) \tag{8.20}$$

where w is the number of parameters estimated from the data and X^2 (α, k-w-1) may be found in Table 8.3.2.5.2-1, reject the distribution under test. Otherwise, we do not have sufficient evidence to reject the assumed underlying distribution.

1. **When to Use**

When failure times are available from a relatively large sample and it is desired to determine the underlying distribution of failure times.

2. **Conditions for Use**

a. In the statistical analysis of failure data it is common practice to assume that failure times follow a given failure distribution family. This assumption can be based on historical data or on engineering judgment. This test for goodness of fit is used to determine if the empirical data disproves the hypothesis of fit to the assumed distribution.

b. The χ^2 test for goodness of fit is distribution free and can therefore be used regardless of the failure distribution that the data is assumed to follow.

c. This test is not directly dependent on sample size but on the number of intervals into which the scale of failure times is divided with the restriction that no interval should be so narrow that there are not at least 5 theoretical failures within the interval. Therefore, the test is only useful if a relatively large number of failures has been observed.

d. A table of χ^2 percentage points is required (see Table 8.3.2.5.2-2).

3. **Method (Example Using Exponential Distribution**

Consider the data in Figure 8.3.2.6.2-1 indicating the failure times obtained from testing a sample of 100 fuel systems. Using a significance level of $\alpha = 0.05$, test whether the assumption of an exponential distribution is reasonable. The sample mean was found to be 8.9 hours.

a. Figure 8.3.2.6.2-2 is used as a means of computing

$$\sum_{i=1}^{k} \frac{\left(O_i - E_i \right)^2}{E_i}$$

b. The expected frequency (E_i) is found by multiplying the sample size by the probability of falling within the ith interval if the assumed (exponential) distribution is true.

$$E_i = n \left[\exp\left(\frac{-L_i}{\hat{\theta}} \right) - \exp\left(\frac{-U_i}{\hat{\theta}} \right) \right] = 100 \left[\exp\left(\frac{-L_i}{8.9} \right) - \exp\left(\frac{-U_i}{8.9} \right) \right]$$

where U_i and L_i are the upper and lower limits of the ith interval, $U_i = L_{i+1}$, and $\hat{\theta} = 8.9$ hours.

Interval (Hours	Frequency
0 - 5.05	48
5.05 - 10.05	22
10.05 - 15.05	11
15.05 - 20.05	7
20.05 - 25.05	3
25.05 - 30.05	5
30.05 - 35.05	2
35.05 - 40.05	0
40.05 - 45.05	1
45.05 - 50.05	0
50.05 - 55.05	1
	100

FIGURE 8.3.2.6.2-1 :   FUEL SYSTEM FAILURE TIMES

Interval (hrs) $(L_i - U_i)$	Observed Frequency (O_i)	Expected Frequency (E_i)	$O_i - E_i$	$(O_i - E_i)^2$	$\dfrac{(O_i - E_i)^2}{E_i}$
0 - 5.05	48	43	5	25	.58
5.05 - 10.05	22	24	-2	4	.17
10.05 - 15.05	11	14	-3	9	.64
15.05 - 20.05	7	8	-1	1	.12
20.05 - 25.05	3	5	-2	4	.80
25.05 - 30.05	5	3	2	4	1.33
30.05 - 35.05	2				
35.05 - 40.05	0				
40.05 - 45.05	1 } 4	3	1	1	.33
45.05 - 50.05	0				
50.05 - ∞	1				3.97

FIGURE 8.3.2.6.2-2 : COMPUTATION

8-56

c. Some of the original intervals were combined to satisfy the requirement that no E_i value be less than 2.5.

$$x^2 = \sum_{i=1}^{7} \frac{\left(O_i - E_i\right)^2}{E_i} = 3.97$$

$$x^2(\alpha, k-w-1) = x^2(.05, 7-1-1) = x^2(.05, 5) = 11.070 \text{ (Table 8.3.2.5.2-1)}$$

Since

$$\sum_{i-1}^{7} \frac{\left(O_i - E_i\right)^2}{E_i} = 3.97 < x^2_{(.05, 5)} = 11.070,$$

we do not have sufficient evidence to reject the exponential distribution as a model for these failure times.

4. Method

a. Observe and record part failure times.

b. Assume a distribution of failure times based on historical information or on engineering judgment.

c. Estimate the parameters of the assumed distribution from the observed data.

Example (Weibull Distribution)

a. The following is the number of cycles to failure for a group of 50 relays on a life test:

1283	6820	16306
1887	7733	17621
1888	8025	17807
2357	8185	20747
3137	8559	21990
3606	8843	23449
3752	9305	28946
3914	9460	29254
4394	9595	30822
4398	10247	38319
4865	11492	41554
5147	12913	42870
5350	12937	62690
5353	13210	63910
5410	14833	68888
5536	14840	73473
6499	14988	

b. Assume failure times are distributed according to the two parameter Weibull distribution.

c. By the graphical method or method of least squares find the Weibull parameters. The Weibull shape parameter β =1.21 and the Weibull scale parameter α =127978.

d. Divide the spectrum of failure times into intervals of such a width that the theoretical number of failures in each interval will be at least five. The width of intervals need not be equal.

d. Divide the relay cycles to failure into the following intervals:

$$0 - 4000$$
$$4001 - 7200$$
$$7201 - 13000$$
$$13001 - 18000$$
$$18001 - 25000$$
$$25001 - $$

e. Calculate the theoretical number of failures for each interval.

e. The expected number of failures in each interval is obtained as follows:

For the Weibull distribution the cumulative failure function is

$$F(x) = 1 - \exp\left(-\frac{x^{\beta}}{\alpha}\right)$$

where x = observed failure times
   β = Weibull shape parameter
   α = Weibull scale parameter

Then $F(x_n) = F(x_{n-1})$ = probability that a failure time falls within the interval.

Then for each interval the probability of failure in that interval multiplied by the sample size = the theoretical number of failures for each interval.

(1) Upper Boundary of Interval	(2) $F(x)$	(3) $F(x_n)-F(x_{n-1})$	(4) Theoretical Failure Frequency (Col. 3x50)
4000	.16	.16	8
7200	.30	.14	7
13000	.52	.22	11
18000	.66	.14	7
25000	.80	.14	7
∞	1.00	.20	10

NOTE: The theoretical frequency must not be less than 5 for any interval.

8-58

f. Calculate the X^2 statistic by the formula

$$X^2 = \sum_{i=1}^{k} \frac{(f_i - F_i)^2}{F_i}$$

where k = number of intervals
       f = observed frequency/interval
       F = theoretical frequency/interval

Upper Boundary of Interval	F	f	$\frac{(f_i - F_i)^2}{F_i}$
4000	8	8	0
7200	7	10	1.29
13000	11	12	.09
18000	7	7	0
25000	7	3	2.29
∞	10	10	0
	50	50	$X^2 = 3.67$

g. Determine if the X^2 statistic indicates that the data could have come from the hypothesized distributions using X^2 tables (Table 8.3.2.5.2-1) and $(k-1) - \rho$ degrees of freedom.

where k = number of intervals
       ρ = number of parameters estimated from data

g. The degrees of freedom for this example are calculated as:

d.f. = $(k-1) - \rho$
d.f. = $(6-1) - 2 = 3$

The value from the X^2 table for 3 degrees of freedom at the 0.05 level of significance is 7.815. Since 3.69 does not exceed the tabled value, then the hypothesis that this data came from a Weibull distribution cannot be rejected.

8.3.2.6.3 COMPARISON OF K-S ('d' test) and X^2 (Chi-square) Tests

The d-test is superior to X^2 in the following ways:

(1) The 'd' test requires only the assumption of a continuous distribution, while the chi-square test requires the assumption that observed frequencies are normally distributed about their expected frequencies.

(2) The exact distribution of 'd' is known and tabled for small sample sizes, while the exact distribution of chi-square is known and tabled only for infinite sized samples.

(3) The 'd' test can be used to test for deviations in a given direction, while chi-square can be used only for a two sided test.

(4) The 'd' test uses ungrouped data so that every observation represents a point of comparison, while the chi-square test requires the data to be grouped into cells with arbitrary choice of interval, size, and selection in starting point.

(5) The 'd' test can be used in a sequential test where data becomes available from smallest to largest, computations being continued only up to the point at which rejection occurs.

The chi-square test is superior to the 'd' test in the following ways:

(1) Chi-square does not require that the hypothesized population parameters be completely known in advance.

(2) Chi-square can be partitioned and added.

(3) Chi-square can be applied to discrete populations.

8.4 RELIABILITY DEMONSTRATION

8.4.1 INTRODUCTION

The single purpose of a reliability demonstration test is to determine conformance to specified, quantitative reliability requirements as a basis for qualification or acceptance, to answer the question, Does the item meet or exceed (not by how much) the specified minimum reliability requirement?

Reliability testing involves an empirical measurement of time-to-failure during equipment operation for the purpose of determining whether an equipment needs the established reliability requirements. A reliability test is effectively a "sampling" test in the same sense that it is a test involving a sample of objects selected from a "population". In reliability testing, the "population" being measured encompasses all failures that will occur during the life span of the equipment. A "test sample" is drawn from this population by observing those failures occurring during a small portion of the equipment's life. In reliability testing, as in any sampling test, the "sample" is assumed to be representative of the population, and the mean value of the various elements of the sample (e.g. times-to-failure) is assumed to be a measure of the true mean (MTBF, etc.) of the population.

A sample in a reliability test consists of a number of times to failure, and the population is all the times-to-failure that could occur either from the one equipment or the more than one equipment on test. The "test" equipments (assuming more than one equipment) are considered identical, and thus their populations are also identical. Under the assumption of an exponential failure model (constant λ), a test of 10 devices for 100 hours each is mathematically equivalent to a test of 1 device for 1000 hours. If all possible samples of the same number of times-to-failure were drawn from the same or identical equipment, the resulting set of sample means would be distributed about the true MTBF (θ) of the equipment, following a normal distribution as is shown in Figure 8.4.1-1.

Since it is not economically feasible to test the complete population, we have to be satisfied with a sample of the population. From the data in the sample we then make some statement about the population parameter.

SAMPLE MEAN
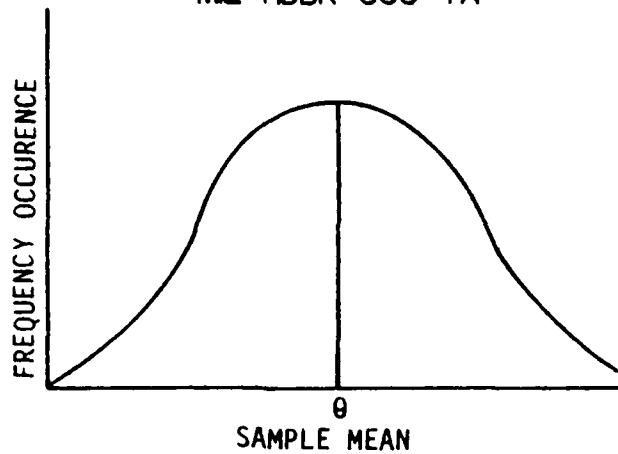
FIGURE 8.4.1-1: NORMAL DISTRUBUTION

What we are doing is testing a statistical hypothesis: For example, we might test

H_o: (null hypothesis) $\theta_o \geq$ 200 hours

H_1: (alternate hypothesis) $\theta_1 \leq$ 100 hours

Based upon the test results, we either accept H_o or reject it. In making our decision we have to keep several risks in mind.

Producer's risk (α) is the probability of rejecting H_o when it is true (probability of rejecting a good equipment)

Consumer's risk (β) is the probability of accepting H_o when it is false (probability of accepting a bad equipment)

Looking at it another way, if θ_o and θ_1 represent the hypotheses
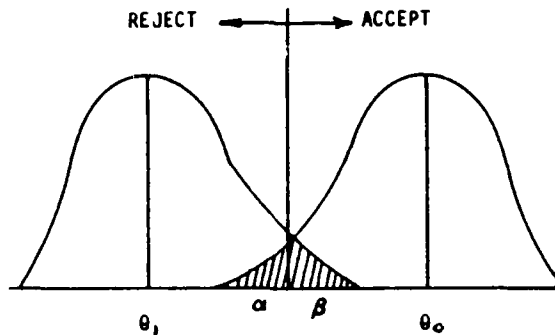
FIGURE 8.4.1-2A: HYPOTHESIS TEST A

Then the α and β errors are the hatched areas shown in Figure 8.4.1-2A. Of course, if we could take enough samples, then the standard deviation about each of the means would be reduced and the α and β errors would be reduced as shown on the following page.

REJECT ← | → ACCEPT

θ_1 θ_0
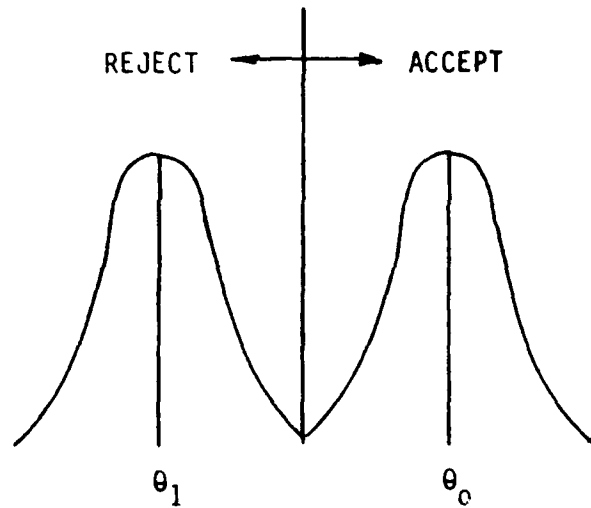
FIGURE 8.4.1-2B: HYPOTHESIS TEST B

However, this is usually impractical so that what we end up doing is to set the sample size as low as possible to reduce costs, by specifying the maximum acceptable α and β risks that can be associated with θ_0 and the smallest acceptable θ_1 as shown in Figure 8.4.1-2B. Why two values? Let's look at our decision rule, or accept/reject criteria. We would like it to look like Figure 8.4.1-3A.

P(accept)

1.0
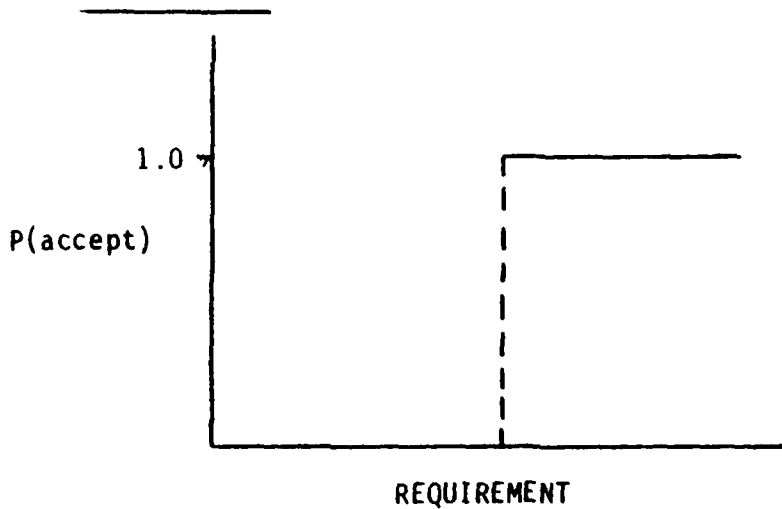
REQUIREMENT

FIGURE 8.4.2-3A: IDEAL OPERATING CHARACTERISTIC (OC) CURVE

This relationship between the probability of acceptance and the requirement (e.g. MTBF) is called the operating characteristic curve. The ideal curve shown above would require an infinite number of samples. In real life we settle for something that gives a small probability of acceptance (P_a) for MTBF's below the requirement and high P_a for MTBF's above the requirement, M_0, as shown below.
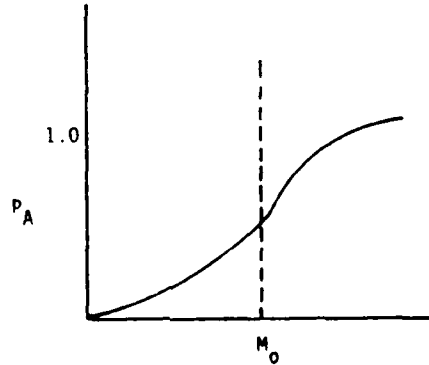
FIGURE 8.4.1-3B: TYPICAL OPERATING CHARACTERISTIC CURVE

For example, suppose we had an MTBF requirement of 200 hours, a demonstration test of 1000 hours, and the decision rule

  Accept if r $\leq$ 5
  Reject of r $>$ 5

where r is the number of failures which is Poisson distributed (fixed time test) as

$$p(r) = \frac{(t/m)^r\ e^{-t/m}}{r!} \qquad (8.21)$$

where m is the MTBF.

We plot P_a (r $\leq$ 5) for various values of m based upon the expected number of failures, as shown in Figure 8.4.1-4.

4 m	t/m	P_a (r < 5)
100	10	0.067
125	8	0.191
167	6	0.446
200	5	0.616
333	3	0.916
500	2	0.983
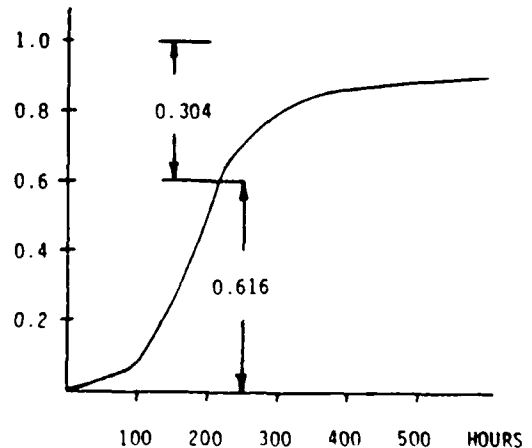
FIGURE 8.4.1-4 A   ACTUAL OPERATING CHARACTERISTIC CURVE

The decision rule "tends" to give the right decision, but won't always result in an accept decision for $m > 200$ or a reject decision for $m < 200$. Remember $P_a + P_r = 1$. Thus, we can see that we have almost a fifty-fifty chance of accepting an m of 167 hours, (0.446), and a greater than 20% chance of rejecting an m = 250 hours. Neither the producer or consumer would be happy with this. Each would like a lower risk probability. But since $P_a = 1 - P_r$, if we lower P_a for $m \leq 200$ to 0.1, we raise P_r for $m > 200$ to $1 - 0.1 = 0.9$. What do we do now?

In order to overcome this difficulty it is necessary to specify the reliability requirements, either explicitly or implicitly, interms of two MTBF values rather than a single MTBF value. The lower value is defined in MIL-STD-781 as the lower test MTBF (M_m or θ_1) and the higher value is defined as the upper test MTBF (M_r or θ_0). The test plan can then be designed to give a low probability of an <u>accept</u> decision for equipment with an MTBF of $m \leq M_m$ (or θ_1) and a low probability of <u>reject</u> decision when $m \geq M_r$. P_a at $m = M_m$ (or θ_1) is the <u>consummer's risk</u> (β); P_r at $m = M_r$ (or θ_0) is the <u>producer's risk</u> (α). Thus, specifying the two MTBF values M_m (θ_1) and M_r (θ_0) and the two risks (α and β) defines two points on the OC curve as shown below.
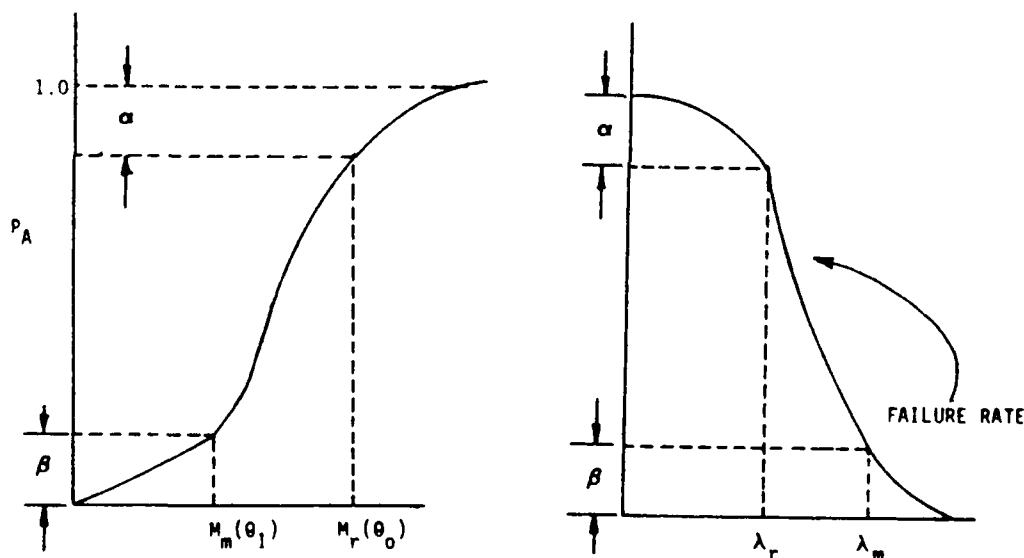
FIGURE 8.4.1-4B: <u>OC CURVE CHARACTERISTICS</u>

The curve on the right is the OC curve for failure rate (λ) rather than MTBF. $\lambda_m = 1/M_m$ is the <u>maximum</u> acceptable failure rate. $\lambda_r = 1/M_r$ is the design required (specified) failure rate with $\lambda_r < \lambda_m$.

The method used to design a <u>fixed time</u> reliability (R) demonstration test is mathematically equivalent to the method used to construct confidence limits for MTBF. Therefore, if a fixed time R demonstration involving a test time T and an accept number r_o provides a consumer risk of β with respect to a minumum acceptable MTBF (M_m or θ_1), it will be found that if the maximum allowable number of failures, r_o, actually occurs, the lower 100 ($1-\beta$)% confidence limit for MTBF as calculated from the test data is exactly M_m. For this reason, the value ($1-\beta$), or $100(1-\beta)$% is often called the <u>confidence level</u> of the demonstration test. Thus, a fixed time R demonstration test providing a 10% consumer risk is called "a demonstration test at a 90% confidence level," or is said to "demonstrate with 90% confidence that the lower test MTBF is achieved." This is not really correct since, technically, confidence level is used in the estimation of a parameter while an R demonstration test is testing a hypothesis about the parameter, m, rather than constructing an interval estimate for m.

There are six characteristics of any reliability demonstration test that must be specified:

(1)   The reliability deemed to be acceptable, R_o. In MIL-STD-781 this is defined as "upper test MTBF".

(2)   A value of reliability deemed to be unacceptable, R_1. In MIL-STD-781 this is defined as "lower test MTBF".

(3)   Producer's risk, **or α.**

(4)   Consumer's risk, **or β.**

(5)   The probability distribution to be used for number of failures or for time to failure.

(6)   The sampling scheme.

Another term frequently used in connection with reliability demonstration tests should be defined here although it is derived from two of the above characteristics. The discrimination ratio is the ratio of upper test reliability to the lower test reliability. R_o/R_1 is an add tional method of specifying certain test plans.

There are, of course, an infinite number of possible values for the actual reliability. In the specification of two numerical values, R_o and R_1, the experimenter achieves the producer's risk, α, and consumer's risk, β, only for those specific reliabilities. For other values, the relationship is:

(a)   Probability of Acceptance $\geq 1-\alpha$ for $R \geq R_o$
(b)   Probability of Acceptance $\leq \beta$ for $R \leq R_1$
(c)   Probability of Acceptance $> \beta$ for $R_1 \leq R \leq R_o$

8.4.2 ATTRIBUTES AND VARIABLES

Demonstration tests are classified according to the method of assessing reliability. If each component tested is merely classified as acceptable or unacceptable, then the demonstration test is an attributes test. If the service life of the items under test is recorded in time units, and service life assumed to have a specific probability distribution such as the normal or Weibull, then the test is a variables test. Attributes tests _may_ be performed even if a probability distribution such as the normal or Weibull is assumed by dichotomizing the life distribution into acceptable and unacceptable time to failure. Attributes tests are usually simpler and cheaper to perform, but require larger sample sizes to achieve the same   and   as variables tests.

8.4.3 FIXED SAMPLE AND SEQUENTIAL TESTS

When R_0, R_1, α , and β have been specified, along with the probability distribution for time to failure, the test designer often has a choice of sampling schemes. To achieve the desired α and β , statistical theory will dictate the precise number of items which must be tested if a fixed sample size is desired. Alternatively, a sequential test may be selected, where the conclusion to accept or reject will be reached after an indeterminate number of observations. For reliability at R_0 or R_1, the _average_ sample size in a sequential test will invariably be lower than in a fixed sample test, but the sample size will be unknown, and could be substantially larger in a specific case. Usually, an upper bound for sample size is known in sequential tests.

8.4.4 DETERMINANTS OF SAMPLE SIZE

Whether a fixed sample or sequential test is selected, the number of observations required will be related to the degree of discrimination asked for. In general,

    (a)   The closer R_1 is to R_0, the larger the sample size required.
    (b)   The smaller α specified, the larger the sample size required.
    (c)   The smaller β specified, the larger the sample size required.

If the test is sequential, substitute "average sample size" for sample size in the above remarks.

8.4.5 TESTS DESIGNED AROUND SAMPLE SIZE

It is possible to set the sample size (or average sample size in sequential tests) independently. For example, the sample size, N, may be limited by test facilities, cost, or time. If this is done, then one cannot specify all of the values R_0, R_1, α, β. One of the four will be fixed when the remaining three and N are specified. The usual practice where N must be fixed is to specify R_0 and   and then to include a plot of 1- β as a function of R_1, the corresponding probability of rejection, 1-β. If the discriminating power is unacceptable, then R_1, α , β or N must be altered in the direction noted in Section 8.4.4.

8.4.6 PARAMETERIZATION OF RELIABILITY

In the case of variables tests, the desired reliability will be a function of the parameters of whatever probability distribution is selected. For example, if equipment mean life is normally distributed, then

$$R = \int_{T}^{\infty} \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{x - u}{\sigma} \right)^2 \right] dx \qquad (8.22)$$

where

T = desired life
μ = population mean
σ = population standard deviation

Suppose that R_o is specified at 0.995 for a service life, T, of 10,000 hours. Clearly, these specifications place numerical requirements on μ and σ to make the equation hold true. Therefore, the demonstration test may be performed on u_o, σ_o), rather than on R_o. Demonstration tests are often specified in terms of the probability distribution parameters, rather than reliabilities.

8.4.7 SUMMARY

MIL-STD-785 describes the essential elements that should be included in a reliability test program plan for development and production testing.

MIL-STD-781 covers the detailed requirements for development and production reliability tests for equipment that experiences a distribution of time-to-failure that is exponential. It contains: test conditions, procedures, and various fixed length and sequential test plans with respective accept/reject criteria. Refs. 5 and 12 provide additional guidance and details on reliability measurement. The reliability test plan should contain, as a minimum the following information:

(1) How the equipment/system will be tested

o the specified test conditions, e.g., environmental conditions, test measures, length of test, equipment operating conditions, accept/reject criteria, test reporting requirements, etc.

(2) Who will perform the tests

o contractor, Government, independent organization

(3) When the tests will be performed

o development, production, field operation

(4) Where the tests will be performed

o contractor's plant, Government organization

Appendix A presents step-by-step instructions on the use of various types of reliability demonstration test plans. Instructions and examples are given for the following test plans:

(1) Attributes Demonstration Tests

    (a) Plans for Small Lots
    (b) Plans for Large Lots
    (c) Plans for Large Lots (Poisson Approximation Method)
    (d) Attributes Sampling Using MIL-STD-105
    (e) Sequential Binomial Test Plans

(2) Variables Demonstration Tests

    (a) Time Truncated Test Plans

        (1) Exponential Distribution
        (2) Normal Distribution
        (3) Weibull Distribution

    (b) Failure Truncated Tests

        (1) Exponential Distribution
        (2) Normal Distribution (σ Known)
        (3) Normal Distribution (σ Unknown)
        (4) Weibull Distribution

    (c) Sequential Tests

        (1) Exponential Distribution
        (2) Normal Distribution

    (d) Interference Demonstration Tests
    (e) Bayes Sequential Tests

8.5 RELIABILITY GROWTH

8.5.1 INTRODUCTION

Experience has shown that programs which rely simply on a demonstration test by itself to determine compliance with the specified reliability requirements generally do not achieve the reliability objectives with the allocated resources. This is particularly true of complex systems. Generally, these systems require new technologies and represent a challenge to the state of the art. Moreover, the requirements for reliability, maintainability and other performance parameters are usually highly demanding. Consequently, striving to meet these requirements represents a significant portion of the entire acquisition process and, as a result, the setting of priorities and the allocation and reallocation of resources such as funds, manpower and time are often formidable management tasks.

In order to help insure that the equipment/system will meet the required operational reliability requirement, the concept of reliability growth testing and management has been developed and implemented as standard DoD policy for equipment/system development programs.

8.5.2 RELIABILITY GROWTH CONCEPT

Reliability growth is defined as the positive improvement of the reliability of an equipment through the systematic and permanent removal of failure mechanisms. Achievement of reliability growth is dependent upon the extent to which testing and other improvement techniques have been used during development and production to "force out" design and fabrication flaws, and on the sign with which these flaws are analyzed and corrected.

Figure 8.5.2-1 suggests an ideal growth process. The initial reliability of the prototype starts at some level that might be considered the state-of-the-art at the beginning of development. Through the development effort reliability grows up to the pilot production stage. At that time, some loss of growth occurs due to the introduction of manufacturing problems. During the pilot production, corrective actions are continuing that cause resumption of growth. At the beginning of full scale production, some loss in the achieved level of reliability occurs because of the effects of mass production. However, growth will resume as these problems are eliminated. And, at a time when the equipment is released to the field it should have achieved the specified level or, under ideal conditions, the inherent or predicted level. The slope of this curve is affected by many variables and these will be discussed later. Thus, reliability growth is the result of an iterative design process. As the design matures, it is investigated to identify actual (via testing) or potential (via analysis) sources of failures. Further design effort is then spent on correcting these problem areas. The design effort can be applied to either product design or manufacturing process design. There are three essential elements involved in achieving reliability growth:

(1) Detection of failure sources (by analysis and test)

(2) Feedback of problems identified

(3) Effective redesign effort based on problems identified

The rate at which reliability grows is therefore dependent on how rapidly activities in this iterative loop can be accomplished, how real the identified problems are, and how well the redesign effort solves the identified problems. It is important to realize that some activities may act as a bottleneck. The bottleneck activities may vary from one development program to the next. Even within a single program they may vary from one stage of development to the next. In most cases, however, failure sources are detected through testing, and the testing process effectively controls the rate of growth. As a consequence, the reliability growth process becomes familiarly known as one of test, analyze, and fix (TAAF). However, the reliability achieved as a result of the growth process only becomes meaningful when the necessary changes developed and proven during TAAF to achieve that reliability are properly and fully incorporated in configuration control documentation for production hardware.
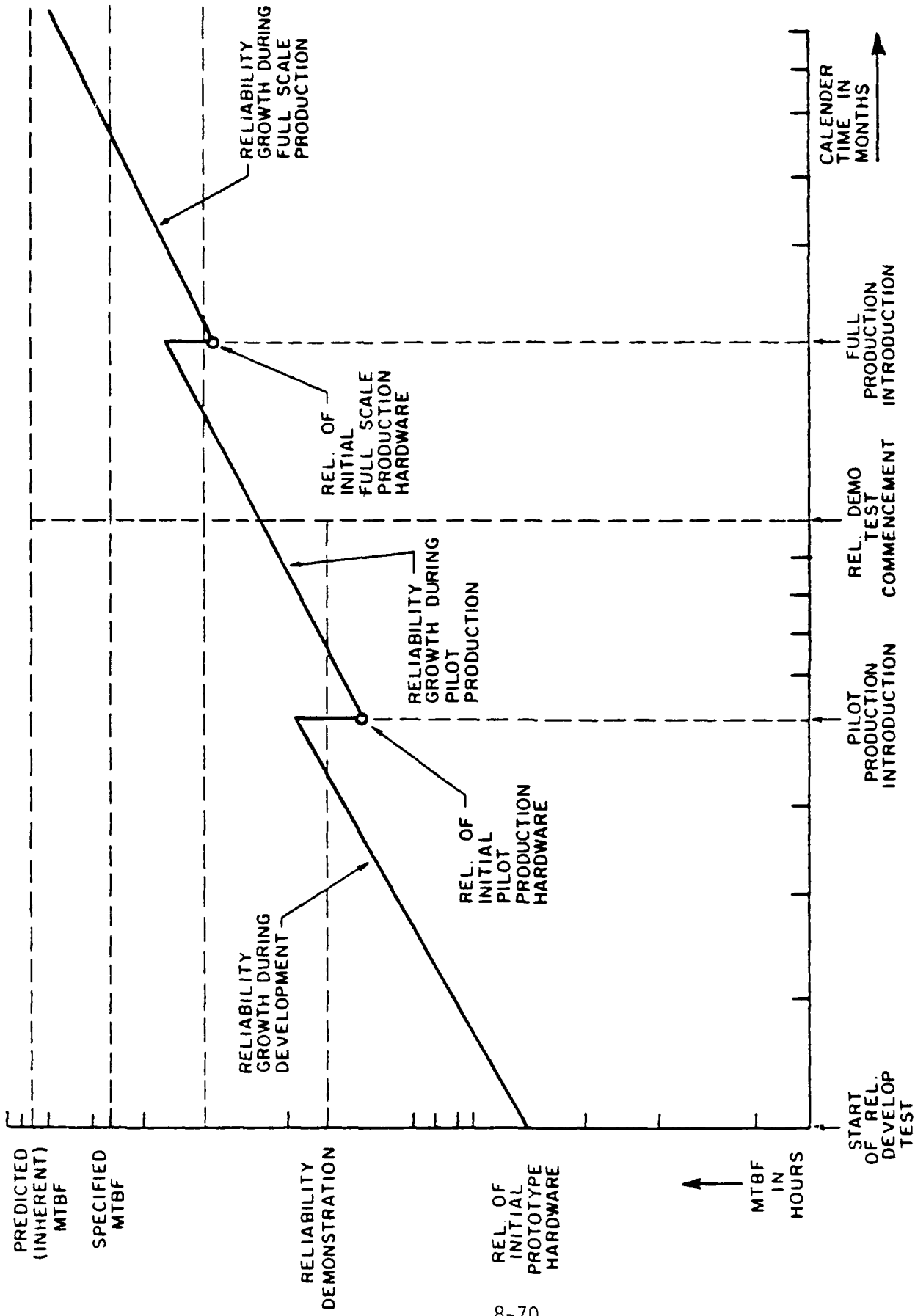
FIGURE 8.5.2-1: RELIABILITY GROWTH PROCESS

Reliability growth testing is only one aspect of a total reliability growth program. It must be accompanied by a reliability growth management program. This involves setting interim reliability goals to be met during the development testing program and the necessary allocation and reallocation of resources to attain these goals. A comprehensive approach to reliability growth management throughout the development program consists of planning, evaluating and controlling the growth process.

Reliability growth planning addresses program schedules, amount of testing, resources available and the realism of the test program in achieving the requirements. The planning is qualified and reflected in the construction of a reliability growth program plan curve. This curve establishes interim reliability goals throughout the program. To achieve these goals it is important that the program manager be aware of reliability problems during the conduct of the program so that he can effect whatever changes are necessary, e.g., increased reliability emphasis. It is, therefore, essential that periodic assessments of reliability be made during the test program (e.g., at the end of a test phase) and compared to the planned reliability growth values. These assessments provide visibility of achievements and focus on deficiencies in time to affect the system design. By making appropriate decisions in regard to the timely incorporation of effective fixes into the system commensurately with attaining the milestones and requirements, management can control the growth process.

8.5.3 RELIABILITY GROWTH MODELING

For complex electronic/electromechanical avionic systems, the model used most often for reliability growth processes, and in particular reliability growth testing, is one originally published by J. T. Duane. (Ref. 16). Essentially, this model provides a deterministic approach to reliability growth such that the system MTBF versus operating hours falls along a straight line when plotted on log-log paper. That is, the change in MTBF during development is proportional to T^{α} where T is the cumulative operating time and α is the rate of growth corresponding to the rapidity with which faults are found and changes made to permanently eliminate the basic causes of the faults observed.

The model is shown graphically in Figure 8.5.3-1, with each of the growth lines having different slopes, depending upon the emphasis given to the reliability growth program.

Duane's postulate was that as long as reliability improvement effort continues, the following mathematical expression would hold,

$$\lambda_\Sigma = \frac{F}{H} = K H^{-\alpha} \tag{8.23}$$

where

λ_Σ = cumulative failure rate
H   = total test hours
F   = failure, during H
K   = constant determined by circumstances
α = growth rate
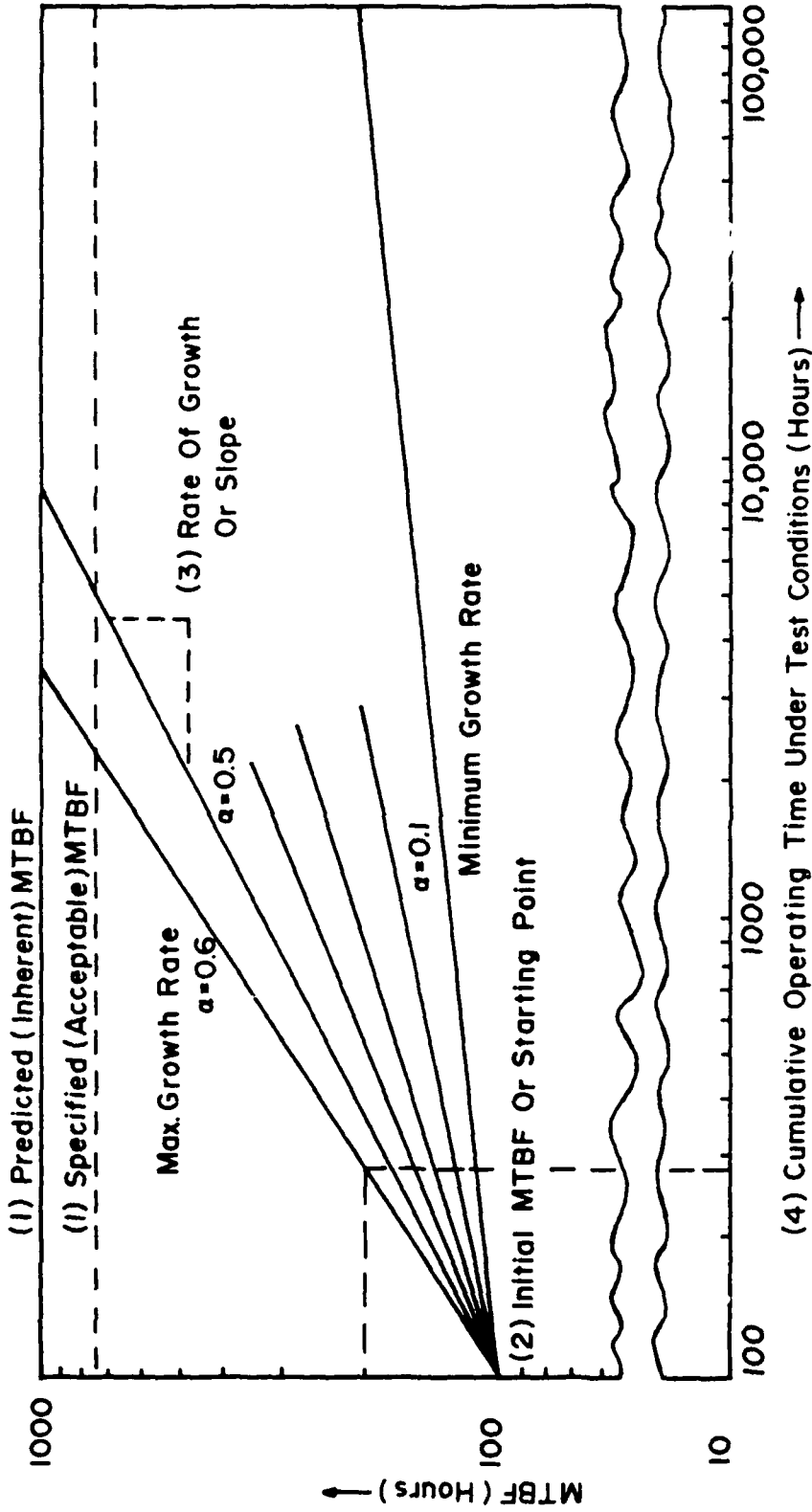
FIGURE 8.5.3-1: RELIABILITY GROWTH PLOT

The original mathematical model was expressed in terms of cumulative failure rate; but, currently since equipment reliability is generally expressed in terms of MTBF, the following expression is used,

$$M_R = M_I \left(\frac{T_t}{t_i}\right)^\alpha \qquad (8.24)$$

where

M_R = required MTBF
M_I = initial MTBF
t_i = time at which initial data point is plotted (preconditioning time)
T_t = time at which the instantaneous MTBF of the equipment under test will reach the MTBF requirement
α = growth rate

Differentiating Eq. (8.23) with respect to time

$$\lambda(t) = \frac{\partial F}{\partial H} = (1-\alpha)KH^{-\alpha} = (1-\alpha)\ \lambda_\Sigma \qquad (8.25)$$

so that the "instantaneous" or current failure rate is $(1-\alpha)$ times the

cumulative failure rate, or the "instantaneous MTBF" is $\frac{1}{1-\alpha}$ times the cumulative MTBF. An adequate interpretation of "instantaneous MTBF" is:

The MTBF that the equipment currently on test would exhibit if we stopped the reliability growth and continued testing. Thus the "instantaneous" or current status curves are straight lines displaced from the cumulative plot by a factor $(1-\alpha)$, which shows up as a fixed distance on a logarithmic plot, as shown in Figure 8.5.3-2.

CUMULATIVE TEST HOURS
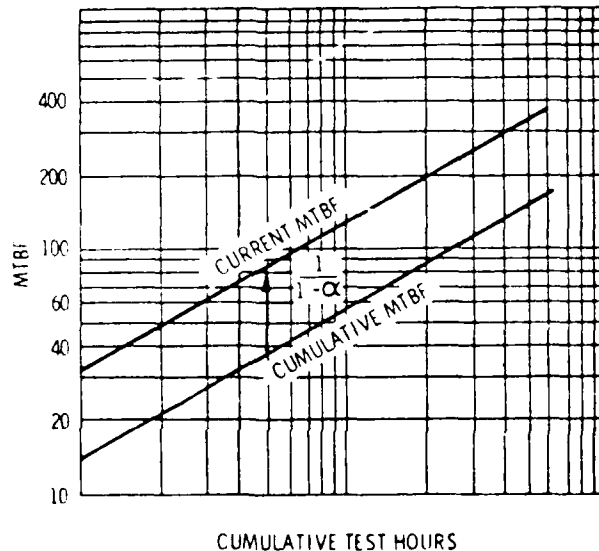
FIGURE 8.5.3-2: UP-IS-GOOD DUANE CHART WITH PLOT OF CURRENT MTBF

Normally, the cumulative MTBF (M_c) is measured in test and converted to instantaneous (or current) MTBF (M_I) by dividing by $1 - \alpha$, that is,

$$M_I = \frac{M_c}{1-\alpha} \qquad (3.26)$$

The cumulative MTBF is plotted versus cumulative test time, a straight line is fitted to the data and its **slope**, α, is measured. The current MTBF line is then drawn parallel to the cumulative line but displaced

upward by an offset equal to $\frac{1}{1-\alpha}$. The corresponding test time at which this line reaches the required MTBF is the expected duration of the growth test. Much evidence has been accumulated since Duane's original report that verifies the adequacy of the Duane model in representing the real world of reliability growth testing.

In fact, recently the Duane model has been successfully applied to software growth modeling (Ref. 18).

Crow presents a formal mathematical development of the Duane model. He showed that when the above conditions hold, the failure rate during development follows the Weibull failure rate curve. The development given below and the notation are similar to that given by Crow (Ref. 17).

Mathematically, this model may be expressed by the equation

$$F(t) = \lambda t^{-\alpha} \qquad (8.27)$$

$$\lambda^* > 0; \quad 0 < \alpha < 1$$

where $F(t)$ is the cumulative failure rate of the system at time t **and** λ and α are parameters. The cumulative failure rate is by definition

$$F(t) = \frac{E(t)}{t} \qquad (8.28)$$

where $E(t)$ is the expected number of failures experienced by the system during t time units of development testing. Thus, from the above two equations

$$E(t) = \lambda t^{1-\alpha} \qquad (8.29)$$

The instantaneous failure rate, $r(t)$, is of the most interest for applications. It is defined as the change in the expected number of failures per unit time. For a nonexponential system, it varies with time while for an exponential system the failure rate is constant.

Differentiating $E(t)$ with respect to time gives the instantaneous failure rate $r(t)$ as follows:

$$r(t) = \frac{dE(t)}{dt} = (1-\alpha) \lambda t^{-\alpha} \qquad (8.30)$$

*Note that λ in these expressions is not failure rate, it is a parameter of the Weibull distribution.

By substituting in the previous equations

$$\beta = 1 - \alpha$$

one gets

$$r(t) = \lambda \beta t^{\beta - 1} \qquad (8.31)$$

which is the Weibull failure rate function for a repairable system.

Thus, if one plans to use the Duane model during a development program, the above expression can be used to determine the failure rate at a particular development time t. The values of λ and β are estimated from test data. Since λ is only a multiplier and β determines how much the failure rate changes with the development time, β is referred to as the growth parameter. For the systems studied by Duane, a β of approximately 0.5 was estimated.

To gain further insight into the Duane model, consider Figure 8.5.3-3 which is a plot of the Weibull failure rate versus development time for $\beta = 0.5$ and $\lambda = 0.4$. During the early stages of development the failure rate decreases rather rapidly due to more failures and more rework going on during this time. As the development progresses, the rate of decrease of the failure rate drops off considerably. The Duane model assumes that at some time t_0, which corresponds to about the time that development ends and production starts, the failure rate levels off to a fairly constant value. At this point in time when the failure rate becomes constant, the time between failures can be described by the exponential distribution with a mean time between failure of

$$MTBF(t_0) = [\lambda \beta t_0^{\beta - 1}]^{-1} \qquad (8.32)$$

Crow (Ref. 22) has developed the maximum likelihood estimates (MLE) of β and λ and also a goodness of fit test to determine if the Duane model fits a particular set of data. The MLE estimate for β is

$$\hat{\beta} = \frac{N}{\sum\limits_{r=1}^{K} \sum\limits_{i=1}^{N_r(T)} \log_e \frac{T}{X_{ir}}} \qquad (8.33)$$

where

K = number of different subsystems,

T = the operating time for each of the K subsystems,

$N_r(T)$ = number of failures observed for the r-th subsystem during T time,

X_{ir} = the age of the r-th subsystem at the i-th failure, beginning of development being 0,

$$N = \sum\limits_{i=1}^{K} N_r(t) \qquad (8.34)$$

The chart shows:

$\beta = 0.5$

$\lambda = 0.4$

$r(t) = \lambda \beta t^{\beta - 1}$

$1/MTBF(t_o)$

with axes: r(t)- Failure Rate (vertical, .01 to .10) vs. t- Development Time (horizontal, 0 to 200), and point t_o at t = 100.
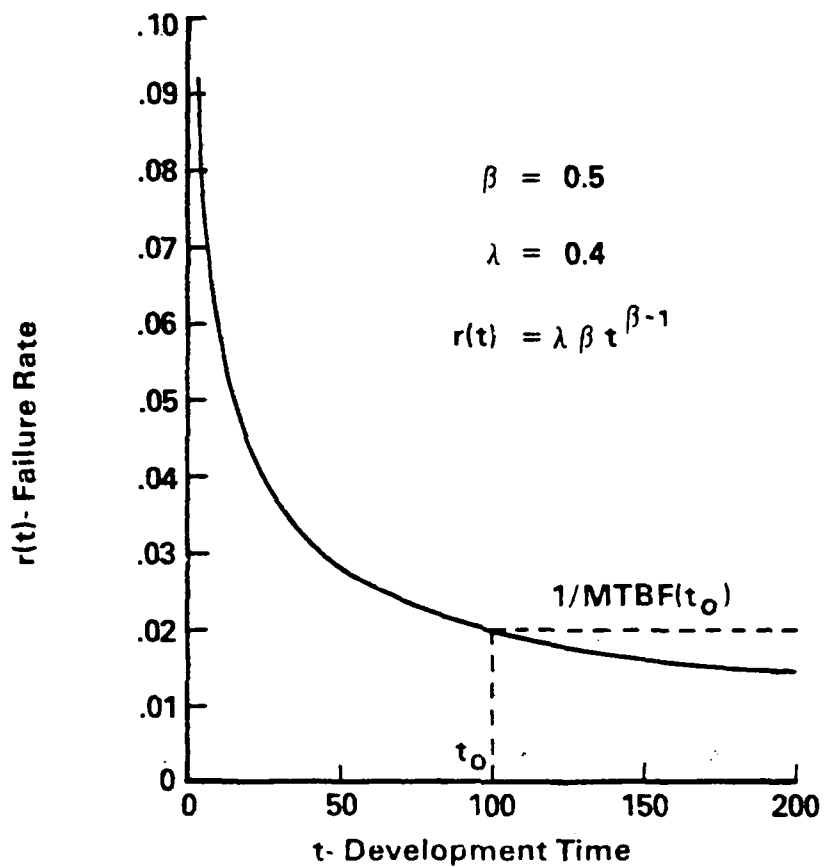
FIGURE 8.5.3-3: FAILURE RATE VS. DEVELOPMENT TIME FOR WEIBULL FAILURE RATE

The previous MLE estimate of β is biased. The unbiased estimate is obtained by using

$$\bar{\beta} = \frac{N-1}{N} \hat{\beta}$$
(8.35)

The MLE of λ is

(8.36)

$$\hat{\lambda} = \frac{N}{KT^{\bar{\beta}}}$$

The chi-square goodness of fit test can be used to determine if the observed data fits the Duane model. The chi-square statistic is calculated using

$$\chi_c^2 = \sum_{i=1}^{c} \frac{(O_i - E_i)^2}{E_i}$$

To compute the statistic the development time is divided into c intervals. The observed number of failures in the i-th interval, O_i, is obtained from the observed data. The expected number of failures in the i-th interval, E_i, is obtained using

$$E_i = \frac{N(t_i^{\bar{\beta}} - t_{i-1}^{\bar{\beta}})}{T^{\bar{\beta}}}$$
(8.37)

where t_{i-1} and T_i are the beginning and ending times for the i-th interval. The χ_c^2 is compared with the tabled value of chi-square, χ_T^2, with degrees of freedom equal to c-1 and the specified level of significance. If

$$\chi_c^2 < \chi_T^2$$

then it can be concluded that the data fits the Duane model.

8.5.3.1 APPLICATION EXAMPLE

An engine system was analyzed for reliability growth using the Duane model. The data available for analysis was based on 8063 hours of development testing. During this time there were 40 failures and the times of each failure were recorded. The average rates for this system during each 1000 hour interval are shown in Figure 8.5.3.1-1.

Using the data the MLE's of λ and β were computed to be

$$\hat{\lambda} = 0.128$$

$$\hat{\beta} = 0.639$$

Failure Times

1, 43, 43, 171, 234, 274, 377, 530, 533, 941, 1074, 1188, 1248,
2298, 2347, 2347, 2381, 2456, 2456, 2500, 2913, 3022, 3038,
3728, 3873, 4724, 5147, 5179, 5587, 5626, 6824, 6983, 7106,
7106, 7568, 7568, 7593, 7642, 7928, 8063
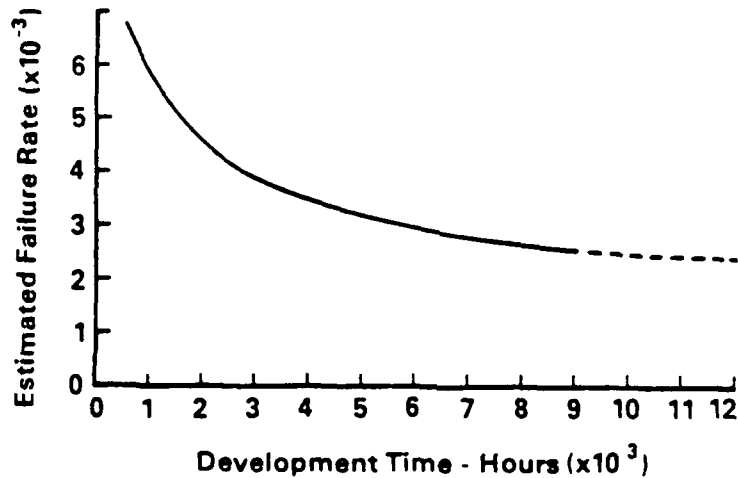
FIGURE 8.5.3.1-1: <u>FAILURE TIMES AND ESTIMATED FAILURE RATE FOR EXAMPLE</u>

The unbiased estimate of β is

$$\bar{\beta} = 0.623$$

The chi-square goodness of fit statistic was calculated next using an interval width of 1500 hours. The result was

$$\chi_C^2 = 1.343$$

Using a 1% level of significance and degrees of freedom of 6-1=5, the tabled value of chi-square is

$$\chi_T^2 = 15.086$$

Thus it can be concluded that the Duane model fits the data.

Using the Eq. (8.31), the estimated failure rate for the engine becomes

$$r(t) = .128(.623) \; t^{.623-1}$$
$$= .08t^{-.377}$$

A plot of this failure rate curve is given in Figure 8.5.3.1-1. Notice how the curve is beginning to flatten out. In fact it would take 100,000 hours of development time to get the failure rate down to .001 failures/hour.

8.5.4 COMPARISON OF RELIABILITY GROWTH MODELS

Parametric models imply that there is a pattern to the growth, while nonparametric models allow the growth curve to "fall where it will". Because of this, only the parametric models are useful for mathematical descriptions of the generic or budgeted growth. Also, the nonparametric models generally do not allow projections to be made. However, either parametric or nonparametric models can be effectively used for controlling reliability growth.

Another consideration is the type of failure distribution that the growth model assumes. Many of the models treat the failure distribution in a nonparametric fashion. However, some models are based specifically on the assumption that the failure distribution is exponential.

Finally, although some of the models utilize a continuous time scale, others utilize a discrete scale, implying that the testing is performed in stages.

Although the Duane reliability growth model has been the one most widely used, a number of other models, both discrete and continuous, have been proposed in the literature. Appendix B provides an overview of a number of proposed models. It may be used as a guideline for choosing a particular model for a particular application.

In forms of a comparison of proposed growth models, RADC performed a study (Ref. 19) of the applicability of six growth models to various classes of ground based and airborne systems in two basic environments:

    (1) "in-house" where failure reporting and analysis is closely controlled and corrective actions are taken

    (2) "in-field" where the equipment or system operates in its intended use environment and where failures are reported.

The six models compared (see Appendix B for model descriptions) were:

    (1) Duane Model
    (2) IBM Model
    (3) Exponential-Single Term Power Series Model
    (4) Lloyd-Lyrow Model
    (5) Aroef Model
    (6) Simple Exponential Model

Table 8.5.4-1 indicates the types of equipment/system studied. Table 8.5.4-2 provides more details in the equipment. Smallest R and R.E. represent best fit. Table 8.5.4-3 provides a comparison of the models in terms of goodness of fit to ground and airborne equipment. Table 8.5.4-4 provides a comparison of models by equipment category.

Ref. 19 also provides guidelines and criteria to help in determining which model is most appropriate for a given equipment and application.

TABLE 8.5.4-1: SYSTEM/EQUIPMENT DESCRIPTION

Shipboard Radar

Ground Based Radar

Satellite Microwave Link

Shipboard Satellite Microwave Communication

Weapon Control

Radar Display

Computer

Ground Based Radar

Shipboard Radar

Computer

Computer

Computer

Shipboard Radar

Radar Display and Computer

Ground Based Radar

Airborne

Laser Range Finder

Laser Bombing System

Visual Scan System

Infrared System

Infrared System

Radar System

Airborne Computer

Radar System

TABLE 8.5.4-2: EQUIPMENT CATEGORIES

(1)	Antenna	Pedestal, dish, driver gears, motor, hydraulics
(2)	Radar	Receiver, exciter, signal processor, transmitter, power supplies
(3)	Microwave	Receiver, exciter, klystron, transmitter, power supplies
(4)	Display	CRT, data input console, display controls, power supplies
(5)	Computer	Computer circuits, CPU, memory, power supplies
(6)	Communication	Radio receiver, teletype, etc.
(7)	System-Radar	Complete radar system
(8)	System-Microwave	Complete microwave system
(9)	System-Laser	Complete laser system
(10)	System-Infrared	Complete infrared system
(11)	System-Visual Scan	Complete system for night time sighting
(12)	Laser Transmitter	Laser transmitter and optics, control electronics, power supplies
(13)	Laser Receiver	Photo diode detector and optics
(14)	Laser Xmtr/Rcvr	Laser transmitter and receiver, control electronics, power supplies
(15)	Infrared Receiver	IR receiver and amplifier, power supplies

TABLE 8.5.4-3: JOINT GOODNESS OF FIT ANALYSIS FOR AIRBORNE/GROUND AND
IN-HOUSE/FIELD CLASSIFICATIONS

| | Ground | | | | Airborne | | | |
| | In-House | | Field | | In-House | | Field | |
	$\bar{R}$	R.E.	$\bar{R}$	R.E.	$\bar{R}$	R.E.	$\bar{R}$	R.E.
Duane	28.64	0.73	24.38	1.01	25.44	0.54	67.88	4.1373
IBM	28.43	1.15	26.85	1.73	23.96	0.42	13.66	0.51
Exponential	24.41	1.21	32.05	2.11	11.41	0.10	7.38	0.07
Lloyd-Lipow	25.32	0.64	20.65	0.66	28.42	0.58	11.79	0.27
Aroef	22.30	0.62	19.21	0.63	23.70	0.55	10.57	0.18
Simple Exponential	16.95	0.36	13.08	0.35	13.76	0.24	12.20	0.31

i)   The Duane model cannot be recommended for airborne field data.

ii)   Conversely, the IBM model is excellent, at its' best, for airborne field data.

iii)   The exponential model is excellent for all airborne data, but is best for airborne field data.

iv)   The Lloyd-Lipow and Aroef models do quite well for airborne-field data.

v)   The simple exponential model is good everywhere although the exponential model is clearly better for all airborne systems/equipments.

$\bar{R}$ = Goodness of Fit (Ideal = 0)
R.E. = Residual Error (Ideal = 0)

TABLE 8.5.4-4: MODEL COMPARISONS BY EQUIPMENT CATEGORIES

		Duane	IBM	Exponential	Lloyd	Aroel	Simple Exponential
Antenna	$\bar{R}$	35.9850	16.7530	23.0410	22.3320	21.5580	16.2990
	R.E.	1.0482	0.7259	0.5796	0.5841	0.5548	0.4177
Radar	$\bar{R}$	20.6280	50.1790	72.3920	26.6380	22.6870	12.3960
	R.E.	0.4015	1.7720	6.2718	0.6765	0.6580	0.3157
Microwave	$\bar{R}$	19.0350	25.4430	15.4510	20.2110	18.7690	11.6750
	R.E.	0.7838	0.9908	0.6356	0.7973	0.8172	0.3025
Display	$\bar{R}$	28.4680	24.8820	33.6450	22.2150	18.6920	12.0720
	R.E.	1.1747	0.7968	1.1845	0.5284	0.4772	0.2424
Computer	$\bar{R}$	28.5570	46.8850	44.9850	19.0615	17.0070	11.7310
	R.E.	1.1587	2.8860	2.9100	0.6077	0.5948	0.3171
Communications	$\bar{R}$	30.7875	19.5005	30.8080	21.8400	20.5840	16.0990
	R.E.	2.4698	0.8457	0.9524	0.6223	0.6389	0.6372
System-Radar	$\bar{R}$	14.5100	26.7090	189.3860	33.2090	27.7325	12.1090
	R.E.	0.1688	1.3847	8.1803	0.7514	0.7769	0.1978
System-Microwave	$\bar{R}$	19.3220	19.1505	16.0805	20.2900	19.1680	11.3010
	R.E.	0.9852	0.7591	0.7144	0.9157	0.9182	0.3717
System-Laser	$\bar{R}$	19.3820	219.9044	8.2890	80.0380	48.1175	30.7790
	R.E.	0.0710	2.3913	0.0189	0.7265	0.7111	0.2242
System-Infrared	$\bar{R}$	65.9675	14.2100	11.6100	12.3915	11.5110	12.5170
	R.E.	4.2379	0.5450	0.1148	0.3028	0.2184	0.3516

TABLE 8.5.4-4: MODEL COMPARISONS BY EQUIPMENT CATEGORIES (Cont'd)

	Duane Model	IBM Model	Exponential Model	Lloyd Lipow	Aroel Model	Simple Exponential	
System-Visual Scan	13.4620	44.3915	8.7810	23.8460	19.6965	18.2945	$\bar{R}$
	0.2909	1.6316	0.1942	0.6400	0.5550	0.3932	R.E.
Laser Transmitter	33.6590	138.9970	15.6250	42.9715	28.8185	31.0705	$\bar{R}$
	0.2355	0.6332	0.0243	0.3465	0.2770	0.3234	R.E.
Laser Receiver	51.2480	126.7180	12.0280	52.5700	32.5030	31.7310	$\bar{R}$
	0.3118	0.9517	0.0394	0.6944	0.6587	0.2164	R.E.
Las-Xmtr/Rcvr	25.2970	158.5719	11.4100	66.1775	42.6435	36.0765	$\bar{R}$
	0.1163	0.9805	0.0293	0.6072	0.5273	0.3072	R.E.
Infrared Receiver	41.4885	16.1805	22.4500	21.4965	16.2760	19.4359	$\bar{R}$
	0.9573	0.3365	0.0816	0.5767	0.5047	0.6174	R.E.

i) For antennas all the models except the Duane model are quite good.

ii) For radar and microwave systems/equipment the Duane model and the simple exponential model are very good.

iii) For display, computer, and communications equipment the Lloyd-Lipow, Aroef and simple exponential models are good.

iv) For infrared systems equipment all models but the Duane model are excellent.

v) For all laser systems/equipments the exponential is vastly superior to all other models.

vi) For the visual scan equipment the exponential model is again superior to the remaining models.

8.5.5 RELIABILITY GROWTH TESTING

8.5.5.1 INTRODUCTION

Reliability growth testing is the formal process of testing an equipment under natural and induced environmental conditions to discover and identify latent failure modes and mechanisms whose recurrence can be prevented through implementation of corrective action, thus causing the growth of equipment reliability. These tests are conducted during the development phase on samples which have completed environmental tests prior to production commitment, and do not replace other tests described in the contract or equipment specification. The requirements and procedures in MIL-STD-781, MIL-HDBK-781, and Ref. 12 contain details on reliability growth test methods and procedures for electronic equipment.

8.5.5.2 WHEN RELIABILITY GROWTH TESTING IS PERFORMED

The formal reliability growth test is to be performed near the conclusion of full scale development after successful completion of environmental qualification testing (MIL-STD-810, for example) and prior to reliability qualification (demonstration) testing (MIL-STD-781 and MIL-HDBK-781, for example). Although all testing should be viewed and planned as contributing to reliability growth, the formal test program dedicated to reliability growth is deferred until after environmental qualification, when the design of the prototype or preproduction equipment which is to be used in the reliability growth test reflects the anticipated configuration and manufacturing processes to be used in production, but prior to commitment to production. The hardware to be tested should have all significant fixes required as a result of environmental qualification testing incorporated before initiating the reliability growth test. The reliability growth test must be successfully concluded, and all significant fixes incorporated in the test hardware prior to initiating the reliability qualification (demonstration) test. The reliability growth test is for the purpose of detecting reliability problems after all performance design and environmental problems have been resolved. The reliability qualification (demonstration) test discussed in Section 8 is for the purpose of proving reliability.

8.5.5.3 RELIABILITY GROWTH APPROACH

The MIL-STD-781 and MIL-HDBK-781 approach to reliability growth is patterned after the Duane model. Essentially, this model provides a deterministic approach to reliability growth. In this way, the system MTBF vs. operating hours falls along a straight line when plotted on log-log paper. That is, the change in MTBF during development is proportional to T^α where T is the cumulative operating time and "α" is the rate of growth corresponding to the rapidity with which faults are found, and changes are made to permanently eliminate the basic causes of the faults observed.

In order to structure a growth test program (based on the Duane model) for a newly designed system, a detailed test plan is necessary. This plan must describe the test-analyze-fix concept, and show how it will be applied to the system under development. The plan must incorporate the following:

(a) Values for specified and predicted (inherent) reliabilities. Methods for predicting reliability (model, data base, etc.) must also be described.

(b) Criteria for reliability starting points, i.e., criteria for estimating the reliability of initially fabricated hardware, must be determined. For avionics systems, the initial reliability for newly fabricated systems has been found to vary between 10% and 30% of their predicted (inherent) values.

(c) The reliability growth rate (or rates) must be defined. to support the selected growth rate, the rigor with which the test-analyze-fix conditions are structured must be completely defined.

(d) Calendar time efficiency factors, which define the relationship of test time, corrective action time and repair time to calendar time, must be determined.

Note that each of the factors listed above impacts the total time (or resources) which must be scheduled to grow reliability to the specified value. Figure 8.5.3-1 (repeated here as Figure 8.5.5.3-1) illustrates the concepts described above.

In addition, Figure 8.5.5.3-1 graphically depicts the four elements needed to structure and plan a growth test program described above. These four elements as identified in the figure are further describe. as follows:

(a) Inherent Reliability - represents the value of design reliability estimated during prediction studies, which may correspond to the value above that specified in procurement documents. Ordinarily, the contract specified value of reliability is somewhat less than the inherent value. The relationship of the inherent (or specified) reliability to the starting point greatly influences the total test time.

(b) Starting Point - represents an initial value of reliability for the newly manufactured hardware. This usually falls within the range of 10%-30% of the inherent or predicted reliability. Estimates of the starting point can be derived from prior experience, or are based on percentages of the estimated inherent reliability. Starting points must take into account the amount of reliability control exercised during the design program, and the relationship of the system under development to the state-of-the-art. Higher starting points, when justified, minimize test time.

(c) Rate of Growth - depicted by the slope of the growth curve. This is, in turn, governed by the amount of control, rigor, and efficiency by which failures are discovered, analyzed, and corrected through design and quality action. Rigorous test programs which foster the discovery of failures, coupled with management supported analysis and timely corrective action, will result in a faster growth rate and consequently less total test time.
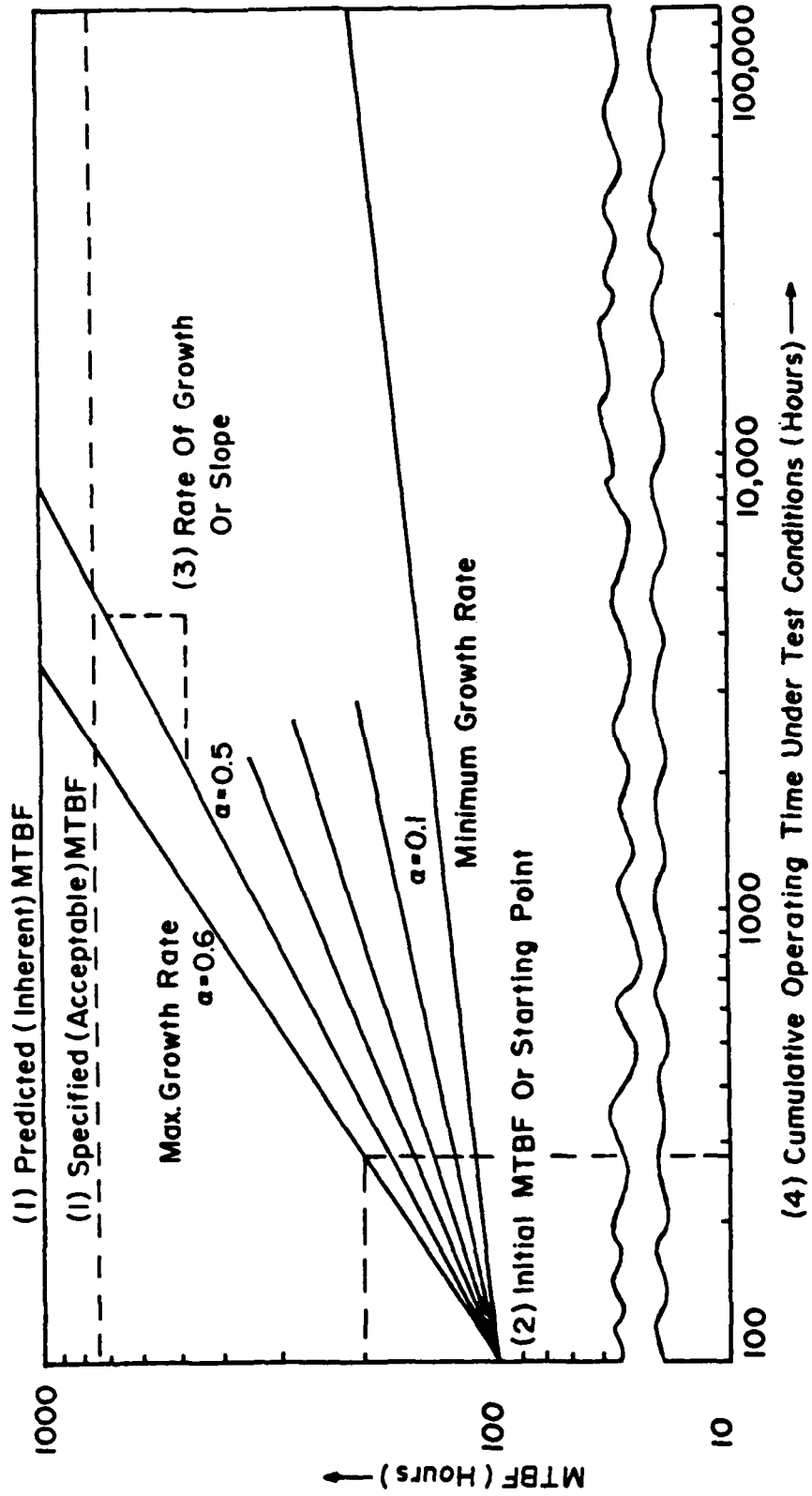
FIGURE 8.5.5.3-1:   RELIABILITY GROWTH PLOT

(d) Calendar Time/Test Time - represents the efficiency factors associated with the growth test program. Efficiency factors include repair time, and operating/nonoperating time as they relate to calendar time. Lengthy delays for failure analysis, subsequent design changes, implementation of corrective action or short operating periods will extend the growth test period.

Figure 8.5.5.3-1 shows that the value of the parameter "α" can vary between 0.1 and 0.6. A growth rate of 0.1 can be expected in those programs where no specific consideration is given to reliability. In those cases, growth is largely due to solution of problems impacting production, and from corrective action taken as a result of user experience. A growth rate of 0.6 can be realized if an aggressive, hard hitting reliability program with management support is implemented. This latter type program must include a formal stress oriented test program designed to aggravate and force defects and vigorous corrective action.

Figure 8.5.5.3-1 shows the requisite hours of operating and/or test time and continuous effort required for reliability growth. It shows the dramatic effect that the rate of growth has on the cumulative operating time required to achieve a predetermined reliability level. For example, Figure 8.5.5.3-1 shows, for an item product whose MTBF potential is 100 hours, that 100,000 hours of cumulative operating time is required to achieve an MTBF of 200 hours when the growth rate is 0.1. And, as previously stated, a 0.1 rate is expected when no specific attention is given to reliability growth. However, if the growth rate can be accelerated to 0.6 (by growth testing and formal failure analysis activities) then only 300 hours of cumulative operating time is required to achieve an MTBF of 200 hours.

Some general guidance on reliability growth test time is given in MIL-STD-781 and MIL-HDBK-781 as follows:

"Fixed length test times of 10 to 25 multiples of the specified MTBF will generally provide a test length sufficient to achieve the desired reliability growth for equipment in the 50 to 2000 hour MTBF range. For equipments with specified MTBFs over 2000 hours, test lengths should be based on equipment complexity and the needs of the program, but as a minimum, should be one multiple of the specified MTBF. In any event, the test length should not be less than 2000 hours or more than 10,000 hours."

Where time is not an appropriate measurement parameter for the particular hardware, the Duane model is adaptable to other measurement parameters such as cycles, events, rounds, etc. Table 8.5.5.3-1 is a list of specific growth documents used by NAVAIR which reflect tailoring of the growth program to the particular requirements of the equipment characteristics.

TABLE 8.5.5.3-1: RELIABILITY GROWTH AERONAUTICAL REQUIREMENTS

Aeronautical Requirement	Title
AR-104	Reliability Development Test for Avionic Equipment
AR-108	Reliability Development Test Program for Fluid and Mechanical Airframe Subsystems and Airborne Special Mission Systems
AR-111	Reliability Development Test Program for Armament Equipment, Gun Systems, and Associated Stores Management Systems
AR-112	Reliability Development Test Program for Crew Systems Equipment
AR-113	Reliability Development Test Program for Ground Support Equipment
AR-114	Reliability Development Test Program for Range Instrumentation Equipment
AR-115	Reliability Development Test Program for Ship Installation Equipment
AR-116	Reliability Development Test Program for Photographic Equipment
AR-117	Reliability Development Test Program for Meteorological Equipment

8.5.5.4 ECONOMICS OF RELIABILITY GROWTH TESTING

The purpose of reliability growth testing is simple - to save the DoD money during the planned service life of the equipment's utilization. Experience has shown that an investment in assuring that specified reliability is, in fact, achieved prior to production, will result in significantly reduced life cycle cost over the planned service life of the equipment due to savings in less maintenance actions, less required spares, and less handling damage among others. This relationship is illustrated in Figure 8.5.5.4-1: Point (1) represents the acquisition cost of an equipment without a reliability growth test requirement and a delivered MTBF (based on post production experience) considerably less than the specified MTBF for that equipment. The DoD cumulative cost of ownership rises with equipment operating time to account for equipment repairs and spares support over the life of the equipment. Point (2) represents the acquisition cost of the same equipment, with the added cost of the reliability growth test program to achieve specified MTBF as a delivered MTBF. The cumulative cost of ownership with equipment operating time increases at a slower rate than the previous case due to less frequent repairs and reduced spares support requirements until a breakeven point is reached. At this point the growth test program has paid for itself and the difference in costs due to the reliabiltiy growth program represents a life cycle cost savings.

8.5.6 RELIABILITY GROWTH MANAGEMENT

8.5.6.1 INTRODUCTION

Reliability growth management is the systematic planning for reliability achievement as a function of time and other resources, and controlling the ongoing rate of achievement by reallocation of resources based on comparisons between planned and assessed reliability values.

Reliability growth management is part of the system engineering process (MIL-STD-499). It does not take the place of the other basic reliability program activities (MIL-STD-785) such as predictions (MIL-STD-756), apportionment, failure mode and effect analysis, and stress analysis. Instead, reliability growth management provides a means of viewing all the reliability program activities in an integrated manner.

It is imperative to recognize that a total reliability program (i.e., a MIL-STD-785 type program) is needed for effective reliability growth management. While it is generally recognized that reliability will grow in the presence of a reliability program, reliability growth planning provides an objective yardstick and an orderly means of measuring progress and directing resources, so that reliability requirements may be achieved in a timely and cost effective manner. A good reliability growth plan can improve the chances of achieving total reliability program objectives. However, it is not intended to be the total reliability program.
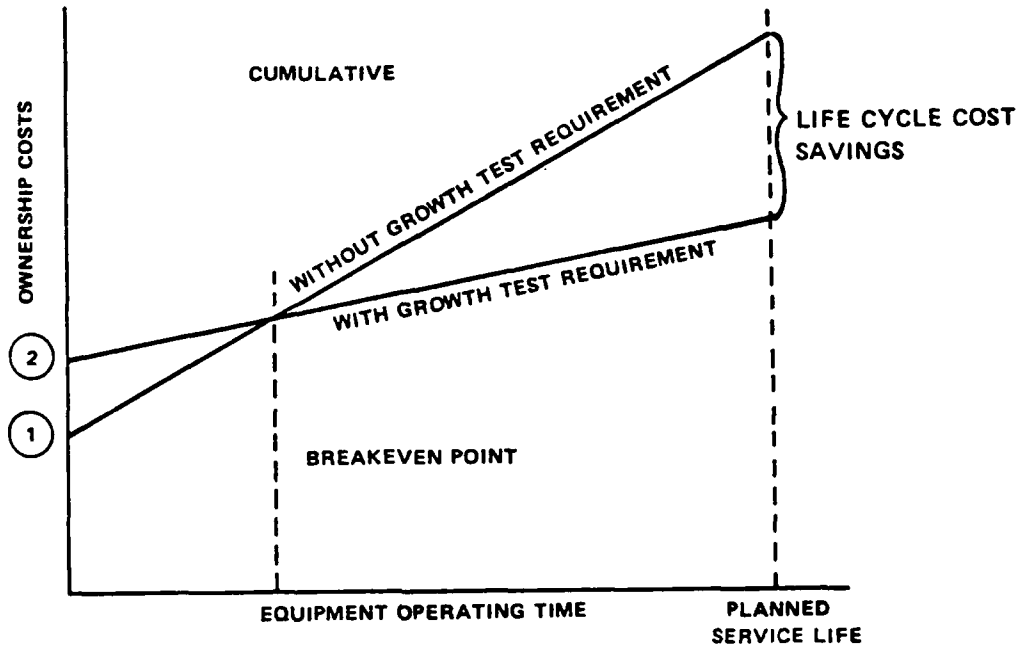
FIGURE 8.5.5.4-1: COMPARISON OF CUMULATIVE LIFE CYCLE COSTS; WITH AND WITHOUT SPECIFIED RELIABILITY GROWTH TEST REQUIREMENTS

MIL-HDBK-189 provides procuring activities and development contractors with an understanding of the concepts and principles of reliability growth, advantages of managing reliability growth, and guidelines and procedures to be used in managing reliability growth. It should be noted that this handbook is not intended to serve as a reliability growth plan to be applied to a program without any tailoring. This handbook, when used in conjunction with knowledge of the system and its development program, will allow the development of a reliability growth management plan that will aid in developing a final system that meets its requirements and lowers the life cycle cost of the fielded systems.

8.5.6.2 MANAGEMENT OF THE RELIABILITY GROWTH PROCESS

There are innumerable ways in which reliability can grow during development. There are, of course, only a finite number of reliability growth models available. Consequently, an acquisition manager cannot conduct the development program in just any fashion, and have an existing reliability growth model available to him for estimation and prediction purposes. The manner in which the development program is managed and the choice of the reliability growth model are, therefore, dependent. Essentially, there are two ways (or models) that the acquisition manager can evaluate the reliability growth process.

(a) He may monitor the various reliability oriented activities (FMEA's, stress analysis, etc.) in the growth process to assure himself that the activities are being accomplished in a timely manner and that the level of effort and quality of work is appropriate. This is a qualitative approach.

(b) He may utilize assessments (quantitative evaluations of the current reliability status) that are based on information from the detection of failure sources.

The assessment approach is, in one respect, preferable in that it is results oriented, in the form of quantitative estimates of planned and achieved reliability as the program progresses. However, the monitoring approach, which is activities oriented, should be used in addition to the assessments. This is especially true since this approach will have to be relied on early in a program, when often the detection of failure sources is not capable of generating objective assessments.

8.5.6.3 MANAGEMENT MODEL (MONITORING)

Figure 8.5.6.3-1 illustrates control of the growth process by monitoring the growth activities such as FMEA's and stress analyses. Since there is no simple way to evaluate the performance of the activities involved, management based on monitoring is less definitive than management based on assessments. Nevertheless, this method of management is a valuable alternative when assessments are not practical. The reliability growth program plan serves, at least partially, as a standard against which the activities being performed can be compared. The program plan serves as a standard of activities to be performed and at what times. But standards for level of effort and quality of work accomplished must, of necessity, rely heavily on the technical judgement of the evaluator.
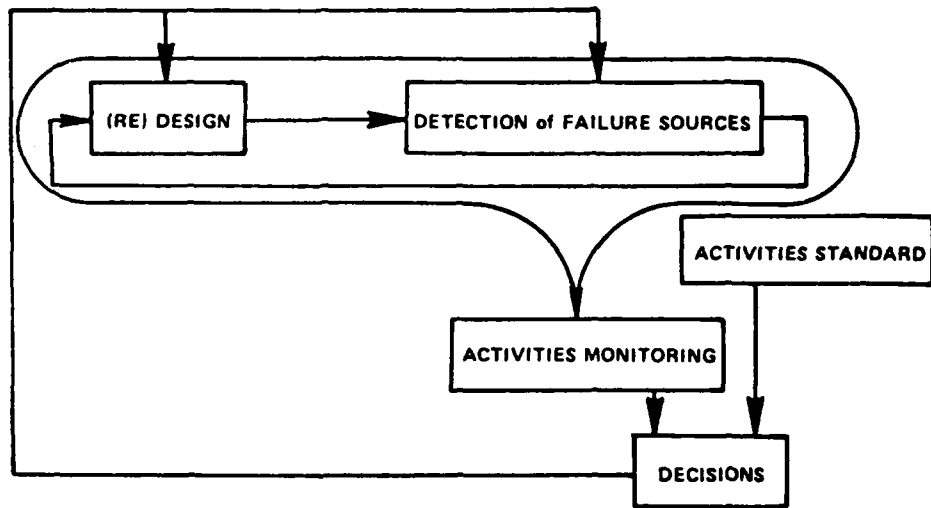
FIGURE 8.5.6.3-1: RELIABILITY GROWTH MANAGEMENT MODEL (MONITORING)

Monitoring is intended to assure that the activities have been performed within schedule, and meet appropriate standards of engineering practice. It is not intended to second guess the designer, e.g., redo his stress calculations.

One of the better examples of a monitoring activity is the design review. The design review is a planned monitoring of a product design to assure that it will meet the performance requirements during operational use. Such reviews of the design effort serve to determine the progress being made in achieving the design objectives. Perhaps the most significant aspect of the design review is its emphasis on technical judgements, rather than quantitative assessments of progress.

8.5.6.4 MANAGEMENT MODEL (ASSESSMENT)

Figure 8.5.6.4-1 illustrates how assessments may be used in controlling the growth process. One of the more important points to emphasize is that assessments have been a way of life in reliability work for many years, as have the resultant decisions.

What, then, is new about reliability growth management? What is new is a formal standard against which the assessment may be compared. The fact that managers in the past have made decisions based on assessments implies that they had at least a subjective standard of acceptable reliability growth against which they were comparing. A formal, objective standard has the advantage of remaining constant, unless formally changed, rather than bending in the hope that "tomorrow will be better."

Figure 8.5.6.4-2 illustrates an example of a reliability growth curve, showing both the budgeted (planned) reliability growth and assessments. A comparison between the assessment and the budgeted value will suggest whether the program is progressing as planned, better than planned, or not as well as planned. Based upon the first two data points of assessed growth, the decision would probably be made to continue development with no changes. If reliability progress is falling short, as the two subsequent assessed data points indicate, new strategies should be developed. These strategies will probably involve the reassignment of resources to work on identified problem areas. They may, as a last resort, result in adjustment of the time frame, or relaxation of the original requirement.

8.5.6.5 INFORMATION SOURCES THAT INITIATE RELIABILITY GROWTH

The detection of failure sources is the activity that effectively initiates the growth process by pointing the way for redesign. Because the information sources that are used for detecting failure sources are so varied, and because they can be relied on at different times during the life cycle, great program flexibility is possible. Although the total number of information sources that can be used to initiate reliability growth is rather large, they can be grouped into five categories: external experience, analysis, tests, production experience, and operational experience.
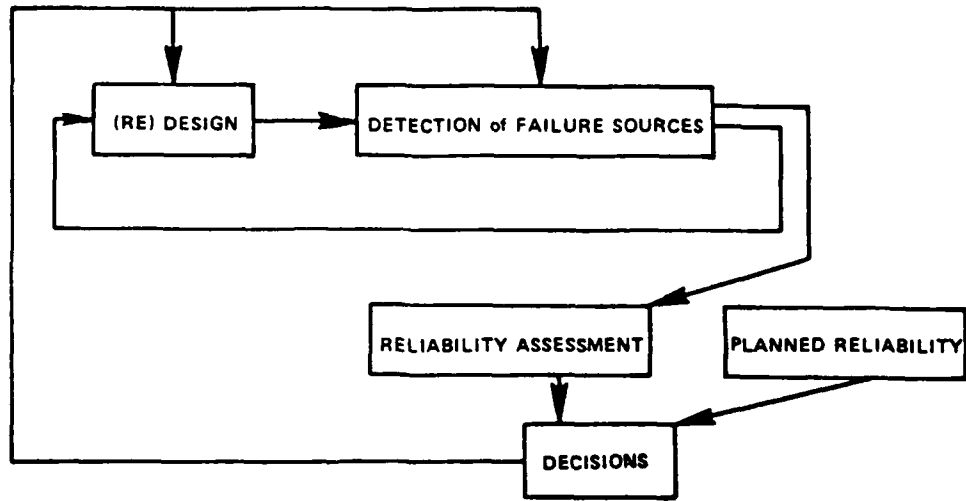
FIGURE 8.5.6.4-1: RELIABILITY GROWTH MANAGEMENT MODEL (ASSESSMENT)
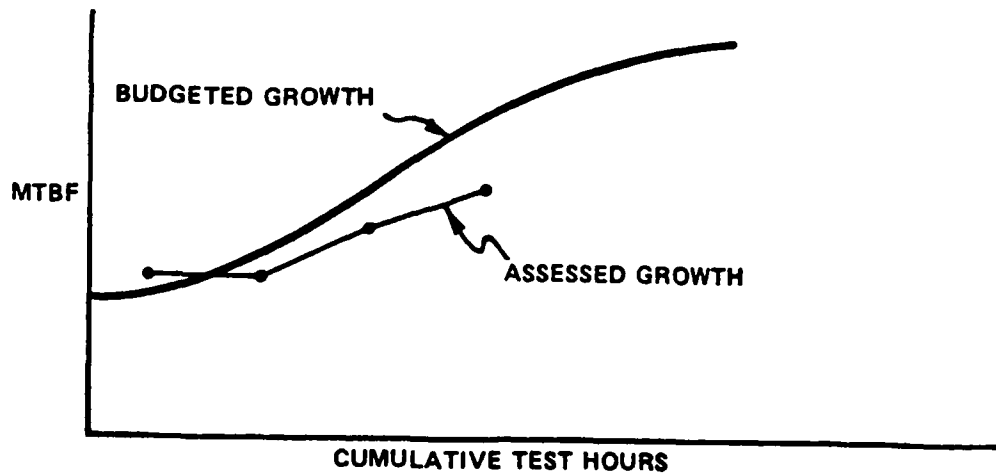
FIGURE 8.5.6.4-2: EXAMPLE OF A RELIABILITY GROWTH CURVE

(a) <u>External Experience.</u> This is information generated outside the specific development program which has applicability within the program. Examples of this type of information are historical data, publications, technical experience of personnel, and information from currently operating systems.

(b) <u>Analysis.</u> This is information generated within the specific development program, excluding the test of hardware. Examples are feasibility studies, probabilistic reliability design, failure mode and effect analysis, and design reviews.

(c) <u>Tests.</u> Although this source of information is self explanatory, the various ways in which testing is performed are important considerations. The hardware may be in any level of maturity, ranging from breadboard to final production configurations. Various levels of assembly may be tested, ranging from components to system level. Finally, the environmental conditions can vary all the way from testing under ambient conditions to overstress or accelerated testing. Testing is the most common source of information for initiating growth, and the source usually modeled, because it yields objective measurements.

(d) <u>Production Experience.</u> The production process itself may identify weak areas in the design.

(e) <u>Operational Experience.</u> The use of fielded systems will identify design deficiencies which point the way toward reliability growth.

8.5.6.6 <u>RELATIONSHIPS AMONG GROWTH INFORMATION SOURCES</u>

The chronological relationship of these information sources is illustrated in Figure 8.5.6.6-1. This figure illustrates that growth is at least possible at any point in the life cycle. However, what are the relative merits of growing reliability at these various points? To a large extent, this question can only be answered with respect to a specific development program. But there are two fundamental considerations that must be made. First, changes can be accomplished very economically early in the life cycle. The example usually given is that a change which would cost $1 on the drawing board will end up costing about $100 if it is made after the equipment is fielded. Therefore, it is desirable to grow reliability as early as possible. However, the information upon which early changes are based tends to contain many unknown factors, such as operational conditions and component interactions. Second, changes which are made later in the life cycle tend to be better directed, as there are fewer unknowns in the information as hardware maturity is approached. The two desired characterisitcs will be referred to as "timeliness" and "credibility".

EXTERNAL EXPERIENCE

ANALYSIS			PRODUCTION EXPERIENCE	
BREADBOARD, MODEL MOCK-UP TEST	ENG. DEVEL HARDWARE TEST	PROTOTYPE HARDWARE TEST	EARLY PROD. TOOLED H/W TEST	LATER PRODUCTION TEST

Operational Experience
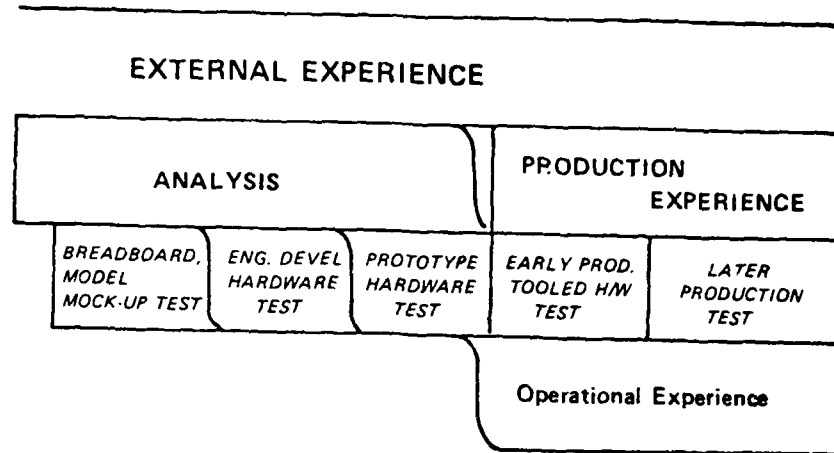
FIGURE 8.5.6.6-1:   INFORMATION SOURCES THAT INITIATE RELIABILITY GROWTH

Depending on the characteristics of the specific program and system, it may be desirable to place particular emphasis on certain combinations of these information sources. In effect, we would like to achieve a reasonable combination of timeliness, credibility, and economy. The following paragraphs give some suggestions about when it may be desirable to place emphasis on various types of information sources. The rationale that is given here could serve as a basis for a more formal economic model for specific applications. The suggestions that are given here are intended to point out those information sources which have the strongest potential under varying situations. A good program would probably utilize all of the information sources to some degree, but the mix and emphasis will vary from one program to the next.

(a) Reliability Growth Through External Experience. The strongest feature of external experience is that it may be available at the very beginning of the life cycle, thus emphasizing timeliness. This is, of course, assuming that appropriate external experience is available.

(b) Reliability Growth Through Analysis. Analysis becomes particularly valuable when the system reliability is high, mainly because the next best alternative, testing, will tend to be time consuming and therefore expensive. However, in order to be able to rely heavily on analysis, much detailed knowledge is necessary. The operation of the system must be well understood. This implies that the development must be reasonably within the state-of-the-art. There must be good, detailed knowledge of the environment and use conditions. Finally, appropriate design analysis techniques must either be available or specially developed, and there must be a good information base to support these techniques. Many reliability programs today put too little emphasis on analysis, and the associated information base. One problem with a reliance on analysis is that the effects cannot be measured objectively.

(c) <u>Reliability Growth Through Testing</u>. Reliability growth models are generally based on test results. Therefore, testing is a very important information source for initiating reliability growth. Testing will have the greatest payoff if many failures are encountered which can be thoroughly analyzed. Therefore, a low system reliability and an ability to perform failed part analysis suggest strong emphasis on testing. One other factor which must be considered is the cost of testing itself. High test costs may discourage strong reliance on testing to achieve growth. However, generally there is no valid substitute for a good test program in the reliability growth process.

(d) <u>Reliability Growth Through Production Experience</u>. The production process and its quality controls are major contributors to reliability. In fact, a drop in reliability during the transition from development to production is a com on phenomenon. It then becomes necessary to grow reliability based on manufacturing process redesign and/or better quality controls. Many process and control problems can be eliminated during the production phase through the use of process capability studies, worst case analyses, and similar producibility related techniques. However, it is unlikely that all process and control problems could be eliminated during preproduction. And almost certainly, the payoff from these techniques, expressed as a function of effort, would show a diminishing returns pattern. It is almost inevitable that some problems can be more cost effectively eliminated after production starts, particularly when the production run is relatively long and the tooling is relatively inexpensive.

(e) <u>Reliability Growth Through Operational Experience</u>. Although some reliability growth through operational experience is inevitable, this method is the least desirable of the five sources listed. Improving reliability through retrofitting of fielded systems often costs up to a hundred times as much as the same change made on the drawing board.

8.5.6.7 TYPES OF MODELS UTILIZED IN RELIABILITY GROWTH MANAGEMENT

In generating the reliability growth plan, the manager must predict the system's changes in reliability as the system matures, as well as track the system's progress. He must also project the system's status at future milestones. Reliability growth models are used to describe these changes in reliability. The majority of reliability growth models express an appropriate reliability parameter as a function of test time. Since these descriptions may be made either before or after the fact and for different purposes, the following discusses how growth models may be used. These uses are illustrated in Figure 8.5.6.7-1.
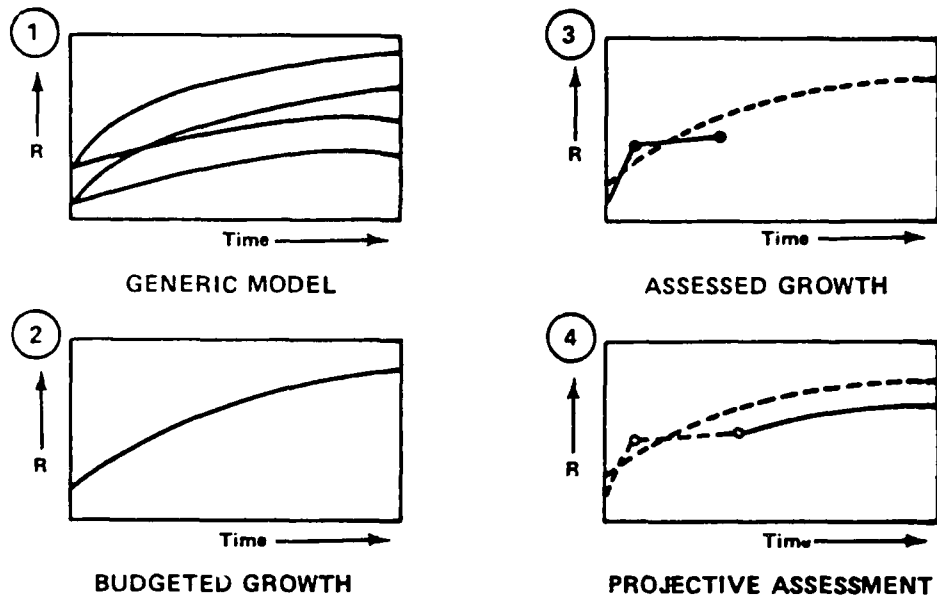
FIGURE 8.5.6.7-1: FOUR TYPES OF RELIABILITY GROWTH MODELS

(a) <u>Generic Growth Model</u>. The generic growth model is used to depict the generalized growth pattern for a particular class of systems developed, utilizing historical data. System characteristics that affect growth patterns include state-of-the-art, system complexity, and the nature of the system (mechanical or electrical). Program characteristics affecting the growth patterns include external experience, analysis, levels and types of tests, failure correction, redesign effort, and resources available. The generic model may be a mathematical model or a series of milestones depicting a typical development program for systems in the class. As an example of a mathematical generic model: "When Organization X develops a system, reliability growth occurs in accordance with the Duane model." As an example of a milestone based generic model: "When Organization Y develops a system, 70% of the operational MTBF is achieved in 1 year, 100% in 3 years.

(b) <u>Budgeted Growth Model</u>. This model defines the reliability we expect to achieve at specific points in the life cycle. The budgeted curve has the same general shape as the generic curve, but passes through a specific set of points. To continue the previous examples: "Organization X has a budgeted reliability growth during development in accordance with a specified model with a growth rate of 0.5; or Organization Y has a budgeted MTBF of 700 hours at the end of 1 year, and an MTBF of 1000 hours at the end of 2 years."

(c) <u>Growth Assessment Model</u>. In order for a manager to control technical activities, he must have knowledge of his system's status on either a continuous or periodic basis. This knowledge is gained through assessment. Assessments can be made from test results in two different ways: the assessment may be based entirely on tests run on the current configuration, ignoring all previous information; or the assessment may be based on the statistically combined results of all tests up through the present, taking into consideration, mathematically, the growth that has occurred.

(d) <u>Projective Assessment Model</u>. Considering where we are today, where do we expect to be at future points in time if we follow certain courses of action? A projective assessment extrapolates beyond the currently assessed value. It utilizes the generic model to establish the general shape and proposed program characteristics to determine the specific path.

8.5.6.8 EVALUATING SYSTEM GROWTH POTENTIAL

When the reliability requirement for a system has been defined, it is important that the reliability program manager analyze, at least qualitatively, the growth potential of the system. This is necessary to give an indication of the resources required to attain the requirements.

Three factors affect the difficulty of achieving growth:

(a) Reliability design effort prior to the growth effort

(b) The specified reliability (MTBF) level

(c) The relationship between the reliability level and the state-of-the-art

The type of reliability design effort prior to a formal growth effort has a distinct effect on the difficulty of achieving fixes. A complete MIL-STD-785 Reliability Program effort prior to the growth effort may have only a small noticeable effect on the initial level of reliability. However, it affords good assurance that the reliability is "growable". The key point to bear in mind is that the growth process is basically a refinement process. As such, this growth process is very inefficient if major design changes are necessary. The rate of reliability growth is usually found to be:

(a) Higher for analog hardware than for digital hardware

(b) Higher in equipment of low maturity than in production hardware

(c) Higher in equipment exposed to severe test conditions than in equipment (for example) undergoing bench tests

(d) Higher in proportion to the hardware oriented reliability improvement effort

The specific level of the reliability has an obvious effect on the growth process. The higher the reliability requirement, the more testing must be performed to uncover each remaining failure source.

Finally, if the reliability level approaches or goes beyond the current state-of-the-art, fixes become very difficult since they often require minor advances in the state-of-the-art. The baseline analysis and the analysis of technological advances can serve as an indicator of the current state-of-the-art.

8.5.6.9 EVALUATING THE RELIABILITY STATUS

If a quantitative assessment of the reliability is desired prior to the initiation of system testing, the only alternative is to base the assessment on a prediction. If subsystem or component test information is available, it may be used to supplement or replace the more theoretical inputs to the prediction model. The problem that is introduced is that most predictions evaluate the reliability of a debugged system. That is, the assumption is made that the parts application problems and interaction and interface problems have been (or will be) rectified. By using actual component test results in the prediction model, the parts applications assumption is tested. However, the interaction and interfaces with other components or subsystems are not tested. Therefore, a prediction based on generic data tends to be optimistic when compared against the hardware intially subjected to test. Even a prediction based on parts test data will be somewhat optimistic.

If assessments were made during a development program based on generic predictions, predictions utilizing component test data, and then system level test data, the results may look somewhat like those illustrated in Figure 8.5.6.9-1. These results make it appear that the reliability was degraded at two points in time. In reality, at these two points in time, problems (which had existed all along) were identified.

In order to more realistically assess the current reliability status, "K-factors" are often used to make up for the problems not identified by the predictions. In fact, the "K-factor" may even be used in closing the gap caused by the differences between test and operational conditions.

The concept of the "K-factor" assumes that equipment initially performs with an MTBF that is approximately 10% of the predicted MTBF. Figure 8.5.6.9-2 illustrates how the application of K-factor serves to close the gaps caused by using different assessment methods.

8.5.6.10 THE RELIABILITY GROWTH BUDGET

Since the reliability growth budget commits the manager to achieving goals, it must be developed with care so as to accurately depict realistic, as well as realizable, reliability growth. While each budgeted curve must be tailored to specific program requirements, there are some considerations which apply to reliability growth budgets in general.
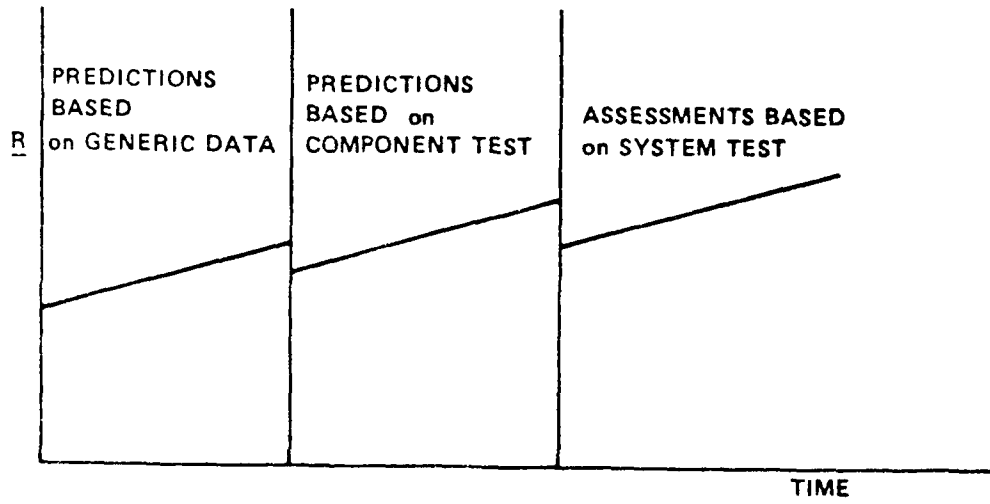
FIGURE 8.5.6.9-1:   ASSESSMENTS BASED ON PREDICTIONS AND TESTING
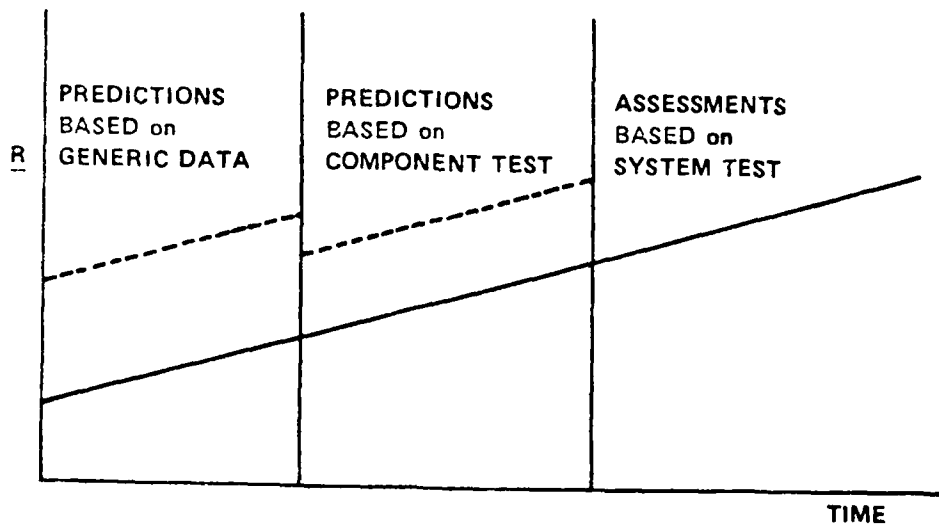
FIGURE 8.5.6.9-2:   ASSESSMENTS BASED ON PREDICTIONS AND TESTING
                    WITH K-FACTORS APPLIED

The first consideration is the general growth pattern displayed by previous systems of a similar type developed under similar programs. In attempting to determine this general growth pattern, or generic model, historical data must be analyzed. It is anticipated that the growth budget will be a reflection of the reliability growth pattern displayed by the historical data. The acquisition manager might be interested in comparing the growth of different systems and programs with their respective complexities, development costs, amounts of testing program activities (FMEA's, design reviews, etc.), program design, and development time, as well as any other factors which caused the historical reliability growth to occur as it did. With this information, knowledge of the new system's requirements and program funds and schedule, the manager is in a position to assess his program in view of past system/program performance. Utilizing some judgment, the manager can now establish his budgeted reliability growth curve, or propose realistic tradeoffs between the schedule, resources, and requirements.

A number of methods of displaying the growth budget are in use. One method is to plot reliability (or failure rate, MTBF, etc.) as a function of test time. An equally popular approach is to plot reliability against calendar time or program milestone. Generally, reliability growth tracking, and its associated budget begin with the first test data for the system or component being tracked. However, in some cases, it may be desirable to track system reliability that is calculated from a math model, using component test inputs.

The initial level of the budgeted reliability can be estimated in various ways. One way is to base this level on analyses of the histories of development programs of similar systems. For example, if previous, similar programs have achieved a reliability of 10% of the design predictions at the beginning of testing, the budgeted curve may be started at this point. In the case of evolutionary systems, the current reliability status may be used as a starting point.

Once a starting point has been determined, the budgeted curve may then be started at this point and extrapolated along the generic model. One of two things might happen. First, this extrapolation may meet or exceed the requirement in the allotted time frame. In this case we are ready to evaluate its cost. Second, it may fail to meet the minimum requirements in the allocated time. In this case the program will have to be re-evaluated.

An alternative method to plotting the budgeted growth curve is to start with the requirement and its scheduled date, and work backwards along the generic model to a starting point. However, this may cause the situation of the initial point on the budgeted curve to be unrealistically high. In this case the program may have to be re-evaluated. In any case, a new starting point may have to be recalculated based on early test results.

In laying out the reliability growth budget, the acquisition manager must keep in mind that one of the purposes of a development program is to design out failure causes. This necessarily involves time to detect and analyze failures as well as time to redesign and, for testing purposes,

time to fabricate hardware. Early in the program, system failures can be detected and corrected relatively easily. However, as test time and severity increases, the increased number and subtlety of failures likely to occur can make correction of the failure causes a time consuming activity. Unless properly planned and scheduled, a bottleneck may be created.

Parametric functions are used in defining, deterministically, the reliability growth budget. These equations are necessarily based on historical data, and readily lend themselves to further mathematical manipulation. It must be recognized, however, that not all types of hardware encounter reliability growth in accordance with previously defined equations. In these instances, the budgeted curve will have to be developed along the historic growth pattern. Managerial judgment, as well as engineering judgment, will have to be exercised. It should also be noted that no models exist for a generic model which covers the entire life cycle. In fact, within a particular phase of the life cycle, the budget might consist of a series of curves, each one being applicable to only a fixed segment of the phase.

The question of when to start growing reliability affects the level at which reliability growth should be planned and controlled. Should it be at the system level, or should consideration by given to major subsystems? If so, what major subsystems should be considered?

The answer is to apply the growth principles at whatever level will give the manager the information needed to manage his system. If information is required at the subsystem level, the manager should not hesitate in doing so. However, when the manager is using information generated at less than the system level, he must be sure to evaluate the information gained with respect to the interface problems that might occur at the system level. He must also evaluate the use conditions under which the reliability manager might be lulled into a false sense of security, and be forced to make a hard, expensive push later in his system's life cycle in order to get the system back on the right track.

The acquisition manager can gain valuable information at the subsystem level if he is aware of these pitfalls. The timeliness of the information gained, plus the generally lower cost of lower level testing vs. system level testing, can be invaluable to the acquisition manager. Many reliability programs could benefit from more emphasis in this area.

8.5.6.11 TAILORING GROWTH MODELS

Quite frequently, growth models must be tailored to reflect the special circumstances in a development program. The following are some suggested tailoring methods:

(a) Choice of Time Scale. If the bottleneck activity in reliability growth during a testing program is the slow occurrence of failures in the test, test time is the critical time variable. Typically, this is the case if design changes can be made and put into hardware rapidly. This is often the case in electronic equipment. On the other hand, there may be

considerable time elapsed between the occurrence of a
significant failure, and the resultant hardware change. If
this is the case, calendar time (representing the time for
redesign and fabrication of hardware) becomes the significant
variable. For planning purposes, it may be convenient to
convert back and forth between test and calendar time scales.
For example, a period of testing may be analyzed using test
time. The results may then be converted to calendar time to
better relate to the growth occurring during other program
phases.

(b) Non-Homogeneous Program. Often, as a program progresses from
one phase to the next, the reliability growth characteristics
change. This is probably most simply handled by using a
piece-wise model, i.e., a series of different growth models
placed end to end as in Figure 8.5.6.11-1. One specific
example of a nonhomogeneous program that occurs often enough
to deserve specific mention is the situation of alternate
periods of test and design. When such a situation occurs,
there is usually very little growth during the test period.
Unfortunately (as far as reliability growth is concerned),
other design changes may be necessary to "grow" other
performance parameters. This introduces new problems, and may
even cause a net decrease in reliability. Of paramount
reliability concern in this type of situation is maintaining
awareness of configuration changes and assessing the potential
impact of those changes on achieved reliability to date.

(c) Partial System Improvement. Frequently, only selected compon-
ents or subsystems of the total system are subject to
modification. Then the reliability growth of the overall
system will occur at a slower rate than usual. This is most
easily handled by breaking the system down into two categories
- those components (subsystems) that are to be held constant,
and those components (subsystems) that are to be modified.
The advantage of this approach is that the planned reliability
growth can be treated in a conventional fashion. This allows
direct application of previously achieved rates of growth for
the planned level of effort. An example of a growth curve for
partial system improvement is shown in Figure 8.5.6.11-2.

8.5.6.12 RELIABILITY GROWTH ASSESSMENT

Just as reliability growth budgeting is one of the first steps in
planning a reliability program to achieve the requirement, reliability
growth assessment is a fundamental step in controlling the activities
necessary for growth.

There are a number of factors involved in determining when to start
reliability assessment. However, a general rule of thumb is that
assessment of reliability should begin as soon as there is any
information on the system's reliability status. In fact, a reliability
prediction can be viewed as an initial assessment of the potential
reliability of the system until such time as prediction data can give
way to actual test data accumulated on the system. Generally, the
growth assessments should start at the same point that the budget does.
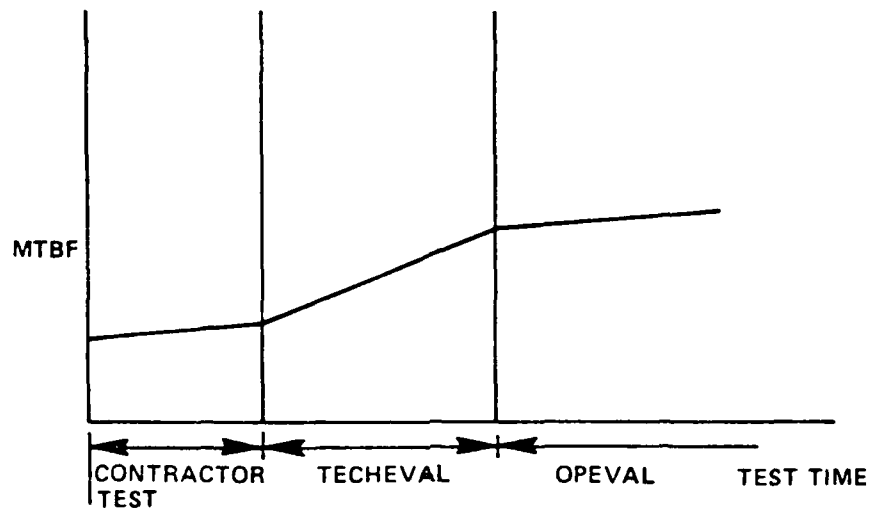
FIGURE 8.5.6.11-1: BUDGETED GROWTH FOR A NON-HOMOGENEOUS PROGRAM
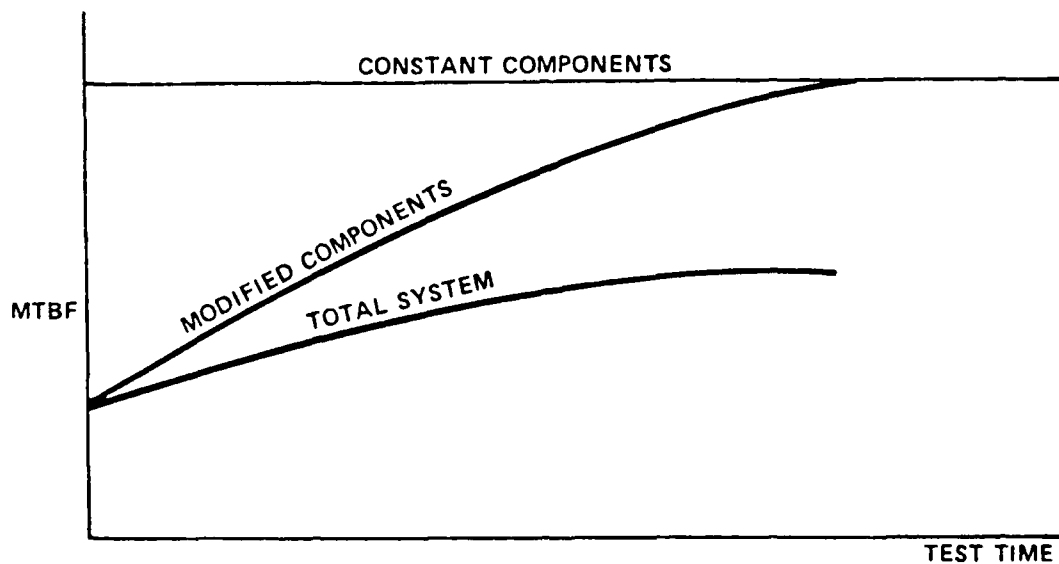
FIGURE 8.5.6.11-2: RELIABILITY GROWTH FOR PARTIAL SYSTEM IMPROVEMENT

In general, assessments for reliability growth management represent an evaluation of the current system configuration on the drawing board. They do not represent an evaluation of future configurations. As previously mentioned, assessments may be based on the test results on the current configuration or on the statistically combined results of all tests up through the present. Or, special statistical techniques may be employed to allow purging of earlier test results to reflect improvements that have been achieved.

While assessments can give the system status, they do not, in themselves, control the reliability effort. The current status, when compared to the budgeted growth curve, can indicate the need for more, less, or no change in the level of reliability growth effort. Discrepancies which exist between the budgeted growth and the assessed growth may be attributed to bottlenecks in the design-assess-redesign loop. For example: "We are assessing according to schedule, but we haven't been able to incorporate all the previous design corrections into our system." Recognizing that things are not moving according to plan, the manager is in a position to reassess the program in terms of resource allocation and schedules. Being on or ahead of schedule, the manager might decide to continue with the current level of effort, or to relax his effort. There is also the fact that any particular assessment might be the result of the luck-of-the-draw, i.e., unrepresentative. However, as the system matures and various assessment techniques are utilized, the luck-of-the-draw risks can be evaluated or minimized.

In some cases, it may be desirable to budget and assess reliability growth at less than system level. Such a situation might be encountered if the reliability apportioned to a particular subsystem, assembly, or even component is relatively high when compared to the past performance of similar items. This situation might also be encountered if it is desired to grow reliability through testing before the full system's hardware has been designed or fabricated. While testing at levels of assembly less than system level yields timely and credible information, perhaps at reduced costs, inferences about the system reliability will not contain concrete information regarding the effects on system reliability of interfaces between these assemblies.

How often to assess the system for reliability growth is a question which must be answered on a case-by-case basis. When there are too few assessments, the concept of reliability growth planning becomes an exercise in futility. In order to control the activities that cause reliability to grow, a manager must have timely feedback of the system's reliability status to compare with the program budget. Too few assessments during design and development and effective control is lost and reliability growth may or may not be achieved. Enough assessments must be made to assure that growth is occurring at the desired rate. Obviously, the assessment plan should be designed in the most cost effective manner.

Coupled with assessments for control purposes is the reliability activities monitoring function previously discussed. It is not enough to say that we have budgeted for the reliability to be at .90 at this stage and it is at .80, therefore pump more money into the design loop. The manager should concentrate on identifying those activities which are restricting growth, and direct his resources at implementing corrective action.

8.5.6.13 RELIABILITY GROWTH PROJECTIVE ASSESSMENT

Projective assessment models were previously discussed; but for management planning and control purposes, certain aspects will be reiterated. The purpose of projective assessment is to force a good, hard look at the overall reliability growth program and the associated design and development effort. In effect, we ask the following questions. If we know what the current system status is and what it should be, what do we expect the reliability of the system to be at the next assessment, if no change is made in the level of effort? Can we reasonably expect to be on or ahead of schedule at the next assessment without a change in our level of effort? What changes must be made in our program or where must resources be spent in order to assure that the end requirement will be met? If resources are allocated to increase effort, where do we expect the system reliability to be at the next assessment?

It must be kept in mind that while, theoretically, there may be no limit to the growth rate, in practice, projective assessments must be based on a realizable growth rate. As the system matures, we may find that the growth budget is too ambitious for funds available or that it has been poorly conceived because of a lack of historical data or experience. Thus, it may be mandatory that schedules, resources, or even system requirements be renegotiated, and a new budget generated before an acceptable system can be fielded.

The Duane and AMSAA (Ref. 17) models have proven to be effective as a projective assessment models. However, it must be realized that when using these models, the basic assumption is made that the level of effort of the reliability program will not change for the duration of the projection. For dealing with jumps in reliability that result from major changes in the reliability program or the system configuration, adjustments will be necessary to the growth model.

Rather than relying on a mathematical extrapolation to project future reliability growth, it may, in some cases, be preferable to consider the specific problems at hand, and reason out the future growth. This approach appears to have the best applicability in cases where the significant time variable is the time for redesign and hardware fabrication, rather than test time. Figure 8.5.6.13-1 illustrates the logical development of such a projection. Point A represents the latest assessment of reliability. In establishing this point, of course, some failures were encountered. What corrective actions can be taken based on these identified areas?

Point B represents an estimate of the reliability that can be achieved if specific corrective actions are taken. However, based on the "batting average" in the past, this estimate may be dropped somewhat to point C. Finally, a judgement of the time required for redesign and modification of hardware slides us out to point D. In effect, point D represents that a certain level of reliability should be demonstrable at that point in time. It might be useful to consider that point A represents an estimate of the demonstrable hardware reliability. However, point B represents an apparent "state of knowledge" reliability. This emphasizes that it is not just the level of hardware reliability which is important, but also what can be done to improve it.

A: CURRENT RELIABILITY
B: RELIABILITY EXPECTED FROM DESIGN CHANGES
C: PROBABLE ACHIEVED RELIABILITY
D: RELIABILITY PROJECTION

CALENDAR TIME
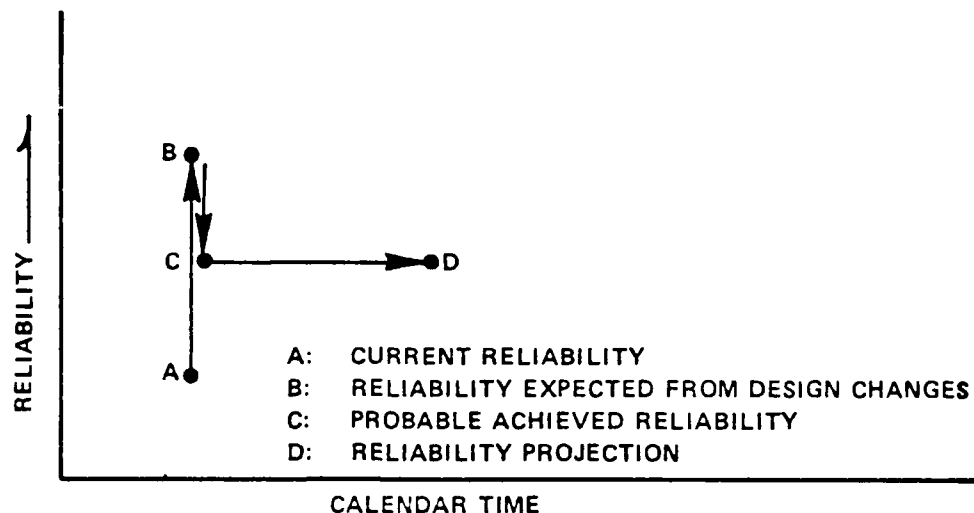
FIGURE 8.5.6.13-1: PROJECTING RELIABILITY GROWTH BASED ON SPECIFIC PROBLEM RESOLUTIONS

8.6 SUMMARY OF THE DIFFERENCES BETWEEN RELIABILITY GROWTH TESTING AND RELIABILITY DEMONSTRATION TESTING

Reliability growth is the result of an iterative design process. As the design matures, it is investigated to identify actual (via testing) or potential (via analysis) sources of failures. Further design effort is then spent on correcting these problem areas. The design effort can be applied to either product design or manufacturing process design. There are three essential elements involved in achieving reliability growth:

(a) Detection of failure sources (by analysis and test)

(b) Feedback of problems identified

(c) Effective redesign effort based on problems identified.

Reliability demonstration tests, on the other hand, are designed for the purpose of proving, with statistical confidence, a specific reliability requirement; not specifically to detect problems, or to grow reliability. The test takes place after the design is frozen and its configuration is not allowed to change. However, in practice, some reliability growth may occur because of the deferred correction of failures observed during the test.

Reliability demonstration is specified in most military system procurement contracts and involves, in many instances, formal testing conducted per MIL-STD-781. This standard defines test plans, environmental exposure levels, cycle times and documentation required to demonstrate formally that the specified MTBF requirements of the equipment have been achieved. Demonstration tests are normally conducted _after_ development has been completed but before high rate production has been initiated. Demonstration tests are normally conducted after growth tests in the development cycle using initial production hardware.

As previously indicated, reliability demonstration testing, conducted per MIL-STD-781, carries with it a certain statistical confidence levels, and the more demonstration testing, the more confidence. The more reliability growth testing that is performed, the higher the actual reliability. Depending on program funding and other constraints, system testing may follow one of two options. The first option maximizes growth testing and minimizes deomonstration testing resulting in a high MTBF at a low confidence. Option two minimizes reliability growth testing with a resultant lower MTBF at higher confidence. These concepts are shown graphically in Figure 8.6-1.
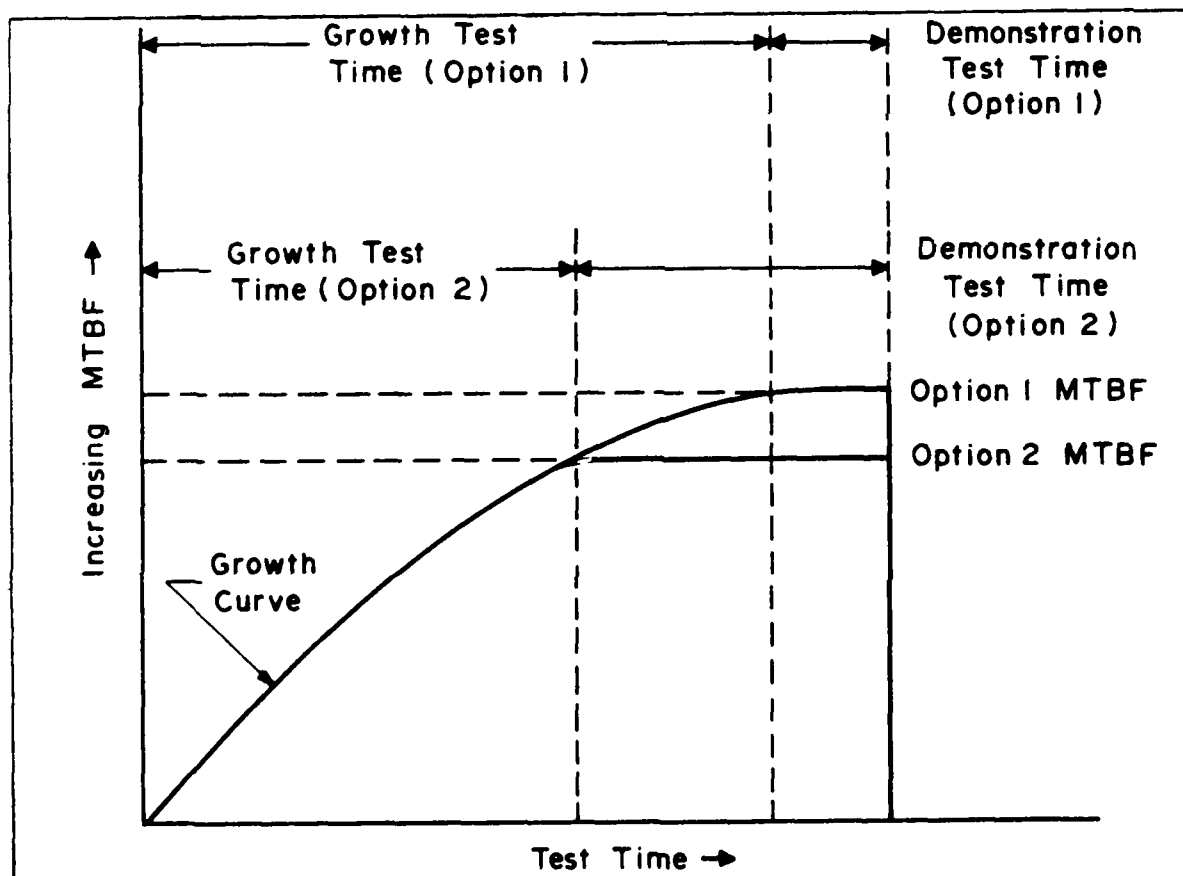
FIGURE 8.6-1: RELIABILITY TESTING OPTIONS

REFERENCES

1. NAVAIR 01-1A-32, Reliability Engineering Handbook, Naval Air Systems Command, Washington DC, July 1977.

2. Arsenhault, J.E. and J.A. Roberts, Reliability and Maintainability of Electronic Systems, Computer Science Press, 9125 Fall River Lane, Potomac, MD 20354, 1980.

3. Doyle, E., and W. Morris, Microelectronics Failure Analysis Techniques, A Procedural Guide, available from the Reliability Analysis Center, RADC/RBRAC, Griffiss AFB, NY 13441.

4. O'Connor, P., Practical Reliability Engineering, Heyden & Son Ltd., London, Philadelphia, 1981.

5. AMCP-706-198, Engineering Design Handbook: Reliability Measurement, January 1976, AD#A027371.

6. Horn, R., and G. Shoup "Determination and Use of Failure Patterns," Proceedings of the Eighth National Symposium on Reliability and Quality Control, January 1962.

7. VanAlvin, W.H., ed., Reliability Engineering, Prentice-Hall Inc., Englewood Cliffs, NJ, 1964.

8. Lloyd, R.K. and M. Lipow, Reliability: Management, Methods, and Mathematics, TRW, Redondo Beach, CA, second edition, 1977.

9. Mann, N., R. Schafer and N. Singpurwalla, Methods of Statistical Analysis of Reliability and Life Data, John Wiley and Sons, New York, NY, 1974.

10. AMCP 702-3, Quality Assurance Reliability Handbook, U.S. Army Materiel Command, Washington DC 20315, AD#702936, October, 1968.

11. Yurkowsky, W., Nonelectronic Reliability Notebook, RADC-TR-69-458, March 1970.

12. NAVAIR-01-1A-32, Reliability Engineering Handbook, Naval Air Systems Command, Washington DC, July 1977.

13. "Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution (Mean Life Criterion)," Quality Control and Reliability Technical Report, TR3, Office of the Assistant Secretary of Defense (Installations and Logistics), September 30, 1961.

14. "Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution (Hazard Rate Criterion)," Quality Control and Reliability Technical Report TR4, Office of the Assistant Secretary of Defense (Installations and Logistics), February 28, 1962.

15. "Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution (Reliable Life Criterion)," Quality Control and Reliability Technical Report, TR6, Office of the Assistant Secretary of Defense (Installations and Logistics), February 15, 1963.

16. Duane, J.T., "Learning Curve Approach to Reliability Monitoring," IEEE Transactions on Aerospace, Volume 2, April 1964, pp 363-366.

17. Crow, L.H., "On Tracking Reliability Growth," Proceedings 1975 Annual Reliability & Maintainability Symposium, pp 438-443.

18. Discrete Address Beacon System (DABS) Software System Reliability Modeling and Prediction, Report No. FAA-CT-81-60, prepared for U.S. Department of Transportation, FAA Technical Center, Atlantic City, New Jersey 08405, June 1981.

19. Reliability Growth Study, RADC-TR-75-253, ADA023926, October 1975.

20. Bezat, A., et al, "Growth Modeling Improves Reliability Prdictions," Proc 1975 Reliability and Maintainability Symp, pp 317-322 (IEEE Cat No 75 CHO 918-3-ROC).

21. Bezat, A.G. and Montague, L.L., "The Effect of Endless Burn-In on Reliability Growth Projections," Proc 1979 Annual Reliability & Maintainability Symp, pp 392-297, (IEEE Cat No 79CH1429-OR).

22. Selby, J.D. and Miller, S.G., "Reliability Planning and Management (RPM)," Paper No SI-471, ASQC/SRE Seminar, Niagara Falls, NY, Sept 26, 1970, pp 1-7.

23. Green, J.E., "Reliability Growth Modeling for Avionics," Proc, AGARD Lecture Series No 81, "Avionics Design for Reliability," April 1976.

24. Codier, E.O., "Reliability Growth in Real Life," Proc 1968 Annual Symp on Reliability, January 1968, pp 458-469.

25. Crow, L.H., "Reliability Analysis for Complex, Repairable Systems," Reliability and Biometry/Statistical Analysis of Life Length, SIAM, 1974, pp 379-410.

26. Haase, R.W., Kapur, K.C., and Lamberson, L.R., "Applications of Reliability Growth Model During Light Truck Design and Development," SAE Paper No 780240, Feb/Mar 1978.

27. Clarke, J.M. and Cougah, W.P., "RPM-A Recent Real Life Case History," Proc 1978 Reliability and Maintainability Symp, pp 279-285.

28. Meade, C., Cox, A., and Lavery, J., "Reliability Growth Management in USAMC," Proc 1978 Reliability and Maintainability Symp, pp 432-437.

29. Simpkins, D.J., "A Reliability Growth Management Approach," Proc, Annual Reliability and Maintainability Symp, 1979, pp 356-360.

30. Lloyd, D.K. and Lipow, M. 1962. Reliability: Management, Methods and Mathematics. Englewood Cliffs, NJ: Prentiss-Hall.

31. Wolman, W. 1963. Problems in System Reliability Analysis. Statistical Theory of Reliability, ed. M. Zelen, pp. 149-160. Madison, WS: The University of Wisconsin Press.

32. Barlow, R. and Scheuer, E. 1966. Reliability Growth During A Development Testing Program. Technometrics. 8:53-60.

33. Virene, E.P. 1968. Reliability Growth and Its Upper Limit. Proceedings Annual Symposium on Reliability, pp. 265-270. New York, NY: IEEE.

34. Barlow, R., Proschan. F., Scheuer, E. 1966. Maximum Likelihood Estimation and Conservative Confidence Interval Procedures in Reliability Growth and Debugging Problems. Report RM-4749-NASA. RAND Corporation. Santa Monica, CA.

35. Singpurwalla, N. 1978. Estimating Reliability Growth (or Deterioration) Using Time Series Analysis: 25: 1-14.

36. Box, G.E.P. and Jenkins, G.M. 1970. Time Series Analysis: Forecasting and Control. San Francisco, CA: Holden-Day.

37. Cox, D.R. and Lewis, P.A.W. 1966. The Statistical Analysis of Series of Events. New York, NY: John Wiley and Sons.

38. Lewis, P. and Shedler, G. 1976. Statistical Analysis of Non-Stationary Series of Events. IBM Journal of Research and Development. 20: 465-482.

39. Rosner, N. 1961. System Analysis - Nonlinear Estimation Techniques. Proceedings National Symposium on Reliability and Quality Control, pp. 203-207. New York, NY: IRE.

40. Perkowski, N. and Hartvigsen, D.E. 1962. Derivations and Discussions of the Mathematical Properties of Various Candidate Growth Functions. Report CRA62-8. Aerojet-General Corporation, Azusa, CA. AD-349304.

41. Aroef, M. 1957. Study of Learning Curves of Industrial Manual Operations. Unpublished Master's Thesis. Cornell University. Ithaca, NY.

42. Englehardt, M. and Bain, L.J. 1978. Prediction Intervals for the Weibull Process. Technometrics. 20: 167-169.

43. Bassin, W.M. 1969. <u>Increasing Hazard Functions and Overhaul Policy</u>. Proceedings Annual Symposium on Reliability, pp. 173-178. New York, NY: IEEE.

44. Crow, L.H. 1977. <u>Confidence Interval Procedures for Reliability Growth Analysis</u>. US Army Materiel Systems Analysis Activity, Technical Report 197. Aberdeen Proving Ground, MD: AD-A044788.

45. Finkelstein, J.M. 1976. <u>Confidence Bounds on the Parameters of the Weibull Process</u>. Technometrics. 18: 115-117.

46. Lee, L. and Lee, S.K. 1978. <u>Some Results on Inference for the Weibull Process</u>. Technometrics. 20: 41-45.

47. Englehardt, M. and L.J. Bain, "Prediction Intervals for the Weibull Process," <u>Technometrics</u> 20: 1978, pp. 167-169.

48. Finklestein, J.M., "Confidence Bounds on the Parameters of the Weibull Process," <u>Technometrics</u> 18: 1976, pp. 115-117.

APPENDIX A

INSTRUCTIONS ON THE USE OF RELIABILITY DEMONSTRATION TEST PLANS

Instructions and examples are given for the following test plans:

(1) Attributes Demonstration Tests

    (a) Plans for Small Lots
    (b) Plans for Large Lots
    (c) Plans for Large Lots (Poisson Approximation Method)
    (d) Attributes Sampling Using MIL-STD-105
    (e) Sequential Binomial Test Plans

(2) Variables Demonstration Tests

    (a) Time Truncated Test Plans

        (1) Exponential Distribution
        (2) Normal Distribution
        (3) Weibull Distribution

    (b) Failure Truncated Tests

        (1) Exponential Distribution
        (2) Normal Distribution (σ Known)
        (3) Normal Distribution (σ Unknown)
        (4) Weibull Distribution

    (c) Sequential Tests

        (1) Exponential Distribution
        (2) Normal Distribution

    (d) Interference Demonstration Tests
    (e) Bayes Sequential Tests

ATTRIBUTES DEMONSTRATION TESTS

ATTRIBUTES PLANS FOR SMALL LOTS

1.   When to use

When testing items from a small lot where the accept/reject decision is based on attributes, the hypergeometric distribution is applicable. Attributes tests should be used when the accept/reject criterion is a go-no go situation, when the probability distribution of times to failure is unknown, or when variables tests are found to be too expensive. The example demonstrating the method is based on a small lot and small sample size. This situation frequently characterizes the demonstration test problem associated with large systems. The sample size limits the discriminatory power of the demonstration test plan but frequently cost and time constraints force us into larger than desired risks.

2. Conditions for Use

The definition of successfully passing the test may be that an item survives the test. The parameter to be evaluated then is the fraction of the items in the lot that survive. The estimation of the parameter would be based on a fixed sample size and testing without repair. The selection of the criteria for success (survive, detonate on impact, time) can be derived from a requirement or, if the items being tested are known to follow a particular probability distribution, the specification of the criteria for success can be based on defining acceptable and unacceptable portions of the range of failures. If the lot size is large, say 30 or more, then the Poisson approximation may be used to make the calculation simpler.

3. Method	Example
a. Define criterion for success/failure.	a. A missile that seeks and destroys the target. Missiles that fail to destroy the target are considered failures.
b. Define acceptable lot quality level $(1 - p_0)$.	b. Lots in which $(1 - p_0)$ = 90% of the missiles will destroy the target are to be accepted by this demonstration test plan with high probability.
c. Specify producer's risk (α), i.e., the probability that acceptable lots will be rejected.	c. Let α = .2. This decision is an engineering one based on the consequences of allowing defective lots to be accepted and based on the time and dollar constraints associated with inspecting the lot.
d. Define unacceptable quality level $(1 - p_1)$.	d. Lots in which only $(1 - p_1)$ = 20% of the missiles destroy the target will be accepted by the demonstrations test plan with low probability.
e. Specify the consumer's risk (β), i.e., the probability that unacceptable quality lots will pass the demonstration test).	e. Let β = .022 (taken for convenience in calculations).
f. Now that α, β, $1-p_0$, and $1-p_1$ have been specified the following steps describe the calculations required to determine the sample size and accept/reject criteria which will satisfy the stated risks.	f. Given: lot size N=10 $1-p_0$ = .9 $1-p_1$ = .2 α = .2 β = .022

g. The process consists of a trial and error solution of the hypergeometric equation using N, $1 - p_o$, $1 - p_1$ and various sample sizes until the conditions of α and β are met. The equation used is

$$Pr(x) = \frac{\binom{r}{x} \binom{N-r}{n-x}}{\binom{N}{n}}$$

$x = 0, 1, 2 \ldots \min(n,r)$

where

x = number of successes in sample
r = number of successes in lot
N = lot size
n = sample size

$$\binom{r}{x} = \frac{r!}{x!(r-x)!}$$

g. The calculations are as follows: If $N = 10$ and it is assumed that the samples are taken from a lot with $1 - p_o = .9$ then that lot contains 9 good items and 1 defective item. As the first step in the trial and error procedure assume a sample size of two. The possible outcomes are either 0, 1 or 2 good items. The probability of each outcome using the hypergeometric formula is

$$Pr(2) = \frac{\binom{9}{2}\binom{1}{0}}{\binom{10}{2}} = .8$$

$Pr(1) = .2$
$Pr(0) = 0$

The same calculations for $1 - p_1 = .2$ result in

$Pr(2) = .022$
$Pr(1) = .356$
$Pr(0) = .622$

h. Find the number of successes which satisfies α and β in the calculations involving $1 - p_o$ and $1 - p_1$.

h. From these 2 sets of results it can be seen that if a sample size of 2 is specified, then α and β will be satisfied if the decision rule is made that if 2 successes are observed in the sample the lot is accepted and for all other outcomes the lot is rejected.

If $1 - p_o = .9$, then $Pr(2) = .8$, therefore $1-.8 = .2 = \alpha$.
If $1 - p_1 = .2$, then $Pr(2) = .022 = \beta$.
NOTE: A different sample size can be traded off against different α, β, $1 - p_o$ and $1 - p_1$.

i. The demonstration test is then specified.

i. The test procedure is as follows:

1. Test a random sample of 2 missiles from a lot of 10 missiles.

2. If both missiles destroy the target, accept the lot.

3. If 0 or 1 successes are observed reject the lot.

4. For Further Information

There are "Tables of the Hypergeometric Distribution" by G.J. Lieberman and D.B. Owen, Stanford University Press, Stanford, California, 1961 to perform the mathematical calculations of Step g. Also if N becomes large (say 30) then the binomial or the Poisson distribution can be used as an approximation for the hypergeometric distribution.

ATTRIBUTES PLANS FOR LARGE LOTS

1. When to Use

When testing parts from a large lot where the accept/reject decision is based on attributes, the binomial distribution is applicable. Strictly speaking, all reliability testing should follow the hypergeometric distribution as long as individual items are placed on test and tested to failure without repair. However, when the lot size is large, the binomial distribution is a good approximation for the hypergeometric and, therefore, the example presented in this section covers the use of the binomial. Attributes tests should be used when the accept/reject criterion is go-no go, when the distribution of failure times is unknown, or when variables tests are found to be too expensive.

2. Conditions for Use

The definition of successfully passing the test may be that an item performs as specified. The parameter to be evaluated then is the fraction of the items in the lot that perform as specified. The estimation of the parameter would be based on a fixed sample size and testing without repair. The selection of the criteria for success can be derived from a requirement, or if the items being tested are known to follow a particular probability distribution, the specification of the criteria for success can be based on defining acceptable and unacceptable portions of the range of failure times. If the lot size is large, say 30 or more, then the Poisson approximation may be used to make the calculation simpler.

∷. Method	Example
a. Define criterion for success/failure.	a. An artillery fuze that detonates on impact is considered a success. Fuzes that fail to detonate on impact are considered failures.
b. Define acceptable lot quality level $(1 - p_0)$.	b. Lots in which $1 - p_0 = .9$ (i.e., 90% of the fuzes in the lot will detonate on impact) are to be accepted by this demonstration test plan with high probability.
c. Specify producer's risk (α), (i.e., the probability that acceptable lots will be rejected).	c. Let $\alpha = .01$.
d. Define unacceptable lot quality level $(1 - p_1)$.	d. Lots with only a true fraction of acceptable parts $1 - p_1 = .5$ are to be accepted by this demonstration test plan with low probability.
e. Specify consumer's risk (β), (i.e., the probability that lots of unacceptable quality level will be accepted.)	e. Let $\beta = .12$ (selected for ease of calculation).
f. Now that α, β, $1 - p_0$, and $1 - p_1$ have been specified, the following steps describe the calculations required to determine the sample size and accept/reject criteria which will satisfy the stated risks.	f. Given: lot size N = large, say, 30 $1 - p_0 = .9$ $1 - p_1 = .5$ $\alpha = .01$ $\beta = .12$
g. The process now consists of a trial and error solution of the binomial equation using $1 - p_0$, $1 - p_1$ and various sample sizes until at a given decision point, the conditions of α and β are satisfied. The binomial equation is:	g. Assume a random sample of size n = 10 is taken from a lot whose true fraction of good parts is .9. Solve the binomial equation for the total number of consecutive outcomes whose summed probabilities

$$Pr(x) = \binom{n}{x}(1-p)^x(p)^{n-x}$$

where

n = sample
x = observed successes in sample
p = lot fraction defective

equal α starting at 0 successes. The calculations for this decision point are:

$$Pr(10) = \binom{10}{10}(.9)^{10}(.1)^0 = .3486$$

Pr(9) = .387
Pr(8) = .1935
Pr(7) = .0574
Pr(7 or more) = .9865

Then

Pr(6 or less) = 1-Pr (7 or more)
= 1.0 - .9865
$\approx$ .01 (which satisfies the risk).

Perform the same type of calculations assuming the true fraction defective is .5. In this instance, sum the probabilities starting at 10 successes until succeeding consecutive probabilities sum of the value of β. This yields the following results:

$$Pr(10) = \binom{10}{10}(.5)^{10}(.5)^0 = .001$$

Pr(9) = .01
Pr(8) = .045
Pr(7) = .117
Pr(7 or more) $\approx$ .12 (which satisfies the β risk).

h. The demonstration test is then specified.

h. The test procedure is as follows:

1. Test a random sample of 10 fuzes.
2. If 7 or more fuzes **detonate** on impact accept the lot.
3. If 6 or less successes are observed, reject the lot.

4. For Further Information

There are several published tables for use in determining binomial probabilities in the event that the sample size makes calculations too lengthy. One of these is "Tables of the Binomial Probability Distribution", National Bureau of Standards, Applied Mathematics Series 6, Washington, D.C., 1950. It gives individual terms and the distribution function for $p = .01$ to $p = .50$ in graduations of .01 and $n = 2$ to $n = 49$ in graduations of 1. If N is large say ≥ 30, the Poisson distribution can be used as an approximation for the binomial distribution.

ATTRIBUTES DEMONSTRATION TEST PLANS FOR LARGE LOTS (THE POISSON APPROXIMATION METHOD)

1. When to Use

In attributes demonstration test plans if the lot size gets much above 20 the calculations required to generate a demonstration test plan become very time consuming. The Poisson distribution can be used as an approximation of both the hypergeometric and the binomial distributions if the lot size is large and if the fraction defective in the lot is small. This method can therefore be used in lieu of the previous two methods in many cases.

2. Conditions for Use

If the lot size is large and the fraction defective is small, this method is applicable. Its use is initiated by specifying a desired producer's risk, consumer's risk, acceptable lot fraction defective and unacceptable lot fraction defective. As before, it is also necessary to specify the characteristics that constitute a defective part since this is an attributes type test.

3. Method	Example
a. Define criterion for success/failure.	a. An artillery fuze that detonates on impact is considered a success. Fuzes that fail to detonate on impact are considered failures.
b. Define acceptable lot quality level $(1 - p_0)$.	b. Lots in which $1 - p_0 = .9$ (90% of the fuzes in the lot detonate on impact) are to be accepted by this demonstration test plan with low probability.
c. Specify the producer's risk $(_{\iota})$, (i.e., the probability that acceptable lots will be rejected).	c. Select $\alpha = .05$.

d. Define unacceptable lot quality level $(1 - p_1)$.

d. Lots with only a true fraction of acceptable parts $1 - p_1 = .75$ are to be accepted by this demonstration test plan with low probability.

e. Specify the consumer's risk (β), (i.e., the probability that lots of unacceptable quality level will be accepted by this plan).

e. Select $\beta = .02$.

f. Now that α, β, $1 - p_0$, $1 - p_1$ have been specified, the Table of the Summation of Terms of Poisson's Exponential Binomial Limit* are used to determine the accept/reject criteria.

f. Given: lot size N = 1000

$1 - p_0 = .9$
$1 - p_1 = .75$
$\alpha = .05$
$\beta = .02$

g. The process now consists of a trial and error solution using Poisson Tables*, $1 - p_0$, $1 - p_1$ and various assumed sample sizes until the conditions of α and β are satisfied.

g. Assume sample size of 100. Now, calculate the expected number of failures for $1 - p_0$ and $1 - p_1$ as follows:

$n(1 - p_0) = 100(.9) = 90$
$n(1 - p_1) = 100(.75) = 75$

The Poisson Tables are constructed for small values of p, so, in this case, to make calculations easier, it is necessary to work with the opposite tail of the distribution. Therefore, the numbers to enter the table with are:

$np_0 = 100(.1) = 10$
$np_1 = 100(.25) = 25$

The procedure now is to enter the column labeled c' or np' with the above numbers. Beginning with $1 - p_0 = .9$ and $np_0 = 10$, search across the np' = 10 row beginning at c or less = 1.0.

*See any good statistical text

Continue to smaller values of c until the probability of c or less = $1 - \alpha$.

In this example at c = 15 or less, the probability of 15 or less is .951 which is approximately $1 - \alpha$.

The same procedure is followed in the table at $1 - p_1$ = .75 and np_1 = 25.

In the np' = 25 row at c = 15, the cumulative probability is .022 which is approximately equal to β.

The decision criteria is now specified as c = 15 or less failures.

h. The demonstration is then fully specified.

h. The demonstration test procedure is as follows:

1. Take a random sample of 100 fuzes from each lot of size N = 1000 and test each part.
2. If 85 or more fuzes (i.e., 15 or less defectives) detonate on impact, accept the lot.
3. If less than 85 successes are observed, reject the lot.

4. **For Further Information**

For additional examples using this method, refer to E. B. Grant "Statistical Quality Control", McGraw Hill, 1964.

ATTRIBUTES SAMPLING USING MIL-STD-105

1. **When to Use**

When the accept/reject criteria for a part is based on attributes decisions MIL-STD-105 is a useful tool. These sampling plans are keyed to fixed AQL's and are expressed in lot size, sample size, AQL and acceptance number. Plans are available for single sampling, double sampling and multiple sampling. The decision as to which type to use is based on a trade-off between the average amount of inspection, the administration cost and the information yielded regarding lot quality.

For example, single sampling usually results in the greatest amount of inspection, but this can be offset by the fact that it requires less training of personnel, and record keeping is simpler, and it gives a greater amount of information regarding the lot being sampled.

2. Conditions for Use

The user of a MIL-STD-105 sampling plan must have the following information:

    a.   Lot Size
    b.   Acceptable Quality Level (AQL)
    c.   Sample Size
    d.   Acceptance Number
    e.   Criteria for Acceptance or Rejection

The specification of the AQL is an engineering decision based on the fraction defective that a user of parts considers acceptable. Lots with this percent defective will be accepted a high fraction of the time. Operating characteristic curves are supplied with each sampling plan and these can be used to evaluate the protection afforded by the plan for various quality levels.

MIL-STD-105 also contains plans for normal, tightened and reduced inspection plans which can be invoked if the fraction defective of lots seems to be varying or trending.

3. Method   Example

    a.   Determine lot size and spec-   a.   Given a lot containing 100 parts and an AQL is specified at 6.5% with single sampling specified.

    b.   Enter the table with lot size   b.   From Table I Sample Size Code Letters on Page 9, MIL-STD-105, find the sample size code letter for a lot of size 100. For this example and for normal sampling, the specified code number is F.

    c.   Enter the single sampling plan   c.   Enter Table II-A Single Sampling Plans for Normal Inspection page 10 with code letter F. Under the column titled Sample Size, find the number 20 in the same row as the letter F. This is the number of parts to be randomly selected and inspected.

d. Enter the same table in the proper column for the specified AQL.

d. Find the column in Table II-A page 10 corresponding to an AQL of 6.5%.

e. Proceed horizontally along the Sample Size Code Number row until it intersects with the AQL column to obtain the acceptance number.

e. At the intersection of row R and column 6.5%, the acceptance number is 3 and the rejection number is 4.

f. The Single Sampling Plan from MIL-STD-105 is to select a random sample of size n from a lot of size N, inspect it and accept the lot if the number of defectives in the lot is equal to or less than the the Acceptance Number. If the observed number of defects is equal to or greater than the rejection number, the lot is rejected.

f. For the single sampling plan N = 100, AQL = 6.5%, select a random sample of size n = 20 and inspect it for attributes criteria. If 3 or less defectives are found in the sample accept the lot. If 4 or more defectives are found in the sample reject the lot.

4. For Further Information

In addition to the example discussed above, MIL-STD-105 contains other plans for any lot size and for selected AQL's from .01 to 1000%. Operating characteristic curves are also included.

SEQUENTIAL BINOMIAL TEST PLANS

1. When to Use

When the accept/reject criterion for the parts on test is based on attributes, and when the exact test time available and sample size to be used are not known or specified then this type of test plan is use;ul. The test procedure consists of testing parts one at a time and classifying the tested parts as good or defective. After each part is tested, calculations are made based on the test data generated to that point and the decision is made either that the test has been passed, failed, or that another observation should be made. A sequential test will result in a shorter average number of parts tested than either failure truncated or time truncated tests when the lot tested has a fraction defective at or close to p_o or p_1.

2. Conditions for Use

a. The parts subjected to test will be classified as either good or defective. In other words, testing will be by attributes.

b. The acceptable fraction defective in the lot p_o, the unacceptable fraction defective p_1, the producer's risk α, and consumer's risk β must be specified.

A-11

c. The test procedure will be to test one part at a time. After the part fails or its test time is sufficient to classify it as a success, the decision to accept, reject or continue testing the lot will be made.

3. **Method**   **Example**

a. Specify p_0, p_1, α, β.

a. Given a lot of parts to be tested by attributes. Lots having only $p_0 = .04$ fraction defective parts are to be accepted by the demonstration test plan 95% of the time (i.e., $\alpha = .05$). Lots having $p_1 = .10$ fraction defective are to be accepted 10% of the time (i.e., $\beta = .10$).

b. Calculate decision points from the following formula

$$\frac{1-\beta}{\alpha} \text{ and } \frac{\beta}{1-\alpha}$$

b. The decision points are:

$$\frac{1-\beta}{\alpha} = \frac{1-.10}{.05} = 18$$

$$\frac{\beta}{1-\alpha} = \frac{.10}{1-.05} = .105$$

c. As each part is tested classify it as a part failure or a success and evaluate the following expression:

$$\left(\frac{p_1}{p_0}\right)^f \left(\frac{1-p_1}{1-p_0}\right)^s$$

where
f = total number of failures
s = total number of successes

c. In this example, if the value of the formula

$$\left(\frac{.10}{.04}\right)^f \left(\frac{.90}{.96}\right)^s$$

1) exceeds 18, reject the lot
2) < .105 accept the lot
3) is between .105 and 18, the test should be continued.

d. A graphical solution for critical values of f and s is possible by solving the following equations.

1) $\ln\left(\frac{1-\beta}{\alpha}\right) = (f)\ln\left(\frac{p_1}{p_0}\right) +$

$(s)\ln\left(\frac{1-p_1}{1-p_0}\right)$

d. The equations for the graphical solution in this example are:

1) $\ln 18 = f \ln 2.5 + s \ln .94$
2) $\ln .105 = f \ln 2.5 + s \ln .94$

Substituting value of f and s in the equations yields the following points

A-12

2) $\ln \frac{\beta}{1-\alpha} = (f)\ln \frac{p_1}{p_0} +$

$(s)\ln\left(\frac{1-p_1}{1-p_0}\right)$

1)
f	s
0	-46.6
3.16	0
3.84	10
10	101

2)
f	s
-2.44	0
-1.78	10
0	36.4
10	184

Figure A-1 shows the graphical solution for this test plan. As each good part is observed a horizontal line is drawn, and each defective part is recorded by a vertical line. When the line crosses either of the decision lines, the appropriate action is taken.

e. The Operating Characteristic Curve calculation is as follows:

Four points can be generated by observation.

p	Probability of Acceptance
0	1
p_0	$1-\alpha$
p_1	β
1	0

One additional point can be calculated with the following formula

$$p = \frac{\ln\left(\frac{1-p_1}{1-p_0}\right)}{\ln\left(\frac{1-p_1}{1-p_0}\right) - \ln\left(\frac{p_1}{p_0}\right)}$$

$$Pr(Acc) = \frac{\ln \frac{1-\beta}{\alpha}}{\ln \frac{1-\beta}{\alpha} - \ln \frac{\beta}{1-\alpha}}$$

where $P_r(Acc)$ = probability of acceptance

e. The OC curve for this test plan yields the following points:

p	Probability of Acceptance
0	1.0
.04	.95
.10	.10
1.00	0

The 5th point of the OC curve in the example

$$p = \frac{\ln 0.94}{\ln 0.94 - \ln 2.5} = .063$$

$$Pr(Acc) = \frac{\ln 18}{\ln 18 - \ln 0.105} = .562$$
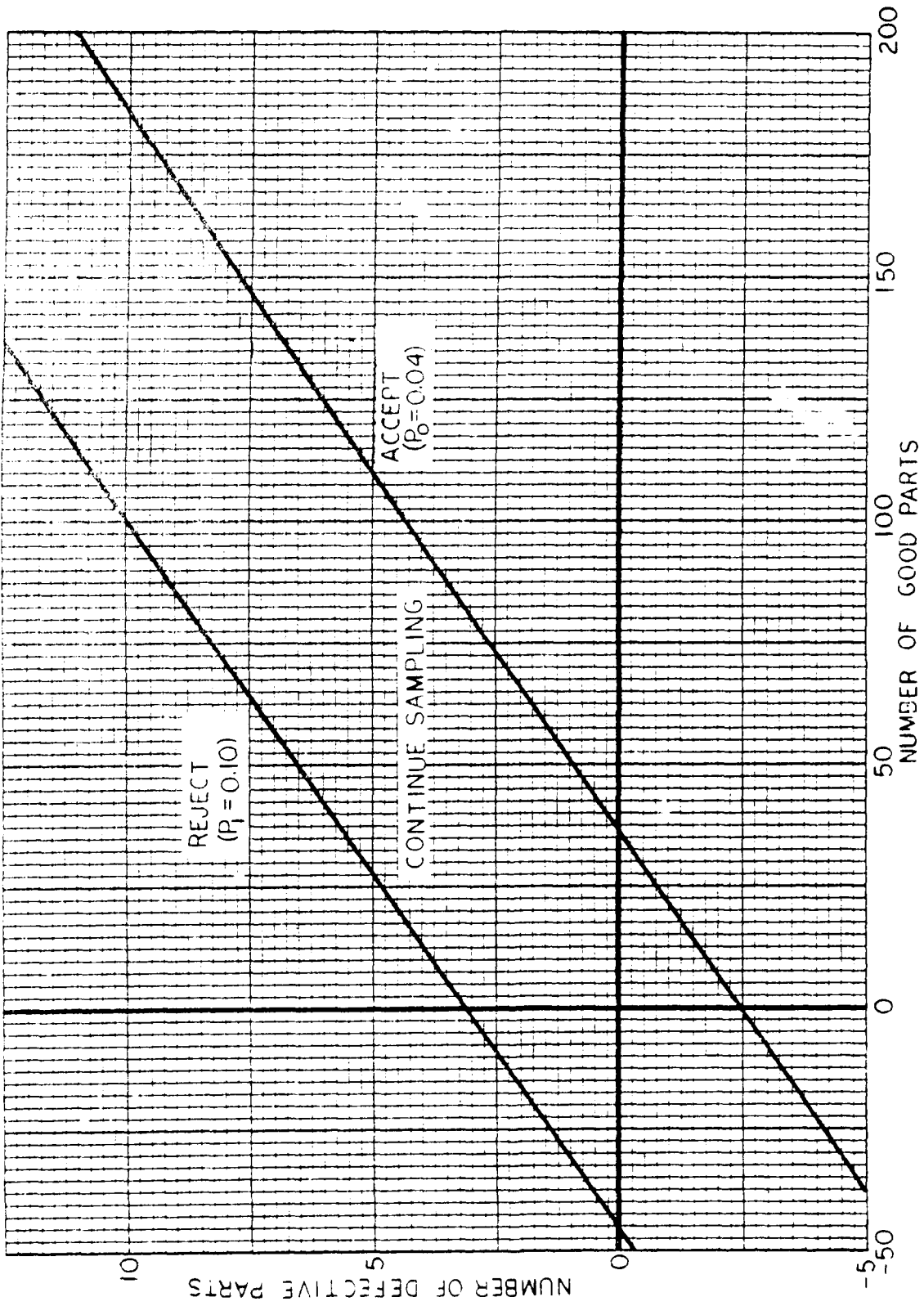
FIGURE A-1: GRAPHICAL SOLUTION OF SEQUENTIAL BINOMIAL TEST

4. <u>For Further Information</u>

A more complete discussion of this demonstration test method is presented in "Introduction to Statistical Analysis" by W.J. Dixon and F.J. Massey, McGraw Hill, New York, 1951. The theory of sequential testing is presented in "Sequential Analysis" by A. Wald, John Wiley & Sons, 1947.

<u>VARIABLES DEMONSTRATION TESTS</u>

<u>TIME TRUNCATED DEMONSTRATION TEST PLANS</u>

<u>EXPONENTIAL DISTRIBUTION (H-108)</u>

1. <u>When to Use</u>

When a demonstration test program is constrained by time or schedule and testing is by variables (in this case the variable is mean life) and the distribution of failure times is known, a test plan of this type can be specified.

2. <u>Conditions for Use</u>

    a. The failure times of the items under test must be exponentially distributed.

    b. The acceptable mean life θ_0, unacceptable mean life θ_1, producer's risk, (α), and consumer's risk, (β), and test time (T) must be specified.

    c. The decision of testing with or without replacement must be made.

3. <u>Method</u>　　　　　　　　　　　　　　　　<u>Example</u>

    a. Specify θ_0, θ_1, α, β.

          a. Given an item type whose failure times are distributed exponentially.

Specify　θ_0 = 1000 hours
θ_1 = 500 hours
α = .10
β = .10

    b. Specify a fixed test time.

          b. The program plan allows time for a 200 hour test.

    c. Specify whether testing will be with or without replacement.

          c. Testing will be carried on without replacement.

    d. Calculate T/θ_0.

          d. $T/\theta_0 = \dfrac{200}{1000} = \dfrac{1}{5}$

e. Calculate θ_1/θ_0.

e. $\theta_1/\theta_0 = \dfrac{500}{1000} = \dfrac{1}{2}$

f. From the appropriate table in H-108 "Sampling Procedures and Tables for Life and Reliability Testing (Based on Exponential Distribution)" select the sample size and number of failures which will cause rejection of the lot from which the parts were randomly selected.

f. Enter Table 2C-3 on page 2.52 of H-108 with α, β, T/θ_0 and θ_1/θ_0 and select the number of items to be placed on test (in this case 59) and the number of failures (in this example 15) which will cause failure of the demonstration test.

g. Summarize test outcome.

g. The demonstration test plan specified here has the following characteristics:

1. Lots having an MTBF of 1000 hours will be accepted 90% of the time.

2. Lots having a MTBF of 500 hours will be accepted 10% of the time.

3. Test 59 items for 200 hours each. Do not replace or repair parts as they fail.

4. If less than 15 failures occur, terminate the test at 200 hours and accept the lot.

5. If 15 or more failures occur reject the lot at the time of the fifteenth failure.

4. For Further Information

The demonstration test method and example discussed in this section are from Quality Control and Reliability Handbook H-108. In addition to the example presented here, H-108 has tabled sample sizes and reject numbers for testing without replacement with α = .01, .05, .10 and .25, and β = .01, .05, .10 and .25 and for all combinations thereof. The tables are also constructed for θ_1/θ_0 values of 2/3, 1/2, 1/3, 1/5 and 1/10 and T/θ_0 values of 1/3, 1/5, 1/10 and 1/20. A like set of tables is presented also for demonstration test plans for the same values of α, β, θ_1/θ_0 and T/θ_0

for testing with replacement. Tables are also provided for time truncated tests in which only $\cdot$, $\cdot_0$ and T (test time) are specified ($\cdot$ = .01, .05, .10, .25 and .50) for plans involving testing with and without replacement. Fixed time test plans are also presented in MIL-STD-781 and MIL-HDBK-781.

NORMAL DISTRIBUTION

1. When to Use

When the underlying distribution of failure times is normal and when a fixed calendar time is available for a test this type of test plan can be specified. This test plan essentially becomes a binomial type problem since the survivors at the end of the time truncation are treated as successes. The failures regardless of their time of occurrence are utilized in specifying the accept/reject criteria.

2. Conditions for Use

a) The distribution of failure times must be normal.

b) The acceptable mean life (θ_0), unacceptable mean life (θ_1), the known or desired standard deviation of the distribution of acceptable mean lives (σ_0), the known or desired standard deviation of the distribution of unacceptable mean life (σ_1), the sample size (n), the test truncation time (T), the producer's risk (α), and the consumer's risk (β), must be specified.

c) The test should be run without replacement of failed parts.

3. Method

a. Specify θ_0, θ_1, α, β, σ_0, σ_1, n, T. If the requirements are stated in terms of reliability at some time t, it is necessary to solve the following equation.

$$z_0 = \frac{t - \theta_0}{\sigma}$$

Where z_0 is the standard normal deviate for the desired probability of R_0, t is the desired mission time, σ is the known standard deviation, and θ_0 is the acceptable mean life. The same procedure is followed to solve for θ_1 and R_1 is specified.

Example

a. Given an item type whose failure times are normally distributed with a known standard deviation = 50. A reliability of .95 is desired that the equipment will last 100 hours. A product with a reliability of .85 is unacceptable.

The standard normal deviate for R_0 = .95 is z_0 = -1.645 and for R_1 = .85 is z_1 = -1.04 from a table of areas under the normal curve (Table A-1, Appendix to Section 5).

$$z_0 = \frac{t - \theta_0}{\sigma}$$

$$-1.645 = \frac{100 - \theta_0}{50}$$

$$\theta_0 = 182 \text{ hours}$$

$$z_1 = \frac{t - \theta_1}{\sigma}$$

$$-1.04 = \frac{100 - \theta_1}{50}$$

$$\theta_1 = 152 \text{ hours}$$

Therefore, it is possible to specify R_0 and R_1 in terms of θ_0 and θ_1.

θ_0 = 182 hours
σ_0 = 50 hours
θ_1 = 152 hours
σ_1 = 50 hours

The schedule and cost of testing allows 182 hours of test time with 30 samples to be placed on test. α is specified as .10 and β = .05.

b. Calculate the expected number of failures during the fixed time test if n samples are tested T hours, for samples from lots with mean lives of θ_0, σ_0 and θ_1, σ_1.

b. The θ_0 = 182, σ_0 = 50, n = 30 then the expected number of failures in a test of 182 hours is 15. If θ_1 = 152, σ_1 = 50, n = 30 the expected number failures in a test of 182 hours is 21.6 using a table of areas under the normal curve.

c. The problem of specifying accept/reject criterion at the end of a fixed test time, T, is now similar to the

c. Items that exceed the fixed test time T = 182 hours are counted as successes. The remaining problem to be solved

A-18

example in <u>Attributes Plans For Large Lots</u>. In other words, it is a binomial distribution problem since items that last T hours are listed as having successfully passed the test, while items that do not last T hours are classed as failures regardless of their exact failure times.

specifying the accept/reject criterion (i.e., r or more failures out of a sample of 30 items on test for 182 hours results in failure of the demonstration test - regardless of the individual part failure times). Additionally the test may be terminated at less than T = 182 hours if r failures are observed, in which case the demonstration test is failed.

d.   The accept/reject criteria can be calculated using the binomial distribution or if the expected number of failures ≥ 5 the normal distribution can be used as an approximation to the binomial.

d.   From Step (b) the expected number of failures of θ_0 = 182 is 15 and the expected number of failures when θ_1 = 152 is 21.6. Therefore the normal distribution as an approximation of the binomial is used.

e.   Calculate the decision point based on θ_0 and α using the normal distribution.

e.   The decision point for θ_0 = 182, σ_0 = 50, α = .10 is calculated as follows:

$$z = 1.28 \text{ for } \alpha = .10$$

$$z = \frac{x - np}{\sqrt{np(1-p)}}$$

$$1.28 = \frac{x - 15}{\sqrt{15\,(.5)}}$$

$$x = 18.5 \text{ failures}$$

The demonstration test plan procedure is now stated as follows:

Take a random sample of 30 items, test them for 182 hours. If 18.5 or less failures are observed the test is passed.

f. Adjust the decision point to a whole number, thus, adjusting α slightly.

f. Either 18 or 19 failures can be set as the rejection number without affecting α too severely. For this example, assume that 19 failures will be allowed and still accepted. α now becomes

$$z = \frac{19 - 15}{15\,(.5)} = 1.46$$

From a Table of Areas under the Normal Curve the probability of exceeding z = 1.46 is .09. Therefore, α = .09.

g. Calculate β based on the accept/reject criteria established in Step f. NOTE: The OC curve for this demonstration test plan can be constructed by assuming different values of θ and performing similar calculations to those of this step. Note that np and 1-p will change for each new value of θ.

g. If $\theta_1 = 152$ hours, $\sigma_1 = 50$, T = 182 hours, n = 30, and the decision rule for passing the test is 19 or less failures, then β is calculated as:

$$z = \frac{x - np}{\sqrt{np(1-p)}} = \frac{18 - 21.6}{\sqrt{21.6(.28)}}$$

$$z = -1.46$$

The area under the normal curve not exceeding a z value of -1.46 is .07. Therefore, β = .07.

h. Summarize the characteristics of the demonstration test plan.

h. Test a random sample of 30 items for 182 hours. If 19 or less failures are observed, the test has been passed. If 19 or more failures are observed the test is failed. If the 19th failure occurs before 182 hours, stop testing when it occurs as the test is failed. This test plan will reject lots with an average mean life of 182 hours and standard deviation of 50 hours approximately 9% of the time. It will accept lots with an average mean life of 152 hours and a standard deviation of 50 hours approximately 7% of the time.

4. **For Further Information**

Additional examples describing this method are presented in most books on elementary statistics.

WEIBULL DISTRIBUTION (TR-3, TR-4, TR-6)

1. **When to Use**

When the distribution of failure times is Weibull and when only a given calendar time is available for a demonstration test, then this type of test plan is useful. Test plans covering this situation have been generated by Kao and Goode and published as a series of Quality Control and Reliability Technical Reports (TR-3, TR-4, TR-6) titled "Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution" by the Office of the Assistant Secretary of Defense (Installations and Logistics), September 1961, February 1962 and February 1963. (Refs. 13, 14, 15). The plans are based on the user of the test plans specifying his reliability parameter of interest in terms of mean life, hazard rate, or reliable life (life at given failure %). The plans were generated based on the assumption of a known shape parameter and give protection against a certain fraction of items in a lot not meeting the acceptance criterion. The test procedure essentially states that a sample of n items should be tested t hours. Those surviving the fixed time are classed as successes, while those not surviving are considered failures regardless of the exact time of failure. From this definition of failure it can be seen that these plans are based on the binomial distribution. Tables of the cumulative binomial distribution can be used to generate the OC curves for specific test plans. Each set of test plans features a set of conversion factors relating to MIL-STD-105 Sampling Plans. Tabled test plans are presented for values of the Weibull shape parameter β of 1/3, 1/2, 1, 1-2/3, 2-1/2, 3-1/3, 4 and 5.

2. **Conditions for Use**

   a. The failure times of the items being evaluated follow the Weibull distribution with known or assumed shape **parameter β**.

   b. The acceptable mean life μ_0, unacceptable mean life μ_1, producer's risk α, consumer's risk β (care must be taken to differentiate this quantity from the Weibull shape parameter which is also symbolized by β) and the test time t must be specified.

   c. Testing is without replacement.

   d. It is also possible to select test plans be specifying the fraction defective allowable in a lot having an acceptable quality level.

3. **Method**

   a. Specify μ_0, μ_1, α, β (consumer's risk), β (Weibull shape parameter) and test time t.

Example

   a. Given a lot of items whose failure times follow the Weibull distribution. Historical failure data on the item

MIL-HDBK-338-1A

indicates the Weibull shape parameter β is approximately 2.0. The program schedule allows 2500 hours of reliability demonstration testing. Lots having a mean life μ_0 of 10,000 hours are to pass the demonstration test 95% of the time (i.e., $\alpha = .05$). Lots having a mean life μ_1 of 5,000 hours are to be accepted by this test plan only 10% of the time (i.e., consumer's risk $\beta = .10$).

b. Determine the sample size and acceptance number for a plan that will give the protection specified in Step a.

b. Enter Table 3e on page 32 on TR-3 "Sampling Procedures and Tables for Life and Reliability Testing Based on the Weibull Distribution" which is for sampling plans for the case of the Weibull shape parameter $\beta = 2.0$. The quantity that is used to enter the table is

$$t/\mu_1 \times 100 = \frac{2,500}{5,000} \times 100 = 50$$

Search the column headed by 50 for the parenthesized value in the body of the table corresponding to

$$t/\mu_0 \times 100 = \frac{2,500}{10,000} \times 100 = 25$$

The table contains values for $t/\mu_0 \times 100$ of 24 and 26. To assure greater protection (i.e., a smaller α) the larger value should be used.

The $t/\mu_0 \times 100 = 26$ row specifies a sample size of 50 with an acceptance number of 5.

c. Summarize the test procedure.

c. The test procedure is as follows

1) Select a random sample of 50 items (from a large lot).

2) Test the items for 2500 hours.

3) If the number of failures observed during the test is 5 or less accept the lot.

4) If there are 6 or more failures the lot is rejected.

5) If the 6th failure occurs before 2500 hours, the test may be discontinued at that point and the lot rejected.

4. For Further Information

Frequently, the exact test desired is not covered in the tabled values in which case it is possible to interpolate to some degree at the expense of changing the risks slightly. Operating characteristic curves can be generated using a table of binomial probabilities.

Each of the Technical Reports contains an extensive bibliography describing other publications in which the details leading to these sampling plans were presented by Professors Goode and Kao.

FAILURE TRUNCATED TESTS

EXPONENTIAL DISTRIBUTION (H-108)

1. When to Use

When tests designed to demonstrate life characteristics of items whose failure times are exponentially distributed are to be performed wherein the test will be terminated after a preassigned number of failures then a test plan of this type can be specified. Plans of this type are available in Quality Control and Reliability Handbook H-108. Plans are presented for testing with and without replacement. Test criteria are tabled for specified values of α and β equal to .01, .05, .1, and .25 and for all combinations thereof, and for values of θ_1/θ_0 of 2/3, 1/2, 1/3, 1/5 and 1/10. A set of tables is also presented for cases in which α and θ_0 only are specified for various values of termination number r. Since a major factor in specifying a demonstration test plan of this type is the expected waiting time before a decision is made (i.e., a given number of failures occur) there is also included a set of tables for calculating this statistic for various sample sizes and termination numbers. Operating characteristic curves are presented for many of the demonstration test plans to enable the assessment of risk for values of mean life other than θ_0 and θ_1.

2. Conditions for Use

a. The failure times of the items placed on test must be exponentially distributed.

b. The acceptable mean life θ_0, unacceptable mean life θ_1, producer's risk α, and consumer's risk should be specified.

c. The decision of whether testing will be with or without replacement must be made.

d. An estimate may be made regarding the time available for the test as this will affect the number of items placed on test.

3. Method	Example
a. Specify θ_0, θ_1, α, β.	a. Given a item type whose failure times are distributed exponentially. Specify θ_0 = 1000 hours θ_1 = 500 hours α = .10 β = .10
b. Specify whether testing will be with or without replacement.	b. Testing will be without replacement.
c. Calculate θ_1 / θ_0.	c. $\theta_1 / \theta_0 = \dfrac{500}{1000} = \dfrac{1}{2}$
d. Enter the appropriate table in H-108 and select a termination number and acceptability constant.	d. Enter Table 2B-5 on page 2.41 of H-108 with α = .10, β = .10, and $\theta_1 / \theta_0 = \dfrac{1}{2}$. The termination number is 15 and the acceptability constant is .687.
e. Establish test procedure.	e. The specified demonstration test has the following characteristics 1) Items with a mean life of 1000 hours will be accepted by this test plan 90% of the time. 2) Items with a mean life of only 500 hours will be accepted by this test plan only 10% of the time.

3) Select a random sample of 15 or more items and test until 15 failures are observed.

4) Multiply the acceptability constant by θ_0 (in this example 1000 (.687)).

5) After 15 failures have been observed stop the test and sum the hours of operating time accumulated on all items that have been on test (both failed and unfailed). Divide the total item operating time by the number of failures (15).

6) If this θ is less than 687 hours reject the item.

7) If $\theta \geq 687$ the demonstration test has been passed.

f. Estimate the expected waiting for an accept/reject decision by entering the appropriate table in H-108.

f. Assume that 20 items had been placed on test in this example and the termination number is 15. From Table 2B-2(a) on page 2.34 of H-108, enter the table at n = 20 and r = 15. This yields an expected waiting time factor of 1.3144. If this is multiplied by θ_0 (1000 hours in this example) the expected time for a decision if the true mean life of the items on test is 1000 hours will be 1314 hours.

4. For Further Information

The statistical theory on which the H-108 sampling plans are based is presented in "Statistical Techniques in Life Testing", Technical Report No. 2, Testing of Hypotheses, by Benjamin Epstein, October 1958, and was prepared under Contract No. 2163(00) (NR-042--18) for the Office of Naval Research.

NORMAL DISTRIBUTION, σ KNOWN

1. When to Use

When the distribution of failure times is normal and when a given number of items are to be tested to failure, this type of test plan can be specified. Testing is without replacement.

2. Conditions for Use

a. The distribution of failure times must be normal.

b. The standard deviation of failure times must be assumed known.

c. The acceptable mean life θ_0, the standard deviation σ_0 of the distribution of acceptable mean life, the standard deviation σ_1 of unacceptable mean life, the sample size n to be tested to failure, the producer's risk α must be specified.

d. Note that unacceptable mean life θ_1 is not specified in this example. If it were desirable to specify a θ_1, it could be done but one of the other four test plan parameters θ_1, α, β, or sample size n would change. In other words, any four of these quantities can be specified but then the fifth is automatically constrained by the selection of the 4.

e. There is also a tradeoff between the sample size and the accept/reject decision point. In the following example, the sample size to be tested has been specified, but it would be possible to specify a mean life which, if the observed average failure time did not exceed, would result in failure of the lot to pass the demonstration test. With this critical mean life specified, it would be necessary to solve for the sample size to be tested.

f. Testing should be without replacement.

3. Method   Example

a. Specify θ_0, σ_0, σ_1, β a. Given a lot whose item failure
   and n.   times are normally distributed
                                                       as follows:

$$\theta_0 = 200 \text{ hours}$$
$$\sigma_0 = 50 \text{ hours}$$
$$\alpha = .01$$
$$\sigma_1 = 50 \text{ hours}$$
$$\beta = .05$$
$$n = 25$$

b. Solve for the accept/reject   b. The accept/reject point is
   decision point.   calculated as follows:

$$z_0 = \frac{\bar{x} - \theta_0}{\sigma_0 / \sqrt{n}}$$

$$-2.33 = \frac{\bar{x} - 200}{50 / \sqrt{25}}$$

$$\bar{x} = 176.7$$

c. Solve for θ_1.

c. Using the result from Step (b) and the specified $\beta = .05$

$$z_1 = \frac{\bar{x} - \theta_1}{\sigma_1/\sqrt{n}}$$

$$+ 1.645 = \frac{176.7 - \theta_1}{50/\sqrt{25}}$$

$$\theta_1 = 160.25$$

NOTE: The z values are from a table of "Areas Under the Normal Curve".

d. Summarize the characteristics of the demonstration test plan.

d. The demonstration test procedure is as follows:

1) Take a random sample of 25 items from a population whose distribution of failure times is normal.

2) Test until all items have failed, recording the exact failure time of each.

3) Take the arithmetic mean of the 25 failures and compare it with the decision point 176.7 hours. If the observed mean equals or exceeds 176.7 hours the demonstration test is passed. If it is less than 176.7 the demonstration test is failed.

4) The demonstration test shown in this example will:

o accept lots with a mean life of 200 hours and a standard deviation of 50 hours 99% of the time.

o accept lots with a mean life of 160.25 hours and standard deviation of 50 hours 5% of the time.

e. Construct the operating characteristic curve.

e. This is done by assuming values of θ other than θ_0 and θ_1 and solving for the probability of acceptance of a lot with that θ. Assume $\theta = 175$, $\sigma = 50$

$$z = \frac{176.7 - 175}{50/\sqrt{25}} = \frac{1.7}{10} = .17$$

From a table of Areas Under the Normal Curve the probability of acceptance of a lot with a mean life of 175 hours, $\sigma = 50$ is approximately .43.

f. Calculate the expected waiting time for a decision.

f. The expected waiting time for a decision is the expected failure time of the last order statistic. In this example and sample size n - 25, $\alpha = 50$ and $\mu = 200$. These values are used with Table 10A.1, page 186 of the book "Contributions to Order Statistics" edited by A.E. Sarhan and B.G. Greenberg, published by John Wiley & Sons, New York, 1962. Table 10A.1 give a z = 1.965 for the last order statistic in a sample of n = 25. Applying the formula

$$z = \frac{x - \mu}{\sigma}$$

$$1.965 = \frac{x - 200}{50}$$

x = 298 hours

Therefore the expected waiting time for a decision of $\theta_0 = 200$, and 25 items are tested to failure, is 298 hours.

4. For Further Information

MIL-STD-414 Section D yields a series of variables demonstration test plans for the normal distribution with σ known. The tests are constructed to assure protection in the form of percent defective of the lot from which the sample was drawn whereas, the example presented here is based on mean life.

NORMAL DISTRIBUTION, σ UNKNOWN (MIL-STD-414)

1. When to Use

When the distribution of failure times is normal, with unknown standard deviation and the criterion for acceptance is a variable (in the case, hours of life expectancy) with the protection desired stated in terms of percent defective in the lot from which the sample was drawn then this type of demonstration test is useful. This procedure basically is an application of MIL-STD-414, It contains plans for both single and double specification limits. The criteria for acceptance can either be stated in terms of an acceptability constant k, stated in standard normal deviates or as a maximum allowable percent defective, M. MIL-STD-414 also presents plans based on the calculation of an estimate of the standard deviation from sample data and also presents the range method. In the range method, the sample is segmented and the range of each sub-sample is used to estimate variability. It also contains test plans for the case when the standard deviation is known.

2. Conditions for Use

    a. The distribution of failure times must be normal.

    b. The standard deviation is unknown and must be assumed equal for both acceptable and unacceptable lots (when it is known, see previous example).

    c. Failure is measured in hours or cycles of operation.

    d. All items in the sample will be tested to failure.

    e. The lot size, acceptable quality level AQL, specification limit or limits, and inspection level must be stated.

    f. Testing is performed without replacement of failed items.

3. Method   Example

    a. Specify the lot size from which the sample is to be randomly drawn, AQL (the percent defective of acceptable lots), the specification limit, and the method

    a. Given an item type whose failure times are normally distributed. The lot to be evaluated contains 100 items with an unknown standard deviation. An AQL of 4% represents an ac-

to be used (standard deviation or range method) to measure variability.

ceptable level of defectives in a lot. The normal inspection level in MIL-STD-414 is IV. The standard deviation method is to be used for determining compliance with the acceptability criterion. The minimum life (L) for items of this type is 300 hours.

b. Determine the sample size to be tested.

b. Enter Table A-2 on page 4 of MIL-STD-414 with the lot size = 100. It is found that for Inspection Level IV, sample size code letter F applies. On page 39 in Table B-1 sample size code letter F calls for a sample size of 10.

c. Determine the acceptability constant k.

c. From Table B-1 enter Row F and the column headed by AQL = 4.00. This yields an acceptability constant k = 1.23.

d. Draw a random sample from the lot and test until all items fail recording exact failure times.

d. Ten failure times are recorded as follows:

Failure Time (Hours)

275
310
315
370
400
425
450
515
625
630

e. Calculate the sample mean and standard deviation from the observed test data.

e. Using standard statistical calculations

$\bar{x} = 432$ hours
$s = 119$ hours

f. Calculate the quantity

$$\frac{(\bar{x} - L)}{s}$$

where L = the specified minimum life.

f.

$$\frac{(\bar{x} - L)}{s} = \frac{432 - 300}{119} = 1.10$$

g. Compare $\frac{(\bar{x} - L)}{s}$ with k.

g. From Step c, the acceptability constant is k = 1.23. From Step f $\frac{(x - L)}{s} = 1.10$ Since 1.05 < 1.23, reject the lot.

4. For Further Information

MIL-STD-414 also presents test plans for cases where the standard deviation is known. Operating characteristic curves are presented in Section A of MIL-STD-414 to enable assessment of the risk at all quality levels. All lot sizes can be accommodated, but only certain values of AQL are covered by test plans. MIL-STD-414 also covers tightened and reduced sampling. A discussion of the methodology of the development of this type of sampling plan is presented in "Quality Control and Statistics" by A. J. Duncan, published by Richard D. Irwin, Homewood, Illinois, 1959.

WEIBULL DISTRIBUTION

1. When to Use

When the underlying distribution of failure time is Weibull, with the shape parameter, β, known or assumed, and the test must be truncated after a specified number of failures has occurred. The ordered failure times are required, along with the number of items on test.

2. Conditions for Use

a. The two parameter Weibull distribution must be assumed for failure times.

b. The parameter, β, must be known and be the same under the null and alternative hypothesis concerning the population mean.

c. The acceptable mean life, μ_0, the unacceptable mean life, μ_1, and the producer's risk must be specified. If the number of failures at which the test is truncated is specified, then the consumer's risk will be determined, and cannot be set arbitrarily.

3. Method

a. The method involves replacement of the original failure times $x_1, \ldots x_r$ by a new variable defined as

$$y_i = x_i^{\beta}$$

This variable has an exponential distribution with mean α. Hence, the previous

Example

a. With producer's risk .05 and consumer's risk .10, test the hypothesis that $\mu_0 = 800$ hours against $\mu_1 = 400$ hours. Assume a Weibull distribution with parameter $\beta = 1.5$. Twenty specimens were placed on test, and the test was concluded after the fourth failure, the observed

method developed for failure-truncated exponential life distributions may be used (See Section <u>Exponential Distribution (H-108)</u>).

failure times being 600, 750, 1000, and 1220 hours.

b. To perform a Weibull demonstration test with parameters μ_0, μ_1, β. Solve the following equations:

$$\mu_0 = \alpha_0 \frac{1}{\beta} \Gamma(\frac{1}{\beta} + 1)$$

$$\mu_1 = \alpha_1 \frac{1}{\beta} \Gamma(\frac{1}{\beta} + 1)$$

for α_0 and α_1

b.

$$\alpha_0 = \left[\frac{\mu_0}{\Gamma(\frac{1}{\beta} + 1)} \right]^{\beta}$$

$$= \left(\frac{800}{\Gamma(1.67)} \right)^{1.5}$$

$$= \left(\frac{800}{.903} \right)^{1.5}$$

$$= 24600$$

$$\alpha_1 = \left(\frac{400}{.903} \right)^{1.5}$$

$$= 9400$$

c. Perform the demonstration test in Section <u>Exponential Distribution (H-108)</u> on the observations y_1, y_2,... y_K from the exponential distribution with

$$\theta_0 = \alpha_0$$

$$\theta_1 = \alpha_1$$

The test is described in H-108.

On page 2.26 of H-108, the formula for $\hat{\theta}$ is

$$\hat{\theta} = \left[\frac{1}{r} \sum_{i=1}^{r} y_i + (n-r)y_r \right]$$

This is compared with acceptability constant, C, given on page 2.28 of H-108. The acceptance region is

$$\hat{\theta} \geq \theta_0 \Big/ (C/\theta_0)$$

c. $y_1 = 600^{1.5} = 14,700$

$y_2 = 750^{1.5} = 20,500$

$y_3 = 1000^{1.5} = 31620$

$y_4 = 1220^{1.5} = 42,600$

$$\hat{\theta} = \frac{1}{4} [14700 + 20500 + 31620 +$$

$$42600 + 16(42600)]$$

$$\hat{\theta} = 197755$$

$$\theta_0 = 26400$$

$C/\theta_0 = .342$ for producer's risk .05 and 4 failures (Table 2B-1) (H-108)

$$\text{Critical Value} = \frac{26400}{.342}$$

$$= 77200$$

Since 197755 > 77200, accept the value, μ_0, for the Weibull population mean.

d. The consumer's risk may be estimated from OC curves provided in the referenced document. Compute θ_1/θ_0 and read the value of the β error from Table 2-A-2.

The larger the value of θ, the smaller the value of β error. To achieve a β error of 0.1, for example, it would be necessary (Table 2-A-2) to continue testing until 9 failures had occurred.

d. $\dfrac{\theta_1}{\theta_0} = \dfrac{9400}{26400} = 0.36$

$\beta = 0.38$ from Table 2-A-2 (H-108)

4. For Further Information

Tables of the Gamma Function are presented on page 497 of the "Handbook of Tables for Probability and Statistics" edited by W. H. Beyer, Chemical Rubber Company, 1966.

SEQUENTIAL TESTS

EXPONENTIAL DISTRIBUTION (MIL-STD-781)

1. When to Use

When the demonstration test is to be based upon time-to-failure data and the underlying probability distribution is exponential, the sequential test is an alternate for the fixed sample size or fixed time tests discussed in Sections Time Truncated Demonstration Test Plans and Failure Truncated Tests. The sequential test leads to a shorter average number of part hours of exposure than either fixed sample or fixed time tests if the lot tested is near θ_0 or θ_1. Sequential tests should not be used where the exact length, or cost, of the test must be known before hand, or is specified.

2. Conditions for Use

a. The failure distribution must be exponential.

b. The upper test MTBF, θ_0, lower test MTBF, θ_1, producer's risk, α, and consumer's risk, β, must be specified.

c. The test may be run either with or without replacement of failed items, since the pertinent statistic is "total item-hours" of test time.

d. The producer's risk, α, and consumer's risk, β, are always equal in these test plans.

3. Method   Example

a. Specify θ_0, θ_1, α, β. If   a. Given equipment type whose
    the requirements are stated   failure times are distributed
    in terms of reliability at   exponentially. A reliability
    a time T_0, this will   of 0.95 is desired for 150
    involve solution of the   hours of operation. A product
    equation.   with a reliability of 0.90
                                          or lower is unacceptable. We
    $$e^{-\left(\frac{T_0}{\theta}\right)} = R$$ specify that $\alpha = 0.10$ for
                                          0.95 reliability and $\beta = 0.10$
                                          for 0.90 reliability.

    for θ. The solution is   We have

    $$\theta = -\frac{T_0}{\ln R}$$ $$\theta_0 = -\frac{150}{\ln.95}$$

                                          $\theta_0 = 2924$ hours

                                          $$\theta_1 = -\frac{150}{\ln.90}$$

                                          $\theta_1 = 1424$ hours

b. Compute θ_0/θ_1 b. $\theta_0/\theta_1 = \frac{3000}{1424} = 2.1$

c. Tests in MIL-HDBK-781 are   c. For $\alpha = \beta = .10$ the nearest
    classified by θ_0/θ_1, α test in MIL-HDBK-781 is Test
    and β. Find the Test   Plan IIIC. The criteria given
    Plan which most nearly fits   for acceptance and rejection
    the three values, and record   are:
    the acceptance and rejection
    criteria. These are given
    in terms of θ_1, and must

No. of Failures	Reject	Accept
0	N/A	4.4
1	N/A	5.79
2	N/A	7.18
3	0.7	8.56
4	2.08	-

be multiplied by θ_1 to con-
vert to "equipment hours"
criteria.

After multiplying by θ_1, or
1424 hours, we obtain

No. of Failures	Equipment Hours Reject	Accept
0	-	6266
1	-	8245
2	-	10224
3	997	12189
4	2962	-

For example, if 3 failures are encountered prior to 997 equipment hours, reject the equipment as unsatisfactory.

d. The OC curve of each sequential test is given as multiples of θ_o and θ_1. The document supplies for each Test Plan the expected length and the O.C. curve.

d. The expected number of equipment hours to reach a decision, when θ_o is the population parameter, is given on page 192 of MIL-HDBK-781. The O.C. curve is shown in page 193.

4. For Further Information

The material presented herein is from MIL-STD-781 and MIL-HDBK-781. The theory of sequential testing is developed in "Sequential Analysis" by A. Wald, John Wiley and Sons, Inc., 1947. Examples of sequential exponential demonstration tests are given in an article by Benjamin Epstein and Milton Sobel, "Sequential Life Tests in the Exponential Case," Annals of Mathematical Statistics, Vol. 25, (1955), pp. 82-93.

NORMAL DISTRIBUTION

1. When to Use

When the underlying failure distribution is assumed to be normal, and random sample observations are gathered sequentially. This method does not apply to ordered sample observations such as are usually obtained in life testing. It is useful where the cost of a single test is high, testing is done one unit at a time, and it is desired to minimize expected sample size.

As an example, consider the destructive testing of an aluminum alloy exhaust fan, where the component is rotated in a "whirl pit" at increasing velocity until a tensile failure occurs. In service, the component will rotate at a maximum velocity v_o, and the purpose of the demonstration test is to assure that the population mean velocity at failure is sufficiently high to provide satisfactory reliability at v_o.

2. Conditions for Use

a. The distribution of failures must be normal.

b. The acceptable population mean, μ_o, unacceptable mean, μ_1, must be specified, along with the known or assumed population standard deviations, σ_o and σ_1, the producer's risk, α, and consumer's risk, β. If α is unknown, and the test involves a strength distribution, α is often assumed to be 5% of the mean, in accordance with the discussion of normal distribution estimation in Section 5 of this handbook.

3. Method	Example

a. Specify μ_0, μ_1, σ_0, σ_1, α, and β. Compute

$$A = \frac{1-\beta}{\alpha}$$

$$B = \frac{\beta}{1-\alpha}$$

a. $\mu_0 = 1000$
$\mu_1 = 800$
$\sigma_0 = \sigma_1 = 100$
$\alpha = \beta = .05$

$$A = \frac{.95}{.05} = 19.0$$

$$B = \frac{.05}{.95} = .053$$

b. Compute, as each new observation is obtained, the corresponding unit normal deviates

$$z_{0i} = \frac{x_i - \mu_0}{\sigma_0}$$

$$z_{1i} = \frac{x_i - \mu_1}{\sigma_1}$$

and the corresponding probability density from a table of the normal distribution ordinates (Table A-2, Appendix A, Section 5). Note that it is not the usual <u>areas</u> under the normal curve but the <u>ordinates</u> that are required.

b. The first sample observation was found to be $x_1 = 1020$, hence

$$z_{01} = \frac{1020 - 1000}{100}$$

$$= 0.2$$

$$z_{11} = \frac{1020 - 800}{100}$$

$$= 2.2$$

The ordinate in the normal table corresponding to 0.2 is 0.3900 while the ordinate corresponding to 2.2 is 0.0355.

c. Form the product of ordinates

$$L_0 = \prod_{i=1}^{K} f(z_{0i})$$

and

$$L_1 = \prod_{i=1}^{K} f(z_{1i})$$

Determine, as each new sample is received, the ratio, $\dfrac{L_1}{L_0}$

c. $L_0 = .3910$

$L_1 = .0355$

$$\frac{L_1}{L_0} = \frac{.0355}{.3910}$$

$$= .091$$

Since this is between B and A, continue testing. The second observation was

$x_2 = 904.$

3. <u>Method</u>

If

$$B \le \frac{L_1}{L_0} \le A$$

continue testing. If

$$\frac{L_1}{L_0} < B, \text{ accept } \mu_0$$

$$\frac{L_1}{L_0} > A, \text{ accept } \mu_1$$

<u>Example</u>

Calculating as before,

$z_{02} = .96$

Ordinate $= .2516$

$z_{12} = 1.04$ Ordinate $= .2323$

$$\frac{L_1}{L_0} = .091 \left(\frac{.2323}{.2516}\right) = .084$$

Therefore, continue testing.

We observe

$x_3 = 1050$

$z_{03} = 0.5$

Ordinate $= .3521$

$z_{13} = 2.5$

Ordinate $= .0175$

$$\frac{L_1}{L_0} = .084 \left(\frac{.0175}{.3521}\right)$$

$$= .004$$

Since this is less than B, accept μ_0 as population mean.

d. The expected sample size (assuming that the true parameter is μ_0) may be obtained from the formula

$$E(N) = \frac{(1-\alpha)\ln B + \alpha \ln A}{\frac{1}{2\sigma^2}[2(\mu_1 - \mu_0)\mu_0 + \mu_0^2 - \mu_1^2]}$$

d. For this test, the expected number of observations was

$$E(N) =$$

$$\frac{.95 \ln .053 - .05 \ln 19.0}{\frac{1}{20000}[2(-200)(1000) + 1 \times 10^6 - 6.4 \times 10^5]}$$

$$\approx 2$$

4. <u>For Further Information</u>

See "Sequential Analysis" by Abraham Wald, John Wiley and Sons, N.Y., 1947, p. 77 and p. 53.

<u>INTERFERENCE DEMONSTRATION TESTS</u>

1. <u>When to Use</u>

Interference demonstration testing is applicable to mechanical systems where a strength distribution and a stress distribution overlap, or interfere. See Section 7 for several detailed examples. In the case of demonstration testing, both the strength and stress distribution must be assumed to be normal. We distinguish four cases:

<u>Case 1</u>: The mean of the stress distribution is assumed to be known, and the standard deviation of the stress distribution is assumed to be zero. See the discussion in Section 7 for conditions where these assumptions are valid. In this case, the interference problem becomes identical to <u>life testing</u> of the normal distribution described in Section <u>Normal Distribution, σ Known</u>. The specified stress level plays the role of the specified life. The strength distribution plays the role of the life distribution, and the demonstration procedure follows the example in Section <u>Normal Distribution, σ Known</u>.

<u>Case 2</u>: The mean of the stress distribution is assumed to be known, along with its standard deviation (often assumed to be 5% of the mean). The standard deviation of the strength distribution is assumed to be known, and its mean unknown. this may be translated to a demonstration test on strength and solved by the methods of Section <u>Normal Distribution, σ Known</u>. An example will be given below.

<u>Case 3</u>: The mean of the stress distribution and the mean of the strength distribution are unknown, but their standard deviations are assumed known. In this instance, sampling data will be required from both stress and strength. It is rare that a sample size for each may be specified ahead of testing. Therefore, it is unlikely that the consumer's risk may be set for this test. β will be a function of N and α. An example will be given below.

<u>Case 4</u>: The means and standard deviations of the strength and stress distributions are unknown. This case cannot be subjected to a demonstration test using standard statistical methods.

2. <u>Conditions for Use</u>

   a. The strength distribution and stress distribution must be stochastically independent.

   b. The strength distribution and stress distribution must be normal.

   c. A random sample of strength and stress observations must be obtained.

3. Method

   If the strength distribution has normal parameters μ_x, σ_x and the stress distribution has normal parameters μ_y, σ_y, then the statistic

   $$w = x - y$$

   is normally distributed with parameters

   $$w = \mu_x - \mu_y$$

   $$\sigma_w = \sqrt{c_x^2 + \sigma_y^2}$$

   and the reliability is defined as the probability that w exceeds zero. Clearly, specifying a particular reliability is the equivalent of requiring the unit normal deviate

   $$z = \frac{(\mu_x - \mu_y) - 0}{\sqrt{\sigma_x^2 + \sigma_y^2}}$$

   to correspond to this reliability in the right tail of the unit normal.

Example

1. Stress has a specified value of 30 KSI* with standard deviation 1.5 KSI. Strength is expected to be in the vicinity of 40 KSI but the mean is unknown. The standard deviation is assumed to be 2.0 KSI. A reliability of 0.99 is acceptable while a reliability of 0.90 is unacceptable. The producer's risk is .05 and the consumer's risk .10.

   Solution:

   $$\sigma_w = \sqrt{2^2 + (1.5)^2}$$
   $$= 2.5 \text{ KSI}$$

   The unit normal deviates corresponding to 0.99 and 0.90 reliability are 2.33 and 1.28 respectively.

   Therefore,

   $$2.33 = \frac{(\mu_0 - 30) - 0}{2.5}$$

   $$1.28 = \frac{(\mu_1 - 30) - 0}{2.5}$$

   and the requirements on the strength distribution are

   $$\mu_0 = 35.9$$

   $$\mu_1 = 33.2$$

   with a known $\sigma = 2.0$, $\alpha = .05$, $\beta = .10$. The methods of Section Normal Distribution, σ Known may now be used.

2. If we retain the data of example 1, and delete the information concerning the mean of the stress distri-

*KSI = thousands of pounds per square inch.

3. <u>Method</u>   <u>Example</u>

bution, then,

$\sigma_x = 2.0$ $\mu_0 - \mu_X = 35.9 - 30 = 5.9$

$\sigma_y = 1.5$ $\mu_1 - \mu_X = 33.2 - 30 = 3.2$

$\alpha = .05$

$\beta = .10$

If N_x observations of strength and N_y observations of stress are obtained, the appropriate statistic is

$$z = \frac{(\bar{x} - \bar{y}) - 5.9}{\sqrt{\dfrac{\sigma_x^2}{N_x} + \dfrac{\sigma_x^2}{N_y}}}$$

Hence, the critical value of $(\bar{x} - \bar{y})$ is

$$z_\alpha \sqrt{\frac{\sigma_x^2}{N_x} + \frac{\sigma_y^2}{N_y}} + 5.9$$

For example, ten observations of strength and four observations of stress are available.

For 0.99 reliability, we have from the previous example, $\mu_x - \mu_y = 5.9$, and $Z_\alpha = Z_{.95} = -1.65$

$$-1.65 \sqrt{\frac{4.0}{10} + \frac{2.25}{4}} + 5.9 = +4.21$$

as the critical value of the statistic $(\bar{x} - \bar{y})$. Accept if

$\bar{x} - \bar{y} \geq 4.21$

Otherwise, reject. The β risk for this example would be

$$z = \frac{4.21 - 3.2}{\sqrt{\frac{4.0}{10} + \frac{2.25}{4}}}$$

$$= + 1.03$$

$$\beta = 0.15$$

A larger sample size for either stress or strength will reduce β.

BAYES SEQUENTIAL TESTS

1. When to Use

A test plan of this type can be specified if mean life θ is the parameter of interest and if a prior dis'ribution on θ is known. The use of a test plan of this type results in a smaller sample size than most other test plans described in this section of the Appendix.

2. Conditions of Use

a. The lot of items being evaluated must have a known prior distribution on the mean life.

b. The parameters of the prior distribution must be specified as well as θ_1, the minimum acceptable mean life. It is necessary to specify two other terms K_2 and K_1 as criteria for terminating the test. K_2 is a probability such that if $Pr(\theta \geq \theta_1/\theta_n) \geq K_2$ the test is deemed passed. It is usually specified at .90, .95 or .99 and is the probability associated with a lower bound at θ_1. K_1 is usually specified as .01, .05, or .10 and $1-K_1$ is the probability associated with an upper bound at θ_1. $K_2 + K_1$ need not equal 1.

c. In this demonstration test procedure it is possible to pass or fail without testing. If testing is called for, one item is tested at a time and a decision is made after each failure to either accept, reject, or continue testing.

3. Method

a. Specify the prior distribution form, its parameters, and the quantities θ_1, K_1 and K_2.

Example

a. It has been found that a given item type has a prior distribution on its mean life θ that is inverted gamma with a shape parameter $\lambda = 3$, a scale parameter $\alpha = 100$, a minimum acceptable mean life $\theta_1 = 60$, $K_1 = .10$ and $K_2 = .90$.

b. Compute P_0 to determine if testing should be performed:

if $P_0 \geq K_2$, accept and do not test

if $P_0 \leq K_1$, reject and do not test

if $K_1 < p_0 < K_2$, place an item on test

b. To solve for P_0 use the Tables of Percentage Points of the χ^2 distribution for 2λ degrees of freedom (d.f.). In this case use 6 d.f.

Next solve the equation

$$\chi^2 = \frac{2a}{\theta_1} = \frac{2(100)}{60} = 3.33$$

In the χ^2 Table for 6 d.f. $\chi^2 = 3.33$ corresponds to a percentage point (P_0 in this problem) of approximately .23.

Therefore, $K_1 < P_0 < K_2 =$ .10 < .23 < .90 resulting in the instruction to begin testing.

c. Construct a table of decision points for each failure time. This is done by solving for

$$\hat{\theta}_n{}^* = \frac{\theta_1 X^2_{K_2, \ 2(n+\lambda)} -2a}{2n}$$

Where n = # of failures

and

$$\hat{\theta}_n{}^* = \frac{\theta_1 X^2_{K_1, \ 2(n+\lambda)} -2a}{2n}$$

c. For 1 failure the following decision points are calculated

$$\hat{\theta}_1{}^* = \frac{60 X^2_{(.90, \ 8)} -2(100)}{2(1)}$$

$$\hat{\theta}_1{}^* = \frac{60(13.36) - 200}{2} = 301$$

$$\hat{\theta}_{1*} = \frac{60 X^2_{(.10, \ 8)} -2(100)}{2(1)}$$

$$\hat{\theta}_{1*} = \frac{60(3.49) - 200}{2} = 4.7$$

The following table gives the accept/reject mean lives for additional failures.

3. Method   Example

c.   c.

n	$\hat{\theta}_n^*$ Accept if $\hat{\theta}_n$ $\geq \hat{\theta}_n^*$	$\hat{\theta}_{n*}$ Reject if $\hat{\theta}_n$ $\leq \hat{\theta}_{n*}$
1	301	4.7
2	190	23.5
3	152	29.7
4	133	33.4
5	.	.
.	.	.
.	.	.

$\hat{\theta}_n^*$ and $\hat{\theta}_{n*}$ eventually terminate at some n. Therefore, the test could not continue idefinitely.

The $\hat{\theta}_n = \dfrac{\sum\limits_{i=1}^{n} t_i}{n}$ where

t = failure time

n = number of failures

d. Test the first part and make the decision to accept, reject or continue testing.

d. Test the first item. If its failure time is:

   1) 4.7 hours or less, reject the product.

   2) 301 hours or more, accept the product.

   3) greater than 4.7 and less than 301, test another sample to failure compare again to the accept/reject criteria of Step c.

4. For Further Information

The theoretical development of this method is presented in "A Sequential Bayes Procedure for Reliability Demonstration", by R.E. Schafer and N.D. Singpurwalla, Naval Research Logistics Quarterly, March 1970.

The methodology of fitting prior distributions is developed in RADC-TR-69-389 "Bayesian Reliability Demonstration - Phase I - Data for A Prior Distribution". Further details are provided in RADC-TR-76-296, Vols I through V, "Reliability Acceptance Sampling Plans Based Upon Prior Distribution", and in RADC-TR-81-106, "Bayesian Reliability Tests Made Practical."

APPENDIX B

GROWTH MODELS

INTRODUCTION

Scope

The intent of this appendix is to provide an overview of various mathematical models for reliability growth that have been proposed in the literature. This listing may be used as a guideline for choosing a candidate model for a particular application. Technical references are given for each of these models where a more complete discussion of the model may be found.

Types of Models

The growth models are distinguished according to two major types as follows:

    o   Discrete Growth Models
    o   Continuous Growth Models

DISCRETE RELIABILITY GROWTH MODELS

General

This section describes a number of discrete reliability growth models which are currently available. Each model is briefly described including the basic assumptions that were made in deriving the models.

Model 1

Lloyd and Lipow (Ref. 30) introduced a reliability growth model for a system which has only one failure mode. For each trial the probability that the system will fail if the failure mode has not been previously eliminated is assumed to be a constant. If the system does not fail, no corrective action is performed before the next trial. If the system fails, then an attempt is made to remove the failure mode from the system. The probability of successfully removing the failure mode is also assumed to be a constant for each attempt. They show that the system reliability, R_n, on the n-th trial is

$$R_n = 1 - Ae^{-C(n-1)}$$

where A and C are parameters.

Model 2

Another reliability growth model was considered by Lloyd and Lipow (Ref. 30) where the development program is conducted in K stages and on the

i-th stage a certain number of systems are tested. The reliability growth function considered was

$$R_i = R_\infty - (\alpha/i)$$

where R_i is the system reliability during the i-th stage, R_∞ is the ultimate reliability as $i \to \infty$ and $\alpha > 0$ is a parameter. Maximum likelihood and least squares estimates of R_∞ and α are given by Lloyd and Lipow along with a lower confidence limit for R_K.

Model 3

Wolman (Ref. 31) considered a situation where the system failures are classified according to two types. The first type is termed "inherent cause" and the second type is termed "assignable cause". Inherent cause failures reflect the state-of-the-art and may occur on any trial while assignable cause failures may be eliminated by corrective action, never to appear again. Wolman assumed that the number of original assignable cause failures is known and that whenever one of these modes contribute a failure, the mode is removed permanently from the system. Wolman uses a Markov-chain approach to derive the reliability of the system at the n-th trial when the failure probabilities are known.

Model 4

Barlow and Scheuer (Ref. 32) considered a nonparametric model for estimating the reliability of a system during a development program. They assumed that the design and engineering changes do not decrease the system's reliability, but, unlike some other models, they do not fit a prescribed functional form to the reliability growth. Their model is similar to Wolman's in that each failure must be classified either as inherent or assignable cause.

It is further assumed that the development program is conducted in K stages, with similar systems being tested within each stage. For each stage, the number of inherent failures, the number of assignable cause failures and the number of successes are recorded. In addition, they assumed that the probability of an inherent failure, q_0, remains the same throughout the development program and that the probability of an assignable cause failure, q_i, in the i-th stage does not increase from stage to stage of the development program. The authors obtained the maximum likelihood estimates of q_0 and of the q_i's subject to the condition that they be nonincreasing. A conservative lower confidence bound for the reliability of the system in its final configuration was also given.

Model 5

Virene (40) considered the suitability of the Gompertz equation

$$R = ab^{c^t}$$

$0 < a < 1, 0 < b < 1, 0 < c < 1,$ for reliability growth modeling. In this equation a is the upper limit approached by the reliability R and a fixed time period as the development time $t_{\to \infty}$. The parameters a, b and

c are unknown. Virene gave estimates of these parameters and demonstrated by examples the application of this model.

Model 6

Barlow, Proschan and Scheuer (Ref. 34) considered a reliability growth model which assumes that a system is being modified at successive development. At stage i the system reliability (probability of success) is p_i. The model of reliability growth under which one obtains the maximum likelihood estimates of p_1, p_2, ..., p_k assumes that

$$p_1 \leq p_2 \leq \cdots \leq p_k$$

That is, it is required that the system reliability not be degraded from stage to stage of development. No particular mathematical form of growth is imposed on the reliability. In order to obtain a conservative lower confidence bound on p_K, it suffices to require only that

$$p_K \geq \max_{i < k} p_i$$

That is, it is only necessary that the reliability in the latest stage of development be at least as high as that achieved earlier in the development program.

Data consist of x_i successes in n_i trials in stage i, i=1, ...,K.

A variation of this model is treated in Barlow and Scheuer. (See Model 4). In that model two types of failure, inherent and assignable cause, are distinguished.

Model 7

Another reliability growth model considered by Barlow, Proschan and Scheuer (Ref. 34) assumed that at stage i of development the distribution of system life length is F_i. The model of reliability growth under which the maximum likelihood estimates of $F_1(t)$, $F_2(t)$,..., $F_K(t)$ are obtained, writing

$$\bar{F}_i(t) = 1 - F_i(t)$$

is

$$\bar{F}_1(t) \leq \bar{F}_2(t) \leq \cdots \leq \bar{F}_K(t)$$

for a fixed $t \geq 0$. In order to obtain a conservative upper confidence curve on $F_K(t)$ and thereby, a conservative lower confidence curve on $f_K(t)$ for all non-negative values on t, it suffices only to require that

$$\bar{F}_K(t) > \max_{i < K} \bar{F}_i(t)$$

for all $t > 0$. That is, the probability of system survival beyond any time t in the latest stage of development is at least as high as that achieved earlier in the development program.

Model 8

Singpurwalla (Ref. 35) considered an approach to reliability growth analysis of discrete data involving the use of time series methods. Since a time series can be defined simply as, "...a set of observations generated sequentially in time" it is straightforward to formulate the growth process as the following time series problem: on a complex system which is undergoing successive developmental changes, tests are performed to monitor progress and to determine whether reliability requirements are being met. The outcome of each test is judged to be either a success or a failure. In particular, at the end of the j-th stage, n_j independent tests are conducted of which v_j are deemed to be successful. If we denote the reliability of the system at the end of the j-th stage by j_p, then v_j is binomially distributed with parameters n_j and p_j. Let p_j^p be an estimator of p_j, j = 1,2, ..., M. Given estimates for p_j, j = 1,2, ... M, we can apply time series methods, (1) to determine whether p_j is increasing with j, (2) to obtain a good estimate of the probability of success at the present stage of testing (p_M), and (3) to obtain forecasts of p at future stages, M + 1, M + 2 ... .

In particular, the methods proposed by Box and Jenkins (Ref. 36) have been found to be powerful and flexible enough for application to many fields. Singpurwalla (Ref. 35) is a specific application of this approach to reliability growth problems. The Box-Jenkins Autoregressive-Integrated Moving Average (ARIMA) model/approach has the following major advantages:

(a) No specific model need be selected in advance. The data themselves lead to selection of a specific model within the very broad and flexible class of ARIMA models.

(b) Models with either deterministic or stochastic indications of growth can be fitted to data. Normally the deterministic model should be used only in cases where the growth process is well understood and controlled. This is particularly true if the model is being used to forecast future reliability.

(c) The Box-Jenkins methodology has a built-in theory of forecasting, as well as techniques to obtain numerical forecasts.

It must be recognized that his approach has some disadvantages as well. For example, data from a relatively large number of stages must be available, i.e., M should be of the order of 20 or so before meaningful conclusions can be drawn in most cases. If the process is a complex one, it is possible that M $\geq$ 50 will be required. Another disadvantage is that the methodology cannot be applied in a cookbook fashion. Considerable judgement is required and it is possible to derive very inappropriate conclusions.

CONTINUOUS RELIABILITY GROWTH MODELS

General

The previous section discussed situations where a device or system either operated successfully when called upon or failed to perform its mission, i.e., a go/no-go situation. The other broad category which must be considered is the repairable system which must operate successfully over periods of time which cannot be regarded as fixed and hence, cannot be divided into a go/no-go categorization. In this case, we must be concerned with the sequence of successive times-between-failures of the system. If the system is improving (as a result of design fixes, debugging of bad parts, better repair procedures, or any other reason) then the successive times-between-failures (inter-failure times) will tend to increase. Reversals will occur for many reasons, including inappropriate design fixes, damage caused by previous repairs, changing environmental stresses, or even sampling variability. Hence, it may not be obvious that growth is occurring without some sort of analysis. Moreover, even if the presence of growth can be verified by inspection, it usually will be necessary to use some systematic technique(s) to estimate the rate at which growth is occurring or to forecast future changes in reliability. Some of the following models are based on the nonhomogeneous Poisson process which is described in Poisson Processes. The discussion for models 13-17 are from Reference (Ref. 48).

Poisson Processes

A stochastic process $(N(t), t \geq 0)$ is said to be a counting process if $N(t)$ represents the total number of events which have occurred in the interval $(0,t)$. The counting process $(N(t), t \geq 0)$ is said to be Homogeneous Poisson process (HPP) if

    (1) $N(0) = 0$

    (2) $(N(t), t \geq 0)$ has independent increments

    (3) The number of events (in our context, failures) in any interval of length $t_2 - t_1$ has a Poisson distribution with mean $\rho(t_2 - t_1)$.

That is, for all $t_2 > t_1 \geq 0$,

$$P(N(t_2) - N(t_1) = n) = \frac{e^{-\rho(t_2 - t_1)} (\rho(t_2 - t_1))^n}{n!}$$

for $n \geq 0$

From condition (3) it follows that

$$E(N(t_2 - t_1)) = \rho(t_2 - t_1)$$

where the constant, ρ, is the rate of occurrence of failures. It can be shown that the successive times-between-failures of the HPP defined above are independent and identically distributed exponential random variables.

The nonhomogeneous Poisson process (NHPP) differs from the homogeneous Poisson process (HPP) only in that the intensity function varies with time rather than being a constant. That is, conditions (1) and (2) are retained and condition (3) is modified to be:

(3a) The number of failures in any interval (t_1, t_2) has a Poisson distribution with mean

$$\int_{t_1}^{t_2} \rho(t) \, dt$$

That is, for all $t_2 > t_1 \geq 0$

$$P(N(t_2) - N(t_1) = n) = \frac{\left(\int_{t_1}^{t_2} \rho(t) \, dt\right)^n e^{-\int_{t_1}^{t_2} \rho(t)dt}}{n!}$$

for $n \geq 0$

From (3a) it follows that

$$E(N(t_2 - t_1)) = \int_{t_1}^{t_2} \rho(t) \, dt$$

Model 9

Duane (Ref. 16) analyzed data for several systems developed by General Electric in an effort to determine if any systematic changes in reliability improvement occurred during development for these systems. His analysis revealed that for these systems, the cumulative failure rate fell close to a straight line when plotted on log - log scale.

Let $c(t)$ denote the number of system failures by time t, $t > 0$. The observed cumulative failure rate $C(t)$ is approximately a straight line. That is, $\log C(t) = \hat{c} = \alpha \log t$, or $C(t) = \gamma t^{-\alpha}$, where $\delta = e^{\delta}$. It follows also that $N(t) = \delta t^{1-\alpha}$.

The change per unit time of $N(t)$, $r(t) = \frac{d}{dt} N(t) = \gamma(1-\alpha)t^{-\alpha}$.

Duane interpreted this as the current failure rate. In this context, the reciprocal of $r(t)$, $m(t) = (\gamma(1-\alpha)t^{-\alpha})^{-1}$, may be interpreted as the current or instantaneous MTBF. This is Duane's postulate which is a deterministic learning curve formulation of reliability growth.

When the test time t is the cumulative test time for the program, then the log -log property of the cumulative failure rate, $C(t)$, indicates an overall trend for reliability growth or an idealized type pattern. Section 5.2.6 of Ref. 47 provides appropriate methods for construction and interpretation of the idealized growth curve and test phase reliability when $C(t)$ is linear on log -log scale.

Model 10

Crow (Ref. 44) considered a model (called the AMSAA model) which can be used for tracking reliability growth within test phases. This approach assumes that within a test phase, reliability growth can be modeled as a NHPP. It also assumes that based on the failures and test time within a test phase, the cumulative failure rate is linear on log - log scale. This is a local, within test phase pattern for reliability growth comparable to the global pattern noted by Duane (21). Let t be the test time from the beginning of the test phase and let $N(t)$ denote the number of system failures by time t. It follows that the expected value of $N(t)$ can be written as $E(N(t)) = \lambda t^\beta$.

The AMSAA model assumes that the test phase reliability growth follows the NHPP with mean value function $\theta(t) = \lambda t^\beta$ and intensity function $\rho(t) = \lambda \beta t^{\beta-1}$. This model allows for the development of vigorous statistical procedures useful for reliability growth tracking. The AMSAA model is thoroughly discussed in Appendix C of MIL-HDBK-189.

Model 11

Lewis and Shedler (38) extended the Cox-Lewis model (Model 11) by developing estimation techniques for the exponential polynomial model for powers up to 10, i.e., for models of the form $\rho(t) = \exp(\alpha_0 + \alpha_1 + \dots + \alpha_{10} t^{10})$.

Model 12

The IBM model, Rosner (Ref. 39) assumes explicitly that: (1) there are random (constant intensity function) failures occurring at rate , and (2) there are a fixed but unknown, number of nonrandom design, manufacturing and workmanship defects present in the system at the beginning of testing. Let $N(t)$ be the number of nonrandom type defects remaining at time $t \geq 0$. This model makes the intuitively plausible assumption that the rate of change of $N(t)$ with respect to time is proportional to the number of nonrandom defects remaining at t. This is,

$$d\,N(t)/dt = K_2 N(t)$$

and hence

$$N(t) = e^{-K_2 t + c}$$

Now if we denote the unknown number of non-random failures present at t = 0 by K_1 then

$$N(t) = K_1 e^{-K_2 t} \quad t > 0, \; K_1, K_2 > 0$$

Defining $V(t)$ to be the expected cumulative number of failures up to time t then

$$V(t) = \lambda t + K_1 (1 - e^{-K_2 t}) \tag{1}$$

Thus, the expected cumulative number of failures by time t is the expected number of random failures by time t plus the expected number of non-random failures removed by time t. It should be noted that $V(0) = 0$ as expected. Moreover as $t \to \infty$, $V(t) \to \lambda t + K_1 \to \lambda t \to \infty$, as expected.

Because of the non-linearity of the model (1) the estimation of λ , K_1, and K_2 must be accomplished by iterative means.

In addition to this model being "plausible," the most interesting feature is the ability of the model to predict the time when the system/equipment is "q" fraction debugged (i.e., q fraction of the original K_1 non-random failures have been removed, $0 > q < 1$). The number of non-random defects removed by time t is clearly

$$N(0) - N(t) = K_1 - K_1 e^{-K_2 t}$$

and hence the fraction (of K_1 initial non-random defects) removed by time t is

$$q = \frac{K_1 - K_1 e^{-K_2 t}}{K_1} = 1 - e^{-K_2 t} \tag{2}$$

Thus having estimated K_2, we can find the time at which $q = 0.95$ of the non-random defects have been removed by solving (2) for $t_{0.95}$. That is,

$$t_{0.95} = \frac{-\ln 0.05}{K_2}$$

In general, for arbitrary q, $0 < q < 1$ the time by which the system/equipment is q fraction debugged is

$$t_q = \frac{-\ln (1-q)}{K_2} \tag{3}$$

Equation (3) is a powerful tool because it can be used to help determine the length of development testing, or, the debugging period.

Another important feature of this model is that the number of non-random failures remaining at time t can be estimated and of course is

$$K_1 e^{-K_2 t}$$

The estimate of λ, say $\hat{\lambda}$, gives the estimate of the long-run achievable MTBF.

In the above model the dependent variable was the expected cumulative number of failures by time t. In all of the following models the dependent variable is the cumulative mean time between failures $Y(t)$ where

$$Y(t) = \frac{t}{\text{Total No. of Failures in } (0,t)}$$

Model 13

Suppose that K is used to denote the limiting value of $Y(t)$ as $t \to \infty$ and suppose the rate of growth $dY(t)/dt$ is jointly proportional to the remaining growth (namely $K-Y(t)$) and some growth function $g(t)$. Thus

$$dY(t)/dt = (K-Y(t)) \, g(t)$$

Taking $g(t)$, the growth function, to be a constant, say $K_2 > 0$, then the solution of the differential equation is easily seen to be

$$Y(t) = K (1 - K_1 e^{-K_2 t}), \quad t > 0$$

This may be referred to as the exponential-single term power series model.

Here $K_1 > 0$ is an intercept parameter arising as a constant of integration.

The growth rate (i.e., $dY(t)/dt$) is largest at $t = 0$ is monotonically decreasing in t so that

$$\lim_{t \to \infty} (dY(t)/dt) = 0$$

It is entirely plausible that the growth rate is largest at $t = 0$ and decreases to 0 as $t \to \infty$. This model is also extremely flexible because it has three parameters

K: The limit of cumulative MTBF.

K_1: When $t = 0$, $Y(0) = K (1-K_1)$. Thus $K (1-K_1)$ may be thought of as the initial MTBF of the system/equipment when $0 < K_1 < 1$. K_1 may also be thought of as the growth potential.

K_2: The growth function; constant in this case.

The disadvantage of this model is clear enough. Like the IBM model it has three parameters and is non-linear in t; nor can it be transformed to a linear function of t. Thus the least squares estimates of K, K_1, and K_2 must be obtained by iterative procedures. More details on this model can be found in Perkowski and Hartvigsen (Ref. 40).

Model 14

A model proposed by Lloyd and Lipow (Ref. 30) supposes that the growth rate is inversely proportional to the square of time t, i.e.,

$$dY(t)/dt = K^2/t^2, K_2 < 0.$$

Then clearly,

$$Y(t) = K - K_2/t.$$

Here K is a constant of integration but it should be noticed that

$$\lim_{t \to 0} Y(t) = K$$

and thus K is the limiting value of cumulative MTBF.

The parameter K_2 is a growth rate parameter which also affects the location of the curve. Since Y(t) cannot be negative and

$$\lim_{t \to 0} Y(t) = -\infty$$

we must define

$$Y(t) = 0, 0 \leq t < K_2K.$$

This definition provides a time period $(0, K_2/K)$ when the cumulative MTBF is 0. This may be realistic for some systems.

By making the change of varible t' = 1/t we see that $Y(t') = K - K_2t'$ and thus $Y(t')$ is linear in t' with slope K_2 and intercept K which means the parameters K and K_2 can be easily estimated by the usual least squares methods.

Model 15

Aroef (Ref. 41) assumed that the growth rate is jointly proportional to the growth achieved at t, i.e., Y(t), a constant multiplier (growth rate parameter) K_2 and inversely proportional to t^2. That is, $dY(t)/dt = K_2 Y(t)/t^2$

This differential equation has the solution

$$Y(t) = K e^{-K_2/t}$$

Since $\lim_{t \to \infty} Y(t) = K$ the reliability growth limit in cumulative

MTBF is K. Also

$$\lim_{t \to 0} Y(t) = 0$$

Since

$$\ln Y(t) = \ln K - K_2/t,$$

letting

$$t' = 1/t,$$

$$\ln Y(t') = \ln K - K_2 t'$$

and usual linear least squares methods can be used to estimate the constants K and K_2.

Model 16

The last model considered is the simple exponential model:

$$Y(t) = K e^{K_2 t}, \quad K > 0, \quad K_2 > 0$$

$Y(0) = K$ which is the "initial" cumulative MTBF. since $\ln Y(t) = \ln K + K_2 t$ then the linear least square method can be used to fit the constants.

9.0 SOFTWARE RELIABILITY

9.1 INTRODUCTION

An operational commander could care less whether his system fails because of a hardware or software failure; either type of failure decreases the operational availability of his system. His primary interest is to maximize the operational availability of his system. To provide the operational commander with a system capable of meeting his operational availability requirements, the system developer, e.g. System Program Office, needs practical procedures for quantitatively specifying, predicting, and measuring system reliability and maintainability (R/M).

In the hardware area, procedures have been developed over the past 25 years that are fairly well established and accepted for quantitatively predicting, specifying, and measuring equipment and system R/M. They are detailed in a number of military specifications, standards, and handbooks, which are discussed in this handbook.

On the other hand, the current status of software R/M may be summarized as follows:

1. There is disagreement on basic definitions

2. Methods for quantitative specification are not available or used

3. A plethora of reliability prediction models have been proposed; none seem to have been adequately validated

4. Demonstration procedures are not available

5. Some basic design procedures are available, e.g. top down design, structured programming, etc., etc.

In terms of combined hardware/software reliability models, several have been recently proposed (Refs. 44, 45); however, they are extremely complex and, hence, impractical in terms of application by system developers.

There are a number of conflicting views as to what software reliability really is and how it should be quantified. The conflict arises because of the disagreement in the basic definition of the term "software reliability." Software reliability as viewed by some people, especially the computer science purists, should be deeply tied to the correctness of the software. They argue that an incorrect software (i.e., a software still containing errors) is doomed to fail sooner or later and thus its reliability should be zero (0). Once the software has been freed of all errors, then its reliability becomes one (1). On the other hand, software reliability, as viewed by many engineers, statisticians, and practitioners, is deeply tied to the concept of "probabilistic reliability." These groups of people argue that many programs used in the real world are known to still contain errors and yet they are executed day after day without any failures appearing. Software reliability, they believe, should be viewed as the probability that a software system will operate without a failure for a specified (mission) time.

One way to resolve this conflict is to look back at the original problem in the real world and ask ourselves the question: "Why do we need to know software reliability?"

The original real world problem, in very simple terms, is as follows:

Develop software that will satisfy the user's requirements in the most efficient (in both time and money sense) way possible.

The solution of this problem turns out to be very difficult basically because of the following facts:

1. Real world software is large and complex

2. Users are not always 100 percent certain about their requirements

3. Resources (time and money) allocated for software development are always limited

Even if we know that we only need 2000 test cases to run to expose all possible embedded errors in a software package, chances are that, in the real world, we may not have enough time and money to perform this exhaustive test. As more and more errors are uncovered by our testing or correctness verification process, the additional cost of exposing the other remaining errors rises very fast. Thus, there is a point when it is almost practically useless to continue testing to achieve 100 percent correctness. This explains the reason why almost all software systems that have been released for public and private use still have embedded errors.

If we adopt the point of view of the computer science purist, then almost all software released to this date (including those software systems that are accepted as very reliable and useful by their users) have zero reliability. Since everything now has zero reliability, the value or usefulness of the software reliability concept is lost.

The reason why people invented the concept of software reliability (or hardware reliability for that matter) is to have a useful measure that may help us in dealing with the original real world software (hardware) problem. This reliability measure is useful in planning and controlling additional resources (time and money) to maximize software (hardware) reliability within the given resource contraints. It is also a useful measure for giving the user confidence about the software quality of the delivered product.

All of the design tools and technique developed in hardware reliability engineering are really aimed at solving the basic problems of:

1. Paying attention to detail (discipline)

2. Handling uncertainties

The same basic problems exist in the software area, so that one should expect to see a strong connection between the proven hardware techniques and the emerging software techniques.

Admittedly there are differences between hardware and software.

Rather than dwelling on the differences, we should look at the similarities. Some of these are:

1. Hardware reliability is a function of equipment complexity; intuitively one would expect the same to be true of software, although an acceptable measure of complexity has yet to be found.

2. Solid state electronic devices, e.g. transistors, microcircuits, if fabricated properly, do not have any wearout mechanisms, that one can see over a long time period. The defects which cause failure (other than obvious misapplication of the device) are built in during the initial fabrication of the device; the same is true of software.

3. Hardware reliability can be improved by reliability growth testing e.g. a test-analyze-and-fix program to discover, identify, and correct failure modes and mechanisms which would cause early equipment failure. This is similar to finding and eliminating "bugs" in a software program, thus increasing its reliability.

Thus, we should be concentrating on the duality that exists between the successful hardware approaches and the emerging software approaches. Once this is accepted, the whole problem is simplified because the hardware and software problems can be approached together, in a total system context.

The duality between hardware and software is graphically portrayed in Figure 9.1-1 which illustrates the key elements of hardware and software programs during the life cycle phases of system development. The basic difference occurs during full scale engineering development, when hardware is fabricated and tested while software is coded (programmed) and debugged.

9.2 THE SOFTWARE PROBLEM

The basic problem in software is the management of complexity. This is very well described in Ref. 1 as follows:

"We have learned from our experience with building and managing complex organizations that when the complexity of any level grows beyond a certain range, function becomes impaired, operation becomes inefficient, and reliability declines. We know that ad hoc corrections and local improvements in efficiency can only go so far in correcting the problems, and that sooner or later we must face a total reorganization of the system that must essentially alter the hierarchical control and levels structure."
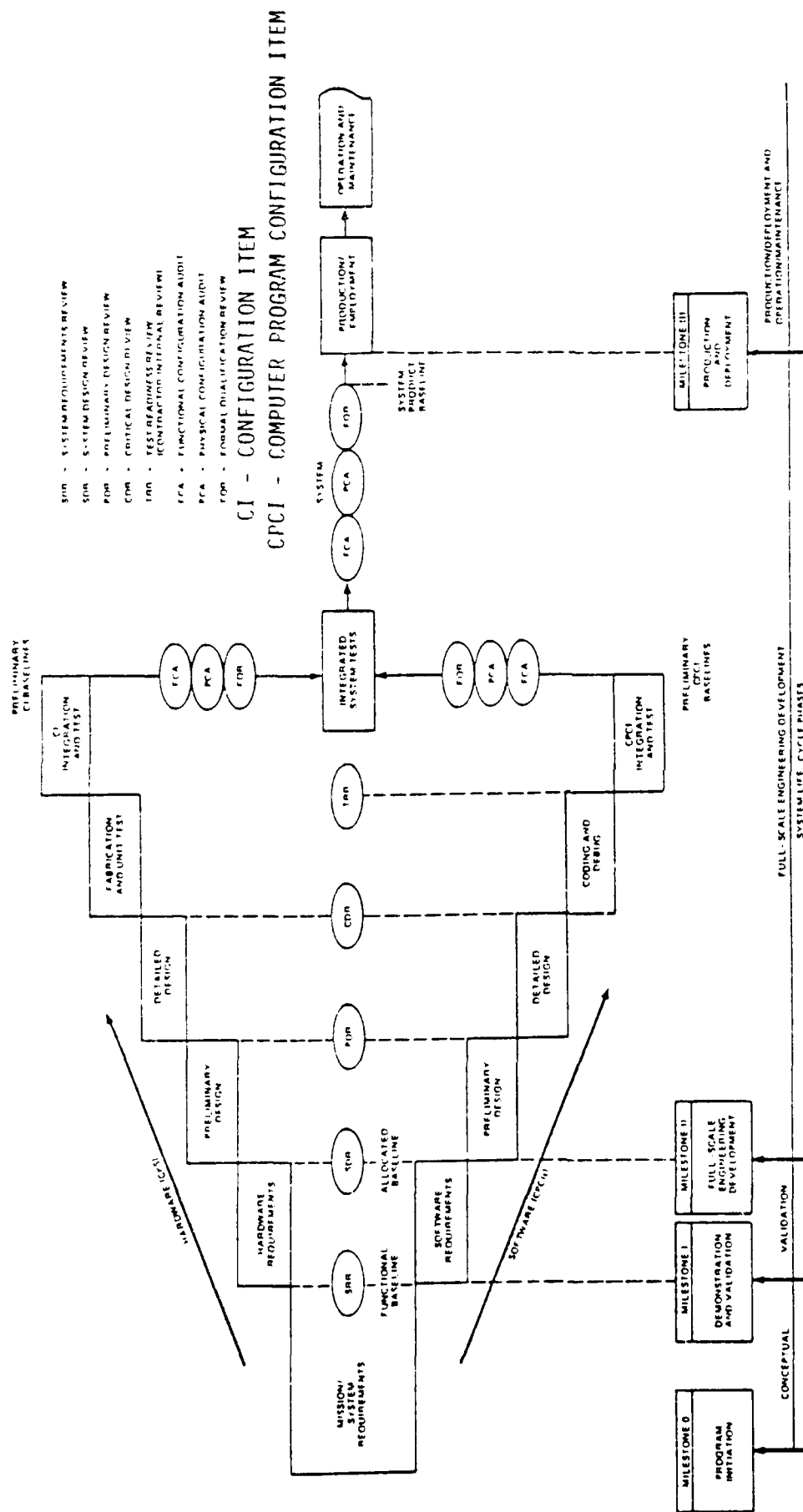
FIGURE 9.1-1: HARDWARE/SOFTWARE SYSTEM LIFE CYCLE RELATIONSHIP

The idea of hierarchy is further developed in Ref. 2 and applied directly to software:

"Now the effect of this relationship, i.e. hierarchy, is profound when you consider system design and reliability. It says that system design time is proportional to the number of levels in the hierarchy used to structure the design. For example, if a designer had to build a system which required 256 elements and he had a choice of building his subassemblies from 16 components and using 2 levels in the hierarchy or using 4 components per subassembly and using 4 levels, he should find that the second structure should take only one half the time to design compared to the first structure. But note the number of specifications that are required. In Figure 9.2-1 the first structure using four components per subassembly requires only 17 descriptions of the relationship of the 16 components to make up a subassembly, whereas the second structure requires 85 descriptions describing a simpler relationship of 4 components required to make up a subassembly. This perhaps explains why our intuition fails us and we choose normally to write 17 specifications; then we rewrite them over and over again instead of 85 specifications which are each 4 times smaller. If we assume that the relative design times are valid, then the level of effort for each of the 17 specifications would be 10 times greater than for any of the 85 specifications used in the first structure ... Similarly the testing and checkout of each subassembly is 10 times more complex instead of our intuitive guess of 4. This is the reason why testing is grossly underestimated for unstructured systems... The problem is that we do not structure our systems into small enough modules."

This idea is portrayed in Figure 9.2-1.

The management of complexity is not unique to software. It is also the heart of the hardware reliability problem. It has been common knowledge for years that hardware reliability is a function of complexity as shown by the expression

$$R = e^{-\sum_{i=1}^{n} \lambda_i t} \tag{9.1}$$

where

R = probability of operation without failure to time, t,

and

λ_i = failure rate of each individual component part

Thus, the more component parts, the higher the probability of failure.

The problem with software reliability is that we have not been able to derive the software equivalent of "the number of component parts."

Another aspect of the software reliability problem has been our inability to easily visualize the dynamic behavior of a program. Consider the program flow chart in Figure 9.2-2. It has 4 blocks of sequential code and 8 decision blocks. Also there are 2 nested loops where the inner can be executed up to 12 times and the outer loop, 2 times. Now this module has 1.6×10^{19} possible ways of traversing through the flow chart. If you tested one path every nanosecond, it
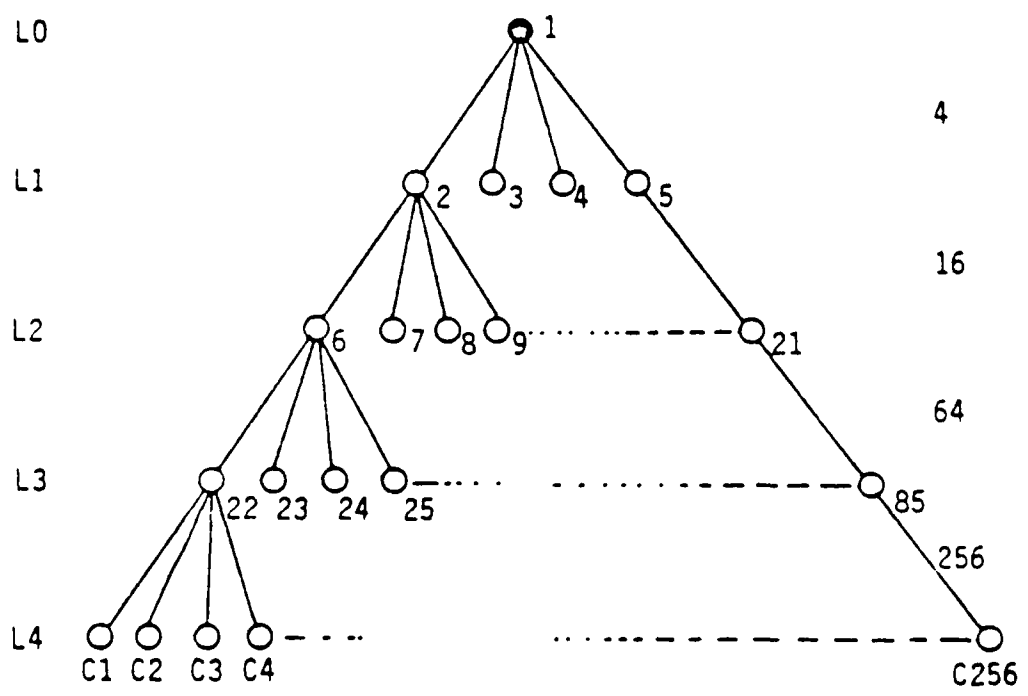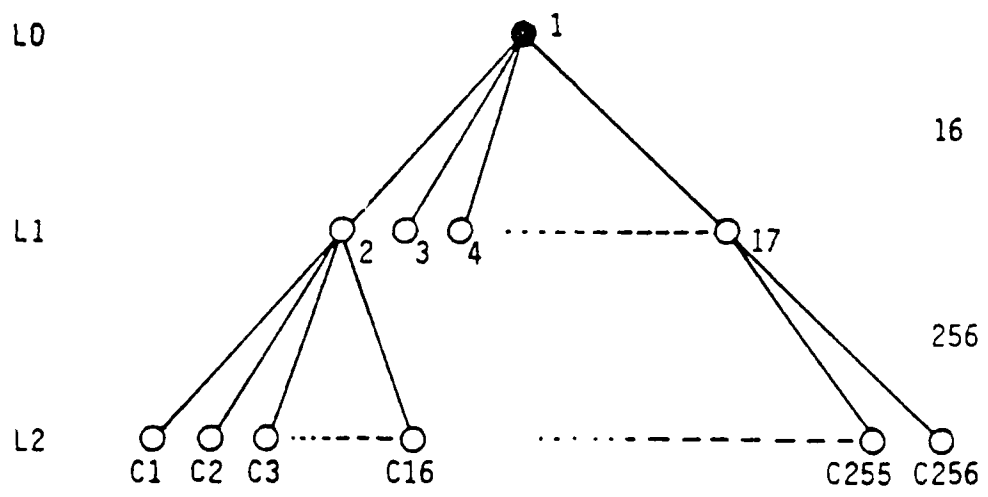
FIGURE 9.2-1: COMPARISON OF TWO ABSTRACT SYSTEMS BY THEIR "STRUCTUREDNESS"
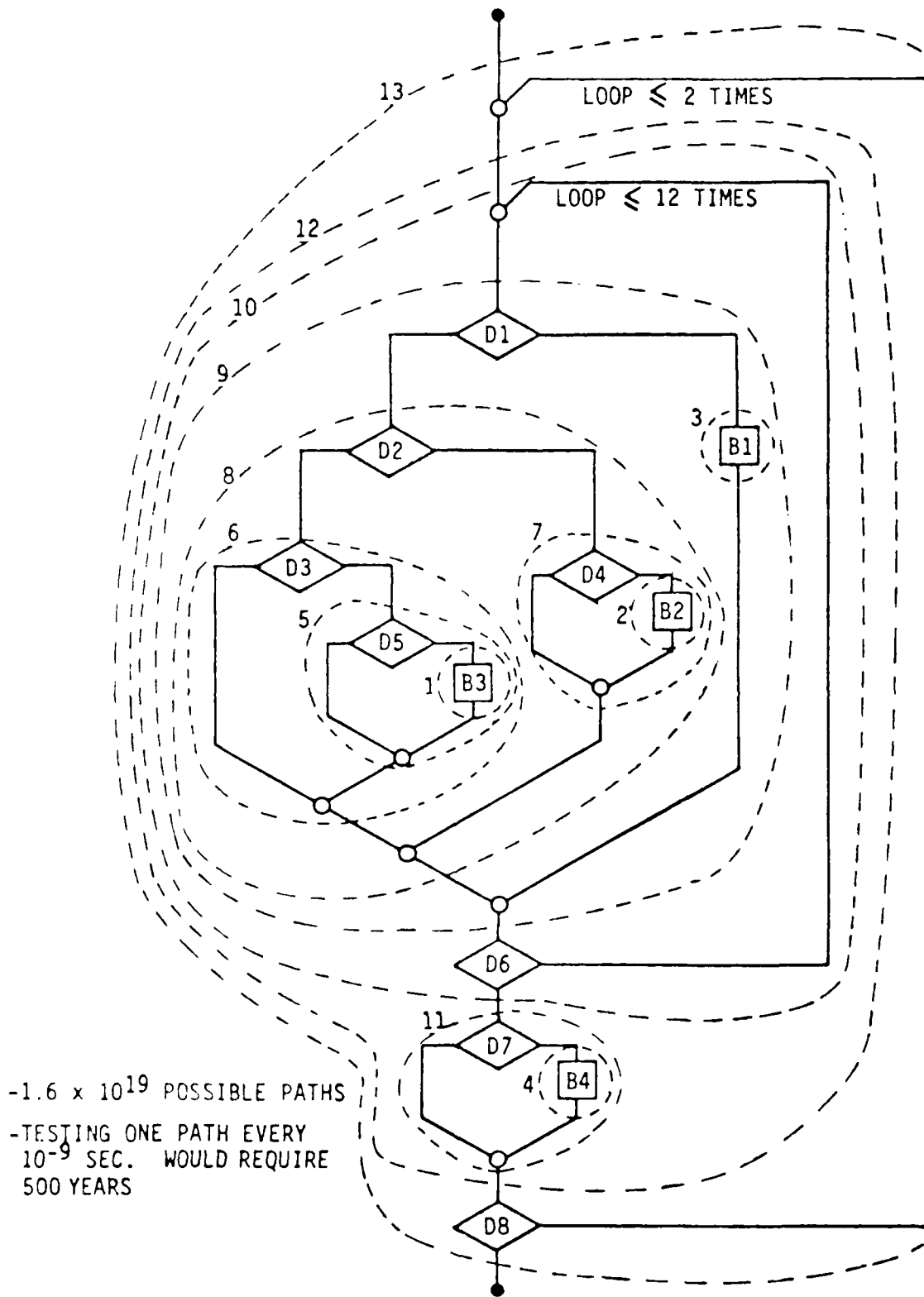
FIGURE 9.2-2: PROGRAM FLOW CHART

would take you over 500 years. Clearly, testing alone will not prove the correctness of this module. The only way in which you can gain confidence in the behaviour of this module is to prove the correctness of each nested substructure. There are 13 blocks nested within each other as shown in the figure. For each block, you must satisfy yourself that for all possible inputs it will generate the correct outputs.

Since each block has a single input and single output, the output from the inner blocks serves as a subset of the outputs or inputs for the outer blocks. Thus only 13 sets of tests have to be derived. Using structured programming techniques the number and difficulty of the proofs is drastically minimized. Only in this way can the reliability of software be achieved in a manageable form.

On the other hand, this testing problem is not unique to software; it is also true of hardware. If one had to test every possible logic path of a typical state-of-the-art microprocessor in order to discover a defective active element, assuming a sampling rate of 10^{-6} seconds, it has been estimated that it would take 2^{17} years.

In an effort to get to the core of the software reliability problem, let us now turn our attention to software errors and their sources.

9.3 SOFTWARE ERRORS AND THEIR SOURCES

Software (also called program) is essentially an instrument for transforming a discrete set of inputs into a discrete set of outputs (see Figure 9.3-1). It comprises a set of coded statements whose function may basically be one of the following:

1. Evaluate an expression and store the result in a temporary or permanent location

2. Decide which statement to execute next

3. Perform input/output operations

Since, to a large extent software is produced by humans, the finished software product is often imperfect. It is imperfect in the sense that a discrepancy exists between what the software can do versus what the user, or the computing environment, wants it to do. The computing environment refers to the physical machine, operating system, compiler and translators, utilities, etc. These discrepancies are what we call software errors (see Figure 9.3-2). Basically, the software errors can be attributed to the following:

1. Ignorance of the user requirements

2. Ignorance of the rules of the computing environment

3. Poor communication of software requirements between the user and the programmer or poor documentation of the software by the programmer

INPUT
DOMAIN

SOFTWARE
(PROGRAM)

OUTPUT
SPACE
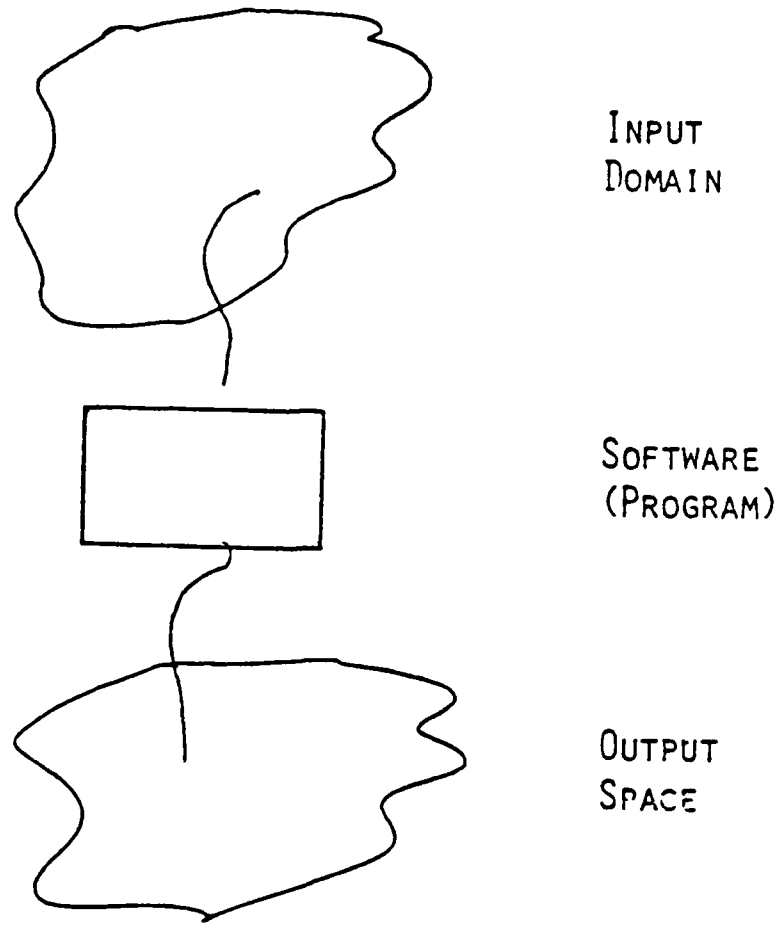
FIGURE 9.3-1: <u>FUNCTIONAL VIEW OF SOFTWARE</u>

SET
AFFECTED BY
ERROR IN
PROGRAM

INPUT
DOMAIN

ERROR
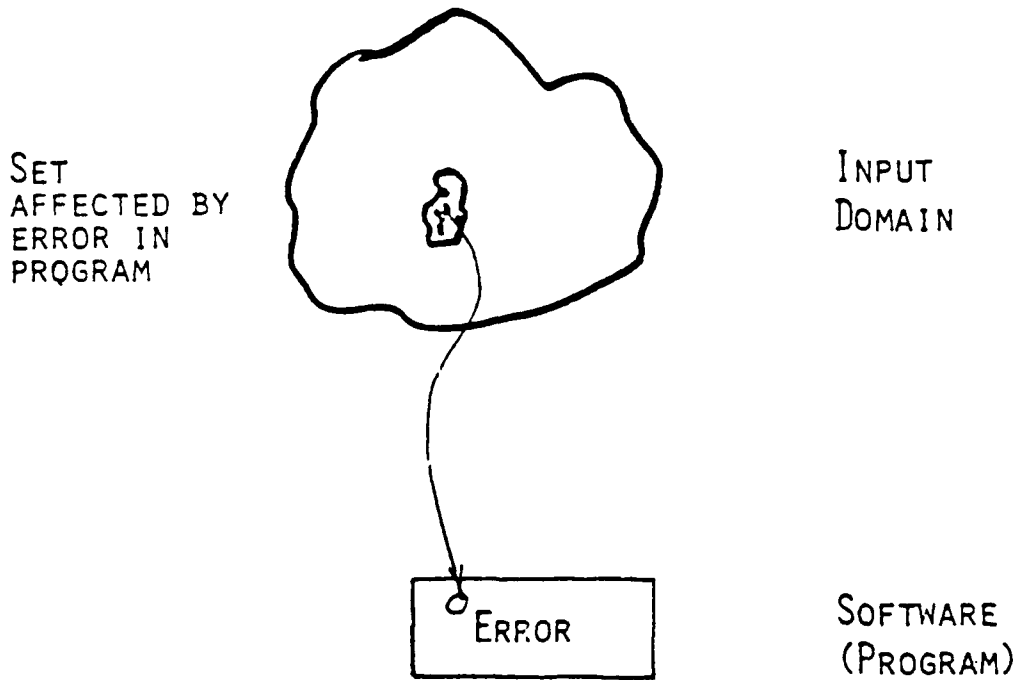
SOFTWARE
(PROGRAM)

FIGURE 9.3-2: SOFTWARE ERROR

The fact of the matter is, even if we know that a software contains errors, we may not known with certainty the exact identity of these errors.

Currently, there are two major paths one can follow to expose software errors:

1. Program proving

2. Program testing.

Program proving is more formal and mathematical, while program testing is more practical, and still remains heuristic in its approach. The approach in program proving is the construction of a finite sequence of logical statements ending in the statement (usually the output specification statement) to be proved. Each of the logical statements is an axiom or is a statement derived from earlier statements by the application of an inference rule. Program proving making use of inference rules is known as the Inductive Assertion Method. Other work on program proving is the work on the Symbolic Execution Method. This method is the basis of some automatic program verifiers. Despite the formalism and mathematical exactness of program proving, it is still an imperfect tool for verifying program correctness. Gerhart and Yelowitz (Ref. 3) showed several programs which were proven to be correct but still contain software errors. The errors were due to failures in defining what exactly to prove and were not failures on the mechanics of the proof itself.

Program testing is the symbolic or physical execution of a set of test cases with the intent of exposing embedded errors (if any) in the program. Like program proving, program testing remains an imperfect tool for verifying program correctness. A given testing strategy is good for exposing certain kinds of errors, but not all possible kinds of errors in a program. An advantage of testing is that it provides accurate information about a program's actual behavior in its actual computing environment; proving is limited to conclusions about the program's behavior in a postulated environment.

Neither proving nor testing can, in practice, guarantee complete confidence on the correctness of programs. Each has its pluses and minuses. They should not be viewed as competing tools. They are, in fact, complementary methods for decreasing the likelihood of program failure (Ref. 4).

9.4 SOFTWARE ERROR CLASSIFICATION

A systematic study of software errors in a program requires knowing what, specifically, these errors are and knowing which tool(s) to use to expose particular types of software errors. Software errors can be grouped as syntax, semantic, runtime, specification and performance errors.

9.4.1 SYNTAX ERRORS

These errors are due to discrepancies between the program code and the syntax rules governing the parser or lexical analyzer of a program translator. These are the easiest errors to detect. They can be

detected by visual inspection of the code or can be detected mechanically during the program compilation process. Experienced programmers rarely commit syntax errors.

9.4.2 SEMANTIC ERRORS

These errors are due to discrepancies between the program code and what the semantic analyzer of the computing environment accepts. Among the popular kinds of semantic errors are typechecking errors and implementation restriction errors. Again, they may be detected by the semantic analyzer of a program translator or by visual inspection.

Syntax and semantic errors are detected during the compilation stage of a program. A program having syntax and/or semantic errors cannot be executed. Syntax and semantic errors are mainly due to the ignorance/negligence on the part of the programmer about the restrictions and limitations of the language (s)he is using.

9.4.3 RUNTIME ERRORS

As the name implies, runtime errors occur during the actual running of a program. They may be further classified into three categories:

Domain Errors

A domain error occurs whenever the value of a program variable exceeds its declared range or exceeds the physical limits of the hardware representing the variable. The declared range of a variable is done implicitly or explicitly. FORTRAN, for example, assigns types to variables based on the variable name or based on a declaration statement. PASCAL requires all variables to be explicitly declared in a declaration statement. PASCAL has facilities to declare ranges by enumeration and/or subsets of numeric domains.

Some program translators produce runtime code for checking certain types of domain errors. Some have built-in recovery features for domain errors (e.g. PL/1, COBOL) and others (e.g. FORTRAN) simply abort execution upon the occurrence of a domain error. Certain compilers, like PASCAL, automatically check for values outside a declared range.

Domain errors are a serious matter because

a) program execution is aborted

b) program results are incorrect

Execution abortion may be fatal, especially in real-time systems. Despite their seriousness, domain errors have never been formally and extensively studied in the literature. This is because detection of domain errors can be very difficult. They require exact specification of the ranges of the input variables. Also, the test values required to expose these errors may occur at the input domain's boundary or inside the input domain itself.

Computational Errors

Computational errors, sometimes known as logic errors, result whenever the program results in an incorrect output. The incorrect output may be due to a wrong formula, an incorrect control flow, assignment to a wrong variable, incorrect parameter passing, etc.

It is not possible to generate runtime code to detect computational errors during program execution. This is because computational errors are really discrepancies between the program's output and the program's specifications.

Computational errors due to incorrect program constructs and statements may be detected by any of the structure dependent or structure independent testing techniques to be discussed in the next section. However, none of these tools can guarantee total absence of these types of computational errors in a program. Computational errors due to missing program constructs and statements may be detected by any of the structure independent testing techniques. Again, none of these tools can guarantee total absence of computational errors due to missing paths.

Non-Termination Errors

Non-Termination error is simply the failure of a program to terminate in finite time without outside intervention. The most common cause of non-termination errors is when the program runs into an infinite loop. Non-termination can also occur if a set of concurrent programs falls into a deadlock.

Infinite loops are detected by simply executing each of the loops in a program. However, this strategy may not guarantee total absence of infinite loops. Some infinite loops may only occur if certain program variables achieve certain values. Program proving may also be used on certain programs to expose infinite loops. The problem of program non-termination, in general, is still an unsolved problem.

9.4.4 SPECIFICATION ERRORS

Presently, detection of specification errors such as:

1. Incomplete specifications

2. Inconsistent specifications

3. Ambiguous specifications

remains an informal process. This is mainly due to the nonexistence of a specification language powerful enough to translate the user requirements into clear, complete and consistent terms.

A testing tool to detect specification errors is yet to be developed.

9.4.5 PERFORMANCE ERRORS

Performance errors exist whenever a discrepancy exists between the actual performance (efficiency) of the program and its desired or specified performance. Program performance may be measured in a number of ways:

1. Response time

2. Elapsed time

3. Memory space usage

4. Working set requirement, etc.

The actual measurement of the above measures of program performance can be a very difficult process. Program complexity theory tries to estimate bounds on the running time of certain program algorithms. Statistical analysis and simulation can also be employed to estimate the above performance variables. However, use of these tools can be very expensive and time consuming.

A performance testing tool that is economical (timewise and costwise) to use is yet to be developed.

The most expensive kind of software errors to eliminate are those which are not discovered until late in the software development, such as when the software becomes operational. These are known as persistent software errors. Glass (Ref. 6) reported that persistent software errors are mostly due to the failure of the problem solution (i.e. the program) to match the complexity of the problem to be solved (i.e. the user requirements). Examples of such errors are computational errors due to missing or insufficient predicates and failure to reset a variable to some baseline value after its use in a functional logic segment. The solution to this software problem is beyond the current state-of-the-art; somehow, the programmer's mind must be extended to encompass complexity beyond its current capability (Ref. 6).

9.5 SOFTWARE RELIABILITY MODELS (REF. 18)

Many studies have been undertaken during the last decade to analyze and study software failure data with the objective of finding ways that will lead to improved software performance. Such studies can be classified into one (or both) of two categories. In the first category, the emphasis is on the analysis of software failure data collected from small or large projects during development and/or operational phases. Studies in the second category are primarily aimed at the development of analytical models which are then used to obtain the reliability and other quantitative measures of software performance.

The analytical modeling work can then be classified into the following two major categories. The first one emphasizes the stochastic nature of software failures, while the second approach uses combinatorial analysis to provide measures of software reliability.

1. Failure (hazard) rate based models

2. Nonfailure rate based models

Failure rate based models can be further classified as shown in Table 9.5-1. This table is not exhaustive but contains the more commonly used failure rate based models for software reliability.

Nonfailure rate based software reliability models can further be classified into:

1. Combinatorial Models

2. Input Domain Based Models

TABLE 9.5-1: TABLE OF FAILURE-RATE BASED SOFTWARE RELIABILITY MODELS

	Classical	Bayesian
Error Count Based Failure Rate Models	De-Eutrophication Process Model of Jelinski-Moranda (Ref. 7)	Littlewood Model (Ref. 8)
	Imperfect Debugging Model (Ref. 9)	
	Linear Function Testing Time Model of Schick and Wolverton (Ref. 10)	
	Parabolic Function Testing Wolverton (Ref. 10)	
	Shooman Model (Ref. 11)	
	Execution Time Model of Musa (Ref. 12)	
	Geometric De-Eutrophication Process Model of Moranda (Ref. 13)	Littlewood and Verrall Model (Ref. 14)
	Geometric Poisson Process Model of Moranda (Ref. 13)	

The list below represents some of the more popular models belonging to the above groups:

Combinatorial Models

1. Mill's Hypergeometric Model (Ref. 15)

2. Binomial Model

Input Domain Based Models

1. Brown and Lipow Model (Ref. 16)

9.5.1 FAILURE RATE BASED MODELS: ASSUMPTIONS

The failure-rate (also known as hazard rate) function $z(t)$ is defined as the conditional probability that an error is exposed in the interval t to $t + dt$, given that the error did not occur prior to time t (Ref. 17). The reliability function $R(t)$ is the probability that no errors will occur from time zero to time t. Further, $z(t)$ and $R(t)$ are related as follows:

$$z(t) = -dR(t)/dt \ /R(t) \qquad (9.2)$$

or

$$R(t) = \exp\left(-\int_0^t z(x)dx\right) \qquad (9.3)$$

The failure rate based models basically differ in their assumption about the failure rate function $z(t)$. Table 9.5.1-1 displays the differences on $z(t)$.

A number of assumptions made by the failure rate based models remain questionable and unrealistic:

1. All the models described above assume that any error detected is immediately corrected. The correction process does not alter the program. All corrections correct the detected error and do not result in the introduction of new errors. It is not hard to accept that correction of a detected error in a program may result in new errors in the program. Goel and Okumoto (Ref. 19) tried to address the second limitation above by formulating the so called Imperfect Debugging Method (IDM). IDM assumes that the number of errors in the system at time t is governed by a Markov process. Time between transitions is exponentially distributed with rates dependent on the current error content of the program. The state transitions are governed by the probability of imperfect debugging. No one has yet addressed the problem in which the debugging process introduces new errors in the software.

2. Models such as those by Jelinski and Moranda, Musa, and Shooman assume that the software failure rate is a constant multiple of the number of remaining errors. This is the same as saying that

TABLE 9.5.1-1: SUMMARY OF FAILURE RATE BASED MODELS

MODEL	ASSUMPTION ON $z(t)$
De-Eutrophication Process Model	The software failure occurrence rate at any time t is assumed proportional to the number of errors remaining in the software, i.e., for the time interval between (i-1)st and ith failure, we have $z(X_i) = \phi \left[N - (i-1) \right]$. N is the initial error content.
Schick-Wolverton Linear Failure Rate Model	Failure rate is assumed proportional to number of remaining errors in software and test time. For ith interval, $Z(X_i) = \phi \left[N - (i-1) \right] (-ax_i^2 + bx_i + c)$ $a,b,c > 0$.
Shooman Model	$Z(\tau) = K \left[E_R/I_T - \int_0^\tau \rho(x)dx \right]$ where: $\quad$ K: proportionality constant $\quad$ E_T: total # errors $\quad$ I_T: total # instructions (object code) $\quad$ τ: debugging time $\quad$ $\rho(x)$: number of errors per instruction at debugging time x $\quad$ $\int_0^\tau (x)dx$: total # of errors per I_T removed during τ time units of debugging time.
Execution Time Model of Musa	$z(\tau) = KfN_0 - Kfn(\tau)$ where: $\quad$ K : error exposure ratio $\quad$ f : linear execution frequency of program $\quad$ N_0: initial error content $\quad$ τ: CPU time utilized in operating the program $\quad$ $n(\tau)$: net number of errors corrected during τ $\quad$ If $dn(\tau)/dt$ = error exposure rate, then $Z(\tau) = KfN_0 \exp(-Kf\tau)$
Geometric De-Eutrophication Process Model of Moranda	Assume that the steps representing the decrease in failure rate between adjacent failure times are geometrically varying. $Z(X_i) = DK^{i-1}$ where: $\quad$ D : initial error detection rate $\quad$ DK: error detection rate after the occurrence of the 1st error. $\quad$. $\quad$ DK^{i-1}: error detection rate after the occurrence of the ith error.

TABLE 9.5.1-1: <u>SUMMARY OF FAILURE RATE BASED MODELS (Cont'd)</u>

<u>MODEL</u>	<u>ASSUMPTION ON $z(t)$</u>
Geometric Poisson Process Model of Moranda	A superposition of a geometric De-Eutrophication process and a Poisson process with parameter $$Z(X_i) = DK^{i-1} + \theta$$
Littlewood and Verrall Model	$z(t) = \lambda$ but λ is treated as a random variable distributed as gamma with shape parameter α and scale parameter Ψ (i), an increasing function of i.
Littlewood Model	$Z(X_i) = \lambda_i$ and λ_i is distributed as gamma $\left[(N-i)\alpha, \beta + \sum_1^{i=1} t_j \right]$, where: $N-i+1$: number of errors remaining when $(i-1)$ failures have occurred. t_j : execution time from $(j-1)$st failure to jth failure. α, β : parameters of gamma distribution
Non-Homogeneous Poisson Process Model of Goel	$$Pr\left\{N(t) = y\right\} = \frac{\left[m(t)\right]^y\, e^{-m(t)}}{y!}$$ $y = 0, 1, 2, \ldots$ where $N(t)$: cumulative number of software errors in time t and $m(t)$: $a(1-e^{-bt})$ = expected number of software failures by time t and $\lambda(t) = abe^{-bt}$ = intensity function (error detection rate) $$R_{X_k}\left|S_{K-1}^{(x/s)}\right. = \exp -\left\{e^{-bs_n} - e^{-b(s_n+x)}\right\}$$ = reliability at time X where s_n represents the cumulative time in which n software failures have occurred a and b can be solved from $$\frac{n}{a} = 1 - e^{-bs_n}$$ $$\frac{n}{b} = as_n\, e^{-bs_n} + \sum_{i=1}^n S_i$$

each error in a given time interval (between failures) has the same chance of being detected. This, obviously, is not true since errors that happen to reside in a portion of the code that is frequently executed by the user (or tested by the user) have a higher probability of being detected. Errors which reside in the unreachable (or never used) portion of the code will obviously have a lower (or zero) probability of being detected. Moranda tried to address this problem by reformulating the De-Eutrophication model into the Geometric De-Eutrophication Model and later to the Geometric Poisson Model. In these variations, the failure rate between adjacent failure intervals is geometrically varying.

3. The Schick-Wolverton models happen to model a process where there is an increasing failure rate between failures. This may be a ridiculous assumption if we argue that software does not wear out. But there can be cases where the software failure rate might in fact increase and this may be attributed to the increased intensity of testing. This phenomenon is usually observed during the early stages of the software development cycle.

4. Basing the time between failures in terms of execution (CPU) time, as was assumed by Musa and Littlewood, may sometimes be unrealistic. An increase in accumulated time between two adjacent failures may not necessarily mean that the software has less and less number of errors or putting it equivalently, that the software's reliability is improving. A very simple example will illustrate this point. Consider a program containing only a single error. The same copy of the program is given to two debuggers. One debugger spends a lot of time running and re-running the program (which can be very tempting to do on on-line and timesharing systems) trying to uncover the error. The second debugger on the other hand spends a lot of time analyzing the program before even attempting to make a test run. Suppose both debuggers are successful in finding the error. What is the resulting reliability of the software? Execution time theory says that since the CPU time between failures of the first software is larger than that of the second software, then the first software is more reliable. We, of course, know that this is not true since both software versions have the same reliability. There still exists controversy on which is the most appropriate time unit to use for interfailure times.

5. Next we consider the assumption of independence of interfailure times. The chances are that this is not a realistic assumption. The testing process that is used to uncover errors is usually not a random process. The time to the next failure may very well depend on the nature and time to failure of the previous error. If the previous error was a very critical one, then we might decide to intensify the testing process and look for more critical errors. This intensification in the testing process may mean a shorter time to next failure than what might have happened if the testing intensity were maintained at normal levels.

6. Most of the models require time between failure data to estimate reliability. There can be cases when the mean time between failure is infinite; as such, these models become useless. The mean time between failure can be infinite if the user of the software has requirements that would only traverse the error free paths of the program.

7. Basing the reliability of the software on the remaining number of errors can also be questionable. A user does not really care whether a software has a certain number of remaining errors. As long as all his requirements are met correctly by the software, then as far as the user is concerned, the software is 100 percent reliable. Littlewood (Ref. 20) argued that a program with two bugs in little exercised portions of code can be more reliable than a program with only one but frequently encountered bug.

8. All the models implicitly assume that the testing process which generated the estimate for the failure rate will be the same as the operating environment. This again is not true. This is why a reliability measure conditioned on the user requirements rather than a simple unconditioned software reliability measure seems more realistic.

9.5.2 NON-FAILURE RATE BASED MODELS: ASSUMPTIONS

Mill's Hypergeometric (Error Seeding) Model:

This model requires that a number of known errors be randomly inserted (seeded) in the program to be tested. The program is then tested for some amount of time. The number of original indigenous errors can be estimated from the number of indigenous and seeded errors uncovered during the test.

Let

n = number of seeded errors
k = number of seeded errors detected during testing
N = total number of indigenous errors
r = number of indigenous errors detected during testing

Then

$$P(k \text{ seeded errors in } r \text{ detected indigenous errors}) = \frac{\binom{n}{k}\binom{N-n}{r-k}}{\binom{N}{r}} \qquad (9.4)$$

$$\text{MLE (maximum likelihood estimate) for } N = \frac{nr}{k} \qquad (9.5)$$

The serious assumption of this model is that the indigenous and seeded errors have the same probability of being detected.

Binomial Model:

Let

$$q_i = p_r \text{ (errors) on each run of } i$$

then

$$Pr(x \text{ errors in } y \text{ trials}) = \binom{y}{x} q_i^x (1-q_i)^y \qquad (9.6)$$

Again, the serious assumption is that all errors have an equal weight or chance of being exposed.

Brown & Lipow Model:

Let

n_e = number of inputs for which execution failures occurred

n = number of test cases

R = reliability

Then

$$R = 1 - \frac{n_e}{n} \qquad (9.7)$$

Again the serious assumption is the equal probability of choosing n_e from n.

Refs. 21 and 22 contain additional information on and discussion of software reliability models.

9.6 EXAMPLES OF CALCULATIONS USING SOFTWARE RELIABILITY MODELS (REF. 5)

9.6.1 THE MUSA MODEL

The Musa model (Ref. 12) uses program execution time as the independent variable. A simplified version of the Musa model is:

$$n = N_0 \left[1 - \exp\left(\frac{-Ct}{N_0 T_0} \right) \right] \qquad (9.8)$$

where N_0 is the inherent number of errors, T_0 the MTTF at the start of testing (MTTF is mean time to failure) and C the "testing compression factor" equal to the ratio of equivalent operating time to testing time.

The present MTTF

$$T = T_0 \exp\left(\frac{Ct}{N_0 T_0}\right)$$

gives

$$R(t) = \exp\left(\frac{-t}{T}\right) \tag{9.9}$$

From these relationships we can derive the number of failures which must be found and corrected, or the program execution time necessary, to improve from T_1 to T_2:

$$\Delta_n = N_0 T_0 \left(\frac{1}{T_1} - \frac{1}{T_2}\right) \tag{9.10}$$

$$\Delta_t = \left(\frac{N_0 T_0}{C}\right) \ln\left(\frac{T_2}{T_1}\right)$$

Example 9.1

A large program is believed to contain about 300 errors and the recorded MTTF at the start of testing is 1.5 hours. The testing compression factor is assumed to be 4. How much testing is required to reduce the remaining number of errors to ten? What will then be the reliability over 50 hours running?

From Eq (9.10 and 9.11)

$$\Delta n = (300 - 10) = 300 \times 1.5 \left(\frac{1}{1.5} - \frac{1}{T_2}\right)$$

$$T_2 = 45 \text{ hours}$$

$$\Delta t = \left(\frac{300 \times 1.5}{4}\right) \ln\left(\frac{T_2}{1.5}\right)$$

$$\Delta_t = 382.6 \text{ hours}$$

giving

$$R_{50} = \exp\left(\frac{-50}{45}\right) = 0.33$$

9.6.2 THE MILLS MODEL

A different approach to software reliabilty prediction has been proposed by Mills (Ref. 15). This is a more pragmatic approach, rather than an attempt to derive a mathematical time-based model. A known number of errors are deliberately introduced into the program. As the debugging (inspection and/or test) is carried out, the record shows which of the "seeded" errors are discovered. The number of remaining unknown errors

is then assumed to be a function of the ratio of discovered to remaining seeded errors:

$$n = N_0 \left[1 - \exp \left(\frac{-n_s}{N_s - n_s} \right) \right] \qquad (9.12)$$

where N_s is the total number of seeded errors and n_s is the number of seeded errors remaining.

Example 9.2

Experience indicates that a program is likely to contain about 100 errors at the start of validation. Ten errors are deliberately seeded, as far as can be arranged at random. Nine of these are discovered at the end of validation. How many of the original number of errors are likely to remain?

$$100 \left[1 - \exp \left(- \frac{1}{10 - 1} \right) \right] = 10.5$$

i.e. about 10 or 11 errors.

The Mills approach avoids the problem of time. However, the practical disadvantages of having to stop testing to correct deliberate errors are obvious. To be a valid predictor of the number of remaining errors, the seeded errors must be the same kinds of errors, and in the same proportion, as the original ones. The method is probably more appropriate for coding errors, since the seeding of specification and design errors is not as straightforward. However, the Mills approach has not been accepted as being practical for typical programs, despite its similarity to methods used for checking the ability of test routines to diagnose deliberately induced faults in hardware.

9.6.3 LITTLEWOOD MODELS

Littlewood (Refs. 8 and 22) attempts to take account of the fact that different program errors have different probabilities of causing failure. If ϕ_1, ϕ_2, ... ϕ_N are the rates of occurrence of errors 1,2,...N, the pdf (probability density function) for the program time to failure, after the ith error has been fixed, is

$$f(t) = \lambda \exp (-\lambda t) \qquad (9.13)$$

where λ is the program failure rate

$$\lambda = \phi_1 + \phi_2 + \dots \phi_N - i$$

ϕ is assumed to be gamma distributed, i.e. errors do not have constant rates of occurrence, but rates which are dependent upon program usage.

If the gamma distribution parameters are (α, β), then it can be shown, using Bayes approach, that:

$$f(t) = \frac{(N - 1)\,\alpha\,(\beta + t')^{(N - i)\alpha}}{(\beta + t' + t)^{(N - 1)\,\alpha + 1}} \qquad (9.14)$$

where t' is the time taken to detect and correct i errors. From which

$$R(t) = \left.\frac{\beta + t'}{\beta + t' + t}\right.^{(N - i)\alpha} \qquad (9.15)$$

and

$$\lambda(t) = \frac{(N - i)\alpha}{\beta + t' + t} \qquad (9.16)$$

At each error occurrence and correction, $\lambda(t)$ falls by an amount $\alpha/(\beta + t')$. It is assumed that all detected errors are corrected, without further errors being introduced.

Example 9.3

A large program is assumed to include a total of 300 errors, of which 250 have been detected and corrected in 20 hours of execution time. Assuming the Littlewood model holds, and the distribution parameters are $\alpha = 0.005$, $\beta = 4$, what is the expected reliability over a further 20 hours?

From Eq. (9.15)

$$R(20) = \left(\frac{4 + 20}{4 + 20 + 20}\right)^{(300 - 250)0.005}$$

$$= 0.86$$

9.6.4 GOEL NHPP MODEL (REF. 18)

It is assumed that errors can exist randomly in a code structure, and that their appearance is a function of the time the program is run. The number of errors occurring in time t is N(t). If the following conditions exist:

1. $N(0) = 0$
2. not more than one error can occur in the time interval (t, t + dt)
3. the occurrence of an error is independent of previous errors

then the occurrence of errors is described by the nonhomogeneous Poisson distribution:

$$P\left[N(t) = n\right] = \frac{\left[m(t)\right]^n}{n!}\,\exp\left[-m(t)\right] \qquad n \geq 0 \qquad (9.17)$$

where

$$m(t) = \int_0^t \lambda(s)\ ds$$

$m(t)$ is the mean (s-expected) number of errors occurring in the interval $(0, t)$.

$$m(t) = a\left[1 - \exp(-bt)\right] \tag{9.18}$$

where a is the total number of errors and b is a constant.

and a and b can be calculated from the expressions

$$\frac{n}{a} = 1 - e^{-bS_n} \tag{9.19}$$

$$\frac{n}{b} = a\ S_n\ e^{-bS_n} + \sum_{i=1}^{n} S_i \tag{9.20}$$

where S_n represents the cumulative time in which software failures have occurred.

The number of errors remaining at time t, assuming that each error which occurs is corrected without the introduction of others, is

$$\bar{N}(t) = a\ e^{-bt} \tag{9.21}$$

The reliability function, after the most recent error occurs and is corrected at time s, is

$$R(t) = \exp\left[\left[-a\left\{\exp(-bs) - \exp\left[-b(s + t)\right]\right\}\right]\right] \tag{9.22}$$

Example 9.4

Consider the first 26 data points of Table 9.6.4-1, for which n = 26 and $S_n = S_{26} = \sum_{k=1}^{26} xk = 250$ days. Substituting the appropriate values from Table 9.6.4-1 into Eqs. (9.19) and (9.20) we get

$$\frac{26}{a} = 1 - e^{-b(250)} \tag{9.23}$$

$$\frac{26}{b} = a(250) \cdot e^{-b(250)} + \sum_{i=1}^{w} S_i \tag{9.24}$$

Solving Eqs. (9.22) and (9.23) numerically, we get

$$\hat{a} = 33.99 \approx 34$$

$$\hat{b} = 0.00579$$

and

$$\hat{m}(t) = \hat{a}\ (1 - e^{-6t})$$

TABLE 9.6.4-1: SOFTWARE FAILURE DATA

Error No.	Time Between Failures x_k, days	Cumulative Time $s_n = \Sigma\, x_k$, days
Production (Checkout Phase)		
1	9	9
2	12	21
3	11	32
4	4	36
5	7	43
6	2	45
7	5	50
8	8	58
9	5	63
10	7	70
11	1	71
12	6	77
13	1	78
14	9	87
15	4	91
16	1	92
17	3	95
18	3	98
19	6	104
20	1	105
21	11	116
22	33	149
23	7	156
24	91	247
25	2	249
26	1	250
Test Phase		
27	87	337
28	47	384
29	12	396
30	9	405
31	135	540
User Phase		
32	258	798
Test Phase		
33	16	814
34	35	849

$$= 34(1 - e^{-0.00579t}) = 26 \text{ at } 250 \text{ hours}$$

the expected number of failures remaining at 250 hours is given by (9.21) as

$$\overline{N}(t) = \hat{a}e^{-bt} = 34e^{-0.00579(250)} = 8$$

this could also have been solved from

$$\overline{N}(t) = a - \hat{m}(250) = 34 - 26 = 8$$

the reliability function at 300 hours is given by (9.22)

$$R(t) = \exp\left[\left[-a\ \left\{\exp(-250)(0.00579) - \exp\left[-0.00579(300)\right]\right\}\right]\right]$$

$$= \exp\left[-34\ (0.235 - 0.176)\right]$$

$$= e^{-34(0.059)} = 0.135$$

9.7 APPROACHES FOR ENHANCING SOFTWARE RELIABILITY

9.7.1 SPECIFICATIONS (REF. 35)

It was previously pointed out that specification errors represent more than half of the software errors generated. The thorough specification of a large software system cannot be by a single specification alone. In fact, a series of timely specifications is required and they must be developed in a logical sequence, suggested by Figure 9.7.1-1. The milestones in the process of specification development are a series of design reviews known individually as SRR, SDR, PDR, and CDR.

SRR System Requirements Review
SDR System Design Review
PDR Preliminary Design Review
CDR Critical Design Review
FQR Formal Qualification Review
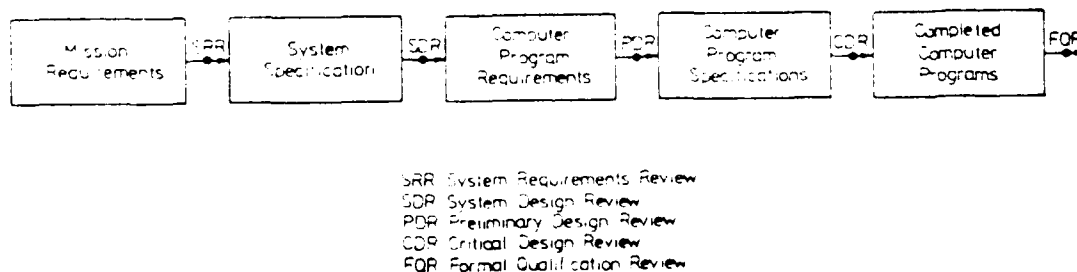
FIGURE 9.7.1-1: SIMPLIFIED SPECIFICATION MODEL

The system specifications are determined after the System Requirements Review (SRR) and are reviewed at the System Design Review (SDR). Computer program requirements are then developed, refined and reviewed during the Preliminary Design Review (PDR). Computer program specification are written and discussed at length during the Critical Design Review (CDR). Permission to proceed with the implementation is given, the computer programs are completed, and a Formal Qualification Review (FQR) is held.

The important point to note is that at each stage the specifications are reviewed in progressively increasing detail by both the customer and

developer so that the direction of development is clear to both parties, and always there exists an approved specification.

The contents of specifications will vary with the nature of the software system to be developed. This is discussed in a later section under Documentation.

9.7.2 DESIGN

The most effective design technique to deal with the hierarchical problem is known as "top down design." Proceeding from an approved software specification the top down approach provides a systematic design methodology that leads to the development of a system structure which can cope with inherent system complexity in an effective and readily understandable way. A brief description of the technique is given in (Ref. 24) as follows:

"(a) Starting with the problem statement (or functional or external specification), design the structure of the entire program or system using one or more forms of analysis. Note that when designing a system (a collection of related programs), an intermediate step is usually necessary. Before the system can be decomposed into modules, it must be decomposed into independent programs, or components...

(b) Review the completed structural design, trying to maximize module strength and to minimize coupling.

(c) Review the design again, using the guidelines of ..... decision structure, input/output isolation, restrictive modules, data access, size, recursion, predictable behaviour..."

Guidelines outlining the methods of decomposition that can be applied to software are given in (Refs. 24 and 25).

Upon identification of the system's various levels of abstraction and of the connections between them, top down design achieves a decomposition of the system into a number of highly independent modules, resulting in a significantly simpler structure.

When the decomposition has been completed a structure similar to Figure 9.7.2-1 should have been achieved.

Arriving at the final structure is a highly iterative technique greatly aided by the Hierarchy, plus Input, Process, Output (HIPO) method fully described in Ref. 26. The end product is a HIPO diagram for each module starting, as in Figure 9.7.2-1, with module 1.0 and proceeding downward until all modules have a HIPO diagram. An example of a completed HIPO diagram is shown in Figure 9.7.2-2.

It may appear as though a detailed HIPO chart prepared for a module would be sufficient to present to a programmer for coding. This is not necessarily the case and represents a narrow application of the HIPO chart, which is intended as a design aid in defining a software system
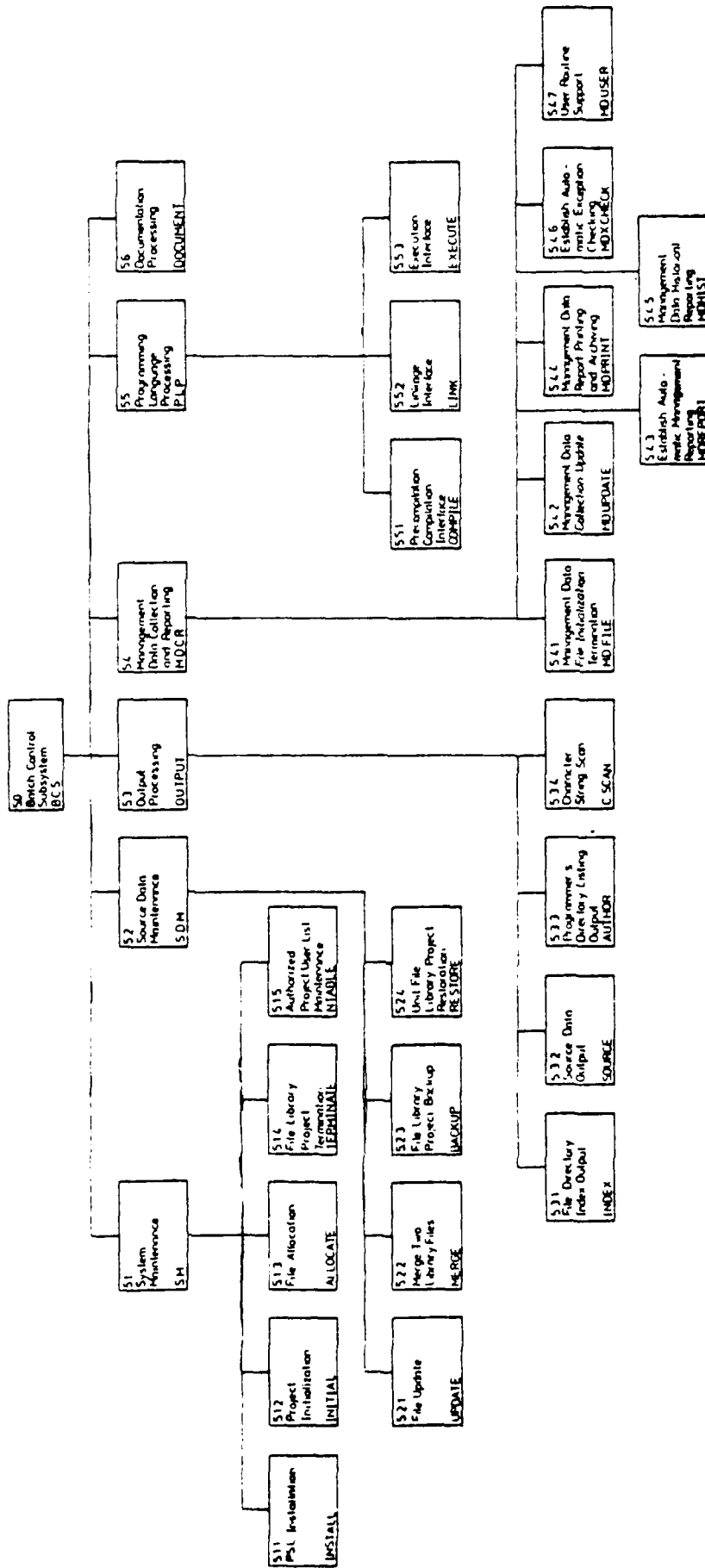
FIGURE 9.7.2-1: DECOMPOSED SOFTWARE SYSTEM
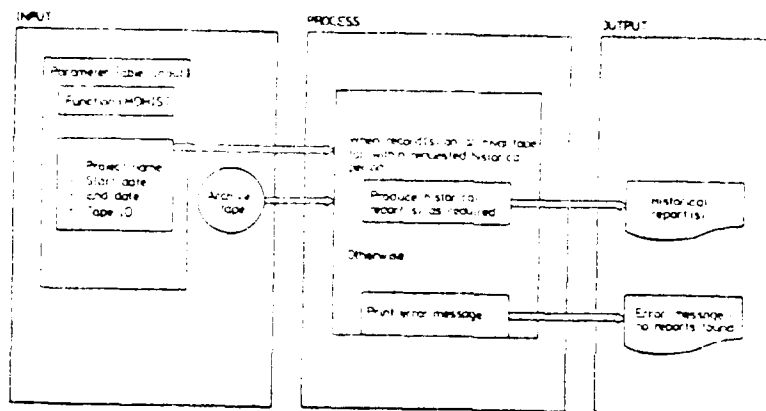
FIGURE 9.7.2-2: HIGH LEVEL HIPO CHART

via a topdown approach to design. Module specifications based on HIPO charts are still recommended for formally documented systems.

At this point, a comment on module size would be appropriate. The recommended finished module size is 10 to 100 high level statements (Ref. 27) which should fit, approximately, on one page about 11 inches long.

The top down approach may also be used to check out the consistency of module specifications before coding them. This is done by "stubbing" the system with a simulation program which, externally, looks like the real program. Using top down decomposition, one begins by specifying overall functions to be performed; then one determines how these general functions are accomplished by more specific functions. The process is repeated until specific functions, which can be accomplished by a single module, are derived. Module specifications are checked directly from the top-down decomposition.

Of the major advantages attributed to the top-down approach, the following are particularly significant to enhancing software reliability & maintainability:

    (a) Emphasis is no longer placed on program implementation and coding, but rather on system design, by far the most critical software development phase.

    (b) Effective modularity of the system can be achieved from the fact that common functions to be performed are identified early enough in the design,

    (c) Modules may be tested at each successive level of development, which greatly simplifies debugging and guarantees program correctness as it proceeds, not as an afterthought following completion of the coding effort.

9.7.3 PROGRAMMING

Software structure is important to reliability, as a well structured program makes program writing and testing easier. It enables changes to be made more easily, so the program is easier to correct or modify. What is a well structured program?

Structured programming (also called modular programming) breaks the program requirement down into separate, smaller program requirements, or modules, each of which can be separately specified, written and tested. The overall problem is thus made easier to understand and this is a very important factor in reducing the scope for error and for easing the task of checking. The separate modules can be written and tested in a shorter time, thus reducing the chances of changes of programmer in mid stream.

Each module specification must state how the module is to interface with other parts of the program. Thus, all the inputs and outputs must be specified. Structured programming (SP) might involve more preparatory work in determining the program structure, and in writing module specifications and test requirements. However, like good groundwork in any development program, this effort is likely to be more than repaid later by the reduced overall time spent on program writing and debugging, and it will also result in a program which is easier to understand and to change.

The early concepts of structured programming were based on three basic software constructs, i.e., Sequence, IF THEN, DO WHILE. These basic structures have evolved into the six now in common use, illustrated in Figure 9.7.3-1 and defined as follows:

(a) Concatenation - statements are executed in the order in which they appear, with control passing unconditionally from one statement to the next. This hardly requires explaining, but is necessary for the construction of a block from statements that are to be executed sequentially.

(b) IF c DO s - the condition c is tested. If c is true, the statement is executed; otherwise, s is not executed, control passes to the next statement. Note that the statement s may itself be a block, or it may be a simple statement. This is true in each of the program constructs, wherever a statement can appear.

(c) IF c THEN a ELSE b - the condition c is tested. If c is true, the statement a is executed and the statement b is skipped; otherwise, the statement a is skipped and the statement b is executed.

(d) WHILE c DO s - the condition c is tested. If c is true, the statement s is executed and control returns to the beginning for another test of c. If c is false, then s is skipped and control passes to the next statement.

(e) REPEAT s UNTIL c - the statement s is executed and then the condition c is tested. If c is false, control returns to s for another iteration. If c is true, control passes to the next statement.
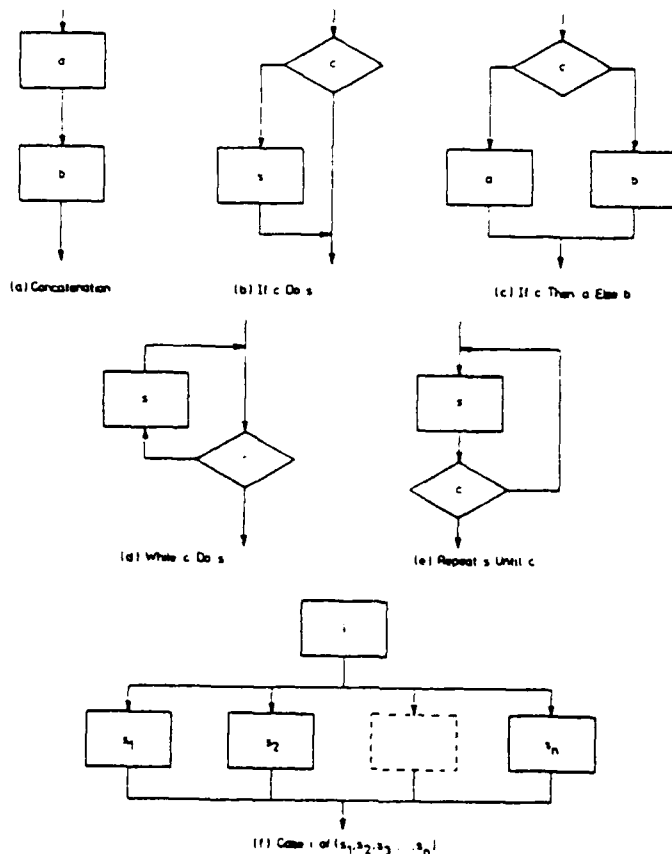
FIGURE 9.7.3-1: STRUCTURED PROGRAMMING CONSTRUCTS

(f) CASE i OF $(s_1, s_2 ..., s_n)$ - the ith statement of the set $(s_1, s_2 ..., s_n)$ is executed, and all other statements of this set are skipped. Control passes to the next statement (following s).

A structured program consists of a sequence of the structures described above and therefore will be highly readable, testable and maintainable. The principles of SP have been developed along similar lines by a number of authors (Refs. 29, 30, and 31), but the basic result is always a disciplined and controlled method of programming. Specific applications of SP to different programming languages are given in Refs. 32, 33, and 34.

The capability of a program to be modified fairly easily can be compared to the maintainability of hardware, and it is often a very important feature. Program changes are necessary when logical corrections have to be made, or when the requirements change, and there are not many software development projects in which these conditions do not arise.

The optimum size of a module depends upon the function of the module, and is not solely determined by the number of program elements. The size will usually be determined to some extent by where convenient interfaces can be introduced. As a rule of thumb, modules should not normally exceed 100 separate statements or lines of code in a high level language.

9.7.4 PROGRAM TESTING

The testing of programs is divided into two phases, i.e., debugging and integration.   In the debugging phase, a module is tested against its specification, while in the integration phase modules are tested as a group against a group specification and so on, until finally the software system is tested against its system specification.

When structured programming is used, a significant degree of program correctness is built in before debugging begins.   Module testing is therefore oriented primarily toward testing that all branches of each program can be properly entered and exited.   Results are precalculated and tested for both sensible and nonsensible input data.   Test cases for module level testing are defined using a simple networking technique, as shown in Figure 9.7.4-1.   This ensures that all paths between decision points are tested at least once, so that, when delivered to integration, the routine will not fail under any circumstance.   The total number of individual tests required is a function of the program complexity.
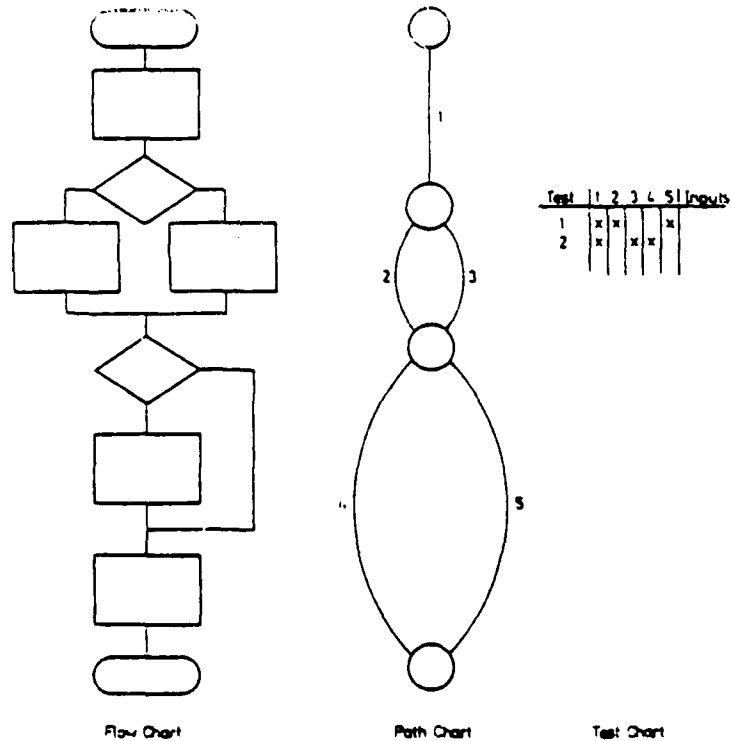
FIGURE 9.7.4-1: TEST PATH TRACING

Top down design assures that proper interfaces and program module compatibility are built into the software design. The purpose of top down integration is to validate that part of the design. The top level modules are integrated first, using simple program stubs to represent lower level modules; lower level modules are then successively integrated, again using the program stubbing technique. Test cases are designed to test each module in its operating environment. At the end of integration testing, all program units operate compatibly in their operational environment. Each stub replaced by a deliverable module represents a measurable milestone.

Based upon analysis of system and software requirements, a set of test scenarios, which exercise the integrated software in all operating modes and ranges of input data, is defined. The software is then qualified by testing with those scenarios to ensure that all performance requirements are satisfied.

Further information on program test methods will be found in Refs. 36 and 37.

9.7.5 DOCUMENTATION

As has been pointed out, software systems evolve in phases from concept through to operation. Reference 38 provides a global approach to the problem of documentation, throughout the various phases and the stages within these phases. The three phases applicable to the software life cycle are: Initiation, Development and Operation. The Development phase is further subdivided into four stages, i.e., Definition, Design, Programming, and Test. In addition each stage will have associated with it one or more documents. Table 9.7.5-1 summarizes the above and definitions follow:

TABLE 9.7.5-1: DOCUMENTATION WITHIN THE SOFTWARE LIFE CYCLE

Initiation Phase	Development Phase				Operation Phase
	Definition Stage	Design Stage	Programming Stage	Test Stage	
	Functional Requirements Document	System/Subsystem Specification	Users Manual		
		Program Specification	Operations Manual		
	Data Requirements Document	Data Base Specification	Program Maintenance Manual		
	Test Plan	Test Plan	Test Analysis Report		

Phases

Initiation - the objectives and general definition of the requirements for the software are established. Feasibility studies, cost benefit analyses, and the documentation prepared within this phase are determined by agency procedures and practices.

Development - the requirements for the software are determined and the software is then defined, specified, programmed, and tested. Documentation is prepared within this phase to provide an adequate record of the technical information developed.

Operation - the software is maintained, evaluated, and changed as additional requirements are identified.

Stages

Definition - the requirements for the software and documentation are prepared. The Functional Requirements and the Data Requirements Document may be prepared.

Design - the design alternatives, specific requirements, and functions to be performed are analyzed and a design is specified. Documents which may be prepared include the System/Subsystem Specification, Program Specification, Data Base Specification, and Test Plan.

Programming - the software is coded and debugged. Documents which may be prepared during this stage include the Users Manual, Operations Manual, Program Maintenance Manual, and Test Plan.

Test - the software is tested and related documentation reviewed. The software and documentation are evaluated in terms of readiness for implementation. The Test Analysis Report may be prepared.

Some of the documents listed in Table 9 7.5-1 specify the use of flowcharts. There is an argument that with top down design, structured programming and commented code, flowcharts may no longer be required.

Document Types

Functional Requirements Document - the purpose is to provide a basis for the mutual understanding between users and designers of the initial definition of the software, including the requirements, operating environment, and development plan.

Data Requirements Documents - the purpose is to provide, during the definition stage of software development, a data description and technical information about data collection requirements.

System/Subsystem Specification - the purpose is to specify, for analysts and programmers, the requirements, operating environment, design characteristics, and program specifications (if desired) for a system or subsystem.

Program Specification - the purpose is to specify, for programmers, the requirements, operating environment, and design characteristics of a computer program.

Data Base Specification - the purpose is to specify the identification, logical characteristics, and physical characteristics of a particular data base.

Users Manual - the purpose is to describe the functions performed by the software in non-ADP terminology, such that the user organization can determine its applicability, and when and how to use it. It should serve as a reference document for preparation of input data and parameters and for interpretation of results.

Operations Manual - the purpose is to provide computer operating personnel with a description of the software and of the operational environment so that the software can be run.

Program Maintenance Manual - the purpose is to provide the maintenance programmer with the information necessary to understand the programs, their operating environment, and their maintenance procedures.

Test Plan - the purpose is to provide a plan for the testing of software; detailed specifications, descriptions, and procedures for all tests; and test data reduction and evaluation criteria.

Test Analysis Report - the purpose is to document the test analysis results and findings, present the demonstrated capabilities and deficiencies for review, and provide a basis for preparing a statement of software readiness for implementation.

It is rather obvious that all the documents listed in Table 9.7.5-1 from Reference 39 also provide scoring criteria to determine those that should apply to any software project. In addition, detailed guidelines are offered for each of the ten document types listed above. Other documents (Refs. 39, 40) offer guidance in the area of software systems documentation.

With respect to the top down approach, the resulting system modularity leads to well structured documentation whereby design structures and program modules can be documented accurately and fully as development progresses. This ensures that, at the design level, none of the original intent of the system purpose is lost during the development process; in addition, good communication is established from the design to the program implementation process, such that better software reliability can be achieved. Furthermore, complete and accurate documentation that can communicate a good understanding of each module, within the framework of the overall system, together with a detailed description of its internal logic, will effectively guarantee the attainment of adequate software maintainability.

9.7.6 A GENERAL METHODOLOGY FOR SOFTWARE FAILURE DATA ANALYSIS

A step-by-step procedure for software failure data analysis is shown in Figure 9.7.6-1 and described below

Step 1: Study the failure data.

The models previously described assume that the failure data represents the data collected after the system has been integrated and the number of failures per unit time is statistically decreasing. If, however, this is not the case, these models may not yield satisfactory results. Furthermore, adequate amount of data must be available to get a satisfactory model. A rule of thumb would be to have at least twenty data points.

Step 2: Obtain estimates of parameters of the model.

Different methods are generally required depending upon the type of available data. The most commonly used ones are the least squares and maximum likelihood methods.

Step 3: Obtain the fitted model.

The fitted model is obtained by first substituting the estimated values of the parameters in the postulated model. At this stage, we have a fitted model based on the available failure data.

Step 4: Perform goodness-of-fit test.

Before proceeding further, it is advisable to conduct the Kolmogorov-Smirnov goodness-of-fit test or some other suitable test to check the model fit.

If the model fits, we can move ahead. However, if the model does not fit, we have to collect additional data or seek a better, more appropriate model. There is no easy answer to either how much data to collect or how to look for a better model. Decisions on these issues are very much problem dependent.

Step 5: Computer confidence regions.

It is generally desirable to obtain 80%, 90%, 95%, and 99% joint confidence regions for the parameters of the model to assess the uncertainty associated with their estimation.

Step 6: Obtain performance measure.

At this stage, we can compute various quantitative measures to assess the performance of the software system. Several useful measures and expressions are shown in Figure 9.7.6 -1. Confidence bounds can also be obtained for these measures to evaluate the degree of uncertainty in the computed values.
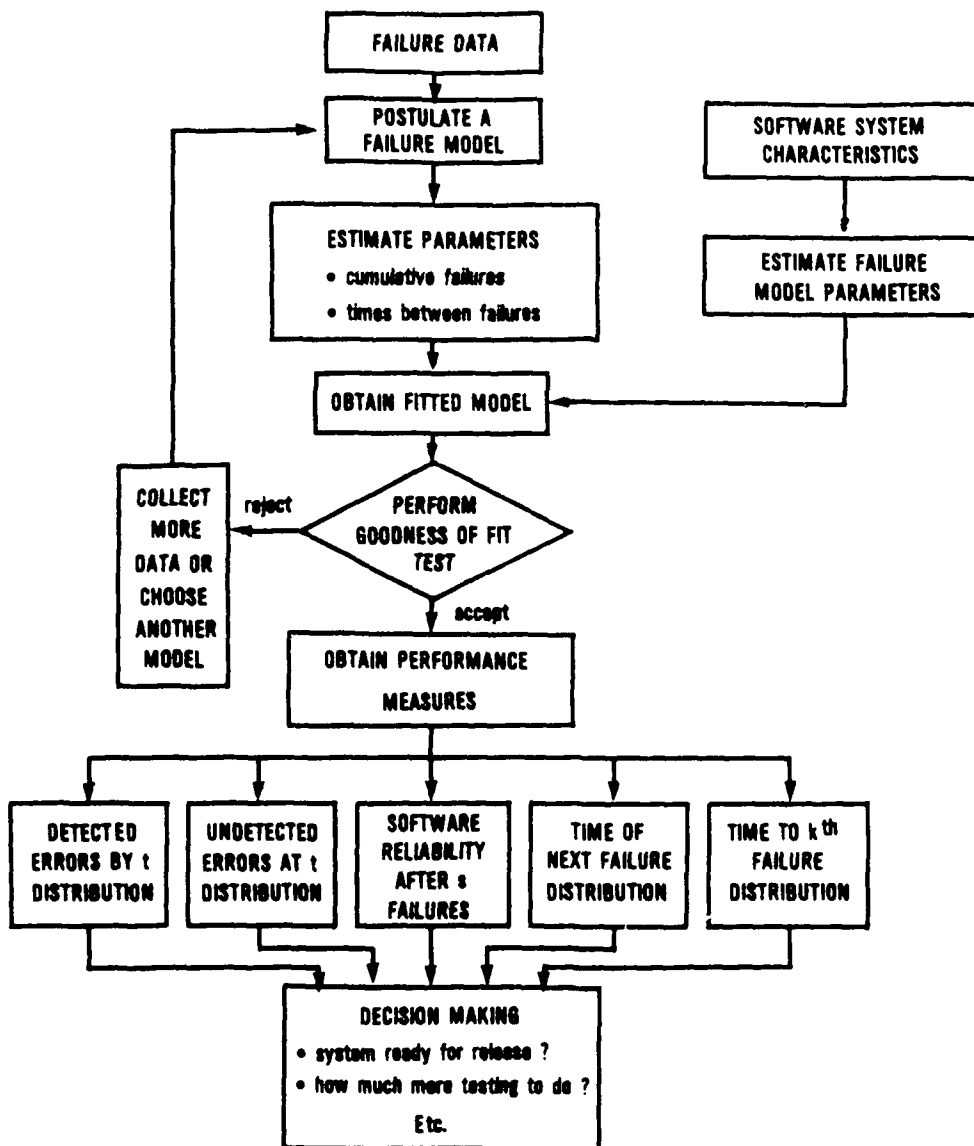
FIGURE 9.7.6-1

FLOWCHART FOR SOFTWARE FAILURE DATA ANALYSIS
AND DECISION-MAKING

9.7.7 MANAGEMENT

Computer programming, not surprisingly, offers an opportunity for a psychological study of the process (Ref. 41). In any case the objective is to obtain reliable and maintainable software.

Organization

A team approach to a project has been found to be an effective way to obtain reliable and maintainable software. This idea has been developed (Ref. 42) and is known generally as the Chief Programmer Team (CPT) approach. This approach offers a disciplined alternative to the seemingly unorganized generation of software. It moves the associated problems from the private to the public domain where they can be recognized early and solved appropriately. Figure 9.7.7-1 shows one such organization structure and is repeated as often as required to match the demands of the system under development.

The Chief Programmer is the key person on the team. He is the team leader, both administratively and technically. He is responsible for completing the software within cost and within schedule, and has approval authority for all aspects of software development. His administrative role is lessened by the Programming Secretary and the Product Coordinator. He has technical responsibility for the overall software design and for design, programming and testing of the software system. His job input is the overall software System Requirement Specification. His first output is a group of subprogram requirement specifications.

As the software requirements are allocated to specific application areas, a Task Programmer is assigned technical responsibility for a specific application. The Task Programmer is assigned a schedule and budget for his application area; he is expected to exercise cost and schedule control and to provide clear visibility to the Chief Programmer on cost and schedule performance. Each Task Programmer is responsible for design, programming and testing of his application; the only constraints being the requirement specification, schedule and cost.
More details on software program management are provided in Section 12 of this handbook.

The Product Coordinator is responsible for maintaining a Software Development Plan and for ensuring adherence to the plan. As part of that responsibility, he participates in software reviews and audits to verify that standards and conventions are followed both in software and in documentation. He also verifies that defined internal and external interfaces are maintained and coordinates software changes. He is the software project interface with the program level configuration management function.
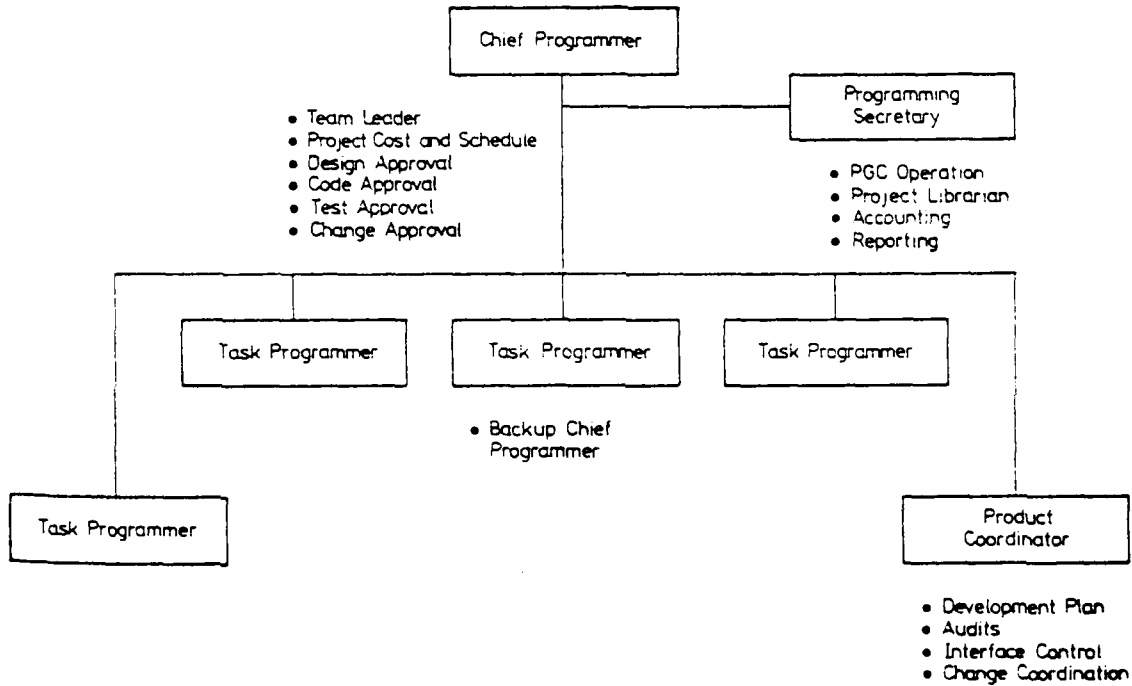
FIGURE 9.7.7-1:   CHIEF PROGRAMMER TEAM ORGANIZATIONAL STRUCTURE

The Programming Secretary acts as the operator for the Program Generation Center (PGC) for making controlled program changes, and is the project librarian. He is also responsible for keeping accurate accounts of all problems reported, changes made, and progress, and he provides regular reports on review status and change status to provide management visibility of development progress.

One of the Task Programmers acts as a Backup Chief Programmer. This is an understudy role; the Backup Chief Programmer must assume the role of Chief Programmer, *either temporarily or permanently*, when called upon. Because of this, he maintains familiarity with the overall software design and the current administrative and technical status. In this role, he performs administrative and technical review functions as assigned by the Chief Programmer.

Design Reviews

Apart from the usual Design Review process which may involve the use of a formal review there are techniques emerging which are oriented toward software. One such technique is "structured workthroughs" (Ref. 43). A structured workthrough procedure involves a peer group review, at the informal level, for each module and the system as a whole. To achieve this, a review kit is prepared containing all the documentation associated with the module, such as the module specification, listing, test results, etc. The kit is then reviewed by the programming team. The process is summarized in Figure 9.7.7-2.
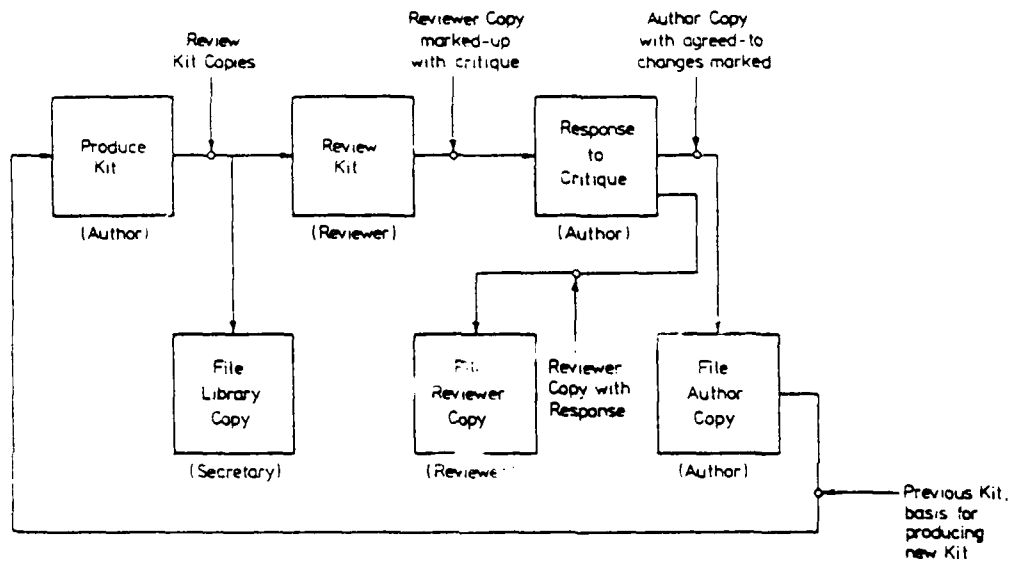
FIGURE 9.7.7-2: REVIEW KIT FLOW

Configuration Control

The fundamentals of configuration control also apply no less to software. A well functioning configuration control system requires that the software currently running on a machine is traceable back to a set of documents. This ensures that controlled software changes are carried out with maximum benefit.

Figure 9.7.7-3 indicates a configuration control system associated with the Chief Programmer Team kind of organization.
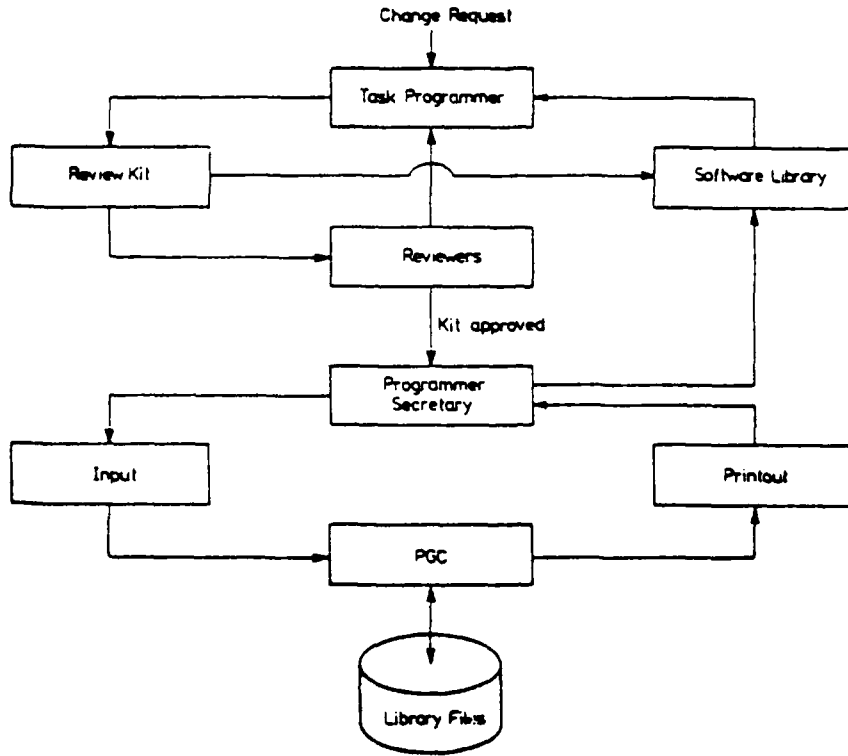
FIGURE 9.7.7-3: CONFIGURATION CONTROL FLOW

REFERENCES

1. Pattee, H., "Postscript: Unsolved Problems and Potential Applications of Hierarchy Theories," pp. 129-156 in Hierarchy Theory, The Challenge of Complex Systems, ed. H. Pattee, Public., George Braziller Inc., New York 1973.

2. Ronbeck, J.A., "Software Reliability - How It Affects System Reliability," Proceedings, 1975 SRE Canadian Reliability Symposium, Permagon Press, New York, pp. 125-127.

3. Gerhart, S. and L. Yelwitz, "Observations of Fallibility in Applications of Modern Programming Methodologies," IEEE Transactions on Software Engineering, 1976.

4. Goodenough, J. and S. Gerhart, "Toward a Theory of Testing; Data Selection Criteria," Current Trends in Programming Methodologies, Vol. 2., R.T. Yeh, Ed., Prentice Hill, Englewood Cliffs, NJ.

5. O'Connor, Patrick D.T., Practical Reliability Engineering, Heyden & Son, Ltd., London - Philadelphia - Rhune, 1981.

6. Glass, R.L., "Persistent Software Errors", IEEE Transactions on Software Engineering, Vol. SE-7, 1981.

7. Jelinski, Z. and P. Moranda, "Software Reliability Research," Statistical Computer Performance Evaluation, W. Freiberger, Ed., Academic Press pp. 465-484.

8. Littlewood, B., "Theories of Software Reliability: How Good Are They and How Can They Be Improved?" IEEE Transactions on Software Engineering, Vol. SE-6, No. 5, 1980.

9. Goel, A.L. and K. Okumoto, "A Time Dependent Error Detection Rate Model for Software Reliability and Other Performance Measures," IEEE Transactions on Reliability, Vol. R. 28, No. 3, pp. 206-211, 1979.

10. Schick, C.J. and R.W. Wolverton, "An Analysis of Computing Software Reliability Models," IEEE Transactions on Software Engineering, Vol. SE-4, No. 2, pp. 104-120, 1978.

11. Shooman, M.L., "Probabilistic Models for Software Reliability Prediction," Statistical Computer Performance Evaluation, W. Freiberger, Ed., Academic Press, pp. 485-502.

12. Musa, J.D., "A Theory of Software Reliability and Its Application," IEEE Transactions on Software Engineering, Vol. SE-1, No. 3, pp. 312-327, 1975.

13. Moranda, P.B, "Prediction of Software Reliability During Debugging," Proceedings 1975 Annual Reliability and Maintainability Symposium, Washington DC, 1975, pp. 327-332.

14. Littlewood, B. and J.L. Verall, "A Bayesian Reliability Growth Model for Computer Software," Applied Statistics Vol. 22, No. 3, pp. 302-346, 1973.

15. Mills, H.D., On the Statistical Validation of Computer Programs, IBM Federal Systems Division, Gaithersburg, MD, Report 72-6015.

16. Lipow, M., Maximum Likelihood Estimation of Parameters of a Software Time-To-Failure-Distribution, TRW Systems Group Report, 2260.1.9-73B-15, Redondo Beach, CA, 1973.

17. Myers, G.J., Software Reliability Principles and Practices, John Wiley and Sons, New York, 1975.

18. Goel, A., Software Reliability Modeling and Estimation Techniques, Final Technical Report on Contract #F30602-78-C-0351, RADC Griffiss Air Force Base, Rome, New York, 13441.

19. Goel, A., and K. Okumoto, "A Markovian Model for Reliability and Other Performance Measures of Software Systems," Proc. National Computer Conference, New York, Vol. 48, pp. 769-744, 1979.

20. Littlewood, B., "Theories of Software Reliability: How Good Are They and How Can They Be Improved?" IEEE Transactions on Software Engineering, Vol. SE-6, No. 5, 1980.

21. Quantitative Software Models, Data and Analysis Center for Software, RADC/ISISI, Griffiss AFB, NY 13441, Report # SRR-1, March 1979.

22. "Special Issue on Software Reliability," IEEE Transactions on Reliability, Vol. R-28, No. 3, August 1979.

23. Reifer, D.J., A New Assurance Technology for Computer Software, the Aerospace Corporation, NTIS Report No. ADA020483, September 1975.

24. Myers, G.J., Reliable Software Through Composite Design, Petrocelli/Charter, New York, 1975.

25. McGowan, C.C. and Kelly, J.R., Top-Down Structured Programming Techniques, Petrocelli/Charter, New York, 1975.

26. Katzan Jr., H., System Design and Documentation - An Introduction to the HIPO Method, Van Nostrand Reinhold, New York, 1976.

27. Myers, G.J., Software Reliability, Wiley Interscience, John Wiley and Sons, New York, 1976.

28. Dijkstra, W.D., A Discipline of Programming, Prentice-Hall, Englewood Cliffs, N.J., 1976.

29. Wirth, N., Systematic Programming - An Introduction, Prentice-Hall, Englewood Cliffs, N.J., 1973.

30. Dahl, OJ., et al., Structured Programming, Academic Press, New York, 1972.

31. Knuth, D.E., Structured Programming with GO TO Statements, Stanford University, NTIS Report No. PB-223 507, May 1974.

32. Kessler, M.M., et al., Programming Language Standards, IBM Corp., NTIS Report No. AD/A-016 771, March 1975.

33. Tenny, T., "Structured Programming in Fortran", Datamation, July 1974, pp. 110-115.

34. Rieks, G.E., "Structured Programming in Assembler Language", Datamation, July 1978, pp. 79-84.

35. Arsenault, J.E. and J.A. Roberts, Reliability and Maintainability of Electronic Systems, Computer Science Press Inc., 9125 Fall River Lane, Potomac, Maryland 20854, 1980.

36. Hetzel, W.C., ed., Program Test Methods, Prentice-Hall, Englewood Cliffs, N.J., 1972.

37. Miller Jr., E.F., ed., "Program Testing", Computer, April 1978, pp. 10-12.

38. FIPS Publication 38 - Guidelines for Documentation of Computer Programs and Automated Data Systems, U.S. Department of Commerce, February 1976.

39. Landon, K.R., Documentation Standards, Petrocelli Books, New York, 1974.

40. Krehne, R.S., et al., Handbook of Computer Documentation Standards, Prentice-Hall, Englewood Cliffs, N.J., 1973.

41. Weinberg, G.M., Psychology of Computer Programming, Van Nostrand, Rheinhold, New York 1971.

42. Baker, F.T., and Mills, H.D., "Chief Programmer Teams", Datamation, December 1973, pp. 58-61.

43. Yourdon, E., Structured Walkthroughs, Yourdon Inc., 1978.

44. Goel, A. and J. Soenjoto, "Models for Hardware-Software System Operational Performance Evaluation," IEEE Transactions on Reliability, Vol. R-30, August 1981, pp. 232-239.

45. James, L. & J. Angus, "Combined Hardware/Software Reliability Models," Proceedings of the Annual Reliability and Maintainability Symposium, January 1982, pp. 176 - 187.

10.0 SYSTEMS RELIABILITY ENGINEERING

10.1 INTRODUCTION

The material presented in the previous sections of this handbook in a sense set the stage for this section. This section combines the R&M theory and engineering practices previously presented into a cohesive design methodology which can be applied at the system level to optimize system "worth" at minimum life cycle costs.

The "worth" of a particular equipment/system is determined primarily by the effectiveness with which it does its job -- its "operational" effectiveness. An acceptable level of effectiveness is required for every operational system.

In the final analysis, the effectiveness of a system can only be really measured when the system is performing its mission in the environment for which it was designed or other accurately simulated environment. Of great concern, however, is how system effectiveness can be predicted while the system design concepts are being formulated and again later when the system is being designed and evaluated. Thus, most system effectiveness methodologies deal more with the predictive design and test aspects of effectiveness of the system than with the later use of the system.

Figure 10.1-1 represents the system effectiveness concept and the parameters that have been traditionally used (with minor variations) for system effectiveness analysis.

SYSTEM EFFECTIVENESS

AVAILABILITY	DEPENDABILITY	CAPABILITY
Measure of system condition at start of mission	Measure of system condition during performance of mission	Measure of results of mission
Reliability Maintainability Human factors Logistics	Repairability Safety Survivability Vulnerability	Range Accuracy Power Lethality

FIGURE 10.1-1: CONCEPT OF SYSTEM EFFECTIVENESS

As can be seen from the figure, availability (How often?), dependability (How long?), and performance capability (How well?), are the primary measures of system effectiveness:

(1) Availability is a measure of the degree to which an item is in the operable and committable state at the start of the mission, when the mission is called for at an unknown (random) time

(2) Dependability is a measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission

(3) Capability is a measure of the ability of an item to achieve mission objectives, given the conditions during the mission

System effectiveness assessment fundamentally answers three basic questions:

(1) Is the system working at the start of the mission?

(2) If the system is working at the start of the mission, will it continue to work during the mission?

(3) If the system worked throughout the mission, will it achieve mission success?

R&M are important contributions to system effectiveness since they are significant factors in consideration of the availability and dependability parameters. However, in the total system design context, as shown in Figure 10.1-1, they must be integrated with other system parameters such as performance, quality, safety, human engineering, survivability/vulnerability, logistics, cost, etc., to arrive at the optimum system configuration.

Just about all of the system effectiveness methodologies which have been developed and/or proposed in the past 15 to 20 years are concerned with this fundamental question of combining the previously mentioned parameters to achieve optimum system design.

It might be instructive, therefore, to discuss and compare the more significant concepts and methodologies that have been proposed, their similarities and differences, and the ease or difficulty of their application.

10.2 SYSTEM EFFECTIVENESS CONCEPTS

The three generally recognized components of system effectiveness previously defined (availability, dependability, capability) will be used as the basis for description and comparison of the concepts and formulations of system effectiveness. It should be recognized that all

of these effectiveness components must be derived from an analysis of the operational needs and mission requirements of the system, since it is only in relation to needs and missions that these basic components can be meaningfully established.

Many semantic difficulties arise when discussing systems effectiveness and its components. These difficulties result from the fact that some people use the same words to mean different things or different words to mean the same things. Definitions of many of the terms used in the following paragraphs were provided in Section 3 and will not be repeated here.

10.2.1 THE ARINC CONCEPT OF SYSTEM EFFECTIVENESS

One of the early attempts to develop concepts of system effectiveness was delineated by ARINC (Aeronautical Research Inc.,) (Ref. 1). It contains some of the earliest published concepts of systems effectiveness and represents one of the clearest presentations of these concepts from which many of the subsequent descriptions have been derived. The definition of systems effectiveness applied in this early work is: "Systems effectiveness is the probability that the system can successfully meet an operational demand within a given time when operated under specified conditions." This definition includes the following concepts; that system effectiveness

(1) can be measured as a probability

(2) is related to operation performance

(3) is a function of time

(4) is a function of the environment or conditions under which it is used

(5) may vary with the mission to be performed

Although it is not essential to describe system effectiveness in terms of probability as opposed to other quantitative measures, it has often been found convenient to do so. The ARINC model may be expressed such that system effectiveness probability, P_{SE}, is the product of three probabilities as follows:

$$P_{SE} = P_{OR} \times P_{MR} \times P_{DA} \qquad\qquad (10.1)$$

where
P_{OR} = operational readiness probability
P_{MR} = mission reliability probability
P_{DA} = design adequacy probability

The above equation states that the effectiveness of the system is the product of three probabilities: (1) the probability that the system is operating satisfactorily or is ready to be placed in operation when needed; (2) the probability that the system will continue to operate satisfactorily for the period of time required for the mission; and (3) the probability that the system will successfully accomplish its mission, given that it is operating within design limits.

10.2.2 THE AIR FORCE (WSEIAC) CONCEPT (Ref. 2)

A more recent definition of system effectiveness resulted from the work of the Weapon System Effectiveness Industry Advisory Committee (WSEIAC) established in late 1963 by the Air Force System Command. The WSEIAC definition of system effectiveness is: "System effectiveness is a measure of the extent to which a system may be expected to achieve a set of specific mission requirements and is a function of availability, dependability, and capability." The definition may be expressed as:

$$E = ADC \tag{10.2}$$

where
    A = availability
    D = dependability
    C = capability

See definitions in Section 10.1.

These are usually expressed as probabilities as follows:

(1) A is the vector array of various state probabilities of the system at the beginning of the mission

(2) D is a matrix of conditional probabilities over a time interval, conditional on the effective state of the mission during the previous time interval

(3) C is also a delineal probability matrix representing the performance spectrum of the system, given the mission and system conditions -expected figures of merit for the system

Basically, the model is a product of three matrices: the Availability row vector A, the Dependability matrix D, and the Capability matrix C. In the most general case, assume that a system can be in different states and at any given point in time is in either one or the other of the states. The availability row vector is then

$$\vec{A} = (a_1 a_2 a_3 \ldots a_i \ldots a_n) \tag{10.3}$$

where a_i is the probability that the system is in State i at a random mission beginning time. Since the system can be in only one of the n states and n is the number of all possible states it can be in including the down states in which the system cannot start a mission, the sum of all the probabilities a_i in the row vector must be unity, i.e.,

$$\sum_{i=1}^{n} A_i = 1 \tag{10.4}$$

The dependability matrix D is defined as a square n x n matrix

$$D = \begin{bmatrix} d_{11} & d_{12} & d_{13} & \cdots & d_{1n} \\ d_{21} & d_{22} & d_{23} & \cdots & d_{2n} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ d_{n1} & d_{n2} & d_{n3} & \cdots & d_{nn} \end{bmatrix}$$

(10.5)

where the meaning of the element d_{ij} is defined as the expected fraction of mission time during which the system will be in State j if it was in State i at the beginning of the mission. If system output is not continuous during the mission but is required only at a specific point in the mission (such as over the target area), d_{ij} is defined as the probability that the system will be in State j at the time when output is required if it was in State i at mission start.

When no repairs are possible or permissible during a mission, the system upon failure or partial failure cannot be restored to its original state during the mission and can at best remain in the State i in which it started the mission or will degrade into lower states or fail completely. In the case of no repairs during the mission, some of the matrix elements become zero. If we define State 1 as the highest state (i.e., everything works perfectly) and n the lowest state (i.e., complete failure), the dependability matrix becomes triangular with all entries below the diagonal being zeros.

$$D = \begin{bmatrix} d_{11} & d_{12} & d_{13} & \cdots & d_{1n} \\ 0 & d_{22} & d_{23} & \cdots & d_{2n} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ 0 & 0 & 0 & \cdots & d_{nn} \end{bmatrix}$$

(10.6)

If the matrix is properly formulated the sum of the entries in each row must equal unity. For example, for the first row we must have

$$d \ + d \ + \ldots + d_n = 1$$

(10.7)

and the same must apply to each subsequent row. This provides a good check when formulating a dependability matrix.

The capability matrix C describes system performance or capability to perform while in any of the n possible system states. If only a single measure of system effectiveness is of importance or of interest, C will be a one column matrix with n elements, such as

$$C = \begin{bmatrix} C_1 \\ C_2 \\ \cdot \\ \cdot \\ \cdot \\ C_n \end{bmatrix}$$

(10.8)

where c_j represents system performance when the system is in State j.

System effectiveness SE in the WSEIAC model is then defined as

$$SE = \begin{bmatrix} a_1 a_2 \cdots a_n \end{bmatrix} \times \begin{bmatrix} d_{11} & d_{12} & \cdots & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & \cdots & d_{2n} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ d_{n_1} & d_{n_2} & \cdots & \cdots & d_{nn} \end{bmatrix} \times \begin{bmatrix} c_1 \\ c_2 \\ \cdot \\ \cdot \\ \cdot \\ c_n \end{bmatrix} \qquad (10.9)$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} a_i d_{ij} c_j \qquad (10.10)$$

in matrix notation:

Reference 2 contains several numerical examples of how to perform system effectiveness calculations using the WSEIAC model. Also, Ref. 3, Chapter VII, discusses the model at length and provides numerical examples.

10.2.3 THE NAVY CONCEPT OF SYSTEM EFFECTIVENESS (Ref. 4)

In the early 1960s the Navy developed a system effectiveness concept which also combines three basic system characteristics: performance, availability and utilization. It can be expressed as "a measure of the extent to which a system can be expected to complete its assigned mission within an established time frame under stated environmental conditions." It may also be defined mathematically as "the probability that a system can successfully meet an operational demand through a given time period when operated under specified conditions."

Mathematically it has been formulated as follows:

$$E_S = PAU \qquad (10.11)$$

where

E_S = index of system effectiveness

P = index of system performance - a numerical index expressing system capability, assuming a hypothetical 100% availability and utilization of performance capability in actual operation

A = index of the system availability - a numerical index of the extent to which the system is ready and capable of fully performing its assigned mission(s)

U = index of system utilization - a numerical index of the extent to which the performance capability of the system is utilized during the mission

The components of the Navy model are not as readily compared as the ARINC and WSEIAC models. The Navy has stated that the terms PU and A are similar to the WSEIAC terms C and AD (Ref. 5) and that PAU can be translated into the analytical terms P_C and P_T where

P_C = performance capability - a measure of adequacy of design and system degradation

P_T = detailed time dependency - a measure of availability with a given utilization

Thus the Navy model is compatible with the WSEIAC model in the following way:

$$f(PAU) = f(P_C, P_T) = f(A,D,C) \qquad (10.12)$$

The WSEIAC, Navy and ARINC concepts of system effectiveness are depicted in Figure 10.2.3-1.

Although these models are relatively simple to describe, their development and application is a rather complex process usually performed by operations research groups and operations analysts utilizing available computerized models (to be discussed later).

10.2.4 AN ILLUSTRATIVE MODEL OF A SYSTEM EFFECTIVENESS CALCULATION

The following simplified example, utilizing the WSEIAC concept, is provided in order to show how R&M parameters are used in system effectiveness calculations.

Problem Statement

The system to be considered is that comprised of a helicopter and its communication equipment. It is to operate in a limited warfare environment where rapid movement of supplies upon request is important. The mission of the system is that of transporting upon random call supplies from a central supply to operational activities within a radius of one-half hour flying time and providing vertical underway replenishment of needed spares. Once the helicopter has reached the target area, proper functioning of the communication equipment enhances the chances of a successful delivery of the supplies in terms of safe delivery, timely delivery, etc. Some major assumptions which are inherent in this example are:

(1) A call for supplies is directed to a single helicopter. If this craft is not in flyable condition (i.e., it is in process of maintenance) the mission will not be started. A flyable craft is defined as one which is in condition to take off and fly with a standard supply load;

(2) The flight time required to reach the target area is one-half hour;

(A) ARINC MODEL

SYSTEM EFFECTIVENESS (SE)

OPERATIONAL READINESS	MISSION RELIABILITY	DESIGN ADEQUACY
PROBABILITY THAT AT ANY POINT IN TIME A SYSTEM OPERATING SATISFACTORILY OR READY TO BE PLACED IN OPERATION ON DE-MAND	PROBABILITY OF A SYSTEM PERFORMING ITS PURPOSE ADEQUATELY FOR THE PERIOD OF TIME INTENDED	PROBABILITY THAT A SYSTEM WILL SUCCESS-FULLY ACCOMPLISH ITS MISSION GIVEN THAT THE SYSTEM IS OPERAT-ING WITHIN DESIGN SPECS
RELIABILITY HUMAN FACTORS MAINTAINABILITY LOGISTIC SUPPORT		

(B) WSEIAC MODEL

SYSTEM EFFECTIVENESS (SE)

AVAILABILITY (A)	DEPENDABILITY (D)	CAPABILITY (C)
MEASURE OF SYSTEM CONDITION AT START OF MISSION	MEASURE OF SYSTEM CONDITION DURING PER-FORMANCE OF MISSION	MEASURE OF RESULTS OF MISSION
RELIABILITY MAINTAINABILITY HUMAN FACTORS LOGISTICS	REPAIRABILITY SAFETY FLEXIBILITY SURVIVABILITY	RANGE ACCURACY POWER LETHALITY

(C) NAVY MODEL

SYSTEM EFFECTIVENESS (SE)

PERFORMANCE (P)	AVAILABILITY (A)	UTILIZATION (U)
ACHIEVED DESIRED	MAN-MACHINE MODULES	TACTICAL ENVIRONMENTAL FUNCTIONAL LOGISTICAL
PRIMARY MISSION SECONDARY MISSION NO MISSION	RELIABILITY MAINTAINABILITY OPERABILITY LOGISTICS SUPPORT-ABILITY SAFETY	
FRACTIONS OF TOTAL MISSION TIME		

FIGURE 10.2.3-1: SYSTEM EFFECTIVENESS MODELS

(3) The communication equipment cannot be maintained or repaired in flight;

(4) A loaded helicopter which goes down while on route to or which does not reach the target area has no delivery value.

Model Determination

For purposes of model formulation, the system condition is divided into three states:

(1) <u>State 1</u>. Helicopter flyable, communication equipment operable

(2) <u>State 2</u>. Helicopter flyable, communication equipment nonoperable

(3) <u>State 3</u>. Helicopter nonflyable

The effectiveness model is defined as

$$E = ADC$$

where A, D and C are defined as follows:

(1) The availability vector is a three element row vector, i.e.,

$$A = (a_1, a_2, a_3)$$

where a_i is the probability that the helicopter will be in State i at the time of call.

(2) The dependability matrix is a 3x3 square matrix, i.e.,

$$D = \begin{bmatrix} d_{11} & d_{12} & d_{13} \\ d_{21} & d_{22} & d_{23} \\ d_{31} & d_{32} & d_{33} \end{bmatrix}$$

where d_{ij} is the probability that if the helicopter is in State i at the time of call it will complete the mission in State j.

(3) The capability vector is a three element column vector, i.e.,

$$C = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

where c_i is the probability that if the helicopter is in State i at the time of arrival at the target area the supplies can be successfully delivered. (For multicapability items, C would be a multicolumn matrix.)

Determination of Model Elements

Past records indicate that the average time between maintenance activities (including preventive and failure initiated maintenance) for this type of helicopter is 100 hours and the average duration (including such variables as maintenance difficulty, parts availability, manpower, etc.) of a maintenance activity is ten hours. Comparable data for the communication equipment shows an average time between maintenance activities of 500 hours and an average duration of a maintenance activity of five hours.

From the preceding data the elements of A can be determined.

A_1 = P(helicopter flyable) P(communication equipment operable)

$$= \left(\frac{100}{100 + 10} \right) \left(\frac{500}{500 + 5} \right) = 0.9$$

A_2 = P(helicopter flyable) P(communication equipment not operable)

$$= \left(\frac{100}{100 + 10} \right) \left(\frac{5}{500 + 5} \right) = 0.009$$

A_3 = P(helicopter not flyable) = $\left(\frac{10}{100 + 10} \right) = 0.091$

Data available from past records indicates that the time between failures of the communication equipment during flight is exponentially distributed with a mean of 500 hours. Also, the probability that a helicopter in flight will not survive the one-half hour flight to its destination is 0.05 (includes probability of being shot down, mechanical failures, etc.). Then the elements of the D matrix may be calculated as follows:

(1) If the system begins in State 1:

d_{11} = P(helicopter will survive flight) P(communication equipment will remain operable

$$= (1 - 0.05) \left[\exp \left(-\frac{1/2}{500} \right) \right] = 0.94905$$

d_{12} = P(helicopter will survive flight) P(communication equipment will fail during flight)

$$= (1 - 0.05) \left[1 - \exp \left(-\frac{1/2}{500} \right) \right] = 0.00095$$

d_{13} = P(helicopter will not survive the flight) = 0.05000

(2) If the system begins in State 2:

d_{21} = 0 because the communication equipment cannot be repaired in flight

d_{22} = P(helicopter will survive flight) = 0.95000

d_{23} = P(helicopter will not survive the flight) = 0.05000

(3) If the system begins in State 3:

d_{31} = d_{32} = 0 because the mission will not start

d_{33} = 1, i.e., if the helicopter is not flyable, it will remain nonflyable with reference to a particular mission

Experience and technical judgment have determined the probability of successful delivery of supplies to be c_i if the system is in State i at the time of arrival in the target area, where

c_1 = 0.95

c_2 = 0.80

c_3 = 0

Determination of Effectiveness

The effectiveness of the subject system becomes

$$E = \begin{bmatrix} 0.900 & 0.009 & 0.091 \end{bmatrix} \begin{bmatrix} 0.94905 & 0.00095 & 0.05 \\ 0 & 0.95 & 0.05 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0.95 \\ 0.8 \\ 0 \end{bmatrix}$$

$$= 0.82$$

which means that the system has a probability of 0.82 of successful delivery of supplies upon random request.

The effectiveness value attained provides a basis for deciding whether improvement is needed. The model also provides the basis for evaluating the effectiveness of alternative systems considered.

10.3 SYSTEM R&M PARAMETERS

In this section we are concerned with those system effectiveness sub-models, e.g., availability, dependability, operational readiness, which can be exercised to specify, predict, allocate, optimize, and measure system R&M parameters.

A Department of Defense Directive on Reliability and Maintainability was published in July 1980 (Ref. 6). Included in this directive is a discussion of "system R&M parameters," recognizing the need for more than one frame of reference for specifying and measuring reliability and maintainability.

The Directive states:

"System R&M shall be measured in four separate ways, using units of measurement directly related to:

o   Operational readiness
o   Mission success
o   Maintenance manpower cost
o   Logistic support cost

These four ways of measuring R&M shall be known as the 'system R&M parameters'."

These four types of parameters and examples of specific R&M terms applicable to their specification and measurement are shown in Figure 10.3-1. Each will be discussed in more detail in the following paragraphs.

OBJECTIVES	EXAMPLE TERMS
● READINESS OR AVAILABILITY	R: Mean Time Between Downing Events M: Mean Time to Restore System
● MISSION SUCCESS	R: Mission Time Between Critical Failures M: Mission Time to Restore Function
● MAINTENANCE MANPOWER COST	R: Mean Time Between Maintenance Actions M: Direct Manhours per Maintenance Action
● LOGISTIC SUPPORT COST:	R: Mean Time Between Removals M: Total Parts Cost per Removal

FIGURE 10.3-1: SYSTEM R&M PARAMETERS

Operational Readiness R&M Parameters. These parameters will define the R&M contribution to the readiness measurement of the system or unit. R&M by itself does not define readiness; there are many other factors relating to personnel, training, supplies, etc., that are necessarily included in any real measure of readiness. The context of readiness includes many factors beyond the realm of equipment capability and equipment R&M achievements. R&M parameters of this type concern themselves with the likelihood of failures occurring that would make a ready system no longer ready and with the effort required to restore the system to the ready condition. Examples of this type of parameter are "mean time between downing events" for reliability and "mean time to restore system" for maintainability.

Mission Success R&M Parameters. These parameters are similar to the classical reliability discussion that is found in most reliability text books. They relate to the likelihood of failures occurring during a mission that would cause a failure of that mission and the efforts that are directed at correcting these problems during the mission itself. Examples would be "mission time between critical failures (MTBCF)" for reliability and "mission time to restore function" for maintainability.

Maintenance Manpower Cost R&M Parameters. Some portion of a system's maintenance manpower requirement is driven by the system's R&M achievement. This category of system R&M parameters concerns itself with how frequently maintenance manpower is required and, once it is required, how many manhours are needed. Examples of this type of parameter are "mean time between maintenance actions" for reliability and "direct manhours to repair" for maintainability. Note that the maintainability example does not address the clock hours to complete the repair. Time to restore the system, i.e., the system downtime, is not as significant to the people concerned with manpower needs as the total manhours required.

Logistic Support Cost R&M Parameters. In many systems, this type of R&M parameter might be properly titled as "material cost" parameters. These parameters address the aspect of R&M achievement that requires the consumption of material. Material demands also relate to the readiness or availability of the system. Examples are "mean time between removals" for reliability and "total parts cost per removal" for maintainability.

MIL-STD-721 reflects the philosophy of DoD Directive 5000.40 and contains definitions from the key R&M terms shown in Figure 10.3-1, Although not specifically shown in Figure 10.3-1, the terms dependability and mission reliability are related to the mission success parameter in Figure 10.3-1.

Let us look in more detail at the similarities and differences among some of the more fundamental system R&M parameters, i.e., availability, operational readiness, mission reliability, and dependability.

10.3.1 AVAILABILITY, OPERATIONAL READINESS, MISSION RELIABILITY, AND DEPENDABILITY - SIMILARITIES AND DIFFERENCES

As can be seen from their definitions in Table 10.3.1-1, availability and operation readiness refer to the capability of a system to perform its intended function when called upon to do so. This emphasis restricts attention to probability "at a point in time" rather than "over an interval of time." Thus, they are point concepts rather than interval concepts. To differentiate between the two: availability is defined in terms of operating time and downtime, where downtime includes active repair time, administrative time, and logistic time; whereas, operational readiness includes all of the availability times plus both free time and storage time, i.e., all calendar time.

Also note that the concepts of availability and operational readiness do not include mission time.

Dependability, although it is a point concept like availability and operational readiness, differs from those concepts in that it is concerned with the degree (or probability) that an item is operable at some point (time) during the mission profile, given its (point) availability at the start of the mission.

Mission reliability, on the other hand, is concerned with the ability of a system to continue to perform without failure for the duration of a specified mission time; in other words, the probability of successful operation over some interval of time rather than at a specific point in time. Thus, mission reliability is an interval concept rather than a point concept. It should be pointed out that mission reliability is also conditional upon the system being operable at the beginning of the mission or its (point) availability.

Further note that dependability and mission reliability do not include nonmission time.

Hopefully, the mathematical models and examples which follow will help to further clarify these concepts.

10.4 SYSTEM R&M MODELING TECHNIQUES

It was previously pointed out in Section 5 that mathematical models represent an efficient, shorthand method of describing an event and the more significant factors which may cause or affect the occurrence of the event. Such models are useful to engineers and designers since they provide the theoretical foundation for the development of an engineering discipline and a set of engineering design principles which can be applied to cause or prevent the occurrence of an event.

TABLE 10.3.1-1: DEFINITIONS OF KEY R&M SYSTEM PARAMETERS

AVAILABILITY: A measure of the degree to which an item is in an operable and commitable state at the start of a mission when the mission is called for at an unknown (random) time. (Item state at start of a mission includes the combined effects of the readiness-related system R&M parameters but excludes mission time.)

OPERATIONAL READINESS: The ability of a military unit to respond to its operation plan(s) upon receipt of an operations order. (A function of assigned strength, item availability, status, or supply, training, etc.)

MISSION RELIABILITY: The ability of an item to perform its required functions for the duration of a specified "mission profile."

DEPENDABILITY: A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission. (Item state during a mission includes the combined effects of the mission-related system R&M parameters but excludes non-mission time.)

MEAN-TIME-BETWEEN-DOWNING-EVENTS (MTBDE): A measure of the system reliability parameter related to availability and readiness. The total number of system life units divided by the total number of events in which the system becomes unavailable to initiate its mission(s) during a stated period of time.

MEAN-TIME-TO-RESTORE-SYSTEM (MTTRS): A measure of the system maintainability parameters related to availability and readiness: the total corrective maintenance time associated with downing events divided by the total number of downing events during a stated period of time. (Excludes time for off-system maintenance and repair of detached components.)

MISSION-TIME-BETWEEN-CRITICAL-FAILURES (MTBCF): A measure of mission reliability: the total amount of mission time divided by the total number of critical failures during a stated series of missions.

MISSION-TIME-TO-RESTORE-FUNCTIONS (MTTRF): A measure of mission maintainability: the total corrective critical failure maintenance time divided by the total number of critical failures during the course of a specified mission profile.

MEAN-TIME-BETWEEN-MAINTENANCE-ACTIONS (MTBMA): A measure of the system reliability parameter related to demand for maintenance manpower: the total number of system life units divided by the total number of maintenance actions (preventive and corrective) during a stated period of time.

DIRECT-MAINTENANCE-MANHOURS-PER-MAINTENANCE-ACTION (DMMH/MA): A measure of the maintainability parameter related to item demand for maintenance manpower: the sum of direct maintenance manhours divided by the total number of maintenance actions (preventive and corrective) during a stated period of time.

MEAN-TIME-BETWEEN-REMOVALS (MTBR): A measure of the system reliability parameter related to demand for logistic support: the total number of system life units divided by the total number of items removed from that system during a period of time. This term is defined to exclude removals performed to facilitate other maintenance and removals for product improvement.

At the system level, models such as system effectiveness models (and their R&M parameter submodels) serve several purposes:

(1) To evaluate the effectiveness of a system of a specific proposed design to accomplish various operations (missions) for which it is designed and to calculate the effectiveness of other competing designs, so the decision maker can select that design which is most likely to meet specified requirements

(2) To perform tradeoffs among system characteristics, performance, reliability, maintainability, etc., in order to achieve the most desirable balance among those which result in highest effectiveness

(3) To perform parametric sensitivity analyses in which the numerical value of each parameter is varied in turn and to determine its effect on the numerical outputs of the model. Parameters that have little or no effect can be treated as constants and the model simplified accordingly. Parameters to which the model outputs show large sensitivity are then examined in detail, since small improvements in the highly sensitive parameters may result in substantial improvements in system effectiveness at very acceptable cost.

(4) To "flag" problem areas in the design which seriously limit the ability of the design to achieve the desired level of system R&M or system effectiveness

The evaluation of system effectiveness and its R&M parameters is an iterative process that continues through all life cycle phases of a system. In each of these phases, system effectiveness is continually being "measured" by exercising the system effectiveness models. In the early design stage, system effectiveness and R&M predictions are made for various possible system configurations. When experimental hardware is initially tested, first real life information is obtained about performance, reliability, and maintainability characteristics, and this information is fed into the models to update the original prediction and to further exercise the models in an attempt to improve the design. This continues when advanced development hardware is tested to gain assurance that the improvements in the system design are effective or to learn what other improvements can still be made before the system is fully developed, type classified, and deployed for operational use. Once in operation, field data starts to flow in and the models are then used to evaluate the operational effectiveness of the system as affected by the field environment, including the actual logistic support and maintenance practices provided in the field. The models again serve to disclose or "flag" problem areas needing improvement.

One may summarize the need for system R&M models as follows. First of all, they provide insight, make an empirical approach to system design and synthesis economically feasible, and are practical methods for circumventing a variety of external constraints. Furthermore, the models aid in establishing requirements, provide an assessment of the odds for successful mission completion, isolate problems to definite areas, and rank problems to their relative seriousness of impact on the mission. They also provide a rational basis for evaluation and choice of proposed system configurations and proposed solutions to discovered problems.

Thus, system R&M models are an essential tool for the quantitative evaluation of system effectiveness and for designing effective weapon systems. Figure 10.4-1 identifies eight principal tasks involved in system effectiveness evaluation. Task 1 is mission definition, Task 2 is system description, Task 3 is selection of figure of merit, and Task 4 is the identification of accountable factors that impose boundary conditions and constraints on the analysis to be conducted. After completing these four tasks, it becomes possible to proceed with Task 5, the construction of the mathematical models. To obtain numerical answers from the models, numerical values of all parameters included in the models must be established or estimated (Task 7). To do this, good and reliable data must first be acquired from data sources, tests, etc. (Task 6). The final Task 8 exercises the models by feeding in the numerical parametric values to obtain system effectiveness estimates and to perform optimizations. Ref. 7 illustrates in more detail the whole process of system effectiveness evaluations, beginning with the military operational requirements and leading through the exercising of the system effectiveness model(s) to the decision making stage.

In terms of system R&M parameter models, reliability and maintainability define system availability and/or operational readiness. Reliability determines the state probabilities of the system during the mission, i.e., the system dependability. If repairs can be performed during the mission, maintainability also becomes a factor in dependability evaluations; this case is often referred to as "reliability with repair." Then, there is the impact of logistic support on the downtime and turnaround time of the system, since shortcomings in the logistic support may cause delays over and above the maintenance time as determined by the system maintainability design. Finally, there are the performance characteristics of the system that are affected by the state in which the system may be at any point in time during a mission, i.e., by the system dependability.

Submodels of availability, operational readiness, downtime distributions, dependability, etc., are required to obtain the numerical answers that may be fed into an overall system effectiveness model, if such can be constructed. Some of these submodeling techniques will now be discussed.
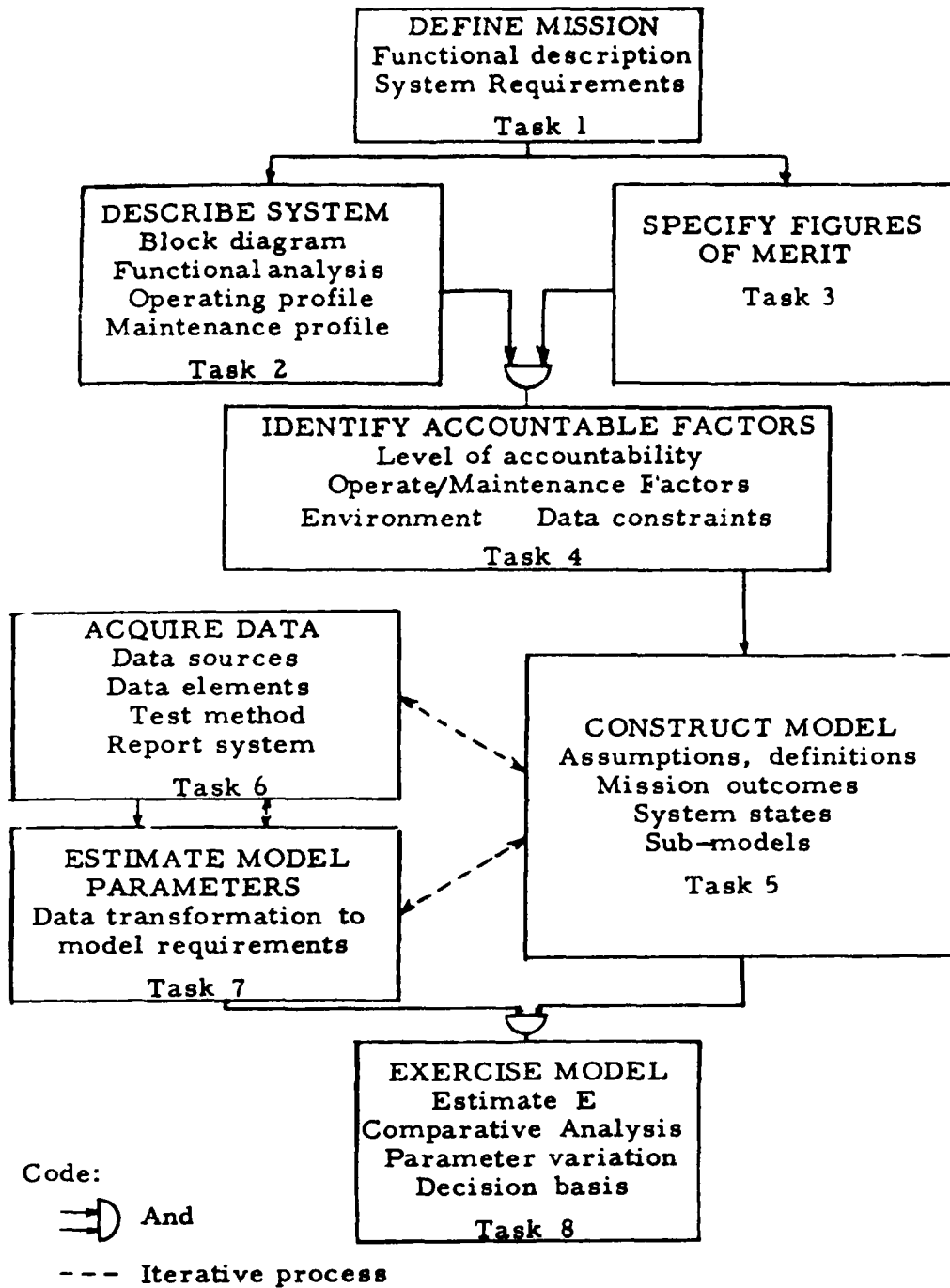
FIGURE 10.4-1: PRINCIPAL TASKS REQUIRED FOR EVALUATION OF SYSTEM EFFECTIVENESS

10.4.1   AVAILABILITY MODELS

The concept of availability was originally developed for repairable systems that are required to operate continuously, i.e., round-the-clock, and are at any random point in time either operating or are "down" because of failure and are being worked upon so as to restore their operation in minimum time.   In this original concept, a system is considered to be in only two possible states -- operating or in repair -- and availability is defined as the probability that a system is operating satisfactorily at any random point in time, t, when subject to a sequence of "up" and "down" cycles which constitute an alternating renewal process.

Availability theory was treated quite extensively in Section 5; this section will concentrate on final results and illustrative examples of the various models.

10.4.1.1   MODEL A - SINGLE UNIT SYSTEM (POINT AVAILABILITY)

Consider first a single unit system or a strictly serial system that has a reliability, R(t) its availability, A(t), that it will be in an "up" state (i.e., will be operating) at time, t, when it started in an "up" condition at t = 0 is given by:

$$A(t) = \frac{\mu}{\lambda + \mu} + \left\{ \frac{\lambda}{\lambda + \mu} \exp\left[- (\lambda + \mu) t \right] \right\} \tag{10.13}$$

If it started in a "down" state at t = 0

$$A(t) = \frac{\mu}{\lambda + \mu} - \left\{ \frac{\lambda}{\lambda + \mu} \exp\left[- (\lambda + \mu) t \right] \right\} \tag{10.14}$$

This assumes that the failure rate, f(t), and the repair rate, g(t), probability density functions are exponentially distributed and given by:

$$f(t) = \lambda e^{-\lambda t} \tag{10.15}$$

$$g(t) = \mu e^{-\mu t} \tag{10.16}$$

We may write Eq. 13 also in terms of the reciprocal values of the failure and repair rates, i.e., in terms of the MTBF and the MTTR, remembering, however, that both time-to-failure and time-to-repair must be exponentially distributed for the equation to hold:

$$A(t) = \frac{MTBF}{MTBF + MTTR} + \left\{ \frac{MTTR}{MTBF + MTTR} \times \exp\left[- \left(\frac{1}{MTBF} + \frac{1}{MTTR} \right)t \right] \right\} \tag{10.17}$$

When we study this equation we see that as t increases the second term on the right diminishes and that availability in the limit becomes a constant, i.e.,

$$\lim_{t \to \infty} A(t) = A_s = \frac{MTBF}{MTBF + MTTR} \qquad (10.18)$$

We call this the steady-state availability or inherent uptime ratio of a serial system. It is equivalent to the intrinsic availability, A_i, discussed in Section 5.

Figure 10.4.1.1-1 shows plots of A(t), instantaneous availability, and A_i or A_s (steady state availability) for a single system whose failure rate (λ) is 0.01 failures/hr. and repair rate (μ) is 1 repair/hr.

Note that the transient term decays rather rapidly; it was shown in Section 5 that the transient term becomes negligible for

$$t \geq \frac{4}{\lambda + \mu} \qquad (10.19)$$

An important point to be made is that Eq (10.18) holds regardless of the probability distribution of time-to-failure and time-to-repair.

Looking again at Eq. (10.18), we may divide the numerator and denominator by the MTBF and write the steady state availability as follows:

$$A = 1/(1 + \alpha) \qquad (10.20)$$

where

α = MTTR/MTBF, the maintenance time ratio (MTR), or alternatively, $\alpha = \lambda/\mu$ which the reader may recognize from queueing theory as the "utilization" factor. Thus, the availability, A, does not depend upon the actual values of MTBF or MTTR or their reciprocals but only on their ratio. Thus, there are a whole range of MTBF ($1/\lambda$), and MTTR ($1/\mu$) values which can satisfy a given availability requirement. The system designer has the option of trading off MTBF and MTTR to achieve the required system availability within technological and cost constraints. This will be discussed later.

Another observation to be made from Eq. (10.20) is that if α, which is equal to MTTR/MTBF, or λ/μ, is < 0.10, then A can be approximated by 1 -MTTR/MTBF, or 1 - λ/μ.

Thus far we have discussed inherent or intrinsic availability which is the fundamental parameter used in equipment/system design. However, it does not include preventive maintenance time, logistic delay time, and administrative time. In order to take these factors into account, we need several additional definitions of availability.

For example, achieved availability, A_a, includes preventive maintenance and is given by the formula:

$$A_a = \frac{MTBM}{MTBM + \bar{M}} \qquad (10.21)$$
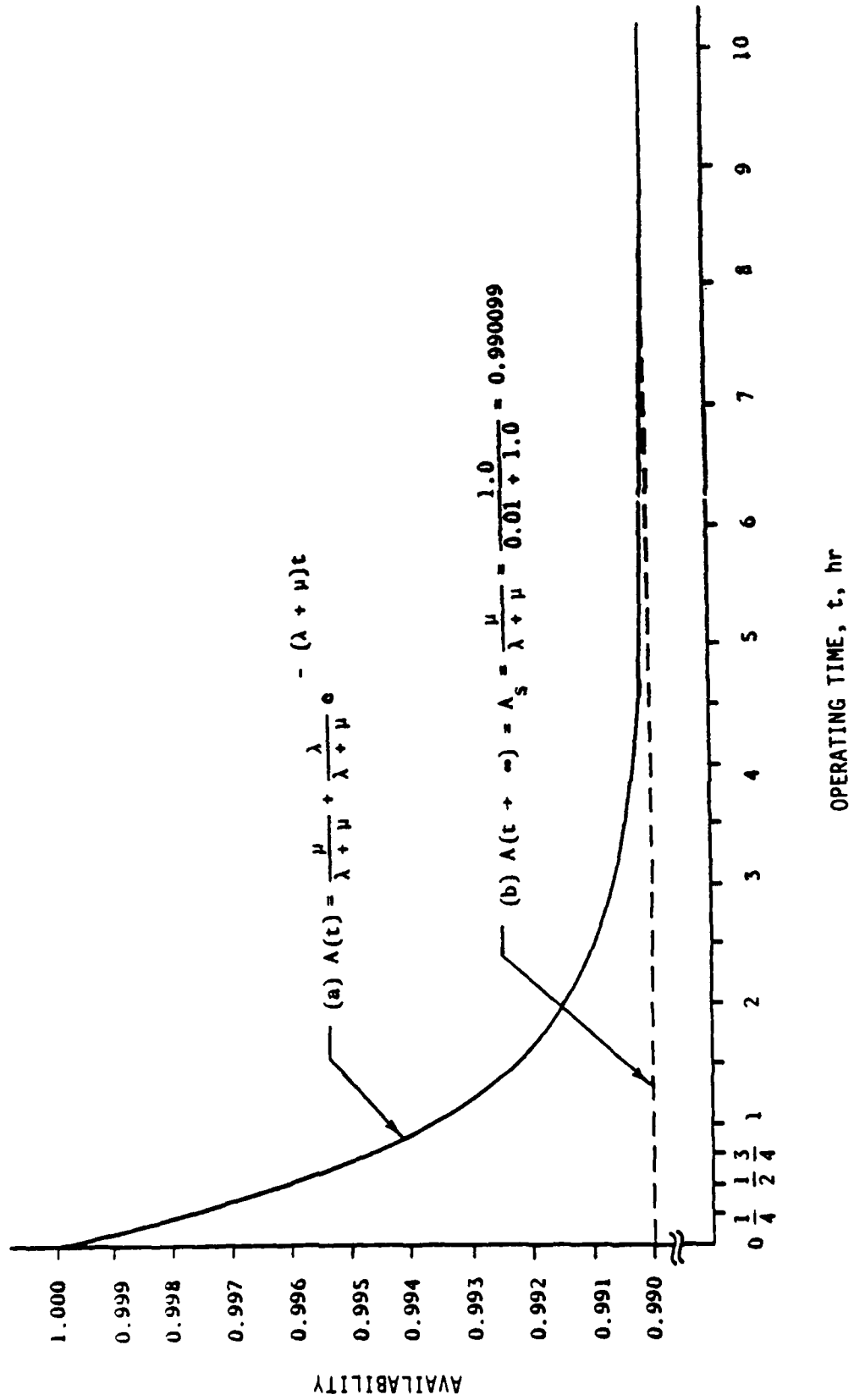
Figure 10.4.1.1-1: THE AVAILABILITY OF A SINGLE UNIT: (a) INSTANTANEOUS
OR POINT AVAILABILITY; (b) STEADY STATE AVAILABILITY
OR INHERENT UPTIME RATIO, $\lambda = 0.01$ fr/hr; $\mu = 1.0$ rp/hr.

Where $\overline{M}$ is the mean active corrective and preventive maintenance time and MTBM is the mean interval between corrective and preventive maintenance actions equal to the reciprocal of the frequency at which these actions occur, which is the sum of the frequency or rate (λ) at which corrective maintenance actions occur and the frequency or rate (f) at which preventive maintenance actions occur. Therefore,

$$MTBM = 1/(\lambda + f)$$

Operational availability, A_o, includes, in addition to A_a, logistic time, waiting time, and administrative time, so that the total mean downtime MDT becomes:

$$MDT = \overline{M} + \text{Mean Logistic Time} + \text{Mean Administrative Time}$$

and adds to the uptime the ready time, RT, i.e.,

$$A_o = \frac{MTBM + RT}{MTBM + RT + MDT} \qquad (10.22)$$

It is important to realize that RT is the system average ready time (available but not operating) in a complete operational cycle, the cycle being MTBM + MDT + RT.

Illustrative Example of Availability Calculations

The following example is provided to clarify the concepts in the subsection. A ground radar system was found to have the following R&M parameters. Determine A_i, A_a, and A_s:

    MTBF = 100 hrs.
    MTTR = 0.5 hr.
    Mean active preventive maintenance time = 0.25 hrs.
    Mean logistic time = 0.3 hr.
    Mean administrative time = 0.4 hrs.
    MTBM = 75 hrs., for either corrective or preventive maintenance
           actions
    Mean ready time = 20 hrs.

Intrinsic or Inherent Availability = A_i

$$A_i = \frac{MTBF}{MTBF + MTTR} = \frac{100}{100 + 0.5} = 0.995$$

Achieved Availability = A_a

$$A_a = \frac{MTBM}{MTBM + \overline{M}} = \frac{75}{75 + 0.5 + 0.25} = 0.99$$

Operational Availability = A_o

$$A_o = \frac{MTBM + RT}{MTBM + RT + MDT} = \frac{75 + 20}{75 + 20 + 0.5 + 0.25 + 0.3 + 0.4}$$

$$= \frac{95}{96.45} = 0.985$$

10.4.1.2 MODEL B - AVERAGE OR INTERVAL AVAILABILITY

What we discussed in the previous section is the concept of <u>point</u>
availability which is the probability that the system is "up" and
operating at any point in time. Often, however, one may be interested
in knowing what percent or fraction of a time interval (a,b) a system
can be expected to operate. For example, we may want to determine the
availability for some mission time. This is called the interval or
average availability, A_{AV}, of a system and is given by the time average
of the availability function A(t) averaged over the interval (a,b):

$$A_{AV}(a,b) \;=\; \left[1/(b-a) \right] \int_b^a A(t)dt \tag{10.23}$$

For instance, if we want to know the fraction of time a system such as
shown in Figure 10.4.1.1-1 will be operating counting from t = 0 to any
time, T, we substitute A(t) of Eq (10.13) into Eq. (10.23) and perform
the integration. The result is:

$$A_{AV}(T) \;=\; \frac{1}{T} \left[\int_0^T \frac{\mu}{\lambda + \mu}\, dt + \int_0^T \frac{\lambda}{\lambda + \mu}\, \exp\left[-(\lambda + \mu)\, t \right] dt \right] \tag{10.24}$$

$$=\; \frac{\mu}{\lambda + \mu} + \frac{\lambda}{T(\lambda + \mu)^2} \left\{ 1 - \exp\left[-(\lambda + \mu)\, T \right] \right\}$$

Figure 10.4.1.2-1 shows the relationship of A(t) to $A_{AV}(t)$ for the
exponential case. Note that in the limit in the steady state we again
get the availability A of Eq. (10.18), i.e.,

$$\lim_{t \to \infty} A_{AV}(t) \;=\; \mu/(\lambda + \mu) \;=\; \frac{MTBF}{MTBF + MTTR} \tag{10.25}$$

But in the transient state of the process, as shown in the figure for an
interval (0, T), before equilibrium is reached $A_{AV}(t)$ is in the
exponential case larger than A(t) for an interval (0, t). This is not
true for all distributions, since A(t) and $A_{AV}(t)$ may be subject to very
large fluctuations in the transient state.

From Eq. (10.24) we may also get the average or expected "on" time in an
interval (0, t) by multiplying $A_{AV}(t)$ and t, the length of the time
interval of interest. Ref. 8, pp. 74-83, contains an excellent
mathematical treatment of the pointwise and interval availability and
related concepts.

Example of Average Availability Calculation

Using our ground radar example from the previous subsection, calculate
A_{AV} for a mission time of 1 hour.

    MTBF = 100 hrs. = 1/λ
    MTTR = 0.5 hr. = 1/μ
    T   = 1 hr.
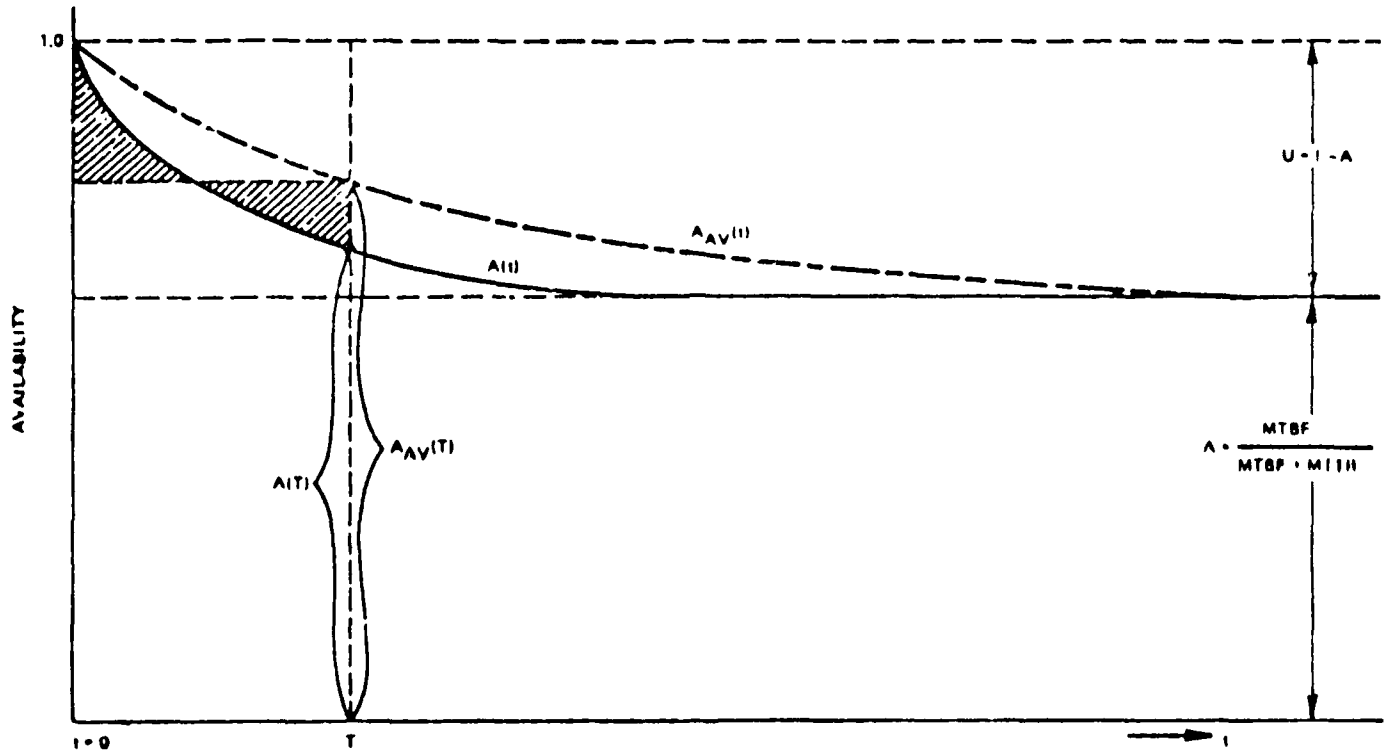
FIGURE 10.4.1.2-1: AVERAGE AND POINTWISE AVAILABILITY

$$A_{AV}(T) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{T(\lambda + \mu)^2} \left\{ 1 - \exp\left[- (\lambda \times \mu) \, T \right] \right\}$$

$$= \frac{2}{2.01} + \frac{0.01}{1(2.01)^2} \left\{ 1 - \exp\left[- (2.01) \, (1) \right] \right\}$$

$$= 0.995 + 0.0025 \, (1 - 0.134)$$

$$= 0.9972$$

and its expected "on" time for a 1-hr. mission would be:

(0.9972) (60) = 59.8 minutes

10.4.1.3 MODEL C - SERIES SYSTEM WITH REPAIRABLE/REPLACEABLE UNITS

When a series system consists of N units (with independent unit availabilities) separately repairable or replaceable whenever the system fails because of any one unit failing, the steady state availability is given by:

$$A = \prod_{i=1}^{N} A_i \tag{10.26}$$

$$= \prod_{i=1}^{N} \left(\frac{1}{1 + \dfrac{MTTR_i}{MTBF_i}} \right) \tag{10.27}$$

$$= \prod_{i=1}^{N} \left(\frac{1}{1 + \lambda_i / \mu_i} \right) \tag{10.28}$$

$$= \prod_{i=1}^{N} \left(\frac{1}{1 + \alpha_i} \right) \tag{10.29}$$

where

$$\alpha_i = \frac{MTTR_i}{MTBF_i} = \frac{\lambda_i}{\mu_i}$$

Furthermore, if each $\frac{MTTR_i}{MTBF_i} \ll 1$, which is usually the case for most practical systems, Eq. (10.29) can be approximated by:

$$A = (1 + \Sigma \, \alpha_i)^{-1} \tag{10.30}$$

Caution is necessary in computing α_i, since Eq. (10.30) applies to the availability of the whole system. Thus, when the units are replaceable as line replaceable units or system replaceable units, the $MTTR_i$ is the mean time required to replace the unit with a good one at the system maintenance level and is not the mean repair time of the failed removed unit. On the other hand, if failed units are not replaced but are repaired at the system level, $MTTR_i$ is the mean-time-to-repair of the

unit, which becomes also the downtime for the system. Thus, when computing the As of the units and the availability As of the system, all MTTRs must be those repair times that the system experiences as its own downtime. The $MTTR_i$ of the ith unit is thus the system mean repair time when the ith unit fails.

If we compare Eq. (10.30) with Eq. (10.20) in Model A we find that they are identical. The system maintenance time ratio (MTR) is:

$$\alpha = MTTR/MTBF \tag{10.31}$$

But the serial system's MTTR as shown in Section 4 is given by:

$$MTTR = \Sigma\lambda_i \ (MTTR_i)/\Sigma\lambda_i \tag{10.32}$$

while its MTBF is

$$MTBF = (\Sigma \ \lambda_i)^{-1}$$

$$= \Sigma\lambda_i \ (MTTR_i) \ \Sigma\lambda_i/\Sigma\lambda_i$$

$$= \Sigma\lambda_i \ (MTTR_i) = \Sigma\alpha_i \tag{10.33}$$

where $\lambda_i = \dfrac{1}{MTBF_i}$

In other words, the system MTR is the sum of the unit MTRs. The maintenance *time ratio (MTR)* is actually the average system downtime per system operating hour. Conceptually, it is very similar to the maintenance ratio (MR) defined as maintenance manhours expended per system operating hour. The difference is that in the MTR one looks only at system downtime in terms of clock hours of system repair, whereas in the MR one looks at all maintenance manhours expended at all maintenance levels to support system operation.

Eq. (10.30) can be still further simplified if $\displaystyle\sum_{i=1}^{N} \lambda_i/\mu_i < 0.1$

In that case

$$A \approx 1 - \sum_{i=1}^{N} \lambda_i/\mu_i \tag{10.34}$$

or the system availability is equal to 1 - (the sum of the unit MTRs).

Let us work some examples.

<u>Example No. 1</u>

Figure 10.4.1.3-1 represents a serial system consisting of 5 statistically independent subsystems, each with the indicated MTBF and MTTR. Find the steady state availability of the system.
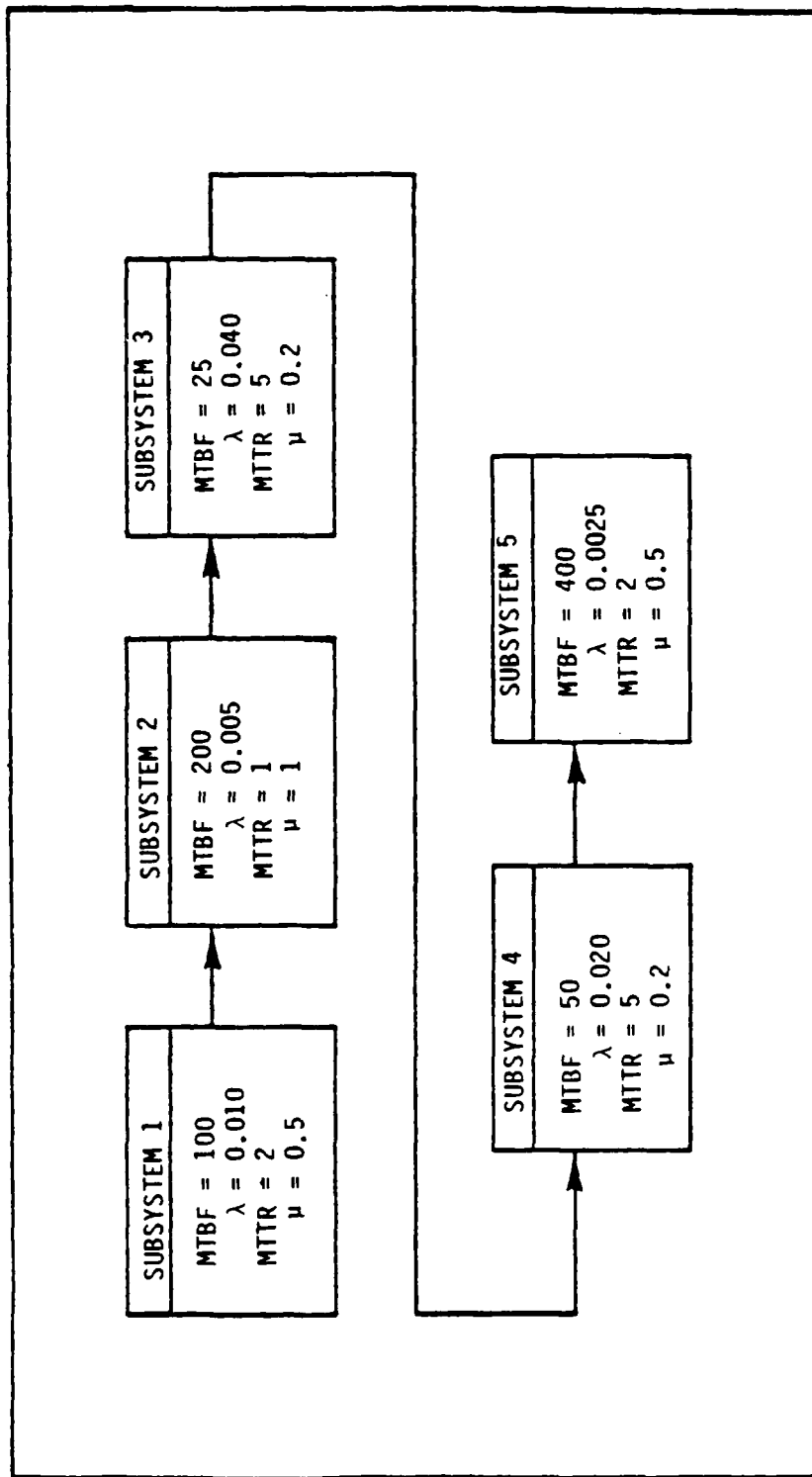
FIGURE 10.4.1.3-1: BLOCK DIAGRAM OF A SERIES SYSTEM

Note that for the system, we cannot use any of the simplifying assumptions since, for example, subsystems 3 and 4 have MTRs of 0.2 and 0.1, respectively which is not $\ll 1$.

Also $\sum_{i=1}^{N} \lambda_i/\mu_i = 0.33$ which is not < 0.1. Therefore, we must use the basic relationship, Eq. (10.27).

$$A = \prod_{i=1}^{5} \left(\frac{1}{1 + \frac{MTTR_i}{MTBF_i}} \right)$$

$$= \left(\frac{1}{1 + \frac{2}{100}} \right) \left(\frac{1}{1 + \frac{1}{200}} \right) \left(\frac{1}{1 + \frac{5}{25}} \right) \left(\frac{1}{1 + \frac{5}{50}} \right) \left(\frac{1}{1 + \frac{2}{400}} \right)$$

$$= (0.98039)(0.99502)(0.83333)(0.90909)(0.99502)$$

$$= 0.73534$$

Example No. 2

Now let us look at a similar series system, consisting of 5 statistically independent subsystems having the following MTBFs and MTTRs, as shown in the table below.

Subsystem	MTBF	MTTR	α	A
1	100	0.5	0.005	0.995
2	200	1	0.005	0.995
3	300	0.75	0.0025	0.9975
4	350	1.5	0.0043	0.9957
5	500	2	0.004	0.996

In this case, each $\alpha_i \ll 1$ and $\sum_{i=1}^{5} \alpha_i < 0.1$, so that we can use the simplified Eq. (10.34).

$$A \approx 1 - \sum_{i=1}^{5} \lambda_i/\mu_i = 1 - 0.0208 = 0.9792$$

Of course, the power and speed of modern hand held calculators tend to negate the benefits of the simplifying assumptions.

10.4.1.4 MODEL D - REDUNDANT SYSTEMS

In this model, the availability of some redundant systems is considered. First we deal with two equal, independent units in a parallel redundant arrangement with each unit being separately repairable or replaceable while the other continues operating. Thus, the system is "up" if both or any one of the two units operates.

If we define the unavailability U of a unit as

$$U = 1 - A = MTTR/(MTBF + MTTR) \tag{10.35}$$

then the probability that the system is unavailable is the probability that both units are down at the same time, which is

$$U_{system} = U^2 \tag{10.36}$$

and system availability is

$$A_{system} = 1 - U^2 \tag{10.37}$$

Further, using the binomial expansion

$$(A + U)^2 = A^2 + 2AU + U^2 \approx 1 \tag{10.38}$$

we find that we may write Eq. (10.38) also in the form

$$A_{system} = A^2 + 2AU \tag{10.39}$$

which gives as the probability A^2 that both units are operating at any point in time and the probability 2 AU that only one unit is working. Over a period of time T, the system will on the average be for a time TA^2 operating with both units up, while for 2 TAU only one unit will be up. If the performance of the system is P_1 when both units are up but only P_2 when only one unit is up, the system output or effectiveness SE over T^2 is expected to be

$$SE = P_1 TA^2 + 2P_2 TAU \tag{10.40}$$

Assume a ship with two engines which are subject to on board repair when they fail. When both engines work, the ship speed is 30 kt, and when only one engine works it is 20 kt. Let an engine MTBF be 90 hr let its MTTR be 10 hr, so that the availability of an engine's is A = 0.9 and its unavailability is U = 0.1. Over a 24-hour cruise the ship will be expected to travel on the average

$$SE = 30 \times 24 \times .81 + 2 \times 20 \times 24 \times 0.9 \times 0.1 = 583.2 + 86.4$$
$$= 669.6 \text{ nmi.}$$

The expected time for the ship to be found idle with both engines out for a 24-hour cruise is:

$$T_{idle} = 24U^2 = 24(0.01) = 0.24 \text{ hr} \tag{10.41}$$

For three units in parallel we get

$$(A + U)^3 = A^3 + 3A^2U + 3AU^2 + U^3 = 1 \tag{10.42}$$

If the system goes down only if all three units are down, system availability is:

$$A_{system} = A^3 + 3A^2U + 3AU^2 = 1 - U^3 \qquad (10.43)$$

but if at least two units are needed for system operation since a single unit is not sufficient, system availability becomes

$$A_{system} = A^3 + 3A^2U \qquad (10.44)$$

In general, for a system with n equal, redundant units, we expand the binominal term

$$(A + U)^n = 1, \text{ or}$$

$$A^n + nA^{n-1}U + \frac{n(n-1)}{2!}A^{n-2}U^2 + \frac{n(n-1)(n-2)}{3!}A^{n-3}U^3 \ldots + U^n = 1 \qquad (10.45)$$

which yields the probabilities of being in any one of the possible states. Then, by adding the probabilities of the acceptable states, we obtain the availability of the system. As stated earlier, the units must be independent of each other, both in terms of their failures and in terms of their repairs or replacements, with no queuing up for repair.

Reference 9 contains, throughout the text, extensive tabulations of availability and related measures of multiple parallel and standby redundant systems for cases of unrestricted as well as restricted repair when failed redundant units must queue up and wait until their turn comes to get repaired.

Returning briefly to Eq. (10.36), when the two redundant units are not equal but have unavailabilities $U_1 = 1 - A_1$ and $U_2 = 1 - A_2$, system unavailability becomes:

$$U_{system} = U_1U_2 \qquad (10.46)$$

and availability

$$A_{system} = 1 - U_1U_2 \qquad (10.47)$$

Again, we may expand the multinomial

$$(A_1 + U_1)(A_2 + U_2) = A_1A_2 + A_1U_2 + A_2U_1 + U_1U_2 \qquad (10.48)$$

and may write system availability in the form

$$A_{system} = A_1A_2 + A_1U_2 + A_2U_1 \qquad (10.49)$$

For n unequal units we expand the term

$$\prod_{i=1}^{n} (A_i + U_i) = 1 \qquad (10.50)$$

and add together the probabilities of acceptable states and other effectiveness measures, as illustrated in the ship engines example.

This approach is analogous to that shown in Section 5 (K out of N configuration) for reliability.

It can be shown that the limiting expression for an n equipment parallel redundant system reduces to the binomial form if there are as many repairmen as equipments. This is equivalent to treating each equipment as if it had a repairman assigned to it or to saying that a single repairman is assigned to the system but that the probability of a second failure occurring while the first is being repaired is very small. The expression for steady state availability is

$$A (1/n) = 1 - (1 - A)^n \qquad (10.51)$$

where n is the number of redundant equipments and 1/n indicates that at least 1 equipment must be available for the system to be available.

In general where at least m out of n redundant equipments must be available for the system to be available.

$$A (m/n) = \sum_{i=m}^{n} \binom{n}{i} A^i (1 - A)^{n-i}$$

$$= \sum_{i=m}^{n} \frac{n!}{(n-i)!\, i!} \left(\frac{\mu}{\mu + \lambda}\right)^i \left(\frac{\lambda}{\mu + \lambda}\right)^{n-i} \qquad (10.52)$$

Table 10.4.1.4-1 (Ref. 10) provides expressions for the instantaneous and steady state availability for 1, 2, and 3 equipments, parallel and standby redundancy, and single and multiple repair maintenance policies.

Single repair means that failed units can be repaired one at a time. If a unit fails, repairs are immediately initiated on it. If more than one unit is down, repairs are initiated on a single unit until it is fully operational; then, repairs are initiated on the second failed unit. For the case of multiple repair, all failed units can have repair work initiated on them as soon as failure occurs, and the work continues until each unit is operational. Also, a repair action on one unit is assumed to be independent of any other unit.

One case not yet addressed is the case of redundant units when repairs cannot be made until complete system failure (all redundant units have failed). The steady state availability can be approximated by (see Ref. 25 for deriving exact expressions):

$$A = \frac{MTTF}{MTTF + MTTR} \qquad (10.53)$$

where

MTTF = mean time to failure for redundant system

TABLE: 10.4.1.4-1 AVAILABILITY OF SOME REDUNDANT SYSTEMS BASED ON EXPONENTIAL FAILURE AND REPAIR DISTRIBUTIONS

No. of Equip-ments	Conditions — Type Redundancy	Conditions — Repair	Instantaneous Availability Model	Definitions of Constants for Instantaneous Availability Model	Steady State Availability — Model	Steady State Availability — Av. for λ = 0.01 μ = 0.2
1	—	—	$A(t) = \dfrac{\mu}{\mu+\lambda} + \dfrac{\lambda}{\mu+\lambda}\,e^{-(\mu+\lambda)t}$	—	$\dfrac{\mu}{\mu+\lambda}$	0.95
2	Standby	Single	$A(t) = \dfrac{\mu^2+\mu\lambda}{\mu^2+\mu\lambda+\lambda^2} - \dfrac{\lambda^2(\beta_2 e^{\beta_1 t} - \beta_1 e^{\beta_2 t})}{\beta_1\beta_2(\beta_1-\beta_2)}$	$\beta_1 = -(\lambda+\mu) - \sqrt{\mu\lambda}$ $\beta_2 = -(\lambda+\mu) + \sqrt{\mu\lambda}$	$\dfrac{\mu^2+\mu\lambda}{\mu^2+\mu\lambda+\lambda^2}$	0.998
	Standby	Multiple	$A(t) = \dfrac{2\mu^2+2\mu\lambda}{2\mu^2+2\mu\lambda+\lambda^2} - \dfrac{\lambda^2(\beta_2 e^{\beta_1 t} - \beta_1 e^{\beta_2 t})}{\beta_1\beta_2(\beta_1-\beta_2)}$	$\beta_1 = -\tfrac{1}{2}(2\lambda+3\mu) + \sqrt{\mu^2+4\mu\lambda}$ $\beta_2 = -\tfrac{1}{2}(2\lambda+3\mu) - \sqrt{\mu^2+4\mu\lambda}$	$\dfrac{2\mu^2+2\mu\lambda}{2\mu^2+2\mu\lambda+\lambda^2}$	0.999
	Parallel	Single	$A(t) = \dfrac{\mu^2+2\mu\lambda}{\mu^2+2\mu\lambda+\lambda^2} - \dfrac{2\lambda^2(\beta_2 e^{\beta_1 t} - \beta_1 e^{\beta_2 t})}{\beta_1\beta_2(\beta_1-\beta_2)}$	$\beta_1 = -\tfrac{1}{2}(3\lambda+2\mu) + \sqrt{\lambda^2+4\mu\lambda}$ $\beta_2 = -\tfrac{1}{2}(3\lambda+2\mu) - \sqrt{\lambda^2+4\mu\lambda}$	$\dfrac{\mu^2+2\mu\lambda}{\mu^2+2\mu\lambda+\lambda^2}$	0.996
	Parallel	Multiple	$A(t) = \dfrac{\mu^2+2\mu\lambda}{\mu^2+2\mu\lambda+2\lambda^2} - \dfrac{2\lambda^2(\beta_2 e^{\beta_1 t} - \beta_1 e^{\beta_2 t})}{\beta_1\beta_2(\beta_1-\beta_2)}$	$\beta_1 = 2(\mu+\lambda)$ $\beta_2 = -(\mu+\lambda)$	$\dfrac{\mu^2+2\mu\lambda}{\mu^2+2\mu\lambda+2\lambda^2}$	0.998
3	Standby	Single	$A(t) = \dfrac{\mu^3+\mu^2\lambda+\mu\lambda^2}{\mu^3+\mu^2\lambda+\mu\lambda^2+\lambda^3} + \dfrac{\lambda^3[\beta_2\beta_3(\beta_2-\beta_3)e^{\beta_1 t} - \beta_1\beta_3(\beta_1-\beta_3)e^{\beta_2 t} + \beta_1\beta_2(\beta_1-\beta_2)e^{\beta_3 t}]}{\beta_1\beta_2\beta_3(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3)}$	$\beta_1,\ \beta_2,$ and β_3 correspond to the three roots of $\beta^3 + \beta^2(3\lambda+3\mu) + \beta(3\lambda^2+4\mu\lambda+3\mu^2)$ $+ (\lambda^3+\mu\lambda^2+\lambda\mu^2+\mu^3)$	$\dfrac{\mu^3+\mu^2\lambda+\mu\lambda^2}{\mu^3+\mu^2\lambda+\mu\lambda^2+\lambda^3}$	0.9999
	Standby	Multiple	$A(t) = \dfrac{6\mu^3+6\mu^2\lambda+3\mu\lambda^2}{6\mu^3+6\mu^2\lambda+3\mu\lambda^2+\lambda^3} + \dfrac{\lambda^3[\beta_2\beta_3(\beta_2-\beta_3)e^{\beta_1 t} - \beta_1\beta_3(\beta_1-\beta_3)e^{\beta_2 t} + \beta_1\beta_2(\beta_1-\beta_2)e^{\beta_3 t}]}{\beta_1\beta_2\beta_3(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3)}$	$\beta_1,\ \beta_2,$ and β_3 correspond to the three roots of $\beta^3 + \beta^2(3\lambda+6\mu) + \beta(3\lambda^2+9\mu\lambda+11\mu^2)$ $+ (\lambda^3+3\mu\lambda^2+6\mu^2\lambda+6\mu^3)$	$\dfrac{6\mu^3+6\mu^2\lambda+3\mu\lambda^2}{6\mu^3+6\mu^2\lambda+3\mu\lambda^2+\lambda^3}$	0.99998
	Parallel	Single	$A(t) = \dfrac{\mu^3+3\mu^2\lambda+6\mu\lambda^2}{\mu^3+3\mu^2\lambda+6\mu\lambda^2+6\lambda^3} + \dfrac{6\lambda^3[\beta_2\beta_3(\beta_2-\beta_3)e^{\beta_1 t} - \beta_1\beta_3(\beta_1-\beta_3)e^{\beta_2 t} + \beta_1\beta_2(\beta_1-\beta_2)e^{\beta_3 t}]}{\beta_1\beta_2\beta_3(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3)}$	$\beta_1,\ \beta_2,$ and β_3 correspond to the three roots of $\beta^3 + \beta^2(6\lambda+3\mu) + \beta(11\lambda^2+9\mu\lambda+3\mu^2)$ $+ (6\lambda^3+6\mu\lambda^2+3\mu^2\lambda+\mu^3)$	$\dfrac{\mu^3+3\mu^2\lambda+6\mu\lambda^2}{\mu^3+3\mu^2\lambda+6\mu\lambda^2+6\lambda^3}$	0.9993
	Parallel	Multiple	$A(t) = \dfrac{\mu^3+3\mu^2\lambda+3\mu\lambda^2}{(\mu+\lambda)^3} + \dfrac{6\lambda^3[\beta_2\beta_3(\beta_2-\beta_3)e^{\beta_1 t} - \beta_1\beta_3(\beta_1-\beta_3)e^{\beta_2 t} + \beta_1\beta_2(\beta_1-\beta_2)e^{\beta_3 t}]}{\beta_1\beta_2\beta_3(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3)}$	$\beta_1,\ \beta_2,$ and β_3 correspond to the three roots of $\beta^3 + \beta^2(6\lambda+3\mu) + \beta(11(\mu+\lambda)^2) + 6(\mu+\lambda)^3$	$\dfrac{\mu^3+3\mu^2\lambda+3\mu\lambda^2}{\mu^3+3\mu^2\lambda+3\mu\lambda^2+\lambda^3}$	0.9999

NOTES:
1. $A(t)$ is the probability of a system being available at time t. $A(t)$ is a function of μ and λ the repair and failure rates. For all functions, the probability of a system being available, time zero is unity. The units of μ and λ must be the same as for t.

2. Instantaneous availability. The probability that the system will be available at any instant in time.

3. Mission availability. Expected availability for a given mission period. This value can be derived from the general model by computing the average value of $A(t)$ for the mission period. Mathematically, this is

$$A_m = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} A(t)\, dt$$

4. Usually t_1 is considered as zero.

Steady state availability. The portion of up time expected for continuous operation.

and

MTTR = mean time to restore all units in the redundant system

In the case of an n - unit <u>parallel</u> system

$$MTTF = \sum_{n=1}^{n} \frac{1}{n\lambda} \qquad (10.54)$$

and

$$MTTR = \frac{m}{\mu} \qquad (10.55)$$

where

m = 1, for the multiple repairs case

and

m = n, for the single repair case

or

$$A(1/n) = \frac{\sum_{n=1}^{n} \frac{1}{n\lambda}}{\sum_{n=1}^{n} \frac{1}{n\lambda} + \frac{m}{\mu}} \qquad (10.56)$$

In the case of an n - unit <u>standby</u> system with one active and n-1 standby units

$$MTTF = \frac{n}{\lambda} \qquad (10.57)$$

and

$$MTTR = \frac{m}{\lambda} \qquad (10.58)$$

where

m = 1, for the multiple repairs case

and

m = n, for the single repair case

Then

$$A = \frac{n/\lambda}{n/\lambda + m/\lambda} \qquad (10.59)$$

Following are some examples utilizing the concepts presented in this section.

Example No. 1

In the case of a 2-unit parallel system with λ = 0.01 fr/hr and μ = 1.0 rp/hr, if the system does not undergo repairs until both units fail the system's steady-state availability is by Eq. (10.56).

$$A(1/2) = \frac{\sum_{n=1}^{2} \frac{1}{n\lambda}}{\sum_{n=1}^{2} \frac{1}{n\lambda} + \frac{m}{\mu}}$$

With single repair (Case 1)

$$A(1/2) = \frac{1/\lambda + 1/2\lambda}{1/\lambda + 1/2\lambda + 2/\mu}$$

$$= \frac{\frac{1}{0.01} + \frac{1}{2(0.01)}}{\frac{1}{0.01} + \frac{1}{2(0.01)} + 2}$$

$$= 150/152 = 0.9868$$

With multiple repairs (Case 2)

$$A(1/2) = \frac{\frac{1}{\lambda} + \frac{1}{2\lambda}}{\frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{1}{\mu}}$$

or

$$A(1/2) = \frac{\frac{1}{0.01} + \frac{1}{2(0.01)}}{\frac{1}{0.01} + \frac{1}{2(0.01)} + \frac{1}{1}}$$

$$A(1/2) = 0.9934$$

If repairs are initiated each time a unit fails, with multiple repairs when both units fail (Case 3) then from Table 10.4.1.4-1.

$$A(1/2) = \frac{\mu^2 + 2\lambda\mu}{\mu^2 + 2\mu\lambda + \lambda^2}$$

or

$$A(1/2) = \frac{(1)^2 + 2(0.01)\,(1)}{(1)^2 + 2(1)\,(0.01) + (0.01)^2}$$

and

$$A(1/2) = 0.9999$$

Looking at the three cases of this example

	Availability	Average Downtime in 10,000 hrs.
Case 1	0.9868	132 hrs.
Case 2	0.9934	66 hrs.
Case 3	0.9999	1 hr.

We can see that the maintenance philosophy plays a significant role. For example, Cases 1 and 2 may not be acceptable for a crucial system such as a ballistic missile early warning system.

Example No. 2

We have three redundant equipments, each with an availability of 0.9. What is the availability of the configuration if two of the three equipments must be available at any time?

(a) from Eq. (10.45)

$$A^3 + 3A^2U + 3AU^2 + U^3 = 1$$

$$A^3 + 3A^2U = (0.9)^3 + 3 (0.9)^2 (0.1)$$

$$= 0.729 + 0.243 = 0.972$$

(b) From Eq. (10.52)

$$A(^2/_3) = \frac{3!}{(3-2)! \; 2!} (0.9)^2 (0.1)^{3-2} + \frac{3!}{(3-3)! \; 3!} (0.9)^3 (0.1)^{3-3}$$

$$= 3 (0.9)^2 (0.1) + (0.9)^3 = 0.972$$

Example No. 3

Given three standby equipments with multiple repair capability, the MTBF of each equipment is 1000 hrs and the repair rate is 0.02/hr. What is the expected steady state availability (A_{ss})?

From Table 10.4.1.4-1, we see that the appropriate formula is

$$A_{ss} = \frac{6\mu^3 + 6\mu^2\lambda + 3\mu\lambda^2}{6\mu^3 + 6\mu^2\lambda + 3\mu\lambda^2 + \lambda^3}$$

$$\lambda = 1/1000 = 0.001/hr$$
$$\mu = 0.02/hr$$

Substituting these values

$$A_{ss} = \frac{6(0.02)^3 + 6(0.02)^2(0.001) + 3(0.02)(0.001)^2}{6(0.02)^3 + 6(0.02)^2(0.001) + 3(0.02)(0.001)^2 + (0.001)^3}$$

$$= \frac{6(0.000008) + 6(0.0004)(0.001) + ((0.06)(0.000001)}{6(0.000008) + 6(0.0004)(0.001) + (0.06)(0.000001) + (0.001)^3}$$

$$= \frac{(0.0000480) + (0.00000240) + (0.00000006)}{(0.00004800) + (0.000002400) + (0.000000060) + (0.000000001)}$$

$$= \frac{5.046 \times 10^{-5}}{5.0461 \times 10^{-5}}$$

$$= 0.99998$$

Example No. 4

Given two standby equipments in an early warning ground radar system. The equipments are operated in parallel and have a single repair capability. The MTBF of each equipment is 100 hrs and the repair rate is 2/hr. What is the expected steady state availability?

From Table 10.4.1.4-1, the appropriate equation is:

$$A_{ss} = \frac{\mu^2 + \mu\lambda}{\mu^2 + \mu\lambda + \lambda^2} = \frac{(2)^2 + 2(0.01)}{(2)^2 + 2(0.01) + (0.01)^2}$$

$$= \frac{4.02}{4.0201} = 0.999975$$

Example No. 5

Let us return to the example of the previous section, Figure 10.4.1.3-1, in which we had a series system consisting of five subsystems with the following R&M parameters:

Subsystem	λ	μ	A (previously calculated)
1	0.01	0.5	0.98039
2	0.005	1	0.99502
3	0.04	0.2	0.83333
4	0.02	0.2	0.90909
5	0.0025	0.5	0.99502

It was previously found that the availability of this system was $\prod_{i=1}^{5} A_i = 0.73534$

Suppose that we would like to raise the system availability to 0.95 by using redundant parallel subsystems with multiple repair for subsystems 3 and 4 (the two with lowest availability). How many redundant subsystems would we need for each subsystem?

We have the situation

$$A_1 \ A_2 \ X_3 \ X_4 \ A_5 = 0.95$$

$$X_3 \ X_4 = \frac{0.95}{A_1 A_2 A_5} = \frac{0.95}{(0.98039)\ (0.99502)\ (0.99502)}$$

$$= \frac{0.95}{0.97065} \approx 0.98$$

This means that the product of the improved availabilities $(X_3 \ X_4)$ of subsystems 3 and 4 must be approximately 0.98. As a first cut, let us assume equal availability for improved subsystems 3 and 4. This means that each must have an availability of 0.99 for their product to be 0.98.

Eq. (10.51) is the general expression for improvement in availability through redundancy

$$A(1/n) = 1 - (1 - A)^n$$

where $A \ (1/n)$ is the improved availability with n redundant units. Let us call this A'. Then,

$$A' = 1 - (1 - A)^n$$

and

$$1 - A' = (1 - A)^n$$

taking the natural logarithm of both sides of the equation

$$\ln(1 - A') = n \ln (1 - A)$$

$$n = \frac{\ln(1-A')}{\ln(1-A)} \tag{10.60}$$

which is a general expression that can be used to determine the number of redundant subsystems required to achieve a desired subsystem availability (A').

Let us look at improved subsystem 3:

$$A' = 0.99$$
$$A = 0.83333$$

$$n = \frac{\ln(1-0.99)}{\ln(1-0.3333)} = \frac{\ln(0.01)}{\ln(0.16667)} = \frac{-4.605}{-1.79}$$

$$= 2.57, \text{ which rounds off to 3 redundant subsystems (total)}.$$

Similarly for subsystem 4:

$$n = \frac{\ln(1-0.99)}{\ln(1-0.90909)} = \frac{\ln(0.01)}{\ln(0.09091)} = \frac{-4.605}{-2.397}$$

= 1.92, which rounds off to 2 redundant subsystems

Thus, in order for the system availability to be raised to 0.95, we need 3 parallel redundant Subsystems 3, and 2 parallel redundant Subsystems 4.

Note that we have not discussed the optimum allocation of failure and repair rates to achieve a given availability; this will be done later in this section.

10.4.1.5 MODEL E - R&M PARAMETERS NOT DEFINED IN TERMS OF TIME

A very different situation in availability modeling is encountered when system "uptime" is not measured in hours of operation or any time parameter but rather in terms of number of rounds fired, miles travelled, actuations or cycles performed, etc. The reliability parameter is then no longer expressed in terms of MTBF but rather in mean-rounds-between-failures (MRBF), mean-miles-between-failures (MMBF), mean-cycles-between-failures (MCBF), etc. The failure rate then also is expressed in number of failures per round, per mile, or per cycle rather than number of failures per operating hour.

For straightforward reliability calculations this poses no problem since the same reliability equations apply as in the time domain, except that the variable time t, in hours is replaced by the variable number of rounds, number of miles, etc. We may then calculate the reliability of such systems for one, ten, one hundred, or any number of rounds fired or miles travelled, as we wish. The maintainability calculations remain as before, since downtime will always be measured in terms of time and the parameter of main interest remains the MTTR.

However, when it comes to availability, which usually combines two time parameters, (i.e., the MTBF and the MTTR into a probability of the system being up at some time, t), a difficult problem arises when the time, t, is replaced by rounds or miles, since the correlation between time and rounds or time and miles is quite variable.

An equation for the steady-state availability of machine guns is given in Reference 11. This equation is based on a mission profile that at discrete times, t_1, t_2, t_3, etc., requires the firing of N_1, N_2, N_3, etc., bursts of rounds. When the gun fails during a firing, for example at time t_3, it fires only f rounds instead of N_3 rounds and must undergo repair during which repair time it is not available to fire; for example, it fails to fire a required N_4 rounds at t_4, and a further N_5 rounds at t_5 before becoming again available (see Figure 10.4.1.5-1). Its system availability, A, based on the rounds not fired during repair may be expressed, for the described history, as:

$$A = (N_1 + N_2 + f)/(N_1 + N_2 + N_3 + N_4 + N_5) \qquad (10.61)$$
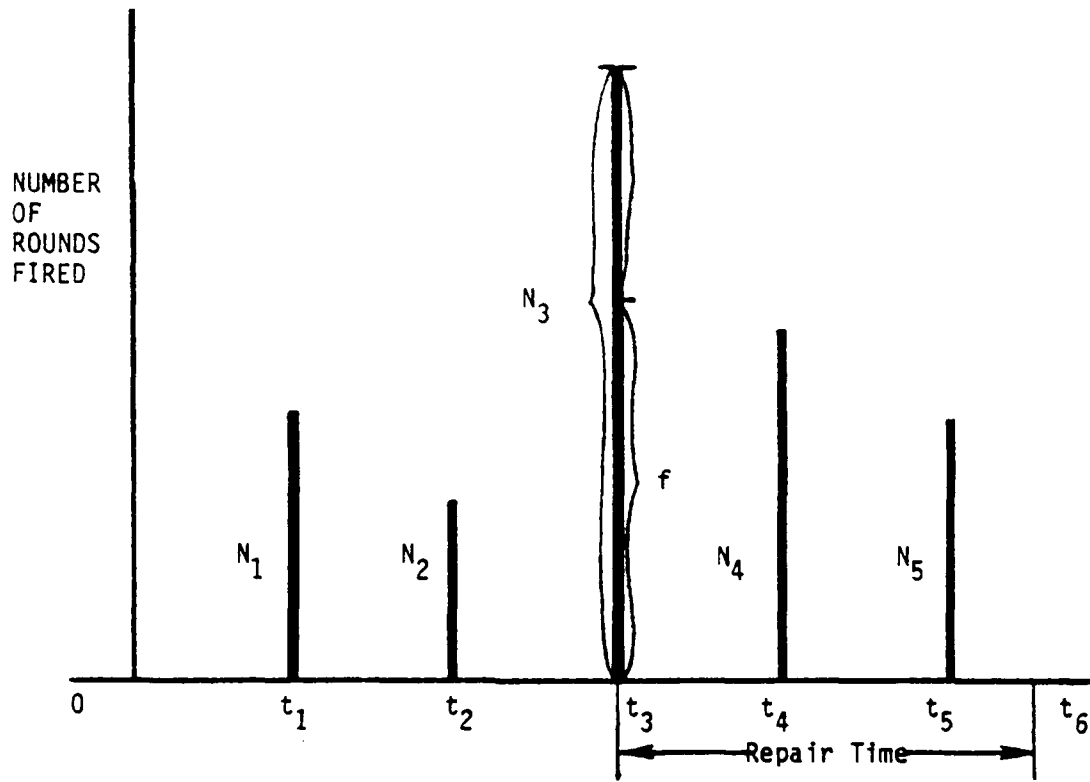
FIGURE 10.4.1.5-1: HYPOTHETICAL HISTORY OF A MACHINE GUN USAGE
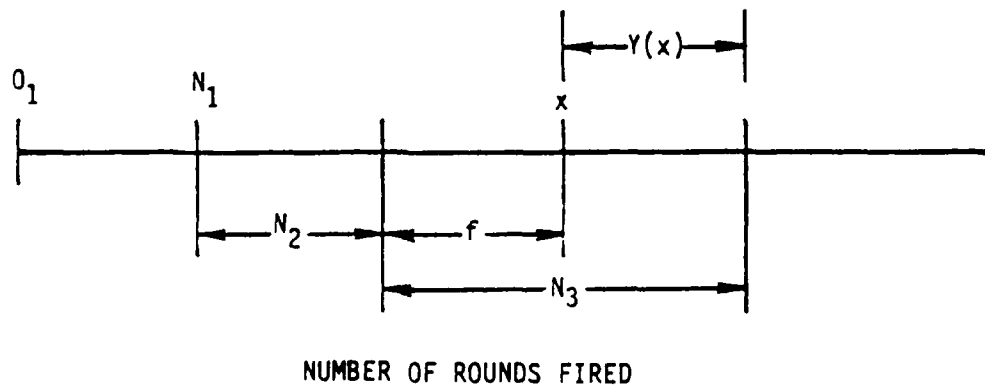
FIGURE 10.4.1.5-2: RENEWAL PROCESS IN TERMS OF ROUNDS FIRED

Each sequence of rounds fired followed by rounds missed (not fired) constitutes a renewal process in terms of rounds fired, as shown in Figure 10.4.1.5-2, where the gun fails after firing x rounds, fails to fire $\gamma(x)$ rounds in the burst of rounds during which it failed and also misses firing the required bursts of rounds while in repair for an MTTR = M. Assume that the requirements for firing bursts of rounds arrives at random according to a Poisson process with rate r and the average number of rounds per burst is N, then the limiting availability of the gun may be expressed as:

$$A = MRBF/(MRBF + N + \gamma MN) \qquad (10.62)$$

where MRBF is the mean number of rounds to failure. The derivation of this formula, developed by R.E. Barlow, is contained in the Appendix of Reference 11. To calculate A from Eq. (10.62) one must know the MRBF and MTTR of the gun, the average rounds N fired per burst, and the rate r at which requirements for firing bursts of rounds arrive.

Similar availability equations can be developed for other types of weapons and also for vehicles where the renewal process is in terms of miles travelled. Other approaches to calculating the availability of guns as well as vehicles are found in Reference 12 and are based on calculating from historical field data the maintenance ratios and, via regression analysis, the maintenance time ratios (called the "maintenance clock hour index") that are in turn used in the conventional time based equation of inherent, achieved, and operational availability.

For example, consider a machine gun system in a tank on which historical data are available, showing that 0.014 corrective maintenance manhours are expended per round fired and that per year 4800 rounds are fired while the vehicle travels for 240 hr per yr. The maintenance ratio (MR) for the gun system is then computed as (Ref. 12, pp. 36-38).

$$MR_{Gun} = \frac{MMH}{Round} \times \frac{Number\ of\ Rounds\ Fired\ per\ Annum}{Vehicle\ Operating\ Hours\ per\ Annum}$$

$$= 0.014 \times (4800/240) = 0.28 \qquad (10.63)$$

The dimensions for 0.28 are gun system maintenance manhours per vehicle operating hour. The corrective maintenance time ratio, α, (called maintenance clock hour index, Ω), is, according to this example, given by:

$$\alpha_{Gun} = 0.628(0.28)^{0.952} = 0.187 \qquad (10.64)$$

The numbers 0.628 and 0.952 are the intercept and the regression coefficients, respectively, obtained by regression analysis as developed in Reference 12, p. 18, Table 1. The dimension for α_{Gun} is gun system

downtime per vehicle operating hour. The inherent availability of the gun system is then, according to the conventional time equation, Eq. (10.20).

$$A_i = (1 + \alpha_{Gun})^{-1} = (1.187)^{-1} = 0.842 \qquad (10.65)$$

This may be interpreted as the gun system being available for 84.2% of the vehicle operating time. Caution is required in using this approach for weapon availability calculations, since in the case where the vehicle would have to be stationary and the gun would still fire rounds MR and α would become infinitely large and the inherent availability of the gun system would become zero.

10.4.2   MISSION RELIABILITY AND DEPENDABILITY MODELS

Although availability is a simple and appealing concept at first glance, it is a point concept, i.e., it refers to the probability of a system being operable at a random point in time. However, the ability of the system to continue to perform reliably for the duration of the desired operating (mission) period is often more significant. Operation over the desired period of time depends, then, on clearly defining system operating profiles. If the system has a number of operating modes, then the operating profile for each mode can be considered.

The term mission reliability has been used to denote the system reliability requirement for a particular interval of time. Thus, if the system has a constant failure rate region so that its reliability R can be expressed as:

$$R = \exp(-\lambda t) \qquad (10.66)$$

where

λ = failure rate = 1/MTBF
t = time for mission

then mission reliability R_M for a mission duration of T is expressed as:

$$R_M = \exp(-\lambda T) \qquad (10.67)$$

This reliability assessment, however, is conditional upon the system being operable at the beginning of its mission or its (point) availability.

In order to combine these two concepts, a simplified system effectiveness model may be used where the system effectiveness may be construed simply as the product of the probabilities that the system is operationally ready and that it is mission reliable.

If A is the mean availability of a system at any point in time t_q when we want to use the system and if R_M is the system reliability during mission time T, then system effectiveness E, not including performance, may be defined as:

$$E = AR_M \qquad (10.68)$$

Thus, A is a weighting factor, and E represents an assessment of system ability to operate without failure during a randomly chosen mission period.

One concept of dependability used by the Navy (Ref. 13) takes into account the fact that for some systems a failure which occurs during an operating period t_1 may be acceptable if the failure can be corrected in a time t_2 and the system continues to complete its mission. According to this concept, dependability may be represented by:

$$D = R_M + (1 - R_M)M_o \qquad (10.69)$$

where

D = system dependability -- or the probability that the mission will be successfully completed within the mission time t_1, providing a downtime per failure not exceeding a given time t_2 will not adversely affect the overall mission

R_M = mission reliability -- or the probability that the system will operate without failure for the mission time t_1

M_o = operational maintainability -- or the probability that when a failure occurs, it will be repaired in a time not exceeding the allowable downtime t_2

t_2 = specified period of time within which the system must be returned to operation

For this model, the exponential approximation of the log normal maintainability function is used, or

$$M_o = (1 - e^{-\mu t_2}) \qquad (10.70)$$

Then, the system effectiveness is:

$$E = AD = A \left[R_M + (1 - R_M) M_o \right] \qquad (10.71)$$

In the case where no maintenance is allowed during the mission ($t_2 = 0$ or $M_o = 0$), as in the case of a missile, then this reduces to Eq. (10.68).

$$E = AD = AR_M$$

This concept of dependability is compatible with the WSEIAC model and indeed can be taken into account in the dependability state transition matrices.

Let us examine an airborne system with the following parameters and requirements:

λ = 0.028 failures/hr
μ = 1 repair/hr
Mission time (T) = 8 hrs
t_a = 30 minutes to repair a failure during a mission

Thus,

$A = \dfrac{\mu}{\mu + \lambda} = \dfrac{1}{1 + 0.028} = .973$ at the start of the mission

$R_M = e^{-\lambda T} = e^{-(0.028)(8)} = 0.8$ (mission reliability)

$M_o = 1 - e^{-\mu t_a} = 1 - e^{-(1)(0.5)} = 0.4$ (probability of repairing failure during mission within ½ hour)

$\therefore E = A \left[R_M + (1 - R_M)\, M_o \right]$

$= 0.973 \left[0.8 + (1 - 0.8)\,(0.4) \right]$

$= 0.973 \left[0.8 + 0.08 \right] = 0.86$

10.4.3 OPERATIONAL READINESS MODELS

Availability, defined as the uptime ratio, is not always a sufficient measure to describe the ability of a system to be committed to a mission at any arbitrary time. In many practical military operations, the concept of operational readiness serves this purpose better. We here define operational readiness as the probability that a system is in an operable condition, i.e., ready to be committed to perform a mission when demands for its use arise. The difference as well as the similarity between availability and operational readiness will become clear by comparing the models developed subsequently with the availability models discussed in the preceding section.

In the development of operational readiness models, one has to consider the usage and the maintenance of the system, i.e., its operating, idle, and repair times. When a call arrives for the system to engage in a mission, the system at such time may be in a state of perfect repair and ready to operate immediately. But it may also be in need of maintenance and not ready. Its state when called upon to operate depends on the preceding usage of the system, i.e., on its preceding mission, in what condition it returned from that mission, and how much time has elapsed since it completed the last mission. Many models can be developed for specific cases, and some are discussed in the following paragraphs.

10.4.3.1 MODEL A - BASED UPON PROBABILITY OF FAILURE DURING PREVIOUS MISSION AND PROBABILITY OF REPAIR BEFORE NEXT MISSION DEMAND

In this model, the assumption is made that if no failures needing repair occurred in the preceding mission, the system is immediately ready to be used again; and, if such failures did occur, the system will be ready for the next mission only if its maintenance time is shorter than the

time by which the demand for its use arises. The operational readiness P_{OR} may then be expressed as:

$$P_{OR} = R(t) + Q(t) \times P(t_m < t_d) \tag{10.72}$$

where

$R(t)$	=	probability of no failures in the preceding mission
$Q(t)$	=	probability of one or more failures in the preceding mission
t	=	mission duration
$P(t_m < t_d)$	=	probability that if failures occur the system maintenance time, t_m, is shorter than the time, t_d, at which the next demand or call for mission engagement arrives

The calculations of $R(t)$ and $Q(t) = 1 - R(t)$ are comparatively simple using standard reliability equations; however, all possible types of failures that need fixing upon return in order to restore in full the system reliability and combat capability must be considered, including any failures in redundant configurations.

As for $P(t_m < t_d)$, one needs to know the probability distributions of the system maintenance time and of call arrivals. Denoting by $f(t_m)$ the probability density function of maintenance time and by $g(t_d)$, the probability density function of time to the arrival of the next call, counted from the instant the system returned from the preceding mission in a state requiring repair, the probability that the system will be restored to its full operational capability before the next call arrives is:

$$P(t_m < t_d) = \int_{t_m=0}^{\infty} f(t_m) \left[\int_{t_d=t_m}^{\infty} g(t_d)\, dt_d \right] dt_m \tag{10.73}$$

The integral in the square brackets on the right side of the equation is the probability that the call arrives at t_d after a variable time t_m. When this is multiplied by the density $f(t_m)$ of the duration of maintenance times and integrated over all possible values of t_m, we get $P(t_m < t_d)$.

Now assume that maintenance time t_m and time to next call arrival t_d are exponentially distributed, with M_1 being the mean time to maintain the system and M_2 the mean time to next call arrival. The probability density functions are thus:

$$f(t_m) = \exp(-t_m/M_1)/M_1 \tag{10.74}$$

$$f(t_d) = \exp(-t_d/M_2)/M_2 \tag{10.75}$$

We then obtain:

$$P(t_m < t_d) = \int_0^\infty M_1^{-1} \exp(-t_m/M_1)$$

$$\times \left[\int_{t_m}^\infty \frac{1}{M_2} \cdot \exp(-t_d/M_2) dt_d \right] dt_m$$

$$= \int_0^\infty M_1^{-1} \exp\left[-(1/M_1 + 1/M_2) t_m \right] dt_m$$

$$= M_2/(M_1 + M_2) \tag{10.76}$$

In this exponential case, system operation readiness becomes

$$P_{OR} = R(t) + Q(t \left[M_2/(M_1 + M_2) \right]) \tag{10.77}$$

As a numerical example let us look at a system with a probability of R = 0.8 of returning from a mission of t = 1 hr duration without requiring repair and therefore had a probability of Q = 0.2 that it will require repair. If system mean maintenance time is M_1 = 1 hr and the mean time to next call arrival is M_2 = 2 hr, the operational readiness of the system becomes:

$$P_{OR} = 0.8 + 0.2 (2/3) = 0.933$$

Comparing this result with the conventional steady-state availability concept and assuming that the system has a mean maintenance time of M_1 = 1 hr and a mean time to failure of M_2 = 5 hr (roughly corresponding to the exponential case of R = 0.8 for a one-hour mission), we obtain a system availability of:

$$A = M_2/(M_1 + M_2) = 5/6 = 0.833$$

which is a result quite different from P_{OR} = 0.933.

10.4.3.2 MODEL B - SAME AS MODEL A EXCEPT MISSICN DURATION TIME, t, IS PROBABILISTIC

The operational readiness model of Eq. (10.72) can be extended to the case when mission duration time t is not the same for each mission but is distributed with a density q(t). We then get:

$$P_{OR} = \int_0^\infty R(t)q(t)dt + P(t_m < t_d) \int_0^\infty Q(t)q(t)dt \tag{10.78}$$

Since the integrals in Eq. (10.78) are fixed numbers, we may write:

$$R = \int_0^\infty R(t)q(t)dt$$

$$Q = \int_0^\infty Q(t)q(t)dt \tag{10.79}$$

and using the symbol P for $P(t_m < t_d)$, i.e., $P = P(t_m < t_d)$, Eq. (10.78) may be written in the form:

$$P_{OR} = R + QP \qquad (10.80)$$

In this equation R is the probability that the system returns without failures from the last mission; $Q = 1 - R$ is the proability that one or more failures developed in the last mission; and P is the probability that the system will be repaired before the next call arrives if it developed failures. The mission times are variable here with density q(t).

10.4.3.3 MODEL C - SIMILAR TO MODEL A BUT INCLUDES CHECKOUT EQUIPMENT DETECTABILITY

The operational readiness of the system at time t_a is given by:

$$P_{OR}(t_a) = R(t_m) + \left[kM(t_r) \right] \left[1 - R(t_m) \right] \qquad (10.81)$$

where

$P_{OR}(t_a)$ = probability of system being available for turnaround time, e.g., t_a of 30 minutes, following completion of preceding mission or initial receipt of alert

$R(t_m)$ = probability that the system will survive the specified mission of duration t_m without failure

t_r = specified turnaround time, or maximum downtime for repair required of the system

k = probability that if a system failure occurs it will be detected during the mission or during system checkout following the mission

$M(t_r)$ = probability that a detected system failure can be repaired in time t_r to restore the system to operational status

Thus, when mission reliability, mission duration, availability, and turnaround time are specified for the system, the detectability-times-maintainability function for the system is constrained to pass through or exceed the point given by:

$$kM(t_r) \geq \frac{P_{OR}(t_a) - R(t_m)}{[1 - R(t_m)]}$$

Consider, for example, the following specified operational characteristics for a new weapons system:

Mission Reliability, $R(t_m) = 0.80$ for t_m of 8 hours

Operational Readiness $P_{OR}(t_a) = 0.95$ for turnaround time, t_a of 30 minutes, following completion of preceding mission or initial receipt of alert.

From the requirements, the required detectability-maintainability product (kM) is derived as follows:

$$kM(30) = \frac{P_{OR}(30) - R(8)}{1 - R(8)} = \frac{0.95 - 0.8}{1 - 0.8} = 0.75$$

Therefore, kM(30) = 0.75 is the joint probability, given that a system failure has occurred, that the failure will be detected (either during the mission or during postmission checkout) and will be repaired within 30 minutes following completion of the mission.

Assume that k is to be 0.9, i.e., built-in test equipment is to be incorporated to detect at least 90% of the system failures and provide go/no-go failure indication.

Then, the maintainability requirement is:

$$M(30) = \frac{0.75}{k} = \frac{0.75}{0.9} \approx 0.83$$

which means that 83% of all system repair actions detected during the mission or during postmission checkout must be completed within 30 minutes.

Using the exponential approximation, maintainability as a function of repair time is expressed as the probability of repair in time t_r:

$$M(t_r) = 1 - e^{-\mu t_r} = 1 - e^{-t_r/\overline{M}_{ct}} \qquad (10.82)$$

where

$$
\begin{aligned}
\overline{M}_{ct} &= \quad \text{MTTR} \\
\mu &= \quad \text{repair rate, } 1/\overline{M}_{ct} \\
t_r &= \quad \text{repair time for which M(t) is to be estimated}
\end{aligned}
$$

The required mean time to repair $(\overline{M}_{ct})$ is found from Eq. (10.82) by taking the natural log of both sides:

$$\overline{M}_{ct} = -\frac{t_r}{\ln[1-M(t_r)]}$$

Substituting t_r = 30 minutes, and $M(t_r)$, which we previously found to be 0.83,

$$\overline{M}_{ct} = -\frac{30}{\ln(0.17)} = \frac{-30}{-1.77} \approx 17 \text{ minutes}$$

And from $M(t_{max})$ = 0.95 we find the maximum time for repair of 95% of detected system failures $(M_{max_{ct}})$ as follows:

$$M(t_{max}) = 0.95 = 1 - e^{-M_{max_{ct}}/\overline{M}_{ct}}$$

$$
\begin{aligned}
M_{max_{ct}} &= -\overline{M}_{ct} \ln(1 - 0.95) \\
&= -(17)(-3) = 51 \text{ minutes}
\end{aligned}
$$

Thus, these requirements could be established as design requirements in a system development specification.

Detectability Factor, k $\quad$ = 0.90

Mean Time To Repair, $\overline{M}_{ct}$ $\quad$ = 17 minutes

Maximum Time To Repair, $M_{max_{ct}}$ = 51 minutes

10.4.3.4 MODEL D - FOR A POPULATION OF N SYSTEMS

Let N be the total population of systems, e.g., squadron of aircraft. The service facility itself shall be considered as having k channels, each servicing systems at a mean rate μ. The analysis is based on an assumed Poisson distribution of arrivals and on a mean service time which is assumed to be exponentially distributed. This service is performed on a first come, first served basis.

The basic equations (derived in Ref. 11) are as follows:

$$P_n = \frac{N!}{(N-n)!} \left(\frac{\rho^k}{k!}\right)\left(\frac{\rho}{k}\right)^{n-k} P_0 \quad \text{when } n > k \tag{10.83}$$

$$P_n = \frac{N!}{(N-n)!} \frac{\rho^n}{n!} P_0 \quad \text{when } n \leq k \tag{10.84}$$

$$P_0 = \left[\sum_{n=0}^{n=k} \frac{N!}{(N-n)!} \frac{\rho^n}{n!} + \sum_{n=k}^{N} \frac{N!}{(N-n)!} \left(\frac{\rho^k}{k!}\right)\left(\frac{\rho}{k}\right)^{n-k}\right]^{-1} \tag{10.85}$$

$$\rho = \frac{\lambda}{\mu} = \frac{\text{Mean arrival rate (failure)}}{\text{Mean service rate}} \tag{10.86}$$

where

p_i $\quad$ = probability of i units awaiting or undergoing service

k $\quad$ = number of repair channels or facilities

N $\quad$ = total number of systems

$$P_{OR} = \frac{N-\overline{n}}{N} \tag{10.87}$$

where P_{OR} = probability that a system is neither awaiting nor undergoing service.

$\overline{n}$ $\quad$ = average number of systems either awaiting or undergoing service at a given time and is defined by:

$$\overline{n} = \sum_{n=0}^{N} np_n \tag{10.88}$$

The specific procedure, which will be illustrated by an example, is as follows:

Step 1   Use Eq. (10.85) to solve for p_0

Step 2   Use p_0 from Step 1 to help derive p_n for all values of $n \leq k$ by use of Eq. (10.84)

Step 3   Use p_0 from Step 1 to help derive p_n for all values of $n > k$ by use of Eq. (10.83)

Step 4   For all values of n, from 0 through N, sum the terms np_n derived from Steps 1 through 3. This, per Eq. (10.88) gives $\bar{n}$ the average number of systems not ready

Step 5   Use Step 4 results and Eq. (10.87) to obtain the operational readiness probability, P_{OR}

Example - P_{OR} of Interceptor Squadron

An interceptor squadron contains fifteen planes and has available four flight line repair channels. Each plane averages 50 operating hours per month out of 24 times 30, or 720 total available hours. Because of five-day, two-shift maintenance each failure requires an average of five clock hours (MTTR) to repair. The plane MTBF is 3.8 operating hours between failures. What is the operational readiness probability for this squadron?

We first compute the utilization factor ρ

$$\rho = \frac{MTTR}{MTBF} \times \frac{\text{(Operating hours per plane per month)}}{\text{(Total hours per month)}}$$

$$= \frac{(5)(50)}{(3.8)(720)} = \frac{250}{2500} = 0.1$$

Step 1.   Use equation (10.85) and obtain p_0 by summing terms (1) and (2).

$$p_0 = \left[\sum_{n=0}^{n=k} \frac{N!}{(N-n)!} \frac{\rho^n}{n!} + \sum_{n=k}^{n=N} \frac{N!}{(N-n)!} \frac{\rho^k}{k!} \frac{\rho^{n-k}}{k} \right]^{-1}$$

$$p_0 = \left[\sum_{n=0}^{4} \frac{15!}{(15-n)!} \frac{(0.1)^n}{n!} + \sum_{n=4}^{15} \frac{15!}{(15-n)!} \frac{(0.1^4)}{4!} \frac{0.1}{4}^{n-4} \right]^{-1}$$

The calculated results are shown in the following table:

n	Term (1)	Term (2)
0	1.0	
1	1.5	
2	1.05	
3	0.455	
4	0.1365	0.1365
5	4.1415	0.0375
6		0.00935
7		0.00211
8		0.00042
9		0.00007
10		0.00001
11		0.00000
12		0.00000
13		0.00000
14		0.00000
15		0.00000
		0.18596

$$p_0 = (4.1415 + 0.18596)^{-1} = (4.3275)^{-1} = 0.23$$

Step 2. Use equation (10.84) and obtain p_n for $n = 1$ through 4.

$$P_n = \frac{N!}{(N-n)!} \frac{\rho^n}{n!} P_0$$

Thus

$$P_1 = \frac{15!}{(15-1)!} \frac{(0.1)^1}{1!} (0.23)$$

$$= 0.3450$$

$$P_2 = \frac{15!}{13!} \frac{(0.1)^2}{2!} (0.23)$$

$$= 0.2415$$

$$P_3 = \frac{15!}{12!} \frac{(0.1)^3}{3!} (0.23)$$

$$= 0.10465$$

$$P_4 = \frac{15!}{11!} \frac{(0.1)^4}{4!} (0.23)$$

$$= 0.0313$$

<u>Step 3.</u> Use equation (10.83) and obtain p_n for $n = 5$ through 15.

$$p_n = \frac{N!}{(N-n)!} \left(\frac{\rho^k}{k!}\right)\left(\frac{\rho}{k}\right)^{n-k} p_0$$

Thus

$$p_5 = \frac{15!}{10!} \left[\frac{(0.1)^4}{4!}\right]\left(\frac{0.1}{4}\right)^1 (0.23)$$

$$= 0.0086$$

$$p_6 = \frac{15!}{9!} \left(\frac{0.1^4}{4!}\right)\left(\frac{0.1}{4}\right)^2 (0.23)$$

$$= 0.00214$$

Similarily,

p_7 = 0.000486
p_8 = 0.000097
p_9 = 0.000017
p_{10} through p_{15} are negligible probabilities.

<u>Step 4.</u> Sum the terms np_n for $n = 0$ through $n = 15$.

n	p_n	np_n
0	0.2300	0
1	0.3450	0.3450
2	0.2415	0.4830
3	0.1047	0.314100
4	0.0313	0.012500
5	0.0086	0.043000
6	0.00214	0.012850
7	0.000486	0.003400
8	0.000097	0.000776
9	0.000017	0.000153
10	---	---
11	---	---
12	---	---
13	---	---
14	---	---
15	---	---
Totals		1.214779

Therefore from equation (10.88):

$$\bar{n} = \sum_{n=0}^{N} np_n$$

$$= 1.215 \text{ planes which are not ready on the average}$$

<u>Step 5.</u> Using Step 4 results and equation (5.87), we obtain P_{OR}, the operational readiness probability

$$P_{OR} = \frac{N - \bar{n}}{N}$$

$$= \frac{15 - 1.215}{15} = \frac{13.785}{15}$$

$$= 0.919$$

As can be seen, the calculations are rather laborious and best done by a computer. Figures 10.4.3.4-1 and 10.4.3.4-2 (from Ref. 10) are a series of curves for N = 15 and N = 20 with k values ranging from 1 to 10 and 1 to 20, respectively. Note that 0.919 checks out the ρ = 0.1, k = 4 point on Figure 10.4.3.4-1.

10.5 COMPLEX MODELS

In summing up the discussion of models, it should be recognized that there may be other measures of system R&M parameters or system effectiveness than those previously discussed. For example, in cases such as manned aircraft models it might be meaningful to combine operational readiness and equipment availability into one index, or we may wish to combine detection probability and availability for a ground radar system to be an index of the probability that a raid launched at any random time will be detected. The important point in selecting an index of system reliability effectiveness is recognizing that it is equivalent to a correct statement of the problem.

When selecting an index of effectiveness we should keep in mind some characteristics without which the index would be of little value. Probably the most important characteristic is that the index be expressed quantitatively. We should be able to reduce it to a number such that comparisons between alternative designs can be made. Furthermore, the index we choose must have a basis in physical reality. Thus it should be descriptive of the real problem, not exaggerated or oversimplified. Yet at the same time the index should be simple enough to allow for mathematical manipulation to permit evaluating alternatives.

In complex system effectiveness mathematical models, an attempt is made to relate the impact of system reliability, maintainability, and performance to the mission profiles, scenario, use, and logistic support. Only in simple situations can a meaningful single model be developed that will relate all these parameters and yield a single quantitative measure of system effectiveness. Numerous complex computerized models exist and, as a matter of fact, every major company in the aerospace business has developed a multitude of such models. In the following paragraphs we discuss some models which have achieved a certain popularity and a degree of acceptance within NASA and DoD. The models do not include system reliability models or life cycle cost models; these will be discussed later.
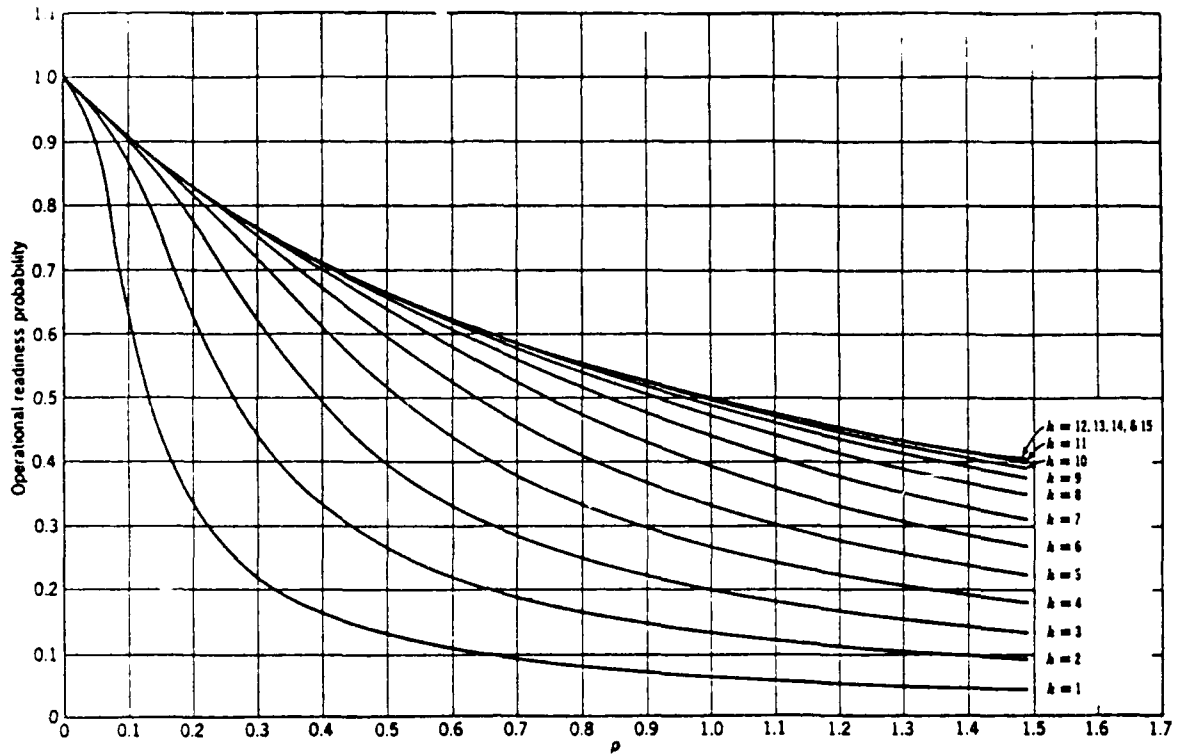
FIGURE 10.4.3.4-1: OPERATIONAL READINESS PROBABILITY VERSUS QUEUING FACTOR p. FOR POPULATION SIZE N = 15; NUMBER OF REPAIR CHANNELS K.
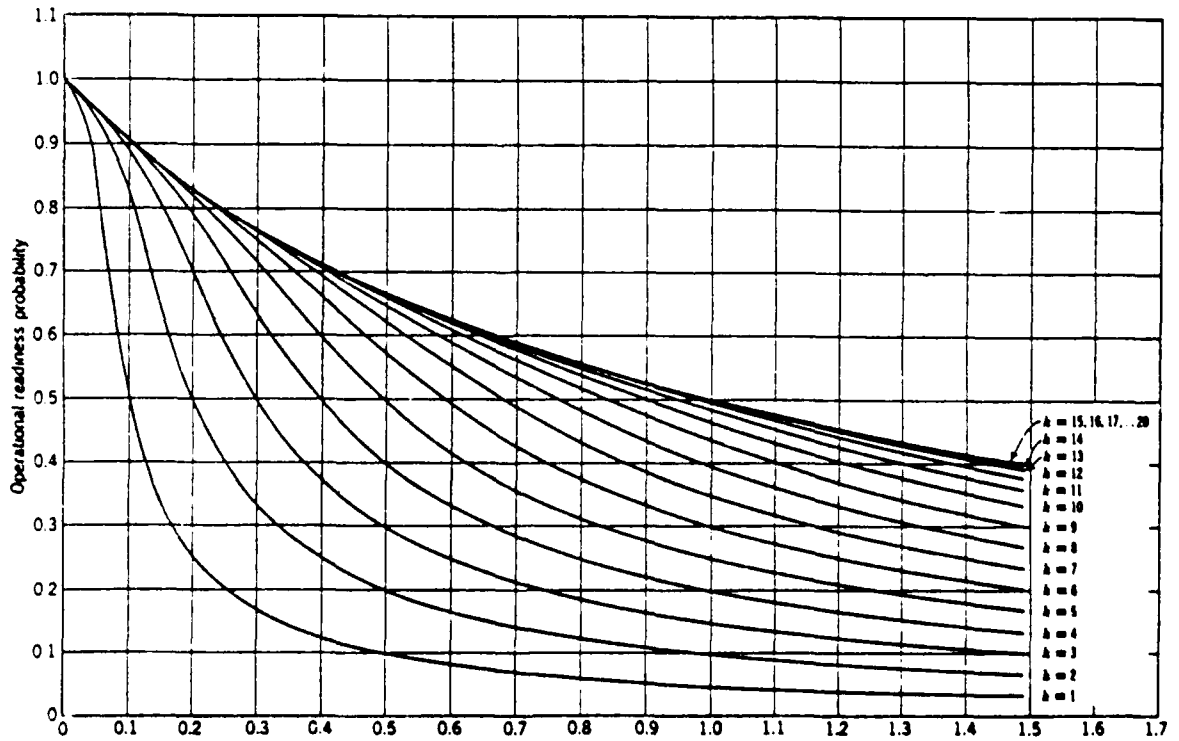
FIGURE 10.4.3.4-2: OPERATIONAL READINESS PROBABILITY VERSUS QUEUING FACTOR p1. FOR POPULATION SIZE N = 20; NUMBER OF REPAIR CHANNELS k.

10.5.1 RELIABILITY, MAINTAINABILITY, AND AVAILABILITY TRADE-OFF TOOL (R&MA2T2)

$R\&MA^2T^2$ has been merged with ORACLE (Optimized Reliability and Component Life Estimates) and allows for the evaluation of complex repairable serial parallel systems. It permits the analysis of system mean-time-to-first-failure, steady state mean-time-to-failure, system mean-time-to-restoration, and availability based on item failure rates (obtained from ORACLE) and repair rates (which must be obtained from the results of maintainability predictions or analyses).

    Contact: RADC/RBE
                 Griffiss AFB, NY 13441

10.5.2 TIGER

TIGER is the generic name for a family of computer programs which can be used to evaluate by simulation a complex system in order to estimate various reliability, readiness, and availability measures. The system can range in complexity from a single equipment, such as a radar or sonar, to a complete weapon system, such as a ship, airplane, or tank. Important TIGER features include: ranking the equipment by degree of unreliability and unavailability; evaluating a mission with multiphase types; and performing sensitivity analyses on a complex system by downgrading or upgrading the characteristics of each equipment.

    Contact: Naval Ship Engineering Center
                 Ship Design Division
                 Department of the Navy
                 Washington, DC 20362

10.5.3 GENERAL EFFECTIVENESS METHODOLOGY (GEM)

The GEM system was developed by the Naval Applied Sciences Laboratory in order to provide engineers with a user oriented reliability evaluation technique (Ref. 14). The user interacts with GEM by means of a language especially developed for use in reliability problems.

GEM can be used to support systems development, trade-off analyses, evaluation, and optimization. The processor is structured to evaluate variables such as reliability with or without repair, instantaneous availability, and interval reliability for systems that include such hardware interdependencies as bridge networks, shared elements, standby equipment, and environmental strategies and priorities including repairmen and spare parts pools.

    Contact: Department of the Navy
                 Washington, DC 20362

10.5.4 AVAILABILITY - RELIABILITY ANALYSIS

This simulation method analyzes the reliability of basic equipment, including Government Furnished Equipment (GFE), taking into consideration its availability, maintainability, operational profile, and mission reliability. The analysis will determine probabilities of success on the basis of these parameters. These probabilities can be used to determine a realistic system reliability requirement and can be used in identifying areas where reliability is not satisfactory.

This has proven useful as a model using real data in evaluating RAM requirements, identifying weak assemblies, and identifying contractual performance requirements.

> Contact: U.S. Army Material Systems Analysis Activity
> Aberdeen Proving Grounds, MD 21005

10.5.5 A COMPARISON OF ANALYTIC AND SIMULATION RELIABILITY AND MAINTAINABILITY (R&M PREDICTION MODELS)

Two methods for predicting the reliability and maintainability (R&M) of systems were evaluated: a simulation method and an analytic method. Two computer programs (SIM3 and GEMJR) incorporating these methods and their input and output were assessed. The simulation method used Monte Carlo techniques in predicting reliability. The analytic method incorporated the Poisson failure process to develop stochastic matrices which can be solved using infinite series to give reliability and availability indices. The advantages and disadvantages of both methods were considered. System configuration changes and complex missions can be considered more effectively using the simulation method. However, the simulation method does not calculate availability and provides only approximate results. In contrast, the analytic method predicts exact results and can examine such maintenance aspects as repairmen, standbys, and redundancies. Both methods are useful tools, depending upon the R&M applications.

> Contact: D.W. Taylor Naval Research and Development Center
> Bethesda, MD

10.5.6 SEE - SYSTEMS EFFECTIVENESS EVALUATION COMPUTER PROGRAM

A system of eight integrated computer programs has been developed to assess the effectiveness of any complex electronic system. The programs were originally developed to assess the reliability and maintainability of twelve sets of Acceptance Checkout Equipment/Spacecraft ZAEC-S/C, each set containing 175 racks of equipment and 1,000 piece parts. Input to the System Effectiveness Evaluation (SEE) programs consists of system configuration data, elapsed time meter readings, and edited failure reports. The outputs of the SEE programs are: (1) Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) for all unique parts of assemblies, for all subsystems and for the system, with associated confidence parameters and flagging of weak links; (2) Printer-Plotter trend charts of the MTBFs and MTTRs; (3) MTBF and MTTR correlation

charts comparing performance of all ground stations; (4) computation of system reliability, availability, and expected cumulative downtime during a simulated mission; and (5) numerous utility programs used in spares prediction and to assist in identification of problem areas. Proper and timely integration of three separate and distinct data areas are essential for desired results: a set of translation tables to precisely encode the complete logical description of all equipment to be assessed; systematic reporting and processing of failure experience; and periodic recording and processing of equipment operating time. The primary feature of the SEE program is the ability to rapidly pinpoint equipment problem areas for corrective action down to the lowest possible level of assembly. The programs can be modified to be utilized by any large complex electronic system.

> Contact: Computer Software Management
> and Information Center (COSMIC)
> 112 Barrow Hall
> University of Georgia
> Athens, Georgia 20602

Table 10.5.6-1 contains a summary of additional computer programs for availability/effectiveness evaluation.

10.6 TRADEOFF TECHNIQUES

10.6.1 GENERAL

A tradeoff is a rational selection among alternatives in order to optimize some system parameter that is a function of two or more variables which are being compared (traded off). Examples of system tradeoffs involve performance, reliability, maintainability, cost, schedule, and risk. A tradeoff may be quantitative or qualitative. Insofar as possible, it is desirable that tradeoffs be based on quantifiable, analytic, or empirical relationships. Where this is not possible, then semiquantitative methods using ordinal rankings or weighting factors are often used.

The methodology for structuring and performing tradeoff analyses is part of the system engineering process described in Section 4. The basic steps, summarized here are:

(1) Define the tradeoff problem and establish the tradeoff criteria and constraints

(2) Synthesize alternative design configurations

(3) Analyze these alternative configurations

(4) Evaluate the results of the analyses with respect to the criteria, eliminating those which violate constraint boundaries

(5) Select the alternative which best meets criteria and constraint boundaries or iterate the design alternatives, repeating Steps 2 through 5 to obtain improved solutions.

TABLE 10.5.6-1: SUMMARY OF PROGRAMS FOR AVAILABILITY/EFFECTIVENESS EVALUATION

Program Description	Organization (Originator or User/Sponsor)	Reference
A simulation program for availability analysis using minimal cuts	RTI/NASL	15
Launch vehicle availability for the Saturn V	Boeing/NASA MSC	16
Availability and support, used on Minuteman	STL/AF	17
Availability re Monte Carlo (MORL)	Douglas,NASA	18
Availability re Monte Carlo, used on BMEWS	PRC	19
Investigation of the difficulties in existing program languages for availability and related problems	Cook Electric/AFSC RADC	20
Availability of aircraft, used on B58, F111	General Dynamics, F.W.	21
Effectiveness portion of a family of programs for early weapon system planning (UNILOG)	Martin, Orlando	21
Operational analysis and availability, used on Atlas and Centaur	General Dynamics, F.W.	22
Support-availability multi-systems operations model (SAMSOM)	RAND/AF	23
Efficient availability evaluation as changes are made	ARINC/NASL	24
Effectiveness and design adequacy simulation and evaluation of aircraft	ARINC/AF ASD	24
WSEIAC model, which combines availability, dependability, and capability	ARINC In-House	24
System effectiveness analyzer (SEA) for prediction and optimization	Computer Applications/NASL	24
Steady-state effectiveness, called system effectiveness evaluation analyzer (SEE/AM)	Auerbach/DCA	24
System simulation (SEE/SIM)	Auerbach/BuShips	24
ASW mission effectiveness in support of advanced ASW ship	ARMA/BuWps	24
Effectiveness of multi-mode systems, for the E2A/ARDS	ARINC/BuWps	24

System effectiveness and cost effectiveness models provide the best tools for performing tradeoff studies on the system level. Through the computerized models, any changes in any of the multitude of reliability, maintainability, performance, mission profile, logistic support, and other parameters can be immediately evaluated as to their effect on the effectiveness and total cost of a system. Thus, cost effectiveness modeling and evaluation, besides being used for selecting a specific system design approach from among several competing alternatives, is a very powerful tool for performing parametric sensitivity studies and tradeoffs down to component level when optimizing designs to provide the most effective system for a given budgetary and life cycle cost constraint or the least costly system for a desired effectiveness level.

At times, however, especially in the case of the more simple systems, tradeoffs may be limited to achieving a required system availability while meeting the specified reliability and maintainability requirements. Comparatively simple tradeoffs techniques can then be used as shown in the following paragraphs.

10.6.2 RELIABILITY - AVAILABILITY - MAINTAINABILITY TRADEOFFS

The reliability-maintainability-availability relationship provides a measure of system effectiveness within which considerable tradeoff potential usually exists, e.g., between reliability, maintainability, and logistic support factors. This potential should be re-evaluated at each successive stage of system development to optimize the balance between reliability, maintainability, and other system effectiveness parameters with respect to technical risks, life cycle cost, acquisition schedule, and operating and maintenance requirements. The latter become increasingly more important as complexity of system designs increases, dictating the need for integration of system monitoring and checkout provisions in the basic design.

As stated earlier in this section and in Section 2, reliability and maintainability jointly determine the inherent availability of a system. Thus, when an availability requirement is specified, there is a distinct possibility of trading off between reliability and maintainability, since in the steady state availability depends only on the ratio or ratios of MTTR/MTBF which was previously referred to as maintenance time ratio (MTR), α, i.e.,

$$\alpha = \text{MTTR/MTBF} = \lambda/\mu \tag{10.88}$$

so that the inherent availability equation assumed the form

$$A_i = 1/(1 + \alpha) \tag{10.89}$$

As an example, consider systems I and II with

$$\text{MTTR}_I = 0.1 \text{ hr.}$$
$$\text{MTBF}_I = 2 \text{ hr.}$$
$$\text{MTTR}_{II} = 10 \text{ hr.}$$
$$\text{MTBF}_{II} = 200 \text{ hr.}$$

Then the steady state availability is

$$A_I = 1/[1 + (0.1/2)] = 0.952$$
$$A_{II}^I = 1/[1 + (10/200)] = 0.952$$

Both systems have the same availability, but they are not equally desirable. A 10-hr MTTR might be too long for some systems, whereas a 2-hr MTBF might be too short for some systems.

Even though reliability and maintainability individually can be increased or decreased in combinations giving the same system availability, care must be taken to insure that reliability does not fall below its specified minimum or that individually acceptable values of reliability and maintainability are not combined to produce an unacceptable level of system availability.

A generalized plot of Eq. (10.88) is given in Figure 10.6.2-1. A plot of A vs. λ/μ, is given in Figure 10.6.2-2. These equations and graphs show that in order to optimize availability it is desirable to make the ratio of MTBF/MTTR as high as possible.

Since increasing MTBF and decreasing MTTR is desirable, the equation for availability can be plotted in terms of MTBF and 1/MTTR (or μ) as shown in Figure 10.6.2-3. Each of the curves representing the same availability in Figure 10.6.2-3 just as each of the lines in Figure 10.6.2-1, is called isoavailability contours; corresponding values of MTBF and MTTR give the same value of A, all other things being equal. Availability nomographs useful for reliability and maintainability tradeoffs are given in Reference 13. Figure 10.6.2-4 is an example of an availability nomograph.

There are obvious practical limits which must be considered in tradeoff optimization. These are called constraints, and all purposeful optimization must be bounded by constraints into feasible regions. For example, there are practical limits as to how high a value for MTBF can be achieved or how low MTTR can be made. In the one case, the reliability of system components or the required redundancy might be so high that the desired reliability could not be realistically achieved within the state-of-the-art or would be so expensive as to violate cost constraints. Similarly, MTTRs close to zero would require extreme maintainability design features, such as completely built-in test features or automatic test and checkout to allow fault isolation to each individual replaceable module, with perhaps automatic switchover from a failed item to a standby item. This also could easily violate state-of-the-art or cost constraints.

It follows, then, that tradeoffs not only involve relationships among system parameters and variables but also they are bounded by both technical and economic constraints. In a sense, all tradeoffs are economic ones, requiring cost-benefit analysis (not necessarily in terms of dollar costs but rather in terms of the availability and consumption of resources, of which dollars are often the most convenient measure). Resource constraints may also include manpower and skill levels, schedule or time availability, and the technical state-of-the-art capability. Later sections of this chapter deal with the cost problem.
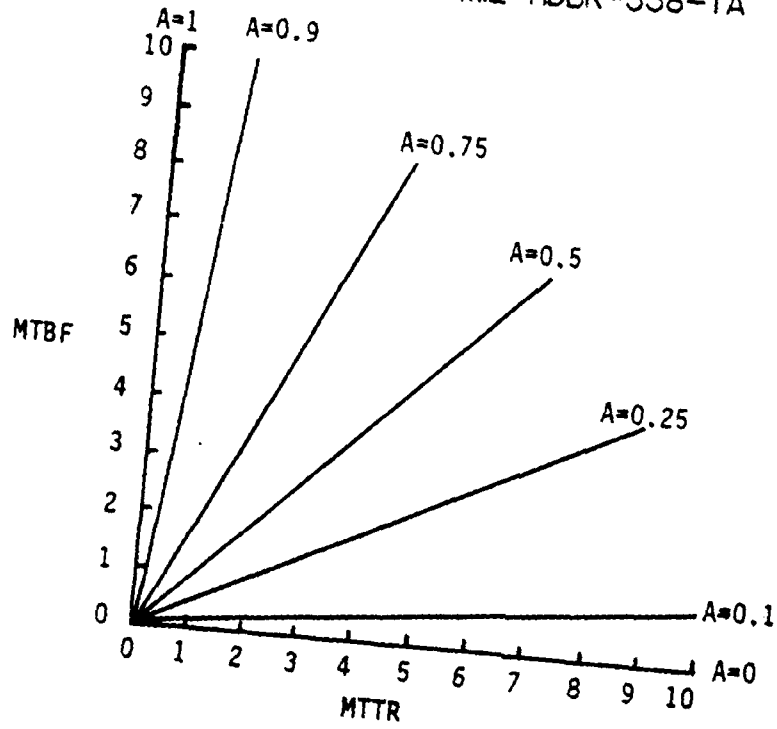
(A) AVAILABILITY AS A FUNCTION OF MTBF AND MTTR
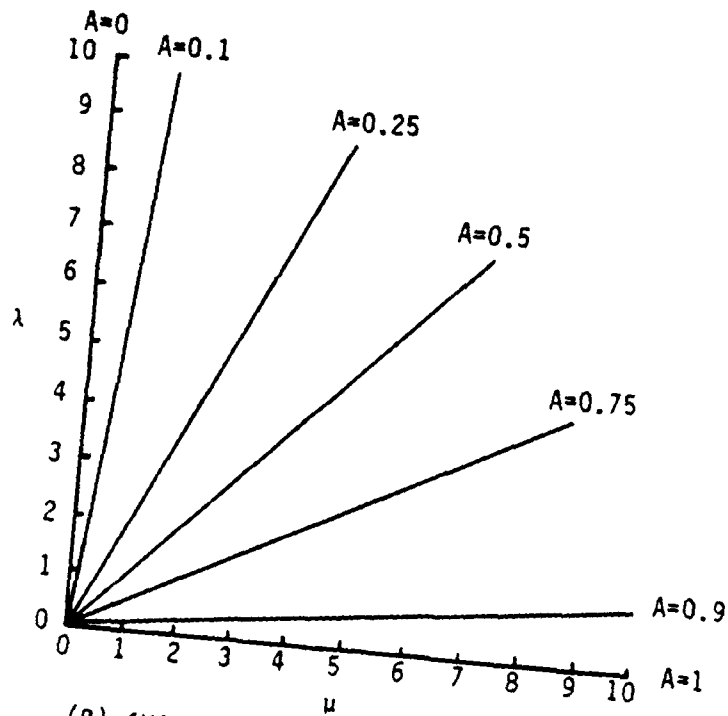
(B) AVAILABILITY AS A FUNCTION OF λ AND μ

FIGURE 10.6.2-1: RELIABILITY-MAINTAINABILITY-AVAILABILITY RELATIONSHIPS
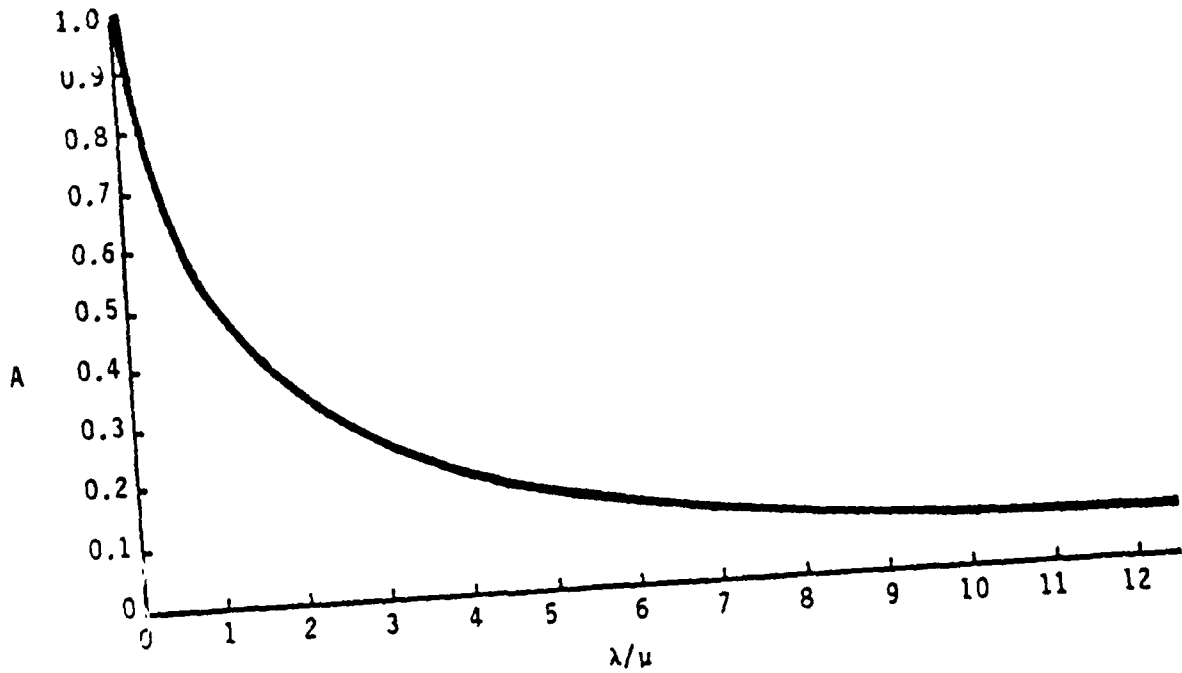
FIGURE 10.6.2-2: <u>AVAILABILITY AS A FUNCTION OF λ/μ</u>
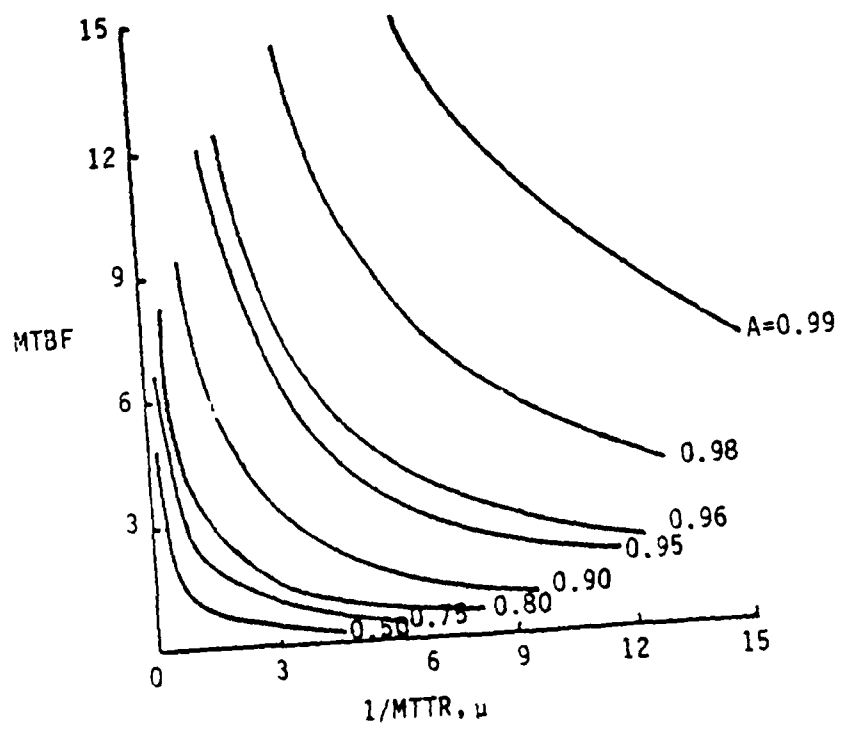
FIGURE 10.6.2-3: <u>AVAILABILITY AS A FUNCTION OF MTBF AND 1/MTTR</u>

10-61
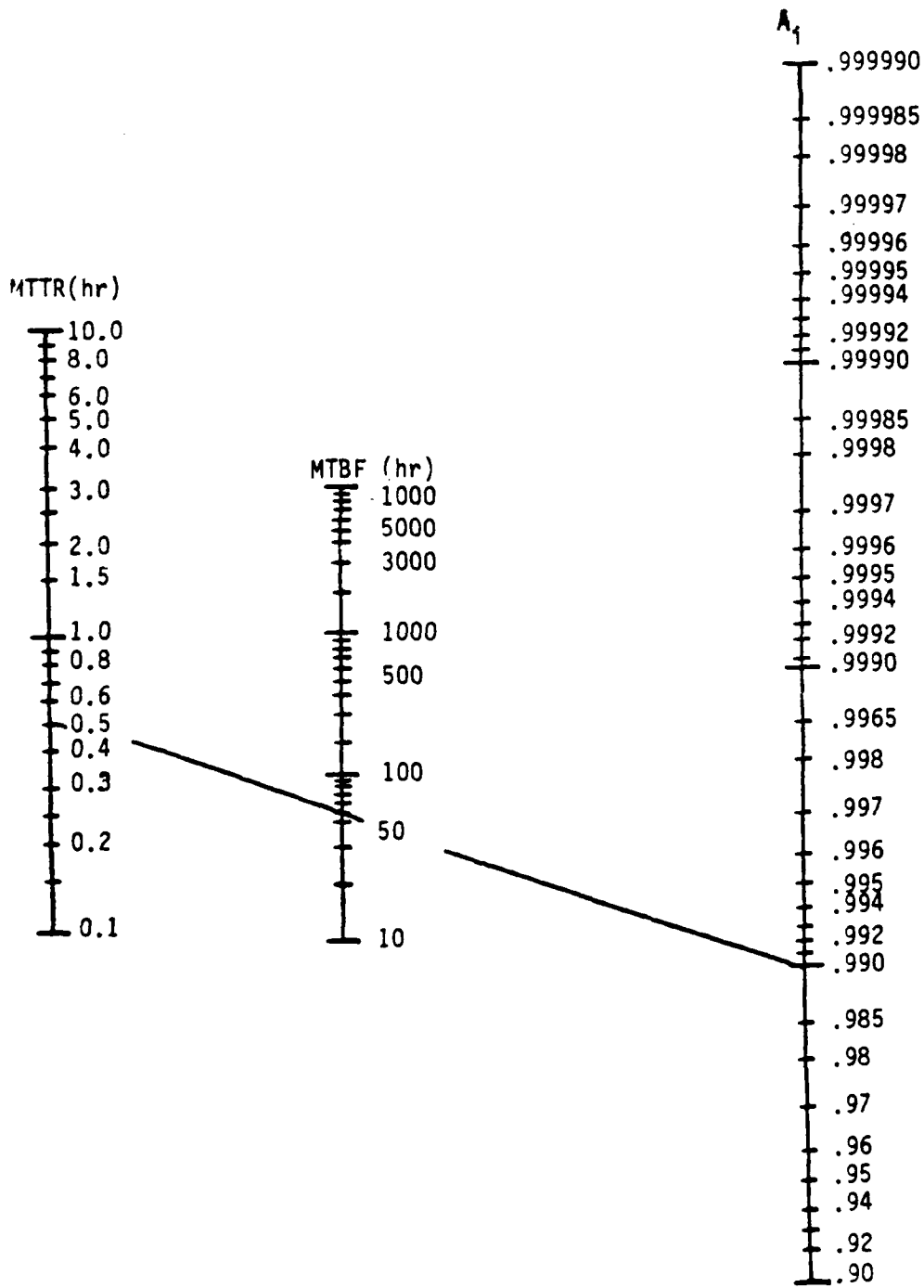
FIGURE 10.6.2-4: AVAILABILITY NOMOGRAPH

There are two general classes of tradeoffs. In the first, the contributing system variables are traded off against one another without increasing the value of the higher level system parameter, for example, trading off reliability and maintainability along an isoavailability contour (no change in availability). This might be done for reasons of standardization or safety or for operational reasons such as the level at which the system and its equipments will be maintained. The other class of tradeoff is one in which the system variables are varied in order to obtain the highest value of the related system parameters within cost or other constraints. For example, reliability and maintainability might be traded off in order to achieve a higher availability. This could result in moving from one isoavailability curve to another in Figure 10.6.2-3, perhaps along an isocline (a line connecting equal slopes).

An example of a reliability - availability - maintainability (RAM) tradeoff is given in the following paragraphs. The design problem is as follows: A requirement exists to design a radar receiver which will meet an inherent availability of 0.99, a minimum MTBF of 200 hours, and an MTTR not to exceed 4 hours. Existing design with the use of Military Standard parts meets an availability of 0.97, an MTBF of 150 hours and an MTTR of 4.64 hr.

Using Eq. (10.88) the area within which the allowable tradeoff may be made is shown by the cross hatched portion of Figure 10.6.2-5. The capability of the present system is also shown in the figure. As indicated in the previous paragraph, there are two approaches which can be used for tradeoff. One is to fix the availability at 0.990. This means that any combination of MTBF and MTTR between the two allowable end points on the 0.990 isoavailability line may be chosen. These lie between an MTBF of 200 hrs with an MTTR of 2 hrs and an MTBF of 400 hrs with an MTTR of 4 hrs. The other approach is to allow availability to be larger than 0.990 and thus allow any combination of MTBF and MTTR within the feasible region.

It is clearly seen that without any additional constraints the designer has a limitless number of combinations from which to choose. Assume that the following four alternative design configurations have been selected for tradeoff as shown in Table 10.6.2-1.

Design Configuration Nos. 1, 2, and 3 all have the required availability of 0.990. Design Configuration No. 1 emphasizes the maintainability aspects in design, while Design Configuration No. 3 stresses reliability improvement. Design Configuration No. 2 is between Nos. 1 and 3 for the same availability. Design Configuration No. 4 is a combination of Nos. 1 and 2 and yields a higher availability.

Since all of these alternatives are within the feasible region shown in Figure 10.6.2-5 some other criterion must be used for selection of the desired configuration. In this case, we will use the least cost alternative or the one showing the greatest life cycle cost savings over the present configuration as the basis for tradeoff decision. A cost comparison of the different alternatives is shown in Table 10.6.2-2.
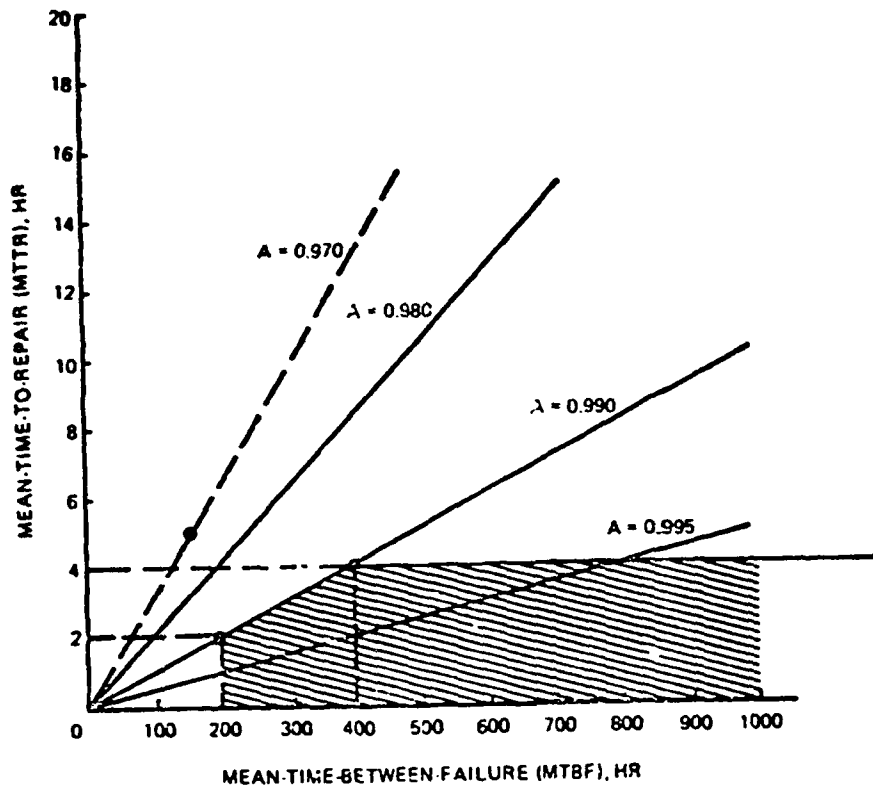
FIGURE 10.6.2-5: RELIABILITY-MAINTAINABILITY TRADE-OFFS

TABLE 10.6.2-1: ALTERNATIVE DESIGN TRADEOFF CONFIGURATIONS

Design Configuration	A	MTBF, hr	MTTR, hr
1. R - derating of military standard parts M - modularization and automatic testing	0.990	200	2.0
2. R - design includes high reliability parts/components M - limited modularization and semi-automatic testing	0.990	300	3.0
3. R - design includes partial redundancy M - manual testing and limited modularization	0.990	350	3.5
4. R - design includes high reliability parts/components M - modularization and automatic testing	0.993	300	2.0

TABLE 10.6.2-2: COST COMPARISON OF ALTERNATIVE DESIGN CONFIGURATIONS

Item	Existing	1	2	3	4
Acquisition (Thousands of Dollars)					
RDT&E	300	325	319	322	330
Production	4,500	4,534	4,525	4,530	4,542
Total	4,800	4,859	4,844	4,852	4,872
10-Year Support Costs (Thousands of Dollars)					
Spares	210	151	105	90	105
Repair	1,297	346	382	405	346
Training and Manuals	20	14	16	18	14
Provisioning & Handling	475	525	503	505	503
Total	2,002	1,036	1,006	1,018	968
LIFE CYCLE COST	6,802	5,895	5,850	5,870	5,840

The cost table shows that Configuration No. 2 is the lowest cost alternative among those with equal availabilities. It also shows that Configuration No. 4, with a higher acquisition cost, has a significantly better 10-year life cycle support cost and lowest overall cost, as well as a higher availability. Thus Configuration No. 4 is the optimum tradeoff, containing both improved reliability and maintainability features.

The tradeoff example previously shown was a relatively simple example for the case of a single equipment. Let us now look at a more complex example. Figure 10.6.2-6 (a repeat of Figure 10.4.1.3-1) represents a serial system consisting of five statistically independent subsystems, each with the indicated $MTBF_i$ and $MTTR_i$. We found by the use of Eq. (10.27) that the steady state availability was:

$$A = \prod_{i=1}^{5} A_i = 0.73534$$

By inspection of the maintenance time ratios (MTRs) of each of the subsystems we note that Subsystems 3 and 4 have the lowest MTRs, given by:

$$\frac{MTTR_i}{MTBF_i} = \frac{5}{25} = 0.2$$

for Sybsystem 3 and $5/50 = 0.1$ for Subsystem 4. These are, therefore, the "culprits" in limiting system availability to 0.73534, which may be unacceptable for the mission at hand. If because of the state-of-the-art limitations we are unable to apply any of the design techniques detailed in Section 7 to reduce MTBF, then our first recourse is to add a parallel redundant subsystem to Subsystem 3, the weakest link in the series chain.

We shall consider two cases: (1) the case where no repair of a failed redundant unit is possible until both redundant subsystems fail and the system stops operating; or (2) repair is possible by a single repair crew while the system is operating.

For case (1) where both units must fail before repair is initiated and a single crew repairs both failed units in sequence:

$$A(1/2) = \frac{\displaystyle\sum_{n=1}^{2} \frac{1}{n\lambda}}{\displaystyle\sum_{n=1}^{2} \frac{1}{n\lambda} + \frac{m}{\mu}} = \frac{\frac{1}{\lambda} + \frac{1}{2\lambda}}{\frac{1}{\lambda} + \frac{1}{2\lambda} + \frac{2}{\mu}}$$

$$= \frac{\frac{1}{0.04} + \frac{1}{2(0.04)}}{\frac{1}{0.04} + \frac{1}{2(0.04)} + \frac{2}{0.2}} = \frac{37.5}{47.5}$$

$$= 0.789$$
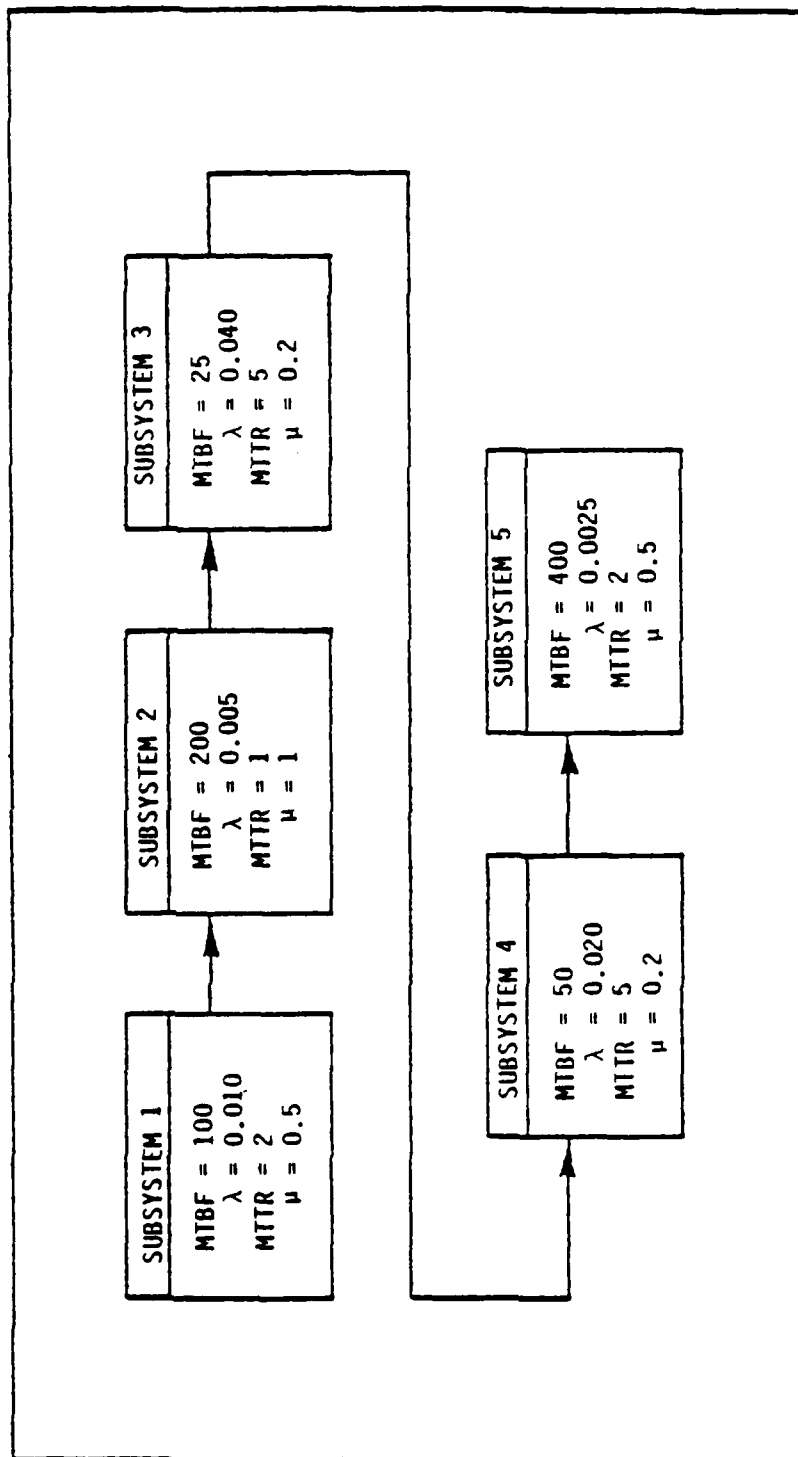
FIGURE 10.6.2-6:   BLOCK DIAGRAM OF A SERIES SYSTEM

This is a lower availability than the nonredundant case!

$$A = \frac{1}{1 + \dfrac{MTTR_i}{MTBF_i}} = \frac{1}{1 + 0.2} = 0.833$$

For case (1), where both units must fail before repair is initiated and two repair crews simultaneously repair both failed units:

$$A(1/2) = \frac{\sum\limits_{n=1}^{2} \dfrac{1}{n\lambda}}{\sum\limits_{n=1}^{2} \dfrac{1}{n\lambda} + \dfrac{1}{\mu}} = \frac{\dfrac{1}{0.04} + \dfrac{1}{2(0.04)}}{\dfrac{1}{0.04} + \dfrac{1}{2(0.04)} + \dfrac{1}{0.2}} = \frac{37.5}{42.5}$$

$$= 0.882$$

which is a slight improvement over the nonredundant case.

For case (2), where a single repair crew initiates repair action on a redundant subsystem as soon as it fails:

$$A = \frac{\mu^2 + 2\mu\lambda}{\mu^2 + 2\mu\lambda + \lambda^2} \quad \text{(from Table 10.4.1.4-1)}$$

$$= \frac{(0.2)^2 + 2(0.2)\,(0.04)}{(0.2)^2 + 2(0.2)\,(0.04) + (0.04)^2}$$

$$= \frac{0.04 + 0.016}{0.04 + 0.016 + 0.0016} = \frac{0.056}{0.0576}$$

$$= 0.972$$

as compared to 0.833 where no redundancy was used.

This corresponds to an increased system availability of:

$$A = 0.73534 \left(\frac{0.972}{0.833}\right) = 0.86$$

If this new value is still not acceptable redundancy might have to be applied to Subsystem 4. For example let us use a 2-unit standby configuration for Subsystem 4 with multiple repairs; then (from Table 10.4.1.4-1), the steady state availability would be:

$$A = \frac{2\mu^2 + 2\mu\lambda}{2\mu^2 + 2\mu\lambda + \lambda^2} = \frac{2(0.2)^2 + 2(0.2)\,(0.02)}{2(0.2)^2 + 2(0.2)\,(0.02) + (0.02)^2}$$

$$= \frac{0.08 + 0.008}{0.08 + 0.008 + 0.0004} = \frac{0.088}{0.0884} = 0.995$$

Thus, the new system availability would be:

$$A = (0.86) \left(\frac{0.995}{0.909} \right) = 0.94$$

where 0.909 was the original availability of subsystem 4.

Note, however, that to achieve these gains in availability, repair of failed redundant units must be possible while the system is operating.

Before leaving the subject of tradeoffs at the system availability level, it should be pointed out that design tradeoff methodologies can also be used at lower levels of the system hierarchy to increase MTBF and reduce MTTR. These are discussed in Section 7.

10.7 ALLOCATION OF AVAILABILITY, AND FAILURE AND REPAIR RATES

The previous sections discussed how availability can be calculated for various system configurations, e.g., series, parallel, etc., and how R&M can be traded off to achieve a given availability. This section discusses methods for allocating availability (and, where appropriate, failure and repair rates) among the system units to achieve a given system availability.

The reader should keep in mind that we are concerned with systems that are maintained upon failure. For the case of nonmaintained systems, e.g., missiles, satellites, etc., the methods presented in Chapter 3 are appropriate for system reliability design, prediction, and allocation.

During the initial design phase of a program, detailed information is not usually available regarding the particular equipments to be employed with the system. For example, we may know that a transmitter with certain power requirements may be designed, but we do not usually know if it is less expensive to design for a low failure rate or a high repair rate. Unless the experience of similar, previously designed transmitters can guide our decisions, estimation of the best set of alternatives is necessary. Having developed a system configuration, a range of values of equipment failure rates and repair rates that would satisfy the system availability requirement can be initially specified. The state-of-the-art limits for these equipments may not be known or the expenditures required for improvement, but we can specify their ratio, which would allow considerable freedom through the design process.

10.7.1 AVAILABILITY FAILURE RATE AND REPAIR RATE ALLOCATION FOR SERIES SYSTEMS

Several cases can be considered:

(1) A single repairman must repair any one of n identical, statistically independent subsystems in series. The ratio of failure rate to repair rate is such that there is a strong possibility that a second subsystem will fail while the first one is being repaired.

(2) Same as (1) except a repairman is assigned to each subsystem and can only work on that particular subsystem.

(3) Same as (1) except some intermediate number of repairmen, r, less than the number of subsystems is assigned. Any repairman can work on any system.

(4) Repeat cases (1)-(3) with nonidentical subsystems.

10.7.1.1 CASE (1)

The steady state availability in Case (1) is from Reference 25:

$$A_s = \frac{(\mu/\lambda)^n}{n! \sum_{i=0}^{n} \frac{(\mu/\lambda)^i}{i!}} \qquad (10.90)$$

where

μ = subsystem repair rate
λ = subsystem failure rate
n = number of subsystems in series
μ/λ = "operability ratio" as opposed to λ/μ (the utilization factor)

For example, if $n = 4$ and $A_s = 0.90$, the allocation equation becomes

$$0.90 = \frac{(\mu/\lambda)^4}{24 \left[1 + \left(\frac{\mu}{\lambda}\right) + \frac{1}{2} \left(\frac{\mu}{\lambda}\right)^2 + \frac{1}{6} \left(\frac{\mu}{\lambda}\right)^3 + \frac{1}{24} \left(\frac{\mu}{\lambda}\right)^4 \right]}$$

or $\mu/\lambda = 38.9$

The complexities of allocating failure and repair rates for even simple examples are apparent. If the subsystems are not identical, the allocation must be solved using the state matrix approach to compute availability.

10.7.1.2 CASE (2)

This represents the situation in which a repairman is assigned to each subsystem. It is equivalent to the condition in which $\mu/\lambda \gg 1$, i.e., failure rate is much smaller than repair rate. Since this is true of many practical systems, a wide variety of practical problems can be solved.

It was previously shown that for this case,

$$A_s = (A_i)^n = \left[\frac{1}{1 + (\lambda/\mu)} \right]^n \qquad (10.91)$$

where

A_i = subsystem availability
n = number of subsystems

From Eq. (10.91)

$$A_i = (A_s)^{1/n} \qquad (10.92)$$

Example No. 1

Three identical series subsystems must operate so as to give a total systems availability of 0.9. What requirement should be specified for the availability of each subsystem? For the ratio of λ/μ for each subsystem?

$$A_i = (0.9)^{1/3} = 0.965$$

$$0.965 = \frac{1}{1 + \lambda/\mu}$$

$$\lambda/\mu = \frac{1}{0.965} - 1 = 0.036$$

Example No. 2

A system consists of three identical, independent subsystems connected in series. The availability requirement is 0.99, and the repair rate is limited to 0.3 per hr. What is the minimum failure rate which must be allocated to each subsystem to satisfy the system requirement? A repairman is assigned exclusively to each subsystem.

Procedure	Example
(1) State the system availability requirement.	$A_s = 0.99$
(2) Compute the availability of each subsystem by $A_i = (A_s)^{1/n}$	$A_i = (0.99)^{1/3}$ $= 0.99666$
(3) For each subsystem compute the ratio λ/μ by: $\frac{\lambda}{\mu} = \frac{1}{A_i} - 1$	$\lambda/\mu = \frac{1}{0.99666} - 1$ $= 0.00336$
(4) Compute λ from the previous equation with $\mu = 0.3$ per hr. The final answer is rounded off to 2 significant figures to avoid implying too much accuracy.	$\lambda = 0.00336 \times (0.3 \text{ per hr})$ $= 1.0 \text{ per } 1000 \text{ hr}$

If for Case (2) the series equipments are not identical the relationship

$$A_s = \prod_{i=1}^{n} A_i \qquad (10.93)$$

can be used to derive the individual subsystem availabilities.

Example No. 3 (using Eq. (10.93))

Three subsystems must operate to give a total system availability of 0.9. Subsystem 1 has an availability of 0.99. What should be specified for the availability of each of the other two subsystems if: (1) they are equally important, or (2) Subsystem 3 should have twice the availability of Subsystem 2 (this is interpreted as Subsystem 3 having one-half the unavailability of Subsystem 2)?

(1) $A_s = 0.99 \, A_2 \, A_3$

$A_2 = A_3$

$0.9 = 0.99 \, A_2^2$

$A_2 = \sqrt{0.91}$

$A_2 = A_3 = 0.954$

(2) $(1 - A_2) = 2 (1 - A_3)$

$1 - A_2 = 2 - 2A_3$

$A_3 = \dfrac{A_2 + 1}{2}$

$0.9 = 0.99 \, A_2 \, A_3 = 0.99 \, A_2 \left(\dfrac{A_2 + 1}{2} \right)$

$= 0.99 \left(\dfrac{A_2^2}{2} + \dfrac{A_2}{2} \right)$

$2 \left(\dfrac{0.9}{0.99} \right) = A_2^2 + A_2$

$A_2^2 + A_2 - 1.82 = 0$

$A_2 = 0.94$

$A_3 = \dfrac{0.94 + 1}{2} = 0.97$

The failure and repair rate allocations for A_2 and A_3 would be

$$\lambda_2/\mu_2 = \frac{1}{A_2} - 1 = \frac{1}{0.94} - 1 = 0.064$$

$$\lambda_3/\mu_3 = \frac{1}{A_2} - 1 = \frac{1}{0.97} - 1 = 0.03$$

The previous example can be expanded to use weighting factors to derive the required subsystem availabilities. The choice of weighting factor would depend upon the system being analyzed and the significant parameters affecting availability. Some examples of weighting factors might be relative cost or equivalent complexity of the subsystem. The latter, for example, should correlate somewhat with increasing failure and repair rates. Let us examine an example of an allocation using equivalent complexity.

Example No. 4

A ground surveillance series system consists of a radar, a data processor, and display subsystem. A system availability of 0.995 is required. Based upon past experience and engineering analysis, it is estimated that the complexity of each subsystem is as follows:

Display Subsystem	≈	1000 component parts
Radar Subsystem	≈	2500 component parts
Data Processor Subsystem	≈	5500 component parts

What availability requirement should be specified for each of the subsystems to meet the system requirement?

The weight assigned to each subsystem is given by:

$$W_i = \frac{\text{Number of parts for subsystem i}}{\text{Total number of parts in system}}$$

$$W_1(\text{Display}) = \frac{1000}{1000 + 2500 + 5500} = 0.11$$

$$W_2(\text{Radar}) = \frac{2500}{1000 + 2500 + 5500} = 0.28$$

$$W_3(\text{Data Processor}) = \frac{5500}{1000 + 2500 + 5500} = 0.61$$

If the system availability requirement is 0.995, then 1 - 0.995 = 0.005 is the unavailability of the system. Using the weights previously derived to apportion the system unavailability to each of the subsystems, we get:

```
Display          =  (0.11) (0.005) = 0.00055
Radar            =  (0.28) (0.005) = 0.00140
Data Processor   =  (0.61) (0.005) = 0.00305
        SYSTEM UNAVAILABILITY       = 0.005
```

Thus, the required availabilities for each subsystem would be

```
A₁ (Display)          =  1 - 0.00055 = 0.99945
A₂ (Radar)            =  1 - 0.0014 = 0.9986
A₃ (Data Processor)   =  1 - 0.00305 = 0.99695
```

A_1 (Display) $= 1 - 0.00055 = 0.99945$

A_2 (Radar) $= 1 - 0.0014 = 0.9986$

A_3 (Data Processor) $= 1 - 0.00305 = 0.99695$

Verifying that the system requirement will be met

$$A_s = (0.99945)(0.9986)(0.99695) = 0.995$$

Also, as was previously shown, failure and repair rate allocation can be derived:

$$\lambda_1/\mu_1 = \frac{1}{A_1} - 1 = \frac{1}{0.99945} - 1 = 5.5 \times 10^{-4}$$

$$\lambda_2/\mu_2 = \frac{1}{A_2} - 1 = \frac{1}{0.9986} - 1 = 1.4 \times 10^{-3}$$

$$\lambda_3/\mu_3 = \frac{1}{A_3} - 1 = \frac{1}{0.99695} - 1 = 3.0 \times 10^{-3}$$

Another slight variation of Case (2) (Section 10.7.1.2) is a series system with nonidentical subsystems, in which each subsystem's

$$\lambda_i/\mu_i < 0.1$$

The availability of such a system with subsystems whose failures and repair are statistically independent is:

$$A_s = \frac{1}{1 + \sum\limits_{i=1}^{n} \alpha_i} \tag{10.94}$$

where

$$\alpha_i = \lambda_i/\mu_i \text{ with all } \alpha_i < 0.1$$

n = number of subsystems in series

$$\alpha_{(system)} = \alpha_1 + \alpha_2 \ldots + \alpha_n \tag{10.95}$$

To design such a system, one merely allocates the subsystem α_i's according to some weighting scheme. For example, there may be a requirement to design a new system with higher availability which is similar in design to the old system, where the relative weighting factors are the same for each new subsystem.

$$W_i = \frac{\alpha_i (new)}{\alpha_i (old)} \tag{10.96}$$

Example No. 5

A system consisting of two statistically independent subsystems has an availability of 0.90. Subsystem 1 has an availability of 0.97, and subsystem 2 has an availability of 0.93. A new system, similar in design to this one, must meet a required 0.95 availability. What are the new subsystem availabilities and ratios of failure-to-repair rate?

Procedure	Example
(1) State the availability requirement A_s of the new system	$A_s = 0.95$
(2) Compute the sum α_s of the $\alpha =$ ratios for the old system	(Remember $\alpha_i = \lambda_i / \mu_i = \frac{1}{A_i} - 1$)
$\alpha_s(\text{old}) = \alpha_1 + \alpha_2$	$\alpha_s(\text{old}) = 0.0309 + 0.0753$ $= 0.1062$
(3) Compute the relative weights W_i by Eq. (10.96)	$W_1 = \frac{0.0309}{0.1062} = 0.291$ $W_2 = \frac{0.0753}{0.1062} = 0.709$
(4) Compute an overall α_s for the new system by: $\alpha_s'(\text{new}) = \frac{1}{A_s'} - 1$	$\alpha_s' = \frac{1}{0.95} - 1 = 0.0526$
(5) Compute the allocated α_i' for each subsystem of the new design by: $\alpha_i' = W_i \alpha_s'$	$\alpha_1' = (0.291)(0.0526) = 0.0153$ $\alpha_2' = (0.709)(0.0526) = 0.0373$
(6) Compute the availabilities A_i' allocated to each subsystem by: $A_i' = \frac{1}{1 + \alpha_i'}$	$A_1' = \frac{1}{1 + 0.0153} = 0.985$ $A_2' = \frac{1}{1 + 0.0373} = 0.964$
(7) Check the allocated availability A_s of the new system by: $A_s' = A_1' \cdot A_2'$	$A_s = (0.985)(0.964) = 0.95$

Since the allocated ratios are known, additional tradeoff studies can be performed to optimize λ_i and μ_i for each subsystem.

10.7.2 FAILURE AND REPAIR RATE ALLOCATIONS FOR PARALLEL REDUNDANT SYSTEMS

A system comprising several stages of redundant subsystems whose λ/μ ratio is less than 0.1 can be treated as if the stages were statistically independent. The system steady-state availability A_s is:

$$A_s = A_1 \cdot A_2 \cdot A_3 \cdots A_n$$

where

$$A_i = \text{the availability of state } i$$

This is equivalent to treating each stage as if it had a repairman assigned to it. It is also equivalent to saying that a single repairman is assigned to the system but that the probability of a second failure occurring while the first is being repaired is very small. If the stages are not statistically independent, the system availability must be computed by the state matrix approach. In either case, the system requirement can be obtained with a range of failure and repair rates. Tradeoff procedures must be used to determine the best set of these parameters.

It will be recalled (from Eq. (10.52)) that the steady-state measure of availability for a stage where at least m out of n equipments must be available for the stage to be available can be expressed by the binomial expansion

$$A_s = \sum_{i=m}^{n} \binom{n}{i} A^i (1 - A)^{n-i} \tag{10.97}$$

and, where m = 1, i.e., only one equipment of n need be available at any one time, Eq. (10.97) simplifies to:

$$A_s = 1 - (1 - A)^n \tag{10.98}$$

If Eq. (10.97) can be expressed in terms of the operability ratio μ/λ, the initial allocation may be made. Eq. (10.97) can be expressed in terms of the operability ratio as:

$$A_s = \sum_{i=m}^{n} \frac{\binom{n}{m}(\mu/\lambda)^i}{(1 + \mu/\lambda)^n} \tag{10.99}$$

Now if a value of A_s is specified and we know the system configuration (at least how many equipments out of n-equipments must be available within each stage), we can solve for the operability ratios μ/λ.

For example, consider Table 10.7 2-1, in which the system availability requirement of 0.992 has been allocated to each of 4 series subsystems (stages) as indicated in column (2). In turn, *in order to achieve the* given stage availability, it has been determined that parallel redundant subsystems are required for each stage (column (3)) in which at least one of the redundant subsystems per stage must be available for the system availability requirement to be met.

TABLE 10.7.2-1: PRELIMINARY SYSTEM AND SUBSYSTEM
RELIABILITY SPECIFICATIONS

(1)	(2)	(3)	(4)	(5)
Stage	Stage Availability	Number of Subsystems (n)	Number of Subsystems Required (m)	Operability Ratio
1	0.9984	4	1	4.0
2	0.9976	5	1	2.5
3	0.9984	4	1	4.0
4	0.9976	5	1	2.5

The final column (5) indicates the calculated μ/λ (operability ratio) required of each subsystem in the redundant configuration of each stage in order to achieve the allocated stage availability. Column (5) results are obtained by the use of Eqs. (10.98) or (10.99). For example, for Stage 1, m = 1, n = 4. Therefore, since m = 1, we may use Eq. (10.98).

$$A_s = 1 - (1 - A)^n$$

$$0.9984 = 1 - \left(1 - \frac{\mu}{\lambda + \mu}\right)^4$$

$$0.9984 = 1 - \left(\frac{\lambda}{\lambda + \mu}\right)^4$$

$$\frac{1}{1 + \mu/\lambda} = (1 - 0.9984)^{1/4} = 0.2$$

$$0.2 \, \mu/\lambda = 1 - 0.2$$

$$\frac{\mu}{\lambda} = \frac{MTBF}{MTTR} \geq 4$$

Obviously, there are a multitude of combinations that would satisfy Figure 10.7.2-1. Until more information becomes available concerning the cost of various failure rates and repair rates of the particular equipments involved, this initial specification allows preliminary equipment design to start with an availability goal that is consistent with the system's requirements. To facilitate calculations of operability ratio, solutions to Eq. (10.99) for n from two through five (Ref. 25) are given in Figures 10.7.2-2a through 10.7.2-2d. The abscissa of the graphs is expressed in terms of unavailability since the plot allows for greater linearity, and, thus, ease of reading. Let us solve an example problem utilizing the graphs.

Example No. 1

A system consists of five identical, statistically independent subsystems connected in a parallel redundant configuration. A system availability of 0.999 is required. Four out of five subsystems must be operating for the system availability requirement to be met. What is the required μ/λ ratio?

Procedure	Example
(1) State the system availability requirement A_s	A_s = 0.999
(2) Compute the system unavailability U_s by: $U_s = 1 - A_s$	U_s = 1 - 0.999 = 0.0010
(3) Enter Figure 10.7.2-2d for m = 4 and U_s = 0.0010, and read the required μ/λ ratio	μ/λ = 100

10.7.3 ALLOCATION UNDER STATE-OF-THE-ART CONSTRAINTS

Following through the example of the previous section, we note that the allocation of an operability ratio μ/λ to each equipment does not recognize limitations on the range of either of these parameters. If R&M predictions indicate what these constraints are and they turn out to be in conflict with the preliminary allocation, revised allocations are warranted. During the reallocation, the cost of reducing the equipment failure rates and repair rates should also be considered to provide for a best balance of operability objectives. For example, in the previous section (see Table 10.7.2-1) the operability ratio allocated to the subsytems within the first stage was $\mu/\lambda \geq 4.0$. If reliability predictions indicate that a failure rate of 0.7/hour can be achieved without much difficulty, this would indicate that a repair rate of at least 2.8/hour is required to meet the specifications. If, however, it is expected that repairs cannot be made at a rate greater than 2.0/hour, the specification will not be met.
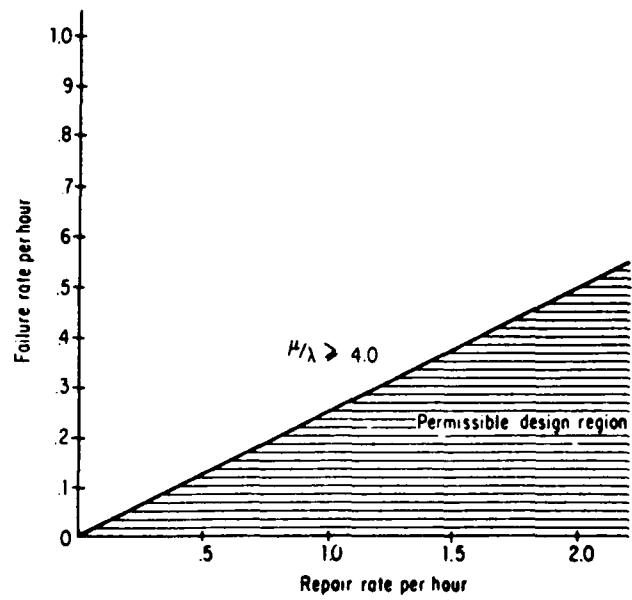
FIGURE 10.7.2-1: PERMISSIBLE EQUIPMENT FAILURE AND REPAIR RATES FOR $\mu/\lambda \leq 4.0$

a

b

c
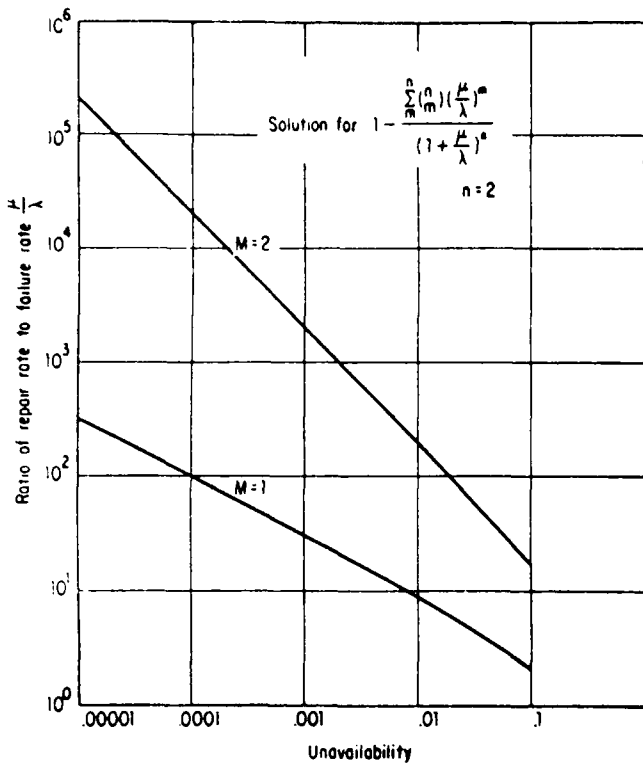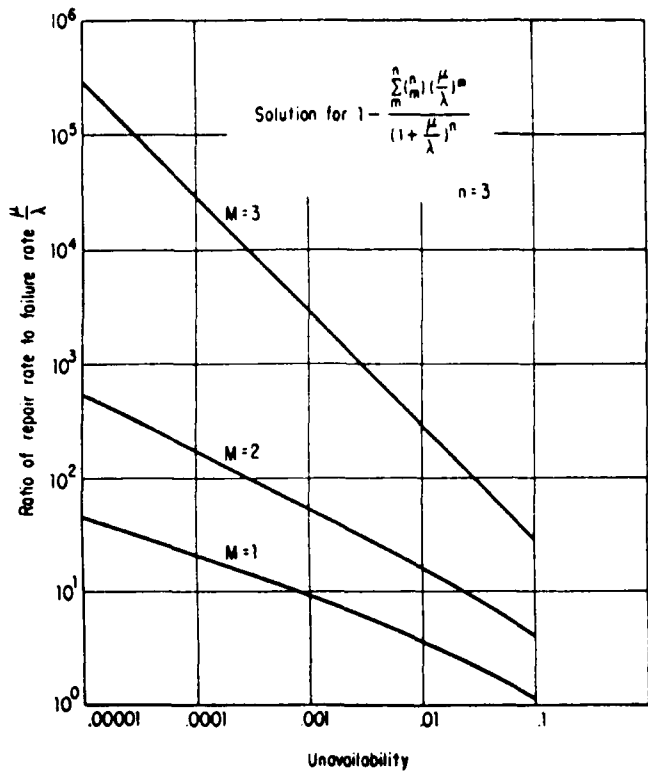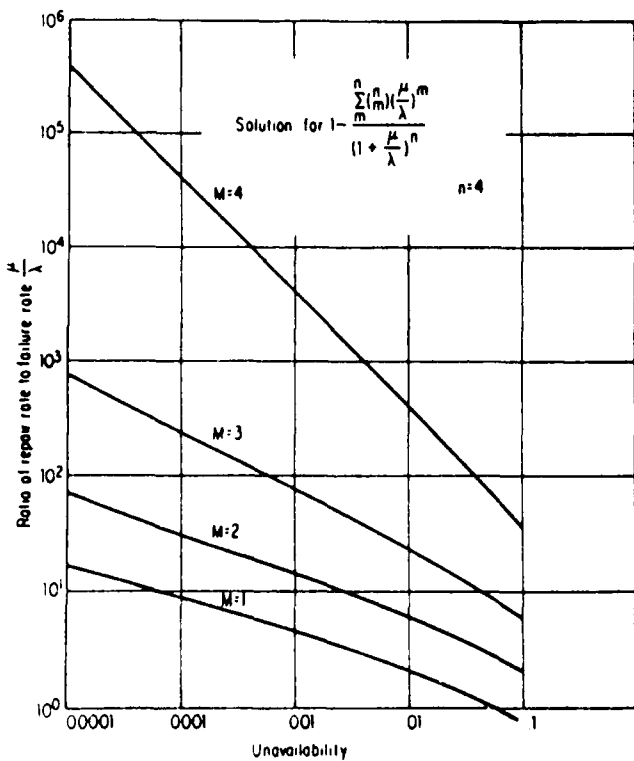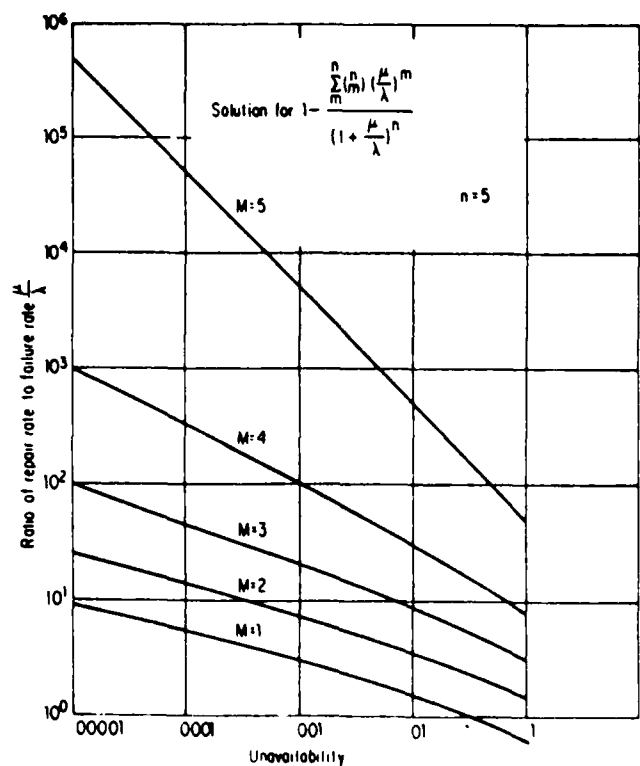
FIGURE 10.7.2-2: <u>UNAVAILABILITY CURVES</u>   d

As an example, let it be assumed that it is possible to design the equipment so that it can achieve a failure rate of 0.1/hour -- however, only at a considerable expenditure over and above that which would be required to design for a failure rate of 0.7/hour. Now, it may be possible that the predicted failure rates and repair rates of the subsystems within the remaining stages are well within the operability ratio. Thus, it may be feasible to tighten the specifications of the subsystems within the other stages while relaxing the specification of the subsystems within the first stage and still achieve the required level of system availability. Again, there may be many ways of balancing the specifications. It is desirable, therefore, to choose that balance which minimizes any additional expenditure involved over that allocated for the system configuration.

Dynamic programming (Ref. 25) is a powerful tool for balancing operability ratios in determining a system configuration at least cost.

Before leaving this subsection on allocation with redundancy, it should be pointed out that if the redundant subsystems in each stage are not identical, state matrix techniques must be used to compute availability.

10.8 SYSTEM RELIABILITY SPECIFICATION, PREDICTION, AND DEMONSTRATION

Sections 6, 7 and 8 presented in great detail methods for specifying, predicting, and demonstrating system reliability.

The methods and design procedures presented in Section 7 are directly applicable to system reliability parameters for the case of nonmaintained systems, e.g., missiles, satellites, "one-shot" devices, etc.

For maintained systems, the methods and procedures presented in References 26, 49 and 50 are directly applicable to system maintainability parameters. When these are combined with the methods of Section 7 and the appropriate sections of this section, they provide a complete capability for specifying, predicting, and demonstrating most system R&M parameters, as well as trading them off to maximize system availability or some other appropriate effectiveness parameter at minimum cost.

Perhaps the only area that may need some further discussion is availability demonstration methods. At the present time no accepted test plans exist for steady state availability; however, MIL-HDBK-781 describes two availability demonstration tests; one for fixed sample size, the other a fixed time test. The tests are based upon a paper presented at the 1979 Annual Reliability and Maintainability Symposium (Ref. 26). The paper also provides a theoretical discussion of sequential test plans, but no standardized plans are presented. Program managers or R&M engineers who wish to consider using sequential availability tests should consult the referenced paper. The proposed demonstration plans are described in the following subsection.

10.8.1 AVAILABILITY DEMONSTRATION PLANS

The availability tests are based on the assumption that a system can be treated as being in one (and only one) of two states, "up" or "down." At t = 0 the system is up (state X) and operates until the first failure at $T = X_1$; it is down for repairs during the restore cycle Y_1. An up/down cycle is complete by time $X_1 + Y_1$. The random variables (X_i) and (Y_i) are each assumed to be independent and identically distributed with means $E(X)$ and $E(Y)$. The sequence of pairs (X_i, Y_i) forms a two dimensional renewal process.

For this system, the availability A(t) = the fraction of time the system is up during (0,t).

The steady state availability is

$$A = \lim_{t \to \infty} A(t) = \frac{E(X)}{E(X)+E(Y)} \qquad (10.100)$$

Assume that $E(X)$ and $E(Y)$ and, therefore, A are unknown. Hypothesize two values of A.

$$H_0 \quad : A = A_0$$
$$\qquad\qquad\qquad\qquad\qquad (10.101)$$
$$H_1 \quad : A = A_1 < A_0$$

On the basis of test or field data, accept or reject the hypotheses by comparing the computed A to a critical value appropriate to the test type and parameters.

It is assumed that both the up and down times are gamma distributed in order to derive the relationships of each test type. However, extremely useful results can be derived assuming the exponential distribution in both cases; the exponential distribution is used in the examples provided below.

10.8.1.1 FIXED SAMPLE SIZE PLANS

This test plan is based on having the system perform a fixed number of cycles R. The result is R pairs of times-to-failure and down times (X_1, Y_1), ..., (X_R, Y_R).

Let A^R = the observed availability of the test

$$A^R = \frac{\sum_{i=1}^{R} X_i}{\sum_{i=1}^{R} X_i + \sum_{i=1}^{R} Y_i} = \frac{1}{1 + Z_R} \qquad (10.102)$$

where

$$Z_R = \frac{\sum\limits_{i=1}^{R} Y_i}{\sum\limits_{i=1}^{R} X_i}$$

(10.103)

and

$$A^R = \text{the maximum likelihood estimate of A}$$

Let

$$\rho_0 = \frac{A_0}{1 - A_0} \quad \text{under the hypothesis } H_0$$

(10.104)

and

$$\rho_1 = \frac{A_1}{1 - A_1} \quad \text{under the hypothesis } H_1$$

(10.105)

The procedure to be followed is:

If

$$\rho_0 Z_R > C \text{ reject } H_0$$

(10.106)

$$\rho_0 Z_R \leq C \text{ reject } H_0$$

where C will be derived below

Assume that the up-times X_i are gamma distributed with parameters (m, Θ) and the down times Y_i are gamma distributed with parameters (n, Φ) with $n \Phi = 1$.

Then it can be shown that

$$\rho Z_R \text{ is F- distributed with parameters (2nR, ZmR)}$$

The critical value C and number of up/down cycles R are determined so that the significance test satisfies the consumer and producer risk requirements α and β, i.e.,

$$P_r(\rho_0, Z_R > C/A_0, R) \leq \alpha$$

(10.107)

$$P_r(\rho_0 Z_R \leq C/A_1, R) \leq \beta$$

(10.108)

which is equivalent to:

$$C \geq F_\alpha (2nR, 2mR)$$

(10.109)

(10.110)

$$\frac{\rho_1}{\rho_0} C \leq F_{1-\beta} (2nR, 2mR)$$

Here F (υ_1, υ_2) denotes the upper α quartile of the F-distribution with parameters υ_1 and υ_2.

This system of inequalities has two unknowns and is solved numerically by finding the smallest integer R satisfying

$$F_\alpha \ (2nR, \ 2mR) \ \times \ F_\beta \ (2mR, \ 2nR) \ \leq \ D \tag{10.111}$$

where D is the discrimination ratio

$$D \ = \ \frac{A_o(1 - A_1)}{A_1(1 - A_o)} \ = \ \frac{\rho_o}{\rho_1} \tag{10.112}$$

The value of R obtained in this way is used to calculate the critical value C

$$C \ = \ F_\alpha \ (2nR, \ 2mR) \tag{10.113}$$

The OC function is

$$OC(A) \ = \ P_r \ (\rho_o \ Z_R \ \leq \ C/A) \ = \ F \ (2nR, \ 2mR; \ \frac{A}{1-A} \cdot \frac{C}{\rho_o}) \tag{10.114}$$

where $F(\upsilon_1, \upsilon_2; x)$ is the c.d.f. of the F-distribution with parameters and υ_2.

The expected test duration is:

$$E(T) \ = \ \frac{R}{1-A} \tag{10.115}$$

The variance of the total test duration is:

$$V_{ar}(T) \ = \ R \cdot \left\{ \frac{1}{n} + \frac{1}{m} \cdot \left(\frac{A}{1-A} \right)^2 \right\} \tag{10.116}$$

For large sample size, $R > 20$, the distribution of T is normal

Example: Exponential Distribution

Let the time-to-failure and downtime distributions be exponentially distributed. Therefore, $n = m = 1$. Let $A_o = 0.9$ and $A_1 = 0.8$ and $\alpha = \beta = 0.2$. Calculate the parameters of the test.

Therefore:

$$\rho_o \ = \ \frac{0.9}{1 - 0.9} \ = \ 9$$

$$D \ = \ \frac{0.9 \ (1 - 0.8)}{0.8 \ (1 - 0.9)} \ = \ 2.25$$

Find the smallest integer satisfying

$$F_{0.2}(2R, 2R) \ \leq \ \sqrt{2.25} \ = \ 1.5 \ \text{where} \ F_\alpha(2nR, \ 2mR) = F_\beta(2nR, \ 2mR)$$

From a Table of Quartiles of the F-distribution we find

$F_{0.2}(16,16) = 1.536$ and

$F_{0.2}(18,18) = 1.497$

Therefore:

R = 9 satisfies the inequality

Therefore:

C = 1.497

The OC function is

$$OC(A) = F\left[18,\ 18;\ 0.166 \cdot \frac{A}{(1 - A)}\right]$$

10.8.1.2 FIXED-TIME SAMPLE PLANS

In fixed-time sample plans, the system performs consecutive up/down cycles until a fixed-time T has elapsed. At this point, the test is terminated and the system may be either up or down. In this case the test time is fixed and the number of cycles is random.

Let A(T) = the observed procedure at the end of the test.

The test procedure is:

$A(T) < A_c$, then reject H_o (10.117)

$A(T) \geq A_c$, then accept H_o (10.118)

Where the critical value A_c and test time T are chosen so that the significance test satisfies the following requirements on α and β.

$P_r(A(T) < A_c/A_0,T) \leq \alpha$ (10.119)

$P_r(A(T) \geq A_c/A_1,T) \leq \beta$ (10.120)

If λ_p is the upper P quartile of the standardized normal distribution and time is in Mean Down Time units, the test time to be used is:

$$T = \left(\frac{1}{m} + \frac{1}{n}\right)\left\{\frac{\lambda\alpha \cdot A_0 \cdot \sqrt{1 - A_0} + \lambda\beta A_1 \sqrt{1 - A_2}}{A_0 - A_1}\right\}^2 \qquad (10.121)$$

The critical value A_c is

$$A_c = \frac{A_0 A_1}{\lambda\alpha A_0\sqrt{1 - A_0} + \lambda\beta A_1 \sqrt{1 - A_1}}\ \lambda\alpha\ \sqrt{1 - A_0} + \lambda\beta\ \sqrt{1 - A_1} \qquad (10.122)$$

The operating characteristic function is given by:

$$OC(A) = 1 - \Phi \frac{A_c - A}{A\sqrt{\dfrac{\dfrac{1}{m} + \dfrac{1}{n} (1 - A)}{T}}} \qquad (10.123)$$

where Φ is the standardized normal c.d.f.

Example: Exponential Distribution

In this example use the same data as in the previous example. $A_o = 0.9$, $A_1 = 0.8$, $m = n = 1$ by the exponential assumption, $\alpha = \beta - 0.2$.

Using Eq. (10.121)

$T = 58.5$ (Mean Down Time Units)

Using Eq. (10.122)

$A_c = 0.856$

The OC function is

$$OC(A) = 1 - \Phi \frac{0.856 - A}{A\sqrt{\dfrac{(1 - A) \times 2}{58.5}}}$$

10.9 SYSTEM DESIGN CONSIDERATIONS

Many of the design techniques and procedures detailed in Section 7 are directly appropriate to system design considerations.

As distinct from equipment design, system design is concerned with the broader aspects of organization and communication as they relate to the design of the individual equipment/systems. In the design of large scale systems, the need to think in terms of the whole in addition to the operation of individual equipment has become apparent. Complexity which characterizes large scale systems is at the root of the need for this broad perspective. Complex systems may perform many functions, process many inputs, translate and display many outputs, and cost a great deal of money. Therefore, only a broad perspective will permit a search for the optimum means of performing the required operations reliably.

A system R&M goal which is determined by some pertinent measure of system effectiveness stems from the system concept. Preliminary system design determines the types and minimum numbers of equipments in the network. The configuration of these equipments to achieve the system reliability goal is then determined. After a configuration is determined, an allocation of failure and repair rates is made to each equipment consistent with the system R&M goal. During the system development process continual adjustments and re-evaluations of the means of achieving the R&M goal at least cost are made.

The overall system design activity begins with the system concept and culminates with a set of equipment specifications that are meaningful enough to permit sound planning and comprehensive enough to present a broad perspective of the system as a single design entity. A basic philosophy of the system design is sought which allows for the determination of all important parameters in such a way that detailed design will not warrant serious redesign and the system will be optimized in its total aspect.

Equipment R&M predictions are most valuable in the early stage of a system's development. Once equipment R&M predictions are available to compare with the allocated operability ratios, discrepancies (if they exist) can be analyzed. It is also desirable to determine the expected state-of-the-art limits of failure rate and repair rate for each equipment in the system. Thus, if predictions indicate that the operability ratio allocated to certain equipments cannot be met without additional expenditures, it may be necessary to reallocate equipment failure and repair rates such that any additional expenditures may be minimized.

Basic to the system design process is the use of comprehensive mathematical models (usually computerized) in order to optimize the system parameters to be achieved at minimum cost. There is a logical sequence to system design, an example of which is presented here for guidance:

(1) Define system R&M parameters in terms of the operational requirements of the system

(2) Develop an index of system R&M effectiveness

(3) Rearrange the system into convenient noninteracting stages and equipments within each stage

(4) Apply mathematical (and statistical) techniques to evaluate alternate system configurations in terms of reliability and cost

(5) If necessary, evaluate the consequences in terms of cost and intangible factors of each alternate configuration

(6) Specify a system configuration, a maintenance philosophy, and the relationship with other factors (interfaces)

(7) Allocate specifications in terms of failure rate (λ) and/or repair rate (μ) to the equipment within the system as design criteria

(8) Predict the reliability and maintainability of each equipment and the system using available data either for similar equipments or, if this is not available, from published part failure rates and estimated repair rates

(9) Compare allocated (goal) and predicted values to determine the next best course of action

(10) Update R&M predictions and compare with goals to allow for continuous information feedback to choose the best course of action on the system level

The procedure is by no means rigid and should vary from system to system. However, what is important are the systematization of objectives and the use of analytic techniques.

Since availability is a system R&M parameter which is a combined measure of reliability and maintainability, it should be maximized in the most cost effective manner. Following are some design guidelines to maximize system availability:

(1) The designed-in failure rate should be minimized, and the MTBF should be maximized

(2) The designed-in repair rate should be maximized, and the MTTR should be minimized

(3) As many maintenance actions as possible should be carried out while the equipment is running normally, thus minimizing equipment downtime

(4) If certain functions must be shut down for maintenance, the time required for shutting down the equipment should be minimized

(5) Should certain components require shutdowns for maintenance actions, these maintenance actions should be required as rarely as possible

(6) Should certain maintenance actions require shutdown, the time needed for these actions should be minimized

(7) If certain components or subsystems require shutdowns for maintenance actions, as few components as possible should be shut down

(8) The time required for logistics should be minimized

(9) The time required for administrative actions should be minimized

(10) Very well written and explicitly illustrated startup and operating manuals should be prepared and made available to the users of the equipment and to the maintenance personnel

(11) Frequent and time consuming prescribed preventive maintenance actions should be minimized

(12) Special effort should be expended to use qualified and well trained maintenance personnel; their training should be updated as required and as design changes and more modern equipment are introduced

(13) The Reliability Design Criteria (Section 7) and the Maintainability Design Criteria given in References 49 and 50 should be diligently pursued

(14) Maintenance actions which require the dismantling, moving and assembling of heavy components and equipment should be facilitated by the provisioning of special lift-off lugs and accessories

(15) Frequently inspected, serviced, maintained, and/or replaced components should be so located in the equipment that they are more accessible and easily visible

(16) Servicing media like lubricants, impregnants, detergents, fuels, and other consumables should preferably be supplied automatically, and waste media should be removed automatically

(17) Whenever possible, automatic diagnostics for fault identification should be provided via failure-indicating hardware and/or special minicomputers with the associated software

(18) There should be maximum utilization of designed and built-in automatic test and checkout equipment

(19) The distributions of all equipment downtime categories should be determined and studied, and those maintenance actions which contribute excessively to the overall equipment downtime should be singled out and their downtimes minimized

(20) The distributions of the equipment downtimes resulting from the failure of key components should be studied; those components contributing significantly to the overall equipment downtime should be singled out and redesigned with lower failure rates and higher repair rates

(21) The design should be such as to achieve maximum availability at minimum life cycle cost

The last item in the previous list is what it's all about: design for maximum availability at minimum cost. The rest of this section is devoted to that aspect of system R&M engineering.

10.10 COST CONSIDERATIONS

The most important constraint that a system designer of today must consider is cost. All of the military services face a problem of designing and fielding systems that they can "afford," i.e., which have reasonable life cycle costs (LCC). R&M have a significant impact on life cycle costs (LCC) because they determine how frequently a system fails and how rapidly it is repaired when it fails.

Thus, a vital system design consideration is how to minimize LCC by maximizing R&M within given design cost constraints.

10.10.1 LIFE CYCLE COST (LCC) CONCEPTS

Life cycle cost is the total cost of acquiring and utilizing a system over its entire life span. LCC includes all costs incurred from the point at which the decision is made to acquire a system, through operational life, to eventual disposal of the system. A variety of approaches can be used to estimate the cost elements and provide inputs to the establishment of a life cycle cost model. The total life cycle cost model is thus composed of subsets of cost models which are then exercised during tradeoff studies. These cost models range from simple informal engineering/cost relationships to complex mathematical statements derived from empirical data.

Total LCC can be considered as generated from two major areas:

(1) system acquisition cost
(2) system utilization cost

In simple mathematical terms, the above can be stated by:

$$LCC = AC + SUC \qquad (10.124)$$

where

LCC = life cycle cost
AC = acquisition cost
SUC = system utilization cost

Figure 10.10.1-1 identifies the more significant cost categories and shows (conceptually) how LCC may be distributed in terms of the major cost categories over a system life cycle.

In general, design and development costs include basic engineering, test and system management; production costs include materials, labor, G&A, overhead, profit, capitalization, handling, and transportation; operational and support (O&S) cost includes a sizeable number of factors including initial pipeline spares and replacement, equipment maintenance (on/off), inventory entry and supply management, support equipment, personnel training, technical data/documentation, and logistics management. Disposal costs include all costs associated with deactivating and preparing the system for disposal through scrap or salvage programs. Disposal cost may be adjusted by the amount of value received when the disposal process is through salvage.

COST OF OWNERSHIP

COST

Production

Operation &
Support Cost (O&S)

Design & Development

Disposal

LIFE-CYCLE   (a)

TOTAL COST OF OWNERSHIP

DISPOSAL

MAINT. & LOGISTICS SUPPORT

OPERATION

PRODUCTION

R & D

UTILIZATION COST

ACQUISITION COST

SYSTEM LIFE

(b)
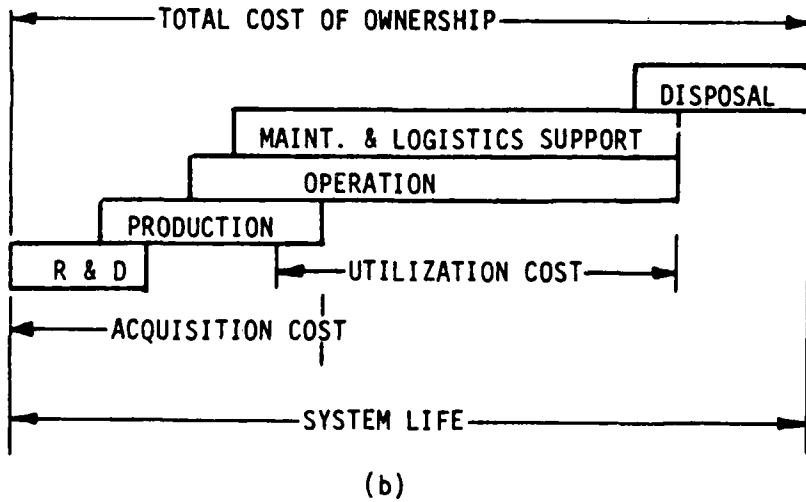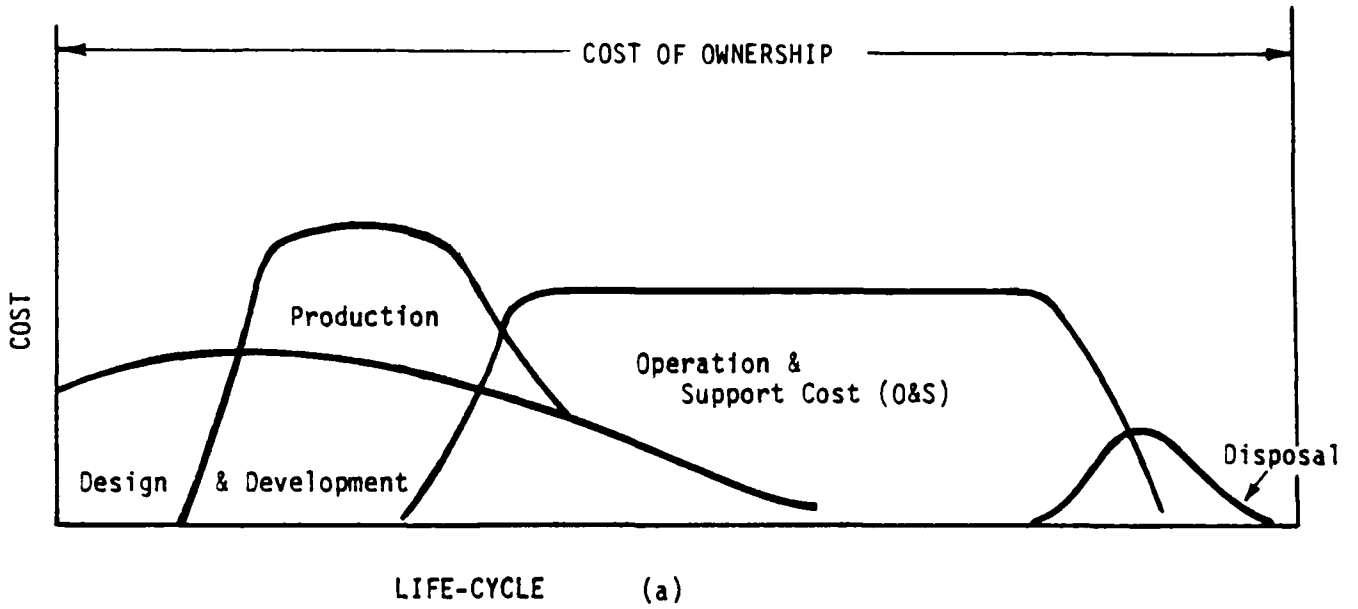
FIGURE 10.10.1-1: LCC CATEGORIES VS. LIFE CYCLE

Life cycle cost elements are influenced by numerous system factors. Among them are:

(1) system performance requirements
(2) reliability/maintainability requirements
(3) technology
(4) system complexity
(5) procurement quantity
(6) procurement type and incentives
(7) production learning curve location
(8) maintenance and logistic support plan

Despite the emphasis on design, development and production cost in contractual requirements, the overriding objective for major DoD systems is to minimize total life cycle cost. The Government requires that life cycle costs are to be estimated during all phases of a major system acquisition program from design through operations to ensure appropriate tradeoffs among investment costs, ownership costs, schedules, and performance. Tradeoffs between acquisition and ownership costs as well as against technical performance and schedule must be performed in selecting from competing system design concept proposals. Life cycle cost factors are used by the Government in selecting systems for full scale development and production.

As shown in Figure 10.10.1-1, the major components of a system life cycle are its operation and support phases and the associated (O&S) cost. The maintenance and logistic factors that comprise O&S cost should be carefully considered and continually evaluated throughout the entire acquisition process but in particular during the conceptual phase where controllability is the greatest. These analyses are performed to provide the O&S cost impact of various design and development decisions and, in general, to guide the overall acquisition process. LCC considerations and analyses provide:

(1) a meaningful basis for evaluating alternatives regarding system acquisition and O&S cost

(2) a method for establishing development and production goals

(3) a basis for budgeting

(4) a framework for program management decisions

The application of R&M disciplines plays a key role in minimizing LCC, since one, (R), determines the frequency of failure and the other, (M), determines the time to fix a failure. System designers must balance performance, reliability, maintainability, and production goals in order to minimize LCC.

To meet this need, attention is focused on structuring a balanced design approach derived from a life cycle cost model that is comprised of and governed by submodels, which calculate R&M and cost variables. Figure 10.10.1-2 presents an overview of the R&M and cost methodology within this framework. This figure shows the life cycle cost model as the
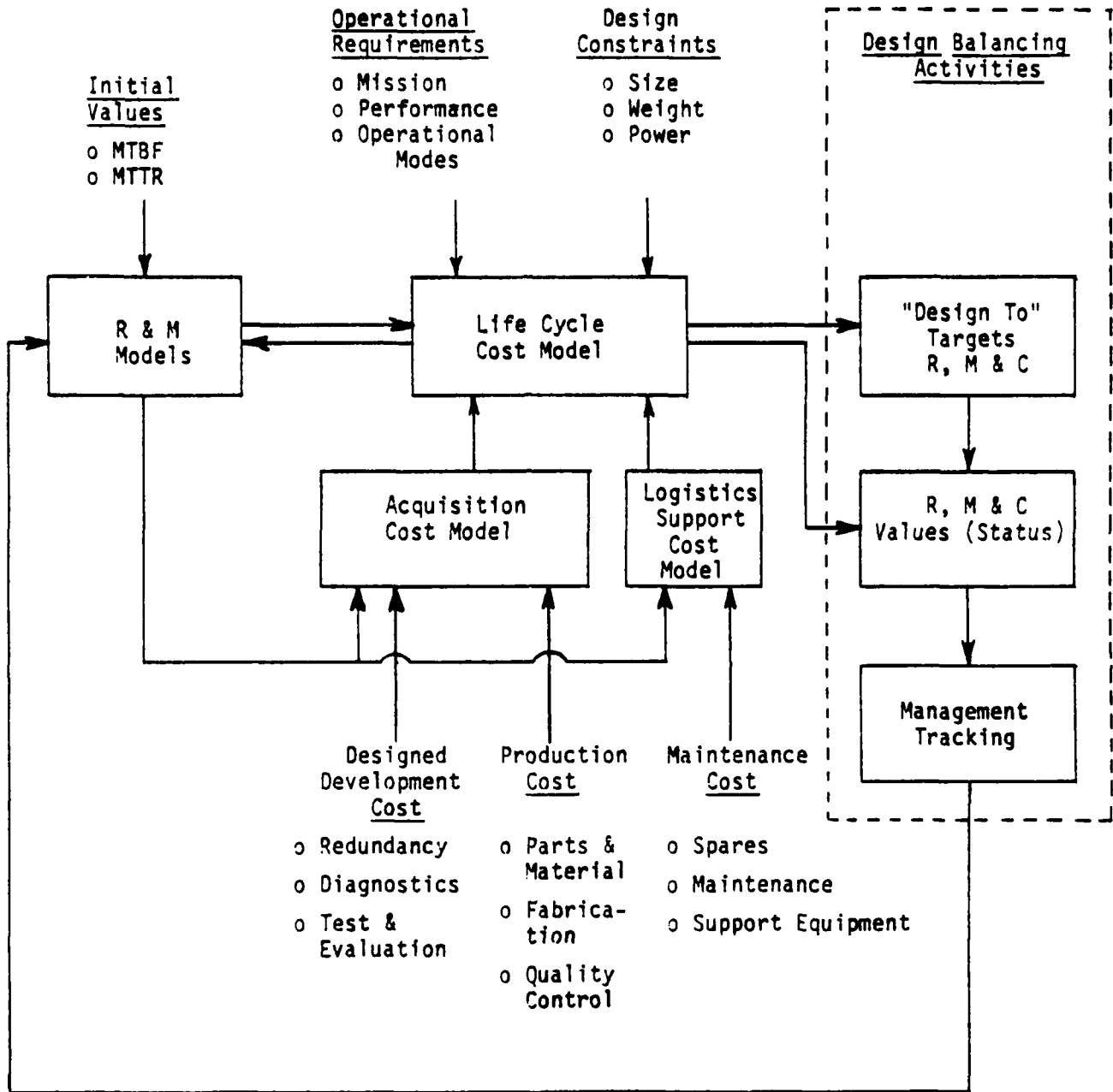
FIGURE 10.10.1-2: **R&M AND COST METHODS**

vehicle which estimates for operation, performance, reliability, maintainability, and cost are traded off to obtain "design to" target goals which collectively represent a balanced design. This life cycle cost model includes submodels which are representative of acquisition costs and maintenance and logistics support costs, subject to the constraints of functional objectives and minimal performance requirements.

Some of the major controllable factors contributing to system life cycle cost related to these cost categories are shown in Table 10.10.1-1. In practice, however, all of these cost factors will not appear in each LCC analysis. Only those factors relative to the objective and life cycle phase of the analysis are included. For example, a comparison of standard commercial equipment would not include design and development costs but would include procurement and support costs. Similarly, a throwaway part or assembly would result in a simpler decision model than an item requiring on site and off site maintenance and repair. Thus, a system LCC decision model should be established that is flexible and capable of being exercised in various modes in keeping with the complexity of the system under analysis and the potential cost benefits to be derived from the analysis.

Figure 10.10.1-3 illustrates (conceptually) the relationships between reliability and cost. The top curve is the total life cycle cost and is the sum of the acquisition (or investment) and O&S costs. The figure shows that as a system is made more reliable (all other factors held constant) the support cost will decrease since there are fewer failures. At the same time, acquisition cost (both development and production) is increased to attain the improved reliability. At a given point, the amount of money (investment) spent on increasing reliability will result in exactly that same amount saved in support cost. This point represents the reliability for which total cost is minimum. Consequently, reliability can be viewed as an investment during acquisition for which the return on investment (ROI) is a substantial reduction of maintenance support (the operational costs tend to remain constant regardless of reliability investment). An analogous relationship exists between maintainability and cost.

The implementation of an effective program based on proven LCC principles complete with analytical models and supporting input cost data will provide early cost visibility and control, i.e., indicate the logistics and support cost consequences of early research, development, and other subsequent acquisition decisions, such that timely adjustments can be made as the program progresses. Although the specific requirements are, of course, peculiar to each system or equipment item, the guidelines given in Table 10.10.1-2 should be considered as a minimum in planning and implementing an LCC program.

10.10.2   LCC MODELS

There are probably more models in LCC than in any other discipline. A number of models have been developed by industrial and Government organizations (Refs. 27, 28, 29) to estimate cost and provide engineering relationships between significant and controllable

TABLE 10.10.1-1: LIFE CYCLE COST BREAKDOWN

Total Life Cycle Cost

Acquisition		Operation & Support	
Basic Engineering	**Recurring Production Costs**	**Logistics & Maintenance Support**	**Operational**
- Design (Electrical, Mechanical)	- Parts & Materials	- Pipeline Spares	- Supply Management
- Reliability, Maintainability	- Fabrication	- Replacement Spares	- Technical Data
- Human Factors Producibility	- Assembly	(organization, inter-	- Personnel
- Component	- Manufacturing Support	mediate, depot)	- Operational Facilities
- Software	- Quality Control	- On-Equipment Maintenance	- Power
	- Inspection & Test	- Off-Equipment Maintenance	- Communications
Test & Evaluation	- Receiving	- Inventory Entry & Supply	- Transportation
	- Inprocess	Management	- Materials (exclud-
- Development	- Screening	- Support Equipment (in-	ing maintenance)
- R Growth	- Burn-In	cluding maintenance	- General Management
- R&M Demonstration	- Acceptance	- Personnel Training &	- Modifications
- R Screening	- Material Review	Training Equipment	- Disposal
- R Acceptance	- Scrap Rate	- Technical Data & Docu-	
	- Rework	mentation	
Experimental Tooling		- Logistics Management	
	Nonrecurring Production Costs	- Maintenance Facilities	
- System		& Power	
- R Program (MIL-STD-785)	- First Article Tests	- Transportation (of failed	
- M Program (MIL-STD-470)	- Test Equipment	items to and from depot)	
- Cost	- Tooling		
	- Facilities		
Manufacturing & Quality Engineering	- System Integration		
	- Documentation (including		
- Process Planning	maintenance instructions		
- Engineering Change Control	& operating manuals)		
- Q.A. Planning, Audits, Liaison, etc.	- Initial spares (organi-		
	zational, intermediate and		
	depot) (pipeline)		

FIGURE 10.10.1-3: LIFE CYCLE COSTS VS. RELIABILITY

TABLE 10.10.1-2: LCC GUIDELINES*

RESEARCH AND DEVELOPMENT ACTIONS

o   Conscious and determined use of technology to reduce cost
o   Creation of viable options which will allow timely lower risk development of new systems by:
  o   Developing and considering alternate paths to the same goal
  o   Developing and testing "brass board" or experimental configurations, prototypes, advanced development models and advanced components in response to anticipated need
o   Using competition wherever possible between technical approaches and developers
o   Selecting programs among competing solutions such that:
  o   Technical feasibility is a necessary but only one of several criteria for proceeding with a program
  o   Program progress is geared to demonstrated performance milestones rather than arbitrary schedules or contract constraints, using a strong test and evaluation program, at the component as well as systems level
  o   Greater emphasis is placed on product improvement as a potentially effective alternative to a new development

ACQUISITION POLICIES

o   Use of end-item minimum performance goals or specifications, selected to allow maximum tradeoff flexibility, rather than detailed design specifications for systems, subsystems and components
o   Clear identification of both mandatory and desirable system performance characteristics
o   Periodic and timely feedback of estimated production, operating and support costs to permit early corrective actions in high risk and design problem areas
o   Appropriate use of standardization
o   Consideration of personnel and training cost factors early in the acquisition process in order to influence design trade-offs
o   Use of producibility and value engineering techniques in high-cost areas early during development

DESIGN ACTIONS

o   Lowering development and acquisition costs through design simplicity, greater use of design inheritance, greater use of standard and commercial products, and use of high production volume technology parts
o   Improving reliability through greater use of proven designs, more design attention to non-random failures, design sim-plicity, improved quality control, more effective development and test procedures, and use of more representative environ-mental tests
o   Improving maintainability through improved accessibility, greater support equipment (SE) standardization, improved test procedures, and more design attention to test equipment
o   Designing equipment to reduce maintenance skills, special training requirements, and manpower requirements

*Derived from joint AFSC/AFLC Commander's Working Group on Life Cycle Cost, ASD/ACL, Life Cycle Cost Analysis Guide, (WPAFB, Ohio, November 1975).

acquisition and logistic support cost factors. Many of the models are basically accounting structures which contain terms and factors for each of the cost elements of a system life cycle. Other models contain relationships between two or more of the cost factors and may contain cost estimating relationships to estimate costs of elements which cannot be easily measured or determined until the system is actually committed to field use.

In order to use the models, a database of engineering/statistical information on system related factors must be developed and/or compiled. Obtaining this information necessitates a firm understanding of the system, its development and production processes, and a historical database on similar systems.

An example of a simple generic LCC model is one which merely adds the recurring and nonrecurring costs (Ref. 27):

$$LCC = NRC + RC \qquad (10.125)$$

where

NRC = nonrecurring costs
RC = recurring costs

The nonrecurring costs can be calculated by adding up the following cost factors:

$$NRC = C_{RD} + C_{RM} + C_Q + C_{LCM} + C_A + C_I + C_{TE} + C_T + C_{TR} + C_S \qquad (10.126)$$

where

C_{RD} = research and development cost
C_{RM} = reliability/maintainability improvement cost
C_Q = qualification approval cost
C_{LCM} = life cycle management cost
C_A = acquisition cost
C_I = installation cost
C_{TE} = test equipment cost
C_T = training cost
C_{TR} = transportation cost
C_S = support cost

The RC costs can be added as follows:

$$RC = C_O + C_M + C_S + C_{MT} + C_{IN}$$

where

C_O = operating cost
C_M = manpower cost
C_S = support cost
C_{MT} = maintenance cost
C_{IN} = inventory

The individual cost terms in each model, which may themselves be rather complex submodels, are derived from historical data, engineering cost estimates, and cost estimating relationships. The first step in developing or applying any model is to structure the system into a breakdown of its cost elements as was shown in Table 10.10.1-1. These are known as LCC Breakdown Structures, which are briefly described in the next section.

10.10.2.1 LCC BREAKDOWN STRUCTURES

The Life Cycle Cost Breakdown Structure is an ordered breakdown of the elements of cost, estimated to arrive at a total life cycle cost. This structure represents the "accounting" model for a life cycle cost estimate. The cost elements to be included in a given LCC estimate/analysis must be defined for each case considered. In order to identify the required life cycle cost elements, a three dimensional matrix can be developed which considers hardware elements (HES), subdivisions of work (SOW), and elements of cost (EOC). Figure 10.10.2.1-1 illustrates the three dimensional concept.
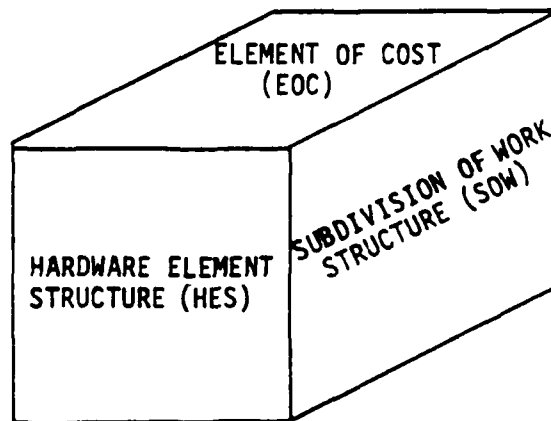
FIGURE 10.10.2.1-1: LIFE CYCLE COST ELEMENT MATRIX CONCEPT (Ref. 29)

Hardware Element Structure. The Hardware Element Structure (HES) is a segregation of all the program level mission hardware successively subdivided into manageable elements in terms of function. This breakdown starts with system level hardware and then successively divides this hardware into subsystems, sections, assemblies, subassemblies, and, as necessary, to lower levels.

Subdivision of Work. The Subdivision of Work structure (SOW) is a phase/functional category segregation of the program. In a typical case, the program is separated into four major phase/functional categories: Research, Development, Test, and Evaluation (RDT&E); Investment Nonrecurring; Investment Recurring; and Operational and Maintenance (O&M).

Elements of Cost. The elements of cost (EOC) reflect the normal accounting classification of program costs. This type of breakdown reflects the nature of expenditures such as labor, materials, overhead, etc.

LCC Breakdown. The LCC breakdown is an intersection of the HESs, SOWs, and EOCs. The SOW tabulation is the Life Cycle Cost Breakdown Structure (LCCBS). It is understood that each element contains the associated HES and EOC elements. The dashed projection lines in Figure 10.10.2.1-2 demonstrate the relationship of the three faces of the matrix.
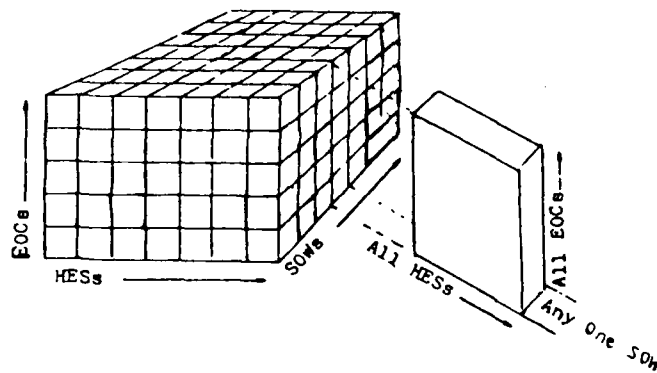
FIGURE 10.10.2.1-2: SOWS ELEMENT CONTENT

For example, the subdivision of work (SOW) item might be the Test and Evaluation (T&E) phase of a system's life cycle, the HES might be all of the subsystems of the system, and the EOCs would be the standard elements of T&E costs for each subsystem.

An example of a generic LCC Breakdown Structure (LCCBS) is shown in Table 10.10.2.1-1; an example of a specific LCCBS for a Large Ground Based Radar System is shown in Table 10.10.2.1-2 (Ref. 29). Reference 29 contains a number of specific examples of LCCBSs for various types of systems and subsystems.

10.10.2.1.1 DOD LCC BREAKDOWN STRUCTURES (LCCBSs)

There are no completely standard LCCBSs used by the services, but there are breakdowns that receive widespread and general endorsement by each service. These are shown in Tables 10.10.2.1.1-1 and 10.10.2.1.1-2.

For software LCCBSs, Air Force regulation 800-14 (Ref. 44) defines the life cycle cost of a computer program to consist of the phases shown in Figure 10.10.2.1.1-1.
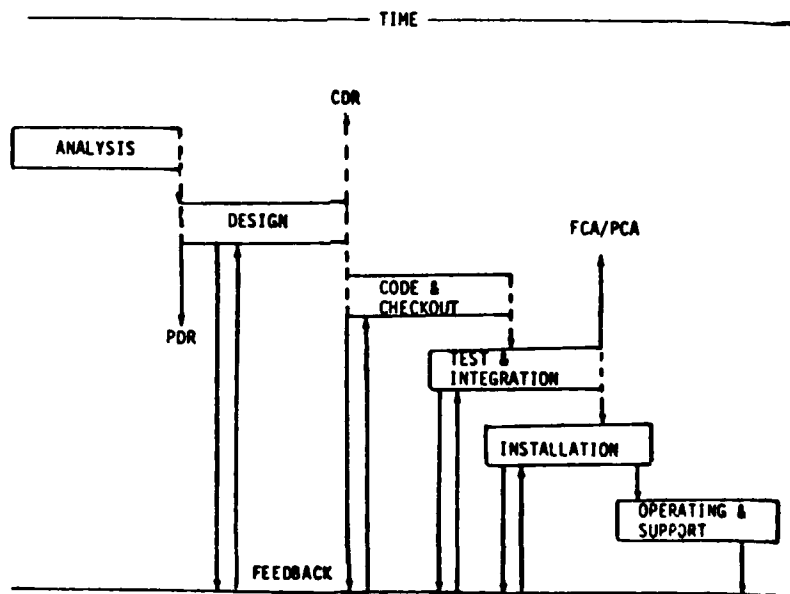
FIGURE 10.10.2.1.1-1: COMPUTER PROGRAM LIFE CYCLE (FROM AF REG. 800-14)

TABLE 10.10.2.1-1: <u>GENERIC LIFE CYCLE COST BREAKDOWN STRUCTURE</u>

```
Development Cost
     Conceptual Phase Cost
     Demonstration/Validation/Advanced Development Phase Cost
     Full-Scale Development Phase Cost
          Program Management
          Engineering
          Fabrication
          Development Tests
          Test and Evaluation Support
          Data
          Producibility Engineering & Planning
Production Phase/Investment Cost
     Non-Recurring Investment Cost
          Program Management
          Producibility Engineering & Planning
          Initial Production Facilities
          Initial Spares and Repair Parts
          Common Support Equipment
          Peculiar Support Equipment
          Data
          Initial Training
          Technical Support
     Recurring Investment Cost
          Labor
          Material
          Sustaining Engineering
          Quality Control and Inspection
          Packaging and Transportation
          Operational Site Activation
Operations and Support Cost
     Operating Cost
          Electric Power
          Consumables
          Operational Personnel
          Operational Facilities
          Leasing
     Support Cost
          System Equipment Maintenance
          Support Equipment Maintenance
          Contractor Services
          Inventory Administration
          Replenishment Spares & Repair Parts
          Repair Material
          Transportation and Packaging
```

TABLE 10.10.2.1-2: <u>LARGE GROUND BASED RADAR SYSTEM LCC BREAKDOWN STRUCTURE</u>

<u>Acquisition Cost</u>

R&D Phase

    Prime Mission Product
      Radar Subsystem
      Computer Subsystem
      Communications Subsystem
      Integration & Assembly

    System Test & Evaluation
      Subsystem Test
      System Performance Test

    System Project Management
      System Eng Mgt/Sys Eng
      Support Prog. Management

    Data
      Engineering Data
      Management Data

    Operations/Site Activation
      Contractor Technical Support
      Site Preparation
      Facility Design & Construction
      System Assy, Installation, C/O

    Supply Support
      Pre-System Test Supply Support
      System Test Supply Support

Evaluation Phase

    Contractor Maintenance

    Site Maintenance Supply Support

Production Phase

    Prime Mission Product
      Radar Subsystem
      Computer Subsystem
      Communications Subsystem
      Integration & Assembly

    System Test & Evaluation
      Subsystem Test
      System Performance Test
      Operational Evaluation
      Test & Evaluation Support

    System Project Management
      System Eng Mgt/Sys Eng
      Support Program Management

    Data
      Technical Orders & Manuals
      Engineering Data
      Management Data

    Operations/Site Activation
      Contractor Technical Support
      Site Preparation
      Facility Design & Construction
      System Assy, Installations, C/O

    Common Support Equipment
      Organizational/Intermediate
      Depot

    Supply Support
      Pre-System Test Supply Support
      System Test Supply Support

    Initial Spares and Repair Parts
      Organizational/Intermediate
      Depot

<u>Utilization Cost</u>

    Replenishment Spares
      Radar Subsystems
      Communications Subsystem
      Facilities Subsystem

    On-Equipment Repairs
      Radar Subsystem
      Communications Subsystem
      Facilities Subsystem

    Off-Equipment Repairs
      Radar Subsystem
      Communications Subsystem
      Facilities Subsystem

    New Item Inventory Management
      Radar Subsystems
      Communications Subsystem
      Facilities Subsystem

    Lease Cost (including maintenance)
      Computer Subsystem

TABLE 10.10.2.1.1-1: LCCBSs USED IN THE MILITARY SERVICES

Department	Document	Reference(s)
Army	Department of the Army Pamphlet No. 11-2 Department of the Army Pamphlet No. 11-3 Department of the Army Pamphlet No. 11-4 Department of the Army Pamphlet No. 11-5	30 31 32 33
Navy	Life Cycle Cost Guide for Major Weapon Systems Life Cycle Cost Guide for Equipment Analysis	34 35
Air Force	Cost Estimating and Analysis, An Introductory Short Course AFLC LSC Model	36 37
Marine Corps	USMC LCCM Manual	38
Joint Service (Tri-TAC)	Cost Effectiveness Program Plan for Joint Tactical Communications	39
OSD/CAIG (Cost Analysis Improvement Group)	Weapon System Operating and Support Cost Element Structures (aircraft, ship, combat vehicle, and air-launched tactical missile)	40 41 42 43

Table 10.10.2.1.1-2 (Ref. 29) gives a software LCCBS derived from Figure 10.10.2.1.1-1.

TABLE 10.10.2.1.1-2: <u>SOFTWARE LIFE CYCLE COST BREAKDOWN STRUCTURE</u>

Analysis

    System Requirements
    Program Requirements
    Interface Requirements
    Design Requirements and Specifications

Design

    Flow Charts
    Data Structure
    Input/Output Parameters
    Test Procedures

Code and Checkout

    Coded Instructions
    Desk Check
    Compile Programs

Test and Integration

    Program Test
    System Integration

Documentation

    Listings
    User Manual
    Maintenance Manual

Installation

    Validation, Verification, Certification

Operating and Support

    Environments
    Modifications
    Documentation Revision
    Test Revisions

Having derived the LCCBS for a system, one then must be able to "plug in" the cost figures for each element. These figures are developed from Cost Estimating Relationships (CERs).

10.10.2.2 COST ESTIMATING RELATIONSHIPS (CERs)

CERs are used to estimate the cost of the individual elements of the LCC Breakdown Structure. Each CER contains variables describing resource consumption and parameters reflecting prices, conversion factors, or empirical relationships. These relationships range from simple averages and percentages to complex equations, resulting from statistical regression analysis, which relate cost (the dependent variable) to physical performance and/or program characteristics (the independent variable).

In general, three basic methods are used to estimate cost or develop CERs:

    (1)   engineering cost method
    (2)   analogous cost method
    (3)   parametric cost method (deterministic or probabilistic)

Engineering Cost Method

This method involves the direct estimation of particular cost elements by examining the system component-by-component. In other words, it uses standard, established cost factors, e.g., firm engineering and manufacturing estimates, to develop the CERs. Table 10.10.2.2-1 lists some examples of standard cost factors which were valid circa 1977 (Ref. 45). They can be readily updated to the present time by the use of annual discounting and escalation factors (to be discussed later).

Analogous Cost Method

This method involves cost estimation based upon experience with similar equipment and technology in the past. It utilizes historical data, updated to reflect escalation due to inflation and the effect of technology advances. A simple example is shown in Figure 10.10.2.2-1.

Parametric Cost Method

This method uses significant parameters and variables to develop CERs which are usually in the form of equations.

A parameter in a CER reflects a conversion factor from one system of units to another. It may be a price, an empirically derived ratio, or a policy parameter. A price like cost per manhour, for example, converts manhours into dollars. An example of an empirical ratio is the number of maintenance manhours per failure of a given component, which may be obtained as a statistical average. An example of a policy parameter is the number of parts per module. Such parameters enter into cost estimating relationships and often are compiled and published as planning factors.

TABLE 10.10.2.2-1: TYPICAL STANDARD COST FACTORS

A. INVENTORY

    o Purchase Order ($/Order)
       Repairable   200
       Non-Repairable   100
    o New Item Entry ($/Item)
       Repairable   375
       Non-Repairable   290
    o Inventory Maintenance ($/$/Yr.)
       25% of Inventory Value/Yr.

B. PERSONNEL LABOR ($/Hour)

    o Operator   15.25
    o Maintenance
       Organization   8.50
       Intermediate   10.25
       Factory   15.50

C. TRAINING ($/Student Week)

    o Operator   300
    o Maintenance   450

D. TRANSPORTATION ($/Pound)

    o Domestic   1.65
    o Foreign   5.45

E. PACKING ($/Pound)

    o Domestic   2.35
    o Foreign   5.55

F. DATA ($/Page)

    o Operating Instructions   250
    o Maintenance Instructions   300
    o Failure Report   100

G. FACILITIES

    o Construction -- Adjust For Geographical Location
    o Operation -- $50/Sq. Ft./Yr.
    o Maintenance -- $100/Sq. Ft./Yr.

H. SUPPORT EQUIPMENT SPARES

    o 20% of Support Equipment Material
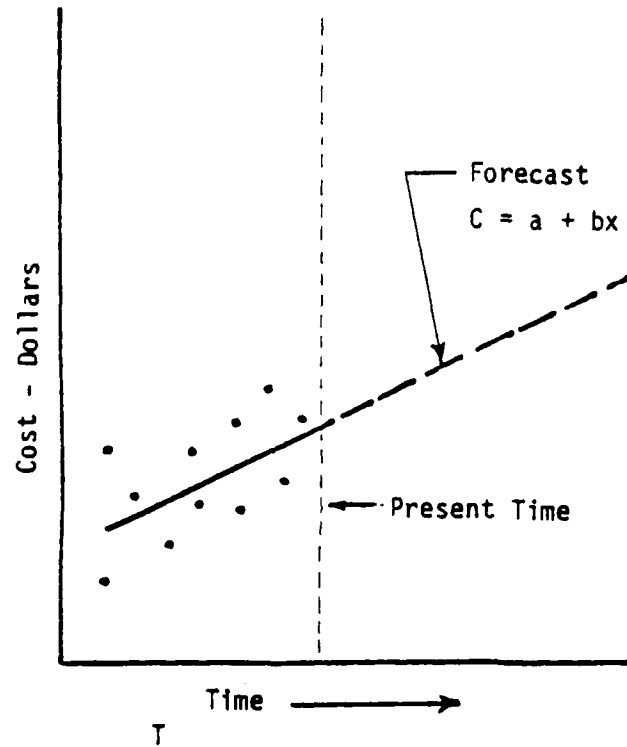
FIGURE 10.10.2.2-1: <u>FORECAST PRESENTING COST TREND BASED ON HISTORICAL DATA</u>

A <u>variable</u> in a CER characterizes resource consumption over time. It may be a physical or performance measure. Variables generate costs. Examples of variables include failure rate, preventive maintenance manhours per unit of equipment, and hardware design characteristics.

The CER equation reflects our belief in the underlying mechanism or relationship which generates costs. Often when a detailed theoretical relationship cannot be developed, a statistically derived, e.g., via least squares or regression analysis, is used. An example will make the difference clear.

Suppose we wished to estimate the annual shipment cost of a type of failed module to a fixed site depot. If we knew the weight per year of such module (say, W) and a cost per pound of packing and shipping for this module type (say, CP), then an engineering relationship (reflecting the physical prices of shipment) for annual, CA, might be:

$$CA = W(CP) \tag{10.128}$$

Suppose instead we had no way of obtaining a direct variable such as weight to measure shipment cost. We might infer that the cost varied with the number of units shipped, which in turn might reflect a fixed number of failures per year plus a variable number dependent on mission hours per year. We could collect historical data on annual shipment costs and mission hours for a number of years and attempt to fit an equation to those data through statistical methods. A reasonable equation might be:

$$CA = a + b(MH) \tag{10.129}$$

where a represents the fixed costs per year, b the shipping cost per mission hour per year, and MH is the annual mission hours. The parameters a and b would be estimated by the method of least squares (see Ref. 46 for an excellent treatment of statistical cost model construction and estimation).

An example of a more complex CER (Ref. 47) for the R&M cost of an airborne fire control radar is given by:

$$\ell n R\&M \text{ cost} = -0.85 + 1.05 \ell n R + 0.54 X_1 + 1.1 X_2 \tag{10.130}$$

where

$$R = \text{single pulse detection range for a } 1m^2 \text{ target in nautical miles}$$
$$\ell n = \text{natural logarithm}$$
$$X_1 = 1 \text{ if frequency is K band}$$
$$ 0 \text{ if frequency is X band}$$
$$X_2 = 1 \text{ if radar has variable transmitter waveform}$$
$$ 0 \text{ if not}$$
$$R\&M \text{ cost} = 10^6 \text{ (FY 1974)}$$

10.10.2.2.1 EXAMPLES OF DETAILED COST ESTIMATING RELATIONSHIPS

As was mentioned previously, a number of CERs have been developed by each of the services for use in LCC analysis of military systems. In addition to being presented in the specific service documents previously referenced, they are very well summarized in Reference 29. Following are two specific examples to give the reader a flavor for the methodology used and the form of the CERs.

Army LCC Estimation Model

References 30, 31 and 32 define the CERs for a standard Army LCC model. The basic model is given by:

$$LCC = \sum_{i=1}^{3} C_i \qquad (10.131)$$

where

C_1 = research and development (R&D) cost
C_2 = investment cost
C_3 = operating and support cost

Each of the C_is of Eq. (10.131) is in turn broken down as follows:

C_1 = cost of research and development

$$= \sum_{i=1.01}^{1.10} C_i \qquad (10.132)$$

where

$C_{1.01}$ = development engineering cost
$C_{1.02}$ = producibility engineering and planning cost
$C_{1.03}$ = R&D tooling cost
$C_{1.04}$ = prototype manufacturing cost
$C_{1.05}$ = R&D data cost
$C_{1.06}$ = R&D test and evaluation cost
$C_{1.07}$ = R&D system/project management cost
$C_{1.08}$ = R&D training services and equipment cost
$C_{1.09}$ = R&D facilities cost
$C_{1.10}$ = other R&D cost

C_2 = Investment cost

$$= \sum_{i=2.01}^{2.11} C_i \qquad (10.133)$$

where

$C_{2.01}$ = nonrecurring investment cost
$C_{2.02}$ = production cost
$C_{2.03}$ = engineering changes cost
$C_{2.04}$ = system test and evaluation cost
$C_{2.05}$ = data cost
$C_{2.06}$ = production phase system/project management cost
$C_{2.07}$ = operational/site activation cost
$C_{2.08}$ = initial training cost
$C_{2.09}$ = initial spares and repair parts cost
$C_{2.10}$ = transportation cost
$C_{2.11}$ = other investment cost

C_3 = cost of operating and support

$$= \sum_{i=3.01}^{3.06} C_i \qquad\qquad (10.134)$$

where

$C_{3.01}$ = military personnel cost
$C_{3.02}$ = consumption cost
$C_{3.03}$ = depot maintenance cost
$C_{3.04}$ = material modifications cost
$C_{3.05}$ = other direct support operations cost
$C_{3.06}$ = indirect *support operations* cost

In turn, each of the terms of Eq. (10.132), (10.133), and (10.134), e.g., $C_{1.01}$, $C_{2.01}$, $C_{3.01}$, is represented by a CER equation.

Air Force Logistics Support Cost Model

The Air Force Acquisition Logistic: Division (AFALD) has a Logistic Support Cost (LSC) model (Ref. 37) that has wide application in life cycle costing. That model is abstracted as follows:

$$LSC = \sum_{i=1}^{11} C_i \qquad\qquad (10.135)$$

where

C_1 = pipeline and replacement spares
C_2 = on-equipment maintenance
C_3 = off-equipment maintenance
C_4 = inventory entry & supply management
C_5 = support equipment
C_6 = personnel training & training equipment
C_7 = management & technical data
C_8 = facilities
C_9 = fuel
C_{10} = spare engines
C_{11} = software support

Once again, each of the C_is in Eq. (10.135) is represented by a CER equation, usually rather complex. The important point is that almost all of the C_is are highly dependent upon the R&M parameters of the system. For example, in the case of C_1 (cost of flight line unit spares) the CER is given by:

$$C_1 = \text{cost of FLU spares}$$

$$
\begin{aligned}
= & \; M \sum_{i=1}^{N} (STK_i)(UC_i) \\[2mm]
& + \sum_{i=1}^{N} \frac{(PFFH)(QPA_i)(UF_i)(1-RIP_i)(NRTS_i)(DRCT_i)}{MTBF_i}(UC_i) \\[2mm]
& + \sum_{i=1}^{N} \frac{(TFFH)(QPA_i)(UF_i)(1-RIP_i)(COND_i)}{MTBF_i}(UC_i)
\end{aligned}
\qquad (10.136)
$$

Ignoring the definitions for each of the terms, note that the second and third terms of the equation (which are summations) are highly dependent upon the MTBF of each of the individual flight units.

Similarly, for C_2

$$C_2 = \text{on-equipment maintenance}$$

$$
\begin{aligned}
= & \sum_{i=1}^{N} \frac{(TFFH)(QPA_i)(UF_i)}{MTBF_i} \\[2mm]
& \Big[PAMH_i + (RIP_i)(IMH_i) + (1-RIP_i)(RMH_i) \Big] BLR \\[2mm]
& + \frac{TFFH}{SMI}(SMH)(BLR) \times \frac{(TFFH)(EPA)}{CMRI}(ERMH)(BLR)
\end{aligned}
\qquad (10.137)
$$

The first term in C_2 is the labor manhour cost to perform on-equipment (flight line) maintenance on FLUs due to unscheduled failures over the life of the system. The element,

$$PAMH_1 + (RIP_i)(IMH_i) + (1-RIP_i)(RMH_i)$$

is the weighted average on-equipment maintenance manhours per failure of the ith FLU including preparation and access time and either in place repair or removal and replacement as appropriate.

The second term is the labor manhour cost to perform scheduled maintenance on the complete system over the life cycle. Thus, C_2 is also highly dependent upon the R&M parameters of the system.

10.10.2.2.2 CERs WITH DISCOUNTING AND ESCALATING

Discounting

Discounting is a measure of the value of money. A dollar today is worth more than a dollar in ten years because of the annual interest that one would receive if the dollar were invested. For example, a dollar in the bank today at 6% interest is worth $1.79 at the end of ten years with interest. Similarly, the present value of a future $1 received ten years from now at a 6% discount rate is (1/1.79) or 0.558. In general, the present value (PV) of K received N years from now at a discount rate D is

$$PV = \frac{K}{(1 + D)^N} \qquad (10.138)$$

In calculating discounted present value of a flow of funds, we multiply the cost in each year by the present value (present worth) factor for that year at the discount rate being used and sum the total discounted operating costs. To that total we add the acquisition costs, which are not discounted in the first year, to obtain the discounted present value of all costs. Repeating this process for alternatives being considered, we may then compare the different present values to arrive at a decision. Note that this process requires accurate time phasing of costs in each year rather than lifetime costs averaged annually.

What should the discount rate be? Cost analysts do not agree on this question, but 6% to 10% rates are commonly used for military tradeoffs. Based upon current interest rates (1981), the 10% discount factor does not seem unreasonable. Table 10.10.2.2.2-1 shows a typical calculation of discounted present value. The system shown has a documented present value (at 10%) of $964,000 compared with an undiscounted value of $1,270,000.

TABLE 10.10.2.2.2-1: DISCOUNTED PRESENT VALUE CALCULATION

Year	Undiscounted Cost ($000)	Discount Factor	Discounted Cost
0 (Investment)	$ 500	1.000	$500
1	70	0.909	64
2	60	0.826	50
3	90	0.751	68
4	60	0.683	41
5	65	0.621	40
6	110	0.565	62
7	65	0.513	33
8	70	0.467	33
9	80	0.424	34
10	100	0.386	39
Total	$1,270		$964

Note: 10% Discounting, 10 Year Life, Zero Salvage Value

Escalating

Just as discounting captures the time-effects of expenditures, escal-
ation captures the change in price levels over time. To estimate costs
in each future year based on current price is the equivalent of assuming
no escalation. This "constant dollar" assumption is unsatisfactory for
budgetary analysis (when we need to know what funds must be requested in
the future) for many kinds of tradeoffs. For an R&M example, if two
alternative systems are being compared, one with automated test
equipment and the other with manual diagnosis, we must make assumptions
about the rise in the price of men (salaries and fringe benefits) over
the life of the system in order to fully credit the automated
alternative with all its savings, including those obtained by purchasing
the automated equipment at today's prices. The method of calculation is
to separate costs that will escalate from costs that will not escalate
in each year, apply the correct escalation factors, total the escalated
costs in each year, and then apply the discount factors. Table
10.10.2.2.2-2 shows a pro-forma cost calculation form which includes all
effects. The formula for the escalation factor EF in year N at
escalation rate E is:

$$(EF) = (1 + E)^N \tag{10.139}$$

Combined Discounting and Escalating

It is often convenient to include escalation and discounting in CERs,
particularly when they are to be used in computerized cost models. If
costs are constant in each year, a CER such as Eq. (10.140) may be
modified to that of Eq. (10.141).

$$C = f(A,B) \tag{10.140}$$

$$C = f(A,B) \left[(1 + E)/(1 + D) \right]^Y \tag{10.141}$$

where

A,B are independent variables

E = escalation rate
D = discount rate
Y = year (1, 2, ..., K)

If costs vary from year to year, the expression $f(A,B)$ must be replaced
with $f(A,B,Y)$ where the structure would express the variation in
undiscounted, unescalated costs with time (as in the familiar U-shaped
failure curve reflecting initial "burn-in," subsequent stability, and
final service life effects on failure rates). In such an analytic cost
model, E may vary among cost elements, expressing inflation in each cost
element but D should not, being a system service or economy-wide
parameter.

TABLE 10.10.2.2.2-2: COST CALCULATION FORM

INVESTMENT

Element	2.013	3.105	4....	Total
Cost	$	$	$	$

OPERATIONS AND SUPPORT

Year	Raw Cost Element 4.015	Escalation Factor At ___%	Escalated Cost	Element	Escalation Factor At ___%	Escalated Cost
1						
2						
3						
4						
.						
.						
20						
Total						

Year	Element	Escalation Factor At ___%	Escalated Cost	Total Escalated Cost	Discount Factor At ___%	Discounted Cost
1						
2						
3						
4						
.						
.						
20						
Total						

Standard tables of discounting and escalation factors are available in most engineering economic textbooks (Ref. 48). Reference 29 also contains a summary of the tables. Tables 10.10.2.2.2-3, 10.10.2.2.2-4, and 10.10.2.2.2-5 provide a set of dollar escalation conversion indices for the fiscal years 1970 to 1981 for RDT&E dollars, procurement dollars, and R&M dollars. These tables are useful for updating CERs developed in the past. For example, EQ. (10.130) depicted a CER for R&D costs of an airborne fire control radar based upon FY-74 dollars. To update the CER to 1981 dollars, one would use Table 10.10.2.2.2-3 as follows:

$$\text{CER(1981)} = \text{CER (\$1974)} \left(\frac{\text{FY 81 INDEX}}{\text{FY 74 INDEX}}\right)$$

$$= \text{CER (\$1974)} \left(\frac{2.192}{1.259}\right)$$

$$= \text{CER(\$1974) (1.74)}$$

10.10.3 COSTING SYSTEM AVAILABILITY

Developing an inherent system availability cost function requires the solution of three problems: (1) finding the least cost design and its cost for each reliability value over the range of interest and feasibility; (2) finding the least cost design and its cost for each maintainability value over the range of interest and feasibility; and (3) finding the least cost combination of reliability and maintainability to achieve each level of system availability over the range of interest and feasibility. Analytically, we can see that this is so since:

$$A_i = \text{MTBF}/(\text{MTBF} + \text{MTTR}) = 1/(1 + \alpha) \tag{10.142}$$

where

A_i = availability
MTBF = mean-time-between-failures
MTTR = mean-time-to-repair
α = maintenance time ratio

For a specified availability, MTTR and MTBF must be in a constant ratio. Increasing one requires increasing the other to maintain a required availability. If we assume that each level of MTTR has a particular cost (more about this in a moment) and similarly for MTBF, we have:

$$C_A = C_M + C_R = f(\text{MTTR}) + g(\text{MTBF})$$

where

C_A = cost of availability
C_M = cost of maintainability
C_R = cost of reliability

TABLE 10.10.2.2.2-3: DOD RDT&E DOLLAR CONVERSION INDICES

FY	70	71	72	73	74	75	76	176	77	78	79	80	81
70	1.000	1.058	1.113	1.164	1.259	1.391	1.487	1.530	1.576	1.685	1.820	2.005	2.192
71	.9455	1.000	1.052	1.101	1.190	1.315	1.406	1.447	1.491	1.593	1.721	1.896	2.072
72	.8984	.9502	1.000	1.046	1.131	1.250	1.336	1.375	1.416	1.514	1.635	1.802	1.969
73	.8588	.9083	.9559	1.000	1.081	1.195	1.277	1.314	1.354	1.447	1.563	1.722	1.882
74	.7945	.8403	.8844	.9251	1.000	1.105	1.181	1.216	1.252	1.339	1.446	1.593	1.742
75	.7189	.7603	.8002	.8371	.9048	1.000	1.069	1.100	1.133	1.211	1.308	1.442	1.576
76	.6726	.7113	.7486	.7831	.8465	.9354	1.000	1.029	1.060	1.133	1.224	1.349	1.474
176	.6536	.6913	.7275	.7610	.8226	.9092	.9718	1.000	1.030	1.101	1.190	1.311	1.433
77	.6343	.6709	.7061	.7386	.7984	.8824	.9431	.9705	1.000	1.069	1.155	1.272	1.390
78	.5935	.6277	.6606	.6910	.7470	.8255	.8831	.9080	.9356	1.000	1.080	1.190	1.301
79	.5494	.5810	.6115	.6397	.6915	.7642	.8168	.8406	.8661	.9251	1.000	1.102	1.204
80	.4986	.5274	.5550	.5806	.6276	.6936	.7414	.7629	.7961	.8402	.9076	1.000	1.093
81	.4562	.4825	.5078	.5312	.5742	.6346	.6783	.6980	.7192	.7687	.8304	.9149	1.000

TABLE 10.10.2.2.2-4: DOD PROCUREMENT DOLLAR CONVERSION INDICES

FY	70	71	72	73	74	75	76	176	77	78	79	80	81
70	1.000	1.046	1.092	1.137	1.215	1.328	1.436	1.483	1.547	1.656	1.800	2.002	2.204
71	.9562	1.000	1.044	1.087	1.161	1.270	1.373	1.418	1.479	1.584	1.721	1.915	2.107
72	.9160	.9580	1.000	1.042	1.113	1.217	1.316	1.358	1.417	1.517	1.649	1.834	2.019
73	.8794	.9198	.9601	1.000	1.068	1.168	1.263	1.304	1.360	1.456	1.583	1.761	1.938
74	.8233	.8610	.8988	.9361	1.000	1.093	1.182	1.221	1.273	1.363	1.482	1.649	1.815
75	.7529	.7874	.8219	.8561	.9145	1.000	1.081	1.116	1.164	1.247	1.355	1.508	1.659
76	.6963	.7282	.7601	.7917	.8458	.9248	1.000	1.032	1.077	1.153	1.254	1.394	1.535
176	.6744	.7054	.7363	.7669	.8192	.8958	.9686	1.000	1.043	1.117	1.214	1.351	1.487
77	.6466	.6762	.7059	.7352	.7854	.8588	.9286	.9587	1.000	1.071	1.164	1.295	1.425
78	.6038	.6315	.6592	.6866	.7334	.8020	.8672	.8953	.9339	1.000	1.087	1.209	1.331
79	.5555	.5809	.6064	.6316	.6747	.7378	.7979	.8236	.8591	.9199	1.000	1.112	1.224
80	.4994	.5223	.5452	.5679	.6066	.6633	.7172	.7404	.7724	.8271	.8991	1.000	1.101
81	.4537	.4745	.4953	.5159	.5511	.6026	.6516	.6727	.7017	.7514	.8168	.9065	1.000

TABLE 10.10.2.2.2-5: DOD O&M DOLLAR CONVERSION INDICES

FY	70	71	72	73	74	75	76	176	77	78	79	80	81
70	1.000	1.076	1.123	1.179	1.298	1.435	1.566	1.792	1.691	1.833	1.960	2.303	2.595
71	.9298	1.000	1.044	1.096	1.207	1.335	1.456	1.666	1.572	1.704	1.822	2.141	2.413
72	.8907	.9579	1.000	1.050	1.156	1.278	1.394	1.596	1.506	1.632	1.746	2.051	2.311
73	.8482	.9122	.9522	1.000	1.101	1.217	1.328	1.520	1.434	1.554	1.662	1.953	2.201
74	.7705	.8287	.8651	.9084	1.000	1.106	1.206	1.381	1.303	1.412	1.510	1.774	1.999
75	.6967	.7493	.7822	.8214	.9042	1.000	1.091	1.248	1.178	1.277	1.365	1.604	1.808
76	.6387	.6869	.7171	.7531	.8290	.9168	1.000	1.1445	1.080	1.171	1.252	1.471	1.657
176	.5581	.6002	.6226	.6580	.7243	.8010	.8737	1.000	.9438	1.023	1.094	1.285	1.448
77	.5913	.6359	.6639	.6971	.7674	.8487	.9257	1.0560	1.000	1.084	1.159	1.361	1.534
78	.5457	.5869	.6126	.6434	.7082	.7832	.8543	.9778	.9228	1.000	1.069	1.256	1.416
79	.5013	.5488	.5729	.6016	.6623	.7324	.7989	.9143	.8630	.9351	1.000	1.175	1.324
80	.4343	.4671	.4876	.5121	.5637	.6234	.6800	.7782	.7345	.7959	.8511	1.000	1.127
81	.3854	.4145	.4327	.4544	.5002	.5532	.6034	.6906	.6518	.7063	.7553	.8874	1.000

and we wish to minimize C_A (find the least cost system achieving specified availability) subject to:

$$\alpha = MTTR/MTBF = (1 - A)/A \qquad (10.143)$$

For a particular availability, we wish to know the cost of the least cost system. But C_M and C_R are themselves variable for a given MTTR and MTBF. There are many ways of achieving a particular MTBF, including redundancy. Each MTBF and similarly each MTTR has a least cost method of achievement (e.g., changing number of technicians versus degree of automatic test).

Let us suppose we wish to cost system availability in early concept design. Then we need two sets of cost functions, C_R and C_M. These CERs must express system costs in terms of MTBi and MTTR, respectively. We therefore need a "perspective" cost model. The maintainability cost model would require CERs that reflect the cost of the least cost system for any MTTR. Such expressions may be derived from historical data, statistically aggregated, or from preparation of a detailed model specifying and costing the least cost maintenance doctrine, amount of automated test equipment, number of men at each level, and related variables for any level of M on a system-by-system basis. Another approach is to use state-of-the-art, military requirements and historical cost data on particular system types and their availability to establish availability requirements and targets. Reliability and maintainability are next "allocated" at system, subsystem, and component levels based on state-of-the-art, cost, and next level R and M requirements. Tradeoffs are next used to make lower level decisions and to reallocate based on excursions from baseline designs. For example, if we allocate availability to R and M portions, and discover that the cost of increased R compared with that allocated is less than that of increased M, we would design in the direction of more R and less M, achieving a lower cost design for the specified availability. This "marginal tradeoff" method is discussed in the next section.

Costing system availability is particularly important under constrained budgets. If the budget constraints are sufficiently low, we may not be able to achieve a desired level of availability. The lower availability can only be caused by reduced reliability or maintainability. Otherwise, we must sacrifice some performance parameter target(s) to "pay for" the required availability. Reduced reliability may be due to less costly components or reduced redundancy, for example. Reduced maintainability may be due to reduced test equipment and automatic checking, reduced maintenance manpower, or reduced sparing and other logistic support, for example. In sacrificing performance parameters we are likely to be tempted to give up an increment of performance having the highest marginal cost per unit of utility. This often results in small reductions of the most essential military factor.

10.10.3.1 THE GEOMETRY OF SYSTEM R&M TRADEOFFS

Let us examine the effect on availability of different amounts of reliability and maintainability and determine the least-cost combination of reliability R (obtained through equipment design) and maintainability M (obtained through test equipment, repair system, and sparing doctrine) which will produce a specified (mission-required) availability A. Since A_i = MTBF/(MTBF + MTTR), a three-dimensional graph or "response surface" will show the relationship among R, M, and A. Note that MTBF is a measure of R, but MTTR is a measure of 1/M. We can show such a response surface, as in Figure 10.10.3.1-1. A1 through A4 are increasing levels of availability; ⌐ny particular availability, for example, A1, may be obtained from many different combinations of R and M. Figure 10.10.3.1-2 shows a two-dimensional projection of such a surface; for the rest of this section we will use such projections as representatives of the response surface. Such projections may be thought of as contour lines on a map, just as we represent topographical features on a two-dimensional map. They are called "iso-availability" (constant availability) contours or "isoquants" for short. The isoquants shown represent availability, increasing from A1 to A4. They say nothing about cost. Along any isoquant, many different costs are represented. The surface and its isoquants are convex to the original, showing decreasing marginal (incremental) returns (benefits). As reliability and maintainability are successively increased by a fixed increment, availability is increased by a decreasing increment. We can quickly see this from the formula A_i = MTBF/(MTBF + MTTR). (Try assuming values for either MTBF or MTTR, holding the other constant. Also, calculate the partial derivative of A with respect to either). The individual isoquants approach asymptotes to either axis because larger and larger amounts of R or M are required to produce a fixed A as M or R becomes small.

R and M are "competitive substitutes" for each other, and the rate of such competitive substitution diminishes as we move along any isoquant. Again, reference to the formula shows the substitution effect. For a target availability A and the resultant constant K, if we take partial derivatives in Eq. (10.143), remembering that MTTR is proportional to 1/M, we obtain:

$$\frac{MTTR}{MTBF} = \left(\frac{1 - A}{A}\right)$$

$$\frac{1}{MR} = \left(\frac{1 - A}{A}\right)$$

$$M = \left(\frac{A}{1 - A}\right)\frac{1}{R}$$

$$\frac{\partial M}{\partial R} = \left(\frac{A}{1 - A}\right)\left(\frac{-1}{R^2}\right)$$

(10.144)

$$A = \frac{R}{R + \frac{1}{M}}$$

(R = MTBF, M=1/MTTR)
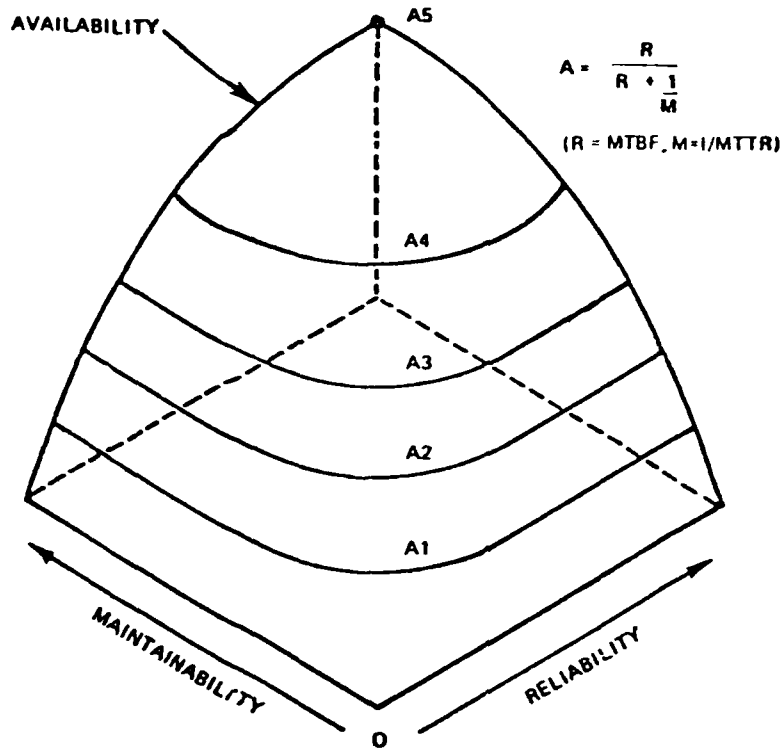
FIGURE 10.10.3.1-1: HYPOTHETICAL AVAILABILITY SURFACE
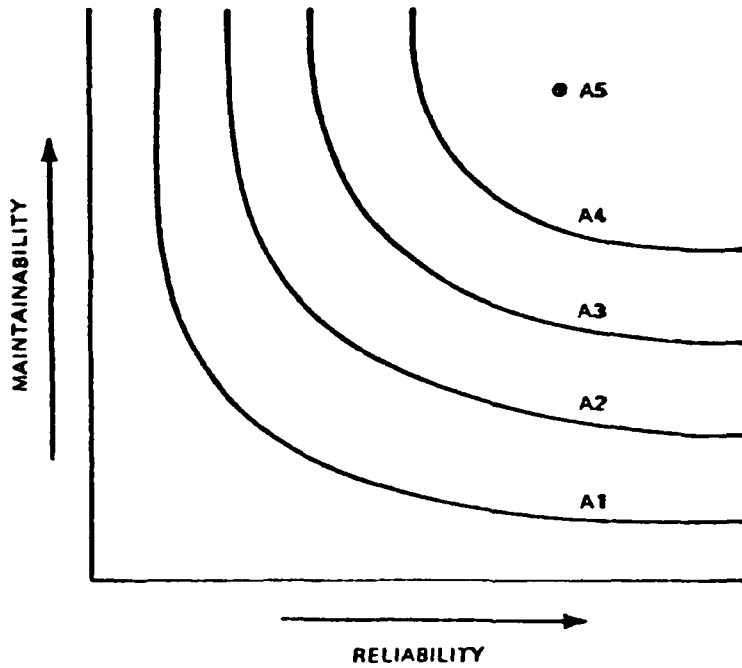
FIGURE 10.10.3.1-2: TWO-DIMENSIONAL PROJECTION OF AVAILABILITY SURFACE

Thus, at any availability, as R increases M decreases proportionately with R^2. At very large R, the slope of an isoquant is almost zero, while at very small R, the slope is almost infinite (the isoquant becomes parallel to either axis as one goes out far enough). Note, finally, that the response surface approaches a point, A5. At some level of availability we have approached the "state-of-the-art" limit: no higher value of R or (perhaps) M is possible and a single combination of R and M is the only way to achieve such a high A. The isoquant has become a single point.

Figure 10.10.3.1-3 shows a series of "budget" or "isocost" curves. Any curve represents combinations of R and M that can be purchased for a particular budget. Budgets increase from B0 to B4. The curves intersect the axes at a point where all of a particular budget is spent on R or on M with nothing spent on the other. The isocost curves say nothing about availability; many different values of availability will likely occur along a particular isocost curve. The isocost curves are somewhat concave to the origin, showing increasing marginal costs. The last increment of R or M is usually much more costly than earlier increments. Thus, as we reduce the amount of R slightly, we can "buy" substantial M and vice versa. This effect, diminishing returns to scale, is a well known economic phenomenon at high levels of output for many kinds of processes. In this case, the highest increments of reliability or maintainability require special, costly techniques (gold plating or redundancy, for example).

Note that in Figure 10.10.3.1-3 any point (say, C) on an isocost curve represents the quantity (qM, qR) of M and R that can be purchased for the fixed budget (B1, in this case). The unit cost or price of M when all resources are spent on M is thus B1/qM (where qM1 is the point of intersection of B1 with the y-axis; the price of R is B1/qR1).

Figure 10.10.3.1-4 combines the isoquants of Figure 10.10.3.1-3 with the isocost curves of Figure 10.10.3.1-2. Let us plot the lowest B-curve just tangent to each A-curve and denote the pair by the same number (A1, B1 or A2, B2 or A3, B3, etc.). The points of tangency, P1 through P4, are the least cost combinations of R and M that will achieve each level of availability. Consider (A1, B1). If B1 were any closer to the origin (any lower budget), it would not be tangent to A1. We would not buy availability A1 for such a lower budget. Conversely, if B1 were further from the origin than shown, it would overlap A1 in several places; we would, however, be spending more than necessary to achieve availability A1. Thus, B1 is the least cost to achieve A1; the tangent point P1 shows the combination M1 and P1 of M and R that will achieve that availability A1.

P2, P3 and P4 are the optimal combination points for R and M to achieve availability A2, A3, and A4 at least cost. The curve connecting P1 through P4, curve QQ', is the "expansion path" and shows the increases in R and M that must be obtained to increase A at least cost in every case. This is the economic mechanism behind the tradeoff between R and M to achieve A.
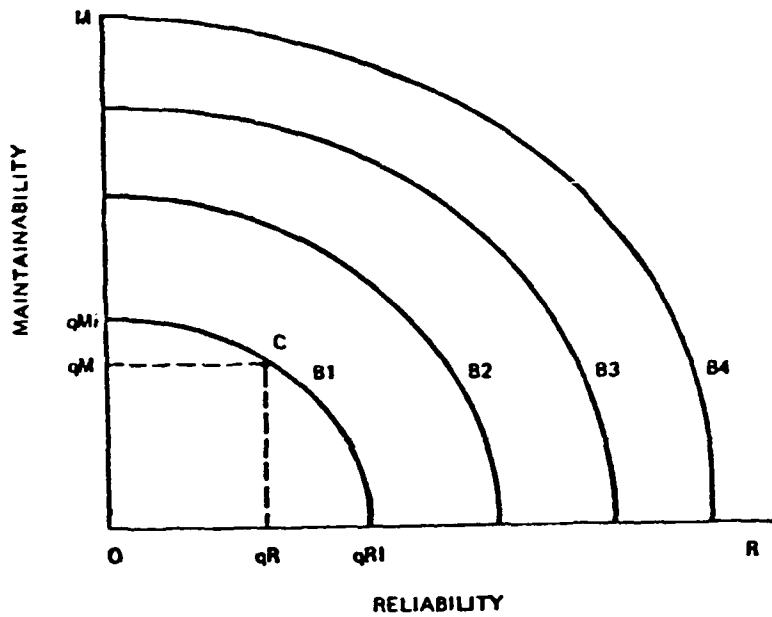
FIGURE 10.10.3.1-3: HYPOTHETICAL BUDGET CURVES
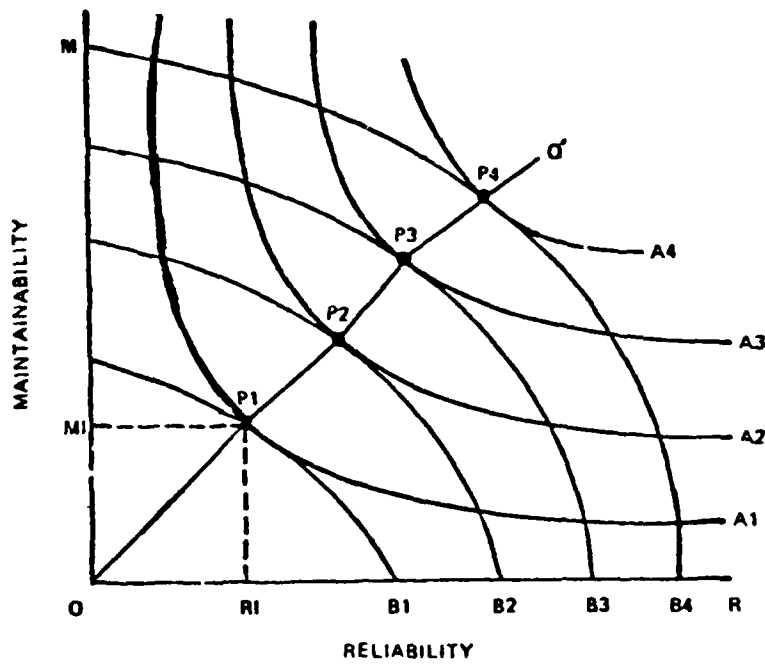
FIGURE 10.10.3.1-4: OPTIMAL COMBINATIONS OF M AND R

Note that at any tangent point (and only at such a point) the slope of both curves must be equal. Thus, for a given availability curve, at the optimum the slope R/M must equal C_M/C_R the slope of the budget curve. (The marginal rate of substitution of R for M must equal the inverse cost ratio.)

How should we search for an optimum (tangent) point? One way is to exploit the behavior of the availability isoquant. Figure 10.10.3.1-5 reviews the cost behavior along such as isoquant. Beginning at a high M, low R combination yielding target availability A1, we move toward the low M, high R end of the same isoquant. As we do so, we pass through isocost curves representing decreasing cost from C5 through C1 (the optimum) and then through curves of increasing cost C2 through C5. Suppose we select a random point (design) on A1. By examining the cost of that design and the cost of a more reliable, less maintainable design, we can tell whether we are moving away from the optimum point or toward it. If the costs increase, we are moving away from the optimum and we would reverse our strategy by reducing R and increasing M to decrease costs. If, at some point, this strategy caused costs to increase, we will have passed through the optimum and must backtrack. On the other hand, if the trial design produced a lower cost for more R and less M, we would be above and to the left of the optimum and would continue to increase R and reduce M. Figure 10.10.3.1-6 shows this effect and the familiar U-shaped cost curve that results.

This discussion centers at achieving a fixed availability at minimum cost. The problem of maximizing availability at a fixed cost is solved in similar fashion. A fixed isocost curve is chosen, and the availability curve just tangent is found. Any higher availability curve will not intersect the isocost curve at any point; the higher availability cannot be bought for the specified budget. Any lower availability curve than the tangent curve would represent less than maximum availability for the specified budget. Note, then, that the solution to the problem of maximizing benefits (effectiveness) for a fixed cost and the solution to the problem of minimizing cost for a fixed benefit are formally identical. In theory, we may start with either and should find the same solution.

10.10.3.1.1 GENERAL R&M TRADEOFF METHODOLOGY

In the previous subsection, we have seen the basic economic mechanism, presented in continuous form, for development of a tradeoff model for comparing elements of cost to produce effectiveness. R and M were the cost elements; A was a measure of effectiveness. In practical cases, the illustrative framework can be applied directly. In order to find an optimal point, we need a mathematical expression (or a table of values in the range of interest) for the cost of any combination of R and M producing, say, a target availability. As we move along the target availability curve (as we examine different combinations of R and M producing the desired A), we cost each combination, searching for the minimum cost solution (the tangent point). We use one of a variety of search techniques. These techniques range from searching all
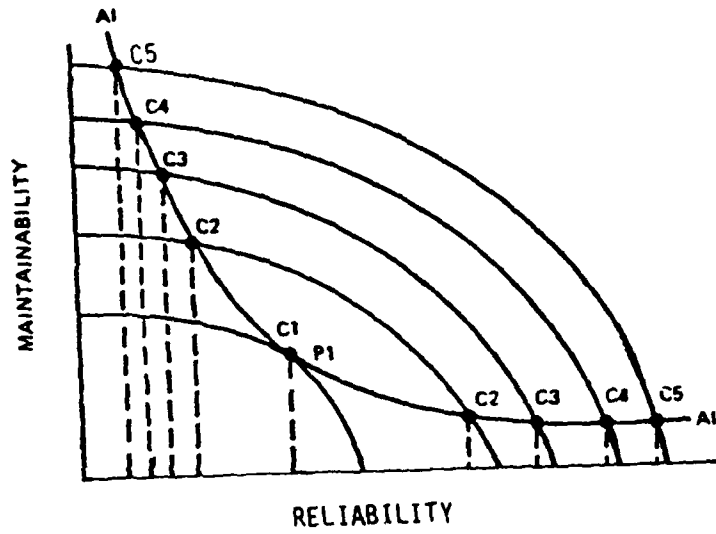
FIGURE 10.10.3.1-5: COST ALONG AVAILABILITY ISOQUANT
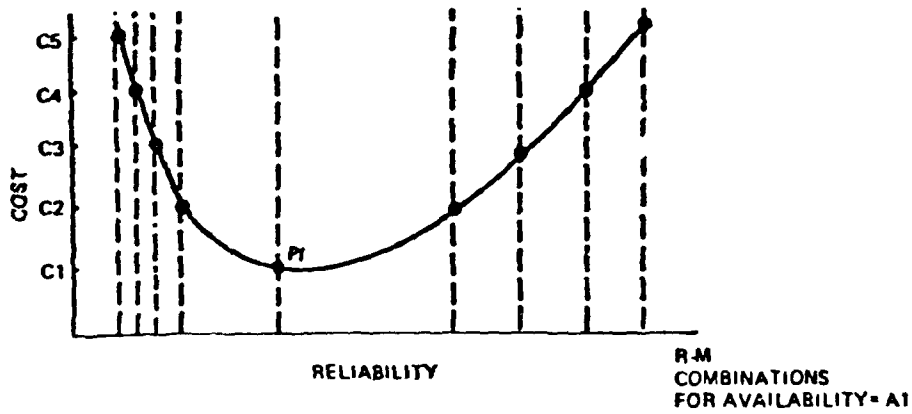
FIGURE 10.10.3.1-6: COST-CURVE FOR FIGURE 10.10.3.1-5

possibilities in the (usually narrow) range of interest defined by the military problem to selection of a single, feasible, conbination of R and M which achieves the desired A and then making excursions from that point on the A curve through system design modifications that reduce total cost until no further benefits (at least commensurate with the cost of continued analysis and design) can be found. The general procedure utilized is as follows:

(1) Pick a reasonable value of R and M which meets required A. Call this set of values RM1.

(2) Find the least cost system which provides that value of R and of M. Call this C1.

(3) Pick a nearby set of values RM2 such that R2 exceeds R1 and M2 is less than M1.

(4) Find the least cost system having RM2. Call it C2.

(5) If C2 is less than C1, continue increasing R and decreasing M, finding the least cost system in each case, as long as this cost continues to decrease.

(6) Otherwise, decrease R and increase M, searching in that direction as long as each least cost system costs less than the previous ones.

(7) If the costs as a result of (5) or (6) start to increase once more, the least cost point has been passed and the search should be reversed, using a smaller increment for R and M1.

(8) Continue the process until a minimum cost system is found or the cost of the search starts to exceed the decreases in cost obtained.

The last two subsections described the theory and general methodology for performing reliability/maintainability/availability/cost tradeoffs. Reference 49 provides a more detailed analysis of these procedures. The R&M tradeoff algorithms have been incorporated into computerized LCC models to be discussed in the next section.

10.10.4 LCC REVISITED

In Section 10.10.1 we discussed LCC concepts; in Section 10.10.2 we discussed LCC models, LCC Breakdown Structures, and CERs; in Section 10.10.3 we discussed methods for costing system availability and R/M/cost tradeoff methodology. This all leads to the conclusion of the process which is to combine the previous information presented to develop the LCC of the selected system.

If we have done the previous work properly, the system life cycle costs for development, ownership and operation will reflect those for a least life cycle cost system within performance and mission envelopes or, if the design task is so specified, the most cost effective system. In performing this "final" life cycle costing we must carefully apply the

same rules applied to the earlier tradeoffs, so that the system we cost is assumed to be in the environment we designed it for. Without such an intimate connection between tradeoff ground rules and final life cycle rules, we might design a system using one set of criteria and evaluate it using contradictory ones. Particularly in a competitive design environment, such consistency is not only desirable but required.

Life cycle costing may also be used to compare or evaluate systems, however designed, for procurement purposes. Components and items may not be subjected to formal design tradeoffs but may be "off-the-shelf." LCC comparison can be used to identify a preferred system after required effectiveness has been assured. Alternatively, in cost-effectiveness comparisons LCC should be used as the relevant cost measure.

When performing LCC analysis at the end of a design process or for comparison of existing hardware, engineering cost estimates are used to estimate many element costs which during design were statistically costed or costed using aggregated techniques. Final LCC analysis considers designed systems: hardware and policies have been determined, and maintenance doctrine is specified in detail, supported by maintenance engineering analysis or prior policy. Logistic doctrine has been established: support by ILS, sparing and provisioning policy, and a logistic system. A complete presentation of life cycle costs for each alternative (in a competitive environment) or for the selected system results. If the final LCC estimates are to be used for selection, they must be carefully validated by examination of analyses, assumptions, and data used to derive them. Otherwise, there is the danger of "competition by assertion." (In a competition a common basis for costing of Government controlled variables must be provided to competitors or specified in a uniform way after competition related LCC analysis is complete. When differing designs incur different Government related costs, these consequences must be made clear to designers in advance.)

Once a single validated set of LCC estimates has been derived for a system, it may be made the basis for incentives and penalties and also used to monitor "returned" (experienced) costs of the system as its life cycle proceeds.

Various cost models, relationships, and specific computer programs have been developed which can be used to estimate acquisition cost, logistic support cost, and LCC and to determine spare requirements and AGE needs; they can also be used as early design tools to perform tradeoff studies among system R&M parameters (see Table 10.10.4-1 for a partial listing). Through application of these models and the associated CERs it is possible to explore various alternative system designs from an R&M viewpoint. They provide the capability to insert into the basic formulas significant R&M design and logistic support approaches. LCC computer printouts can be obtained that directly show the lowest cost approach. Factors can be further refined and adjusted to show the sensitivity of costs to system parameter (e.g., R&M) variations, thereby providing quantitative data for optimum system design and specification as well as to guide the overall development process.

TABLE 10.10.4-1: COMPUTERIZED MODELS IN CURRENT USE

Model Name	Acronym
Acquisition Based on Consideration of Logistic Effects	ABLE
Analysis Method for System Evaluation and Control	AMSEC
Aircraft Reliability/Maintainability/Availability Design Analysis	ARMADA
Base Depot Stockage Model	BDSM
Base Operations Maintenance Simulation	BOMS
Cargo Airline Evaluation Model	CAEM
Computer Analysis of Maintenance Policies	COAMP
Computerized Reliability Optimization System	CROS
Cost Effectiveness/Life-Cycle Cost Analysis	CELCCA
Determining Economic Quantities of Maintenance Resources	DEQMAR
Forecasts and Appraisals for Management Evaluation	FAME
Generalized Effectiveness Methodology	GEM
Generalized Electronics Maintenance Model	GEMM
Ground Operations Support Simulation	GOSS
Inventory Policy Model	IMP
Life Cycle Cost Model	LCCM
Life Cycle Computer Program	LCCP
Logistics Composite Model	LCOM
Logistic Cost	LOGCOST
Level of Repair - Aeronautical Material	LORAM
Maintenance Assembly and Checkout Model	MACOM
Material Readiness Index System	MARIS
Military/Commercial Transport Aircraft Simulation	MCTAS
Multi-Echelon Markov Model	MEMM
Multi-Echelon Technique for Recoverable Item Control	METRIC
Multi-Indenture MORS Evaluator	MIME
Maintainability/Reliability Simulation Model	MRSM
Optimum Life Cycle Costing	OLCC
Operations, Maintenance, and Logistics Resources Simulation	OMLRS
Optimum Repair Level Analysis	ORLA
Planned Logistics Analysis and Evaluation Technique	PLANET
Project Modeling	PROJMOD
Quantification of Uncertainty in Estimating Support Tradeoffs	QUEST
Resource Allocation Model	RAM
Range Model	RGM
Reliability Maintainability Tradeoff	RMT
Support Availability Multi-System Operations Model	SAMSOM
System Support Cost Analysis Model	SCAM
Support Concept Economic Evaluation Technique	SCEET
Space Craft Operational Performance Evaluation	SCOPE
System Cost and Operational Resource Evaluation	SCORE
Support Effectiveness Evaluation Procedure	SEEP
Single Echelon Multi-Base Resources Allocation Technique	SEMBRAT
Spares Kit Evaluator Model	SEEM
Sortie Generation Model	SOGEM
Spares Requirements and Evaluation Model	SPAREM
Scheduling Program for Allocating Resources to Alternative Networks	SPARTAN
Spares Provisioning Model	SPM
Subsystem Simulation Model	SSM
Throwaway/Repair Implications on Maintenance Cost	TRIM
Validated Aircraft Logistics Utilization Evaluation	VALUE

The following paragraphs provide brief descriptions of some computerized cost models not included in Table 10.10.4-1:

Reliability and Cost Model; TACOM TR-12365

The failure distribution curve for each component of a system is estimated or determined from test data. The curves are stored in the computer and the computer assembles the system by randomly selecting components from their respective distribution curves. The cost of each component, the time to replace it, and the cost to replace it are also stored in the computer.

The computer "runs" the system for its life cycle and logs each failure and cost and time to replace each component.

The program allows the user to incrementally increase the reliability of a component to determine the effect on system reliability and the decrease in life cycle cost.

The Program is in FORTRAN and is documented in TACOM Technical Report Number 12365.

        Contact: TACOM
                    Warren, MI   48090

Cost Optimizing System to Evaluate Reliability (COSTER)

It is less expensive to improve reliability in an equipment's development phase than during subsequent phases of the life cycle. The cost incurred to achieve a particular level of reliability must be compared to the cost saved after the equipment is deployed. There would be the savings from the decreased number of failures experienced in field deployment because of improved reliability.

In order to quantitatively analyze the cost trade-off in achieving a particular level of reliability, a computerized cost model (COSTER) was developed. The model elaborates on the cost and reliability improvements resulting from six major reliability processes prior to an equipment's field deployment which consist of:

    (1) design review
    (2) reliability prediction program
    (3) failure mode, effects, and criticality analysis (FMECA)
    (4) parts program, in which MIL-STD and high reliability parts are
         selected in place of commercially available parts
    (5) reliability testing programs
    (6) burn-in

COSTER is not a Life-Cycle-Cost Model but is used as a comparative analysis tool for selecting the best reliability program plan and the optimal value of MTBF for the reliability specification.

        Contact: CORADCOM DRDCO-PT-P
                    Fort Monmouth, NJ   07703

Operating and Support Cost Model

The PERSHING Project Office has developed an Operating and Support Cost Model to provide the capability to determine the effects of operating and support costs during the early design phase of weapon system changes. The model provides single day turnaround for cost effects with attendant traceability as the basis for any cost changes. The most unusual feature of the model is its ability to synthesize tactical operational testing and evaluation (OT&E) that results from design of the mission essential equipment. In addition, the maintenance portion of the OT&E is constructed on the basis of annual maintenance manhour requirements and reliability and maintainability data.

        Contact: MICOM-DRCPM-PE-S
                    Redstone Arsenal, AL 35809

The Avionics Laboratory Predictive Operations and Support (ALPOS) Cost Model

Recent DoD experience shows that a prime factor in the evaluation of alternative weapon systems for performing a particular mission is Life Cycle Cost (LCC). Since 70% of the system LCC is determined by the end of the conceptual phase, it is important that techniques to predict LCC be available during this phase. Since system definition is not complete enough in this phase to perform detailed analysis using accounting models, the major tool which can be used is parametric estimating models. The study report describes a model which relates the available design parameters to LCC via various cost estimating relationships (CERs). The Final Report describes the mathematical and statistical techniques used to obtain the cost estimating needed to develop the Avionic Laboratory Predictive Operations and Support (ALPOS) Cost Model.

The ALPOS model is used for estimated downstream operations and support costs based upon design parameters available during conceptual or preliminary design phases.

        Contact: AFWAL/AFAL/XRP
                    Wright Patterson AFB, OH 45433

STEP (Standardization Evaluation Program)

Assesses the cost impact of avionics standardization across weapon systems.

        Contact: AFWAL/AFAL/XRP
                    Wright Patterson AFB, OH 45433

SAVE (Systems Avionics Value Estimation) Model for Logistic Support Costs

It greatly facilitates tradeoff studies of different hardware designs or sensitivity analysis. An interactive graphics package permits visual display of pie charts or coordinate plots of the output. Among the

items covered by the present models are hardware costs, spares costs personnel costs, and support equipment costs for based, intermediate, and depot level management.

Computer Model for Analysis of Army Aircraft RAM Improvement Proposals

A computer model has been developed for preparing cost tradeoff studies of RAM (Reliability/Availability/Maintainability) efforts. The model is specifically directed to RAM efforts involving Army aircraft. It determines the total life cycle effect of RAM effort utilizing various RAM parameters. It is a modification of an economic analysis model and is a preliminary effort to combine the methods of cost analysis and product assurance.

      Contact: AVRADCOM-DRDAV-BCA
                     St. Louis, MO 63166

Logistics Cost Analysis Model 5

Logistics Cost Analysis Model 5 is an upgraded model of maintenance policies utilized by the U.S. Army Missile Command and the U.S. Army Weapons Command. Model progression included Missile Command, Weapons Command cost analysis of maintenance policies, and Logistics Cost Analysis Models 2, 3 and 4. It is an analytical computer program capable of representing field logistic support functions and flow. It computes life cycle costs and operational availability for alternate system support concepts. Output includes provisioning requirements and operational elements both by numbers and cost. Variable dimensions are limited only by the computer. Parameters include extensive specification of factors for deployment, equipment, supply maintenance, and test equipment. Sensitivity to all input factors is possible.

      Contact: MICOM
                     Redstone Arsenal, AL 35809

Analytic Methodology for System Evaluation and Control (AMSEC)

AMSEC is a technique developed by the Army for use in support of management planning of major programs. AMSEC comprises three basic components:

(1)   A reliability, maintainability, availability, and life cycle support cost (RMAC) model which develops estimates of system or subsystem reliability, availability, and cost from real or postulated data describing the system design, the support parameters, and the plan for use.

(2)   A field data transducer routine which accepts data routinely generated by the Army and converts it to RMAC model input parameters.

(3)   An executive routine which directs the RMAC model in a systematic search for optimal management actions.

AMSEC can provide a rapid assessment of vehicle and subsystem reliability, availability, and life cycle support cost under the present framework of design, support, and use parameters; it can search out improved maintenance plans or search through alternative product improvement programs to select a preferred course of action; it can determine the preferred times for rebuilding major components of the vehicle or for buying new, provide estimates of optimal sparing levels for components, and recommend cost effective routes by which to adapt to changing needs imposed by a shift from peacetime to wartime operations.

      Contact: AVRADCOM-DRDAV-QR
                    St. Louis, MO 63166

An Appraisal of Models Used in Life-Cycle-Cost Estimation for USAF Aircraft Systems; AD-A064333

Although life cycle analysis is widely used as a management tool, considerable uncertainty still exists about its effectiveness with respect to economic tradeoffs, funding decisions, and resource allocations. This report (AD Number A064333) evaluates some of the most widely used life-cycle-cost (LCC) models, AFR 173-10 models (BACE and CACE), the Logistics Support Cost model, the Logistics Composite model, the MOD-METRIC model, AFM 26-3 Manpower Standards, Air Force Logistics Command Depot Maintenance Cost Equations, the DAPCA model, and the PRICE model. The models are rated within a framework incorporating a set of life-cycle-cost elements and a set of cost driving factors. Color coded illustrations summarize the results. The models are shown to have many shortcomings that limit their usefulness for life cycle analyses in which estimates of absolute, incremental cost are required. Specific areas are identified where driving factor/cost element combinations are not adequately addressed.

Although this is not a model in itself, it represents a valuable source of information for model evaluation.

      Contact: AFWAL/AFAL/XRP
                    Wright Patterson AFB, OH 45433

Another source of information on LCC models is the Cost Analysis of Software and Hardware (CASH) Center, which was established by the Air Force in 1974 as a center of expertise and collection point for LCC models, literature, and data bases. The CASH Center developed the Avionics Evaluation Program (AEP), a library of avionics performance assessment models for doing detailed tradeoff analysis of cost, reliability, maintainability, and performance of system configurations. The CASH center has supported requests for assistance from other DoD agencies. Contact is AFWAL/AFAL/XRP, Wright Patterson AFB, OH 45433.

In addition to the above, further details on available computerized LCC models can be found in the cited references (e.g., Refs. 24, 29 through 42, 49). The important point to be made is that there are a host of computerized cost models available which can be used to meet most system R&M design applications.

REFERENCES

1. Von Alven, W.H., Ed., Reliability Engineering, Prentice-Hall, Inc. Englewood Cliffs, NJ, 1964.

2. AFSC-TR-65-6, Chairman's Final Report, Weapon System Effectiveness Industry Advisory Committee (WSEIAC), Air Force Systems Command, January 1965, (AD-467816), also

    AFSC TR-65-1   Final Report of Task Group I, Requirements Methodology
    AFSC TR-65-2   Final Report of Task Group II, Prediction Measurement (Concepts, Task Analysis, Principles of Model Construction)
    AFSC TR-65-3   Final Report of Task Group III, Data Collection and Management Reports
    AFSC TR-65-4   Final Report of Task Group IV, Cost Effectiveness Optimization
    AFSC TR-65-5   Final Report of Task Group V, Management Systems

3. Elements of Reliability and Maintainability, DoD Joint Course Book, U.S. Army Management Engineering Training Agency, Rock Island, IL, 1967.

4. Systems Effectiveness, System Effectiveness Branch, Office of Naval Material, Washington, DC, 1965, (AD-659520).

5. NAVMAT P3941, Navy Systems Performance Effectiveness Manual, Headquarters Naval Material Command, Washington, DC, 1 July 1960.

6. DOD Directive 5000.40, "Reliability and Maintainability," July 8, 1980.

7. Blanchard, B.S., "Cost Effectiveness, System Effectiveness, Integrated Logistic Support, and Maintainability," IEEE Transactions in Reliability, R-16, No. 3, December 1967.

8. Barlow, R.E., and F. Proschan, Mathematical Theory of Reliability, John Wiley & Sons, Inc., NY, 1965.

9. Kozlov, B.A., and I.A. Ushakov, Reliability Handbook, Holt, Rinehart and Winston, Inc., NY, 1970.

10. Myers, R.H., K.L. Wong and H.M. Gordy, Reliability Engineering for Electronic Systems, John Wiley and Sons, Inc., NY, 1964.

11. Mathematical Models for the Availability of Machine Gun Systems, Technical Report No. 3, prepared by Igor Bazovzky and Associates, Inc., for the Small Arms System Laboratory, U.S. Army Weapons Command, February 1970.

12. PAM 69-8, Availability, U.S. Army Combat Development Command Maintenance Agency, Aberdeen Proving Ground, MD, November 1970.

13. NAVSHIPS 94324, Maintainability Design Criteria Handbook for Designers of Shipboard Electronic Equipment, Department of the Navy, Change 2, 1965.

14. Orbach, S., The Generalized Effectiveness Methodology (GEM) Analysis Program, U.S. Naval Applied Science Laboratory, Brooklyn, NY, May 1968.

15. "Evaluation of Computer Programs for System Performance Effectiveness, Volume II," RTI Project SU-285, Research Triangle Institute, Research Triangle Park. North Carolina 27709, August 1967.

16. "Computer Tells Launch Vehicle Readiness," Technology Week, April 1967.

17. Dresner, J., and K.H. Borchers, "Maintenance, Maintainability and System Requirements Engineering," Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference, 1964.

18. Economos, A.M., "A Monte Carlo Simulation for Maintenance and Reliability," Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference, 1964.

19. Faragher, W.E., and H.S. Watson, "Availability Analyses - A Realistic Methodology," Proceedings of the Tenth National Symposium on Reliability and Quality Control, 1964, pp. 365-378.

20. Horrigan, T.J., "Development of Techniques for Prediction of System Effectiveness, RADC-TDR-63-407, Cook Electric Company, February 1964, AD-432844.

21. "Maintairability Trade-Off Techniques," Maintainability Bulletin No. 8, Electronic Industries Association, July 1966.

22. Ruhe, R.K., "Logic Simulation for System Integration and Design Assurance," Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference, 1964.

23. Smith, T.C., "The Support Availability Multi-System Operations Model," Proceedings of the Third Annual Aerospace Reliability and Maintainability Conference, 1964.

24. Survey of Studies and Computer Programming Efforts for Reliability, Maintainability, and System Effectiveness, Report OEM-1, Office of the Director of Defense Research and Engineering, September 1965, AD-622676.

25. Sandler, G.H., System Reliability Engineering, Prentice-Hall, Englewood Cliffs, NJ, 1963.

26. Rise, J.L., "Compliance Test Plans for Availability," <u>Proceedings of the 1979 Annual Reliability and Maintainability Symposium</u>, Washington, DC, January 1979.

27. Arsenault, J.E., and J.A. Roberts, <u>Reliability and Maintainability of Electronic Systems</u>, Computer Science Press, 9125 Fall River Lane, Potomac, MD 20854, 1980.

28. Blanchard, B., <u>Design and Manage to Life Cycle Cost</u>, M/A Press, P.O. Box 92, Forest Grove, OR, 1978.

29. Earles, M., <u>Factors, Formulas, and Structures for Life Cycle Costing</u>, 89 Lee Drive, Concord, MA 01742, 2nd edition, 1981.

30. Department of the Army Pamphlet No. 11-2, "Research and Development Cost Guide for Army Materiel Systems," Department of the Army, Alexandria, VA, May 1976.

31. Department of the Army Pamphlet No. 11-3, "Investment Cost Guide for Army Materiel Systems," Department of the Army, Alexandria, VA, April 1976.

32. Department of the Army Pamphlet No. 11-4, "Operating and Support Cost Guide for Army Materiel Systems," Department of the Army, Alexandria, VA, April 1976.

33. Department of the Army Pamphlet No. 11-5, "Standards for Presentation and Documentation of Life Cycle Cost Estimates for Army Materiel Systems," Department of the Army, Alexandria, VA, May 1976.

34. Naval Material Command, "Life Cycle Cost Guide for Major Weapon Systems," Naval Weapon Engineering Support Activity, Washington, DC, January 1977.

35. Naval Material Command, "Life Cycle Cost Guide for Equipment Analysis," Naval Weapon Engineering Support Activity, Washington, DC, January 1977.

36. Air Force Armament Development Test Center, "Cost Estimating and Analysis, An Introductory Short Course," Department of the Air Force, Eglin AFB, FL, February 1974.

37. Air Force Logistics Command, "Logistic Support Cost Model Users Handbook," Wright Patterson AFB, January 1979.

38. USMC LCCM Manual, "Volume II, Data Collection Workbook," USMC LCC Model Steering Committee, Headquarters, USMC, February 1981.

39. TTO-ORT-032-80-V3, "Cost Effectiveness Program Plan for Joint Tactical Communications, Life Cycle Costing, Vol. III," Joint Tactical Communication Office, Ft. Monmouth, NJ, January 1980.

40. Betaque, N.E., and M.R. Fiorello, "Aircraft System Operating and Support Costs: Guidelines for Analysis," Logistics Management Institute, Defense Documentation Center, March 1977, ADA 039369.

41. Fiorelli, M.R., R.S. Saizer, and J.R. Wilk, "Ship Operating and Support Costs: Guidelines for Analysis," Logistics Management Institute, Defense Documentation Center, May 1977, ADA 040447.

42. Fiorelli, M.R., and L.G. Jones, "Combat Vehicles System Operating and Support Costs: Guidelines for Analysis," Logistics Management Institute, Defense Documentation Center, June 1977, ADA 041508.

43. OSD Cost Analysis Improvement Group Memorandum (M.A. Margolis, Chairman), "Weapon System Operating and Support Cost Element Structures and Definitions," Office of the Secretary of Defense, Washington, DC, August 1977.

44. AF 800-14, "Management of Computer Resources in Systems, Volume III," 26 September 1975.

45. Blanchard, B., "Tutorial Session Lecture Notes," Proceedings of the 1980 Annual Reliability and Maintainability Symposium, San Francisco, CA, January 1980.

46. Fischer, G.H., Cost Consideration in System Analysis, American Elsevier, NYC, NY, 1971.

47. "Cost Analysis of Avionics Equipment, Vol. 1," Air Force Systems Command, Wright Patterson Air Force Base, OH, February 1974, AD 781132.

48. Barish, N.I., Economic Analysis for Engineering and Management Decision Making, McGraw-Hill Book Co., NY, 1962.

49. AMCP-706-133, Engineering Design Handbook, Maintainability Engineering Theory and Practice, Army Material Command, January 1976, AD A026006.

50. NAVAIR 01-1A-33, Maintainability Engineering Handbook, Naval Air Systems Command, July 1977.

11.0 PRODUCTION AND USE (DEPLOYMENT) R&M

11.1 INTRODUCTION

An effective system reliability engineering program begins with the recognition that the achievement of a high level of actual use R&M is a function of design as well as all life cycle activities. Design establishes the inherent R&M potential of a system or equipment item, plus the transition from the paper design to actual hardware, and ultimately to operation, many times resulting in an actual R&M that is far below the inherent level. The degree of degradation from the inherent level is directly related to the inspectability and maintainability features designed and built into the system, as well as the effectiveness of the measures that are applied during production and storage prior to deployment to eliminate potential failures, manufacturing flaws and deterioration factors. Lack of attention to these areas can result in an actual system reliability as low as 10% of its inherent reliability potential.

The impact of production, shipment, storage, operation and maintenance degradation factors on the reliability of a typical system or equipment item and the life cycle growth that can be achieved is conceptually illustrated in Figure 11.1-1. The figure depicts the development of a hardware item as it progresses through its life cycle stages. The figure shows that an upper limit of reliability is established by design, and that, as the item is released to manufacturing, its reliability will be degraded and as production progresses, with resultant process improvements and manufacturing learning factors, reliability will grow. The figure further shows that when the item is released to the field, its reliability will again be degraded. As field operations continue and as operational personnel become more familiar with the equipment and acquire maintenance experience reliability will again grow.

As was discussed in Section 7, reliability design efforts include: selecting, specifying and applying proven high quality, well derated, long life parts; incorporating adequate design margins; using carefully considered, cost effective redundancy; and applying tests designed to identify potential problems. Emphasis is placed on incorporating ease of inspection and maintenance features, including use of easily replaceable and diagnosable modules (or components) with built-in test, on-line monitoring and fault isolation capabilities. During development reliability efforts include the application of systematic and highly disciplined engineering analyses and tests to stimulate reliability growth and to demonstrate the level of reliability that has been achieved and the establishment of an effective, formal program for accurately reporting, analyzing, and correcting failures which would otherwise occur during operation.

Once the inherent or design-in R&M is established, engineering efforts focus on the prevention or reduction of degradation. Well planned and carefully executed inspections, tests, and reliability/quality control methods are applied during production (as well as during storage and operation), to eliminate defects and minimize degradation.
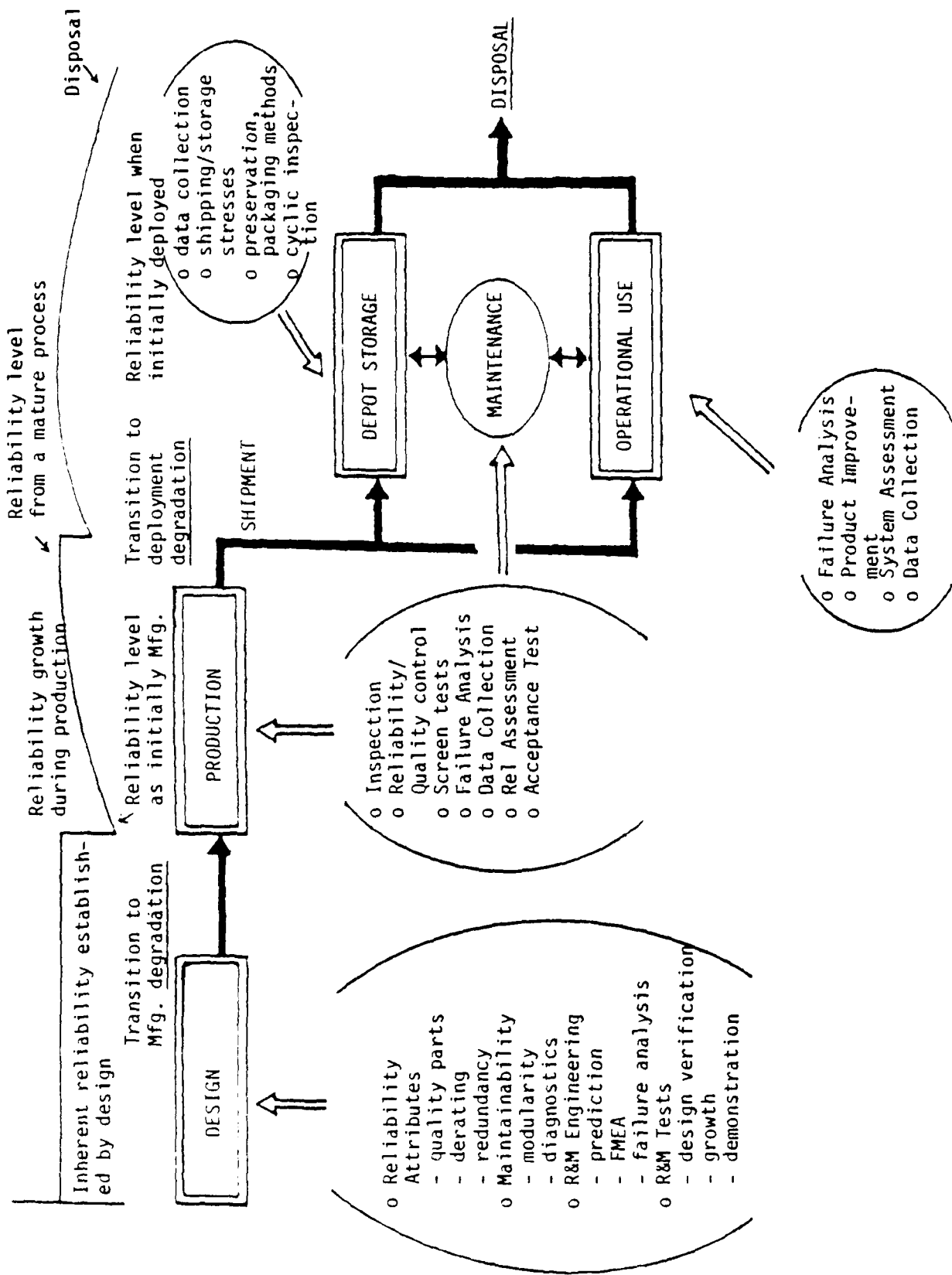
FIGURE 11.1-1: RELIABILITY LIFE CYCLE DEGRADATION & GROWTH CONTROL

Manufacturing, transportation and storage environmental stresses as well as inspection methods and operational/maintenance procedures are continually assessed to determine the need for better inspection, screening, and control provisions to improve R&M.

This section discusses reliability degradation and growth during production and deployment. Basic procedures and guidelines are described that can be used to plan post design reliability control measures, including the assessment and improvement of reliability during production, shipment, storage and use. Also discussed are maintainability control procedures during production and deployment.

11.2 PRODUCTION RELIABILITY CONTROL

The need for a reliability program applicable to production becomes evident when considering that:

(1) manufacturing operations introduce unreliability into hardware that is not ordinarily accounted for by reliability design engineering efforts and,

(2) inspection and test procedures normally interwoven into fabrication processes are imperfect and allow defects to escape which later result in field failure.

Therefore, if the reliability that is designed and developed into an equipment/system is to be achieved, efforts must also be applied during production to insure that reliability is built into the hardware. To realistically assess and fully control reliability, the degradation factors resulting from production must be quantitatively measured and evaluated. This is particularly important for a newly fabricated item, where manufacturing learning is not yet complete and a high initial failure rate can be expected.

Since the effectiveness of inspection and quality control relates directly to reliability achievement, it would be useful to discuss basic quality engineering concepts prior to discussing specific aspects of production reliability degradation and improvement.

11.2.1 QUALITY ENGINEERING (QE) AND QUALITY CONTROL (QC)

The quality of an item is the degree to which it satisfies the user or may be stated as a measure of the degree to which it conforms to specified requirements. It can be expressed in terms of a given set of attributes defined in measurable quantitative terms to meet operational requirements. Quality level is measured by the rate of defectiveness in a given lot or item.

The purpose of a quality control program is to assure that these attributes are defined and maintained throughout the production cycle (and continued during storage and operation). Included as part of the quality control program is the verification and implementation of inspection systems, statistical control methods, and cost control and acceptance criteria. Critical to the quality control function is the establishment of adequate acceptance criteria for individual items to assure appropriate quality protection.

Quality, as with reliability, is a controllable attribute which can be planned during development, measured during production, and sustained during storage and field repair actions. The achievement of acceptable quality for a given item involves numerous engineering and control activities. Figure 11.2.1-1 depicts some of these activities as they apply throughout the system's life cycle phases. These activities represent an approach to a comprehensive and well rounded Quality Control Program.

Keys to assuring the basic quality of a hardware item as depicted in Figure 11.2.1-1 are: the specification of cost effective quality provisions and inspections covering the acquisition of new hardware items; the storage of hardware and material; and the repair, reconditioning or overhaul of deployed items. This means that quality requirements should be included in procurement specifications, in-storage inspection requirements, and in maintenance work requirements, as applicable, and that responsive quality programs are to be planned and implemented to meet these requirements. This section discusses quality control during the acquisition of new systems and hardware items.

The quality requirements applied during acquisition generally follow Military Specification MIL-Q-9858. MIL-Q-9858 is the basic standard for planning quality programs for Department of Defense development and production contracts. It outlines provisions to insure appropriate levels of quality over the production (or depot reconditioning and overhaul) cycle through effective management actions. The essential elements of a hardware quality program as defined in MIL-Q-9858 are given in Table 11.2.1-1.

TABLE 11.2.1-1: MIL-Q-9858 QUALITY PROGRAM ELEMENTS

o   Quality Program Management
Organization
Initial Quality Planning
Work Instructions
Records
Corrective Action
o   Facilities and Standards
Drawings, Documentation and Changes
Measuring and Testing Equipment
Production Tooling Used as Media of Inspection
Use of Contractor's Inspection Equipment
Advanced Metrology Requirements
o   Control of Purchases
Responsibility
Purchasing Data
o   Manufacturing Control
Materials and Material Control
Production Processing and Fabrication
Completed Item Inspection and Testing
Handling, Storage, and Delivery
o   Statistical Quality Control and Analysis
Indication of Inspection Status

TRANSITION PHASE

o Perform tradeoffs-
  cost quality
o Establish Quality
  program reqmts
  i.e. MIL-Q-9858
  MIL-I-45208
o Prepare Quality
  rqmts for procure-
  ment specifications
o Participate in
  source selection

PRODUCTION PHASE

o Plan and implement
  Q.C. System
  -inspection & test
   procedures
  -test data
  -records and
   reports
  -change orders
  -waiver requests
o Prepare Q.C. re-
  quirements
  -product imprmts.
  -value eng. changes
  -engineering
   change orders

STORAGE PHASE

o Prepare & perform
  in-storage accept-
  ance cyclic inspect-
  ion requirements
o Prepare test & in-
  spection procedures
o Review discrepancy
  reports
o Compile reject rate
  data

DEPLOYMENT PHASE

o Structure mainten-
  ance/acceptance re-
  quirements
o Compile reject rate
  data
o Evaluate quality
  aspects of product
  improvements

QUALITY DATA UTILIZATION AND FEEDBACK

o Q.E. GUIDELINES
o DATA CLASSIFICATION

PRODUCTION/DPLOT/
USER DATA

FIGURE 11.2.1-1: QUALITY ENGINEERING AND CONTROL LIFE CYCLE PHASES

Where requirements are less stringent, MIL-I-45208 may be implemented. This specification applies to contracts when technical requirements are such as to require control of quality by in-process as well as final and end-item inspection. MIL-I-45208 establishes general contractor requirements for inspection systems and, as such, provides a basis for the contractor to plan and define the quality provisions particular to a specific item. Of particular importance is the requirement for clear inspection instructions, complete with criteria for acceptance and rejection, and the need for accurate inspection equipment calibrated in accordance with MIL-C-45662. The contractor's inspection system, once fully planned, is then documented with full descriptions of the applicable requirements and is available for review prior to start of fabrication. Table 11.2.1-2 delineates some of the requirements included in MIL-I-45208.

TABLE 11.2.1-2: <u>MIL-I-45208 INSPECTION SYSTEM REQUIREMENTS</u>

o   Overall Contractor Inspection Responsibilities
o   Documentation, Including Inspection Instructions, Records, Corrective Action, Drawings and Changes
o   Measuring and Test Equipment
o   Process Controls
o   Inspection Status
o   Government Furnished Materials
o   Nonconforming Material
o   Qualified Products
o   Sampling Inspection
o   Inspection Provisions
o   Government Inspection at Subcontractor or Vendor Facilities
o   Receiving Inspection
o   Government Evaluation

Although the specific requirements in each new item specification are, of course, peculiar to that item, MIL-Q-9858 and MIL-I-45208 provide a basis for organizing and defining the quality and inspection provisions. The degree of quality control for a given item is determined by considering the benefits derived from and the cost of the provisions. There are numerous examples of the considerations which apply to quality control in the production environment. These include:

(1)   Sampling vs. 100% inspection
(2)   Extent of quality controls during design and manufacturing
(3)   Defect analysis and rework program
(4)   Inspection level and expertise
(5)   Special test and inspection equipment, fixtures, gauges, etc., vs. general purpose equipment
(6)   Prototype tests and inspection vs. full production control
(7)   Quality of purchased material
(8)   Extent of quality control audits and vendor surveillance
(9)   Extent of line certification

One of the basic functions of a manufacturer's quality control organization is to make tradeoff decisions relative to the above areas and to assure that quality is adequately planned and controlled, consistent with specified requirements and the constraints of the particular system.

Accomplishment of the quality control function, like reliability, requires a comprehensive and highly detailed program comprised of effective, systematic, and timely management activities, engineering tasks, and controlled tests. The production and acceptance of high quality hardware items requires definition and implementation of an effective quality management and control program that includes:

(1) Performance of detailed quality analysis, planning and cost tradeoff analyses during hardware development;

(2) Application of systematic and highly disciplined quality control tasks during production whose purpose is to identify and correct problems during production prior to an item's release to storage and field use;

(3) The establishment of a storage/field quality and reliability assurance program. This program provides controls and procedures which allow a smooth transition from production to storage and field use without degrading the reliability/quality level. It also emphasizes nondestructive testing at critical stages in the production/storage/depot maintenance process.

Once the quality program has been planned, efforts then focus on the performance of engineering tasks on an ongoing basis to control the quality of the hardware items. Many of the manufacturer's quality engineering and control tasks are outlined in Table 11.2.1-3.

TABLE 11.2.1-3: QUALITY ENGINEERING & CONTROL TASKS

o Review engineering drawings and specifications, prototype test data, and R&M engineering data to determine impact on item quality.

o Review purchased material from a quality standpoint. This would include:
 	
   o evaluation of purchase requisitions and orders
   o selection and certification of vendors
   o approval of vendor component part/assembly samples
   o review of part/material specifications (in particular critical component identification and control)
   o evaluation of purchased material through inspection planning, incoming inspection, and complete test data documentation control
   o disposition and allocation of inspected material, discrepant material, review board provisions

o Evaluate material item manufacturing through a review of process inspection planning, workmanship and acceptance standards, instructions and procedures, production and QA inspection and testing.

TABLE 11.2.1-3: QUALITY ENGINEERING & CONTROL TASKS (Cont'd)

o   Determine adequacy (accuracy, calibration program, etc.) of inspection tests, production equipment, and instrumentation.

o   Provide engineering direction and guidance for the acceptance inspection and test equipment in support of new item procurement production, reconditioning, and maintenance activities.

o   Exercise control over the acquisition, maintenance, modification, rehabilitation, and stock level requirements of final acceptance inspection and test equipment.

o   Provide product assurance representation to Configuration Control Boards, and serve as the control point for evaluation and initiation of all configuration change proposals.

o   Advise, survey, and provide staff guidance for special materials and processes technology, as applied to quality control systems.

o   Evaluate the adequacy, effect, and overall quality of process techniques, particularly those processes which historically have a significant impact on an item's quality.

o   Evaluate reliability/quality data stemming from production, storage and use to:

    o   identify critical items having high failure rates, poor quality or requiring excessive maintenance
    o   identify significant failure modes, mechanisms, and causes of failure
    o   reduce and classify data and, in particular, define and classify quality defect codes
    o   formulate Q.C. guidelines to support preparation of procurement specifications
    o   prepare failure data and statistical summary reports

o   Identify critical material items where cost effective reliability and quality improvement can be effectively implemented. Candidates for improvement include those items which have poor quality, frequent failure, require extensive maintenance effort, and have excessive support costs.

o   Make general reliability/quality improvement recommendations on selected equipment.

o   Provide product assurance engineering impact evaluations for configuration change, product improvement, and value engineering or cost improvement proposals.

o   Determine the effectiveness of improvements on item reliability/quality.

o   Develop calibration procedures and instructions, maintain and recommend changes to publications, equipment improvement recommendations and new calibration requirements, addressing calibration parameters.

An integral part of an effective quality control program is to make available to its engineers documented instructions, procedures and/or guidance which fully describe the functions and tasks required to achieve its objective. Data collected during early production and testing activities, as well as historical data on similar systems from depot storage, maintenance actions, and field operations, can be compiled, reduced and applied to improve the production quality engineering and control activities. This data, for example, can be used to:

(1) Track quality

(2) Compare the benefits of various quality programs and activities:

    o   MIL-Q-9858 provisions
    o   MIL-I-45208 provisions
    o   Production quality control techniques
    o   Vendor control and audits
    o   100% inspection
    o   Sampling (MIL-STD-105) inspection
    o   Special quality assurance procedures

(3) Determine the effectiveness of quality control programs related to:

    o   Materials and materials control
    o   Inspection and testing of piece parts and subassemblies
    o   Production processing fabrication
    o   Completed item inspection and testing
    o   Handling, storage and delivery
    o   Corrective action implementation

(4) Determine the effects of depot storage, operation and maintenance factors:

    o   Depot level inspections
    o   Personnel
    o   Logistics
    o   Operational environment
    o   Mission profile
    o   Maintenance organization
    o   Develop quality classification codes
    o   Formulate quality guidelines to support preparation of procurement specifications, storage inspection requirements and maintenance requirements

11.2.2 PRODUCTION RELIABILITY DEGRADATION ASSESSMENT & CONTROL

As was previously shown, the extent of reliability degradation during production is dependent on the effectiveness of the inspection and quality engineering control program. Reliability analysis methods are applied to measure and evaluate its effectiveness and to determine the need for process improvement or corrective changes. The accomplishment

of the analysis task and, more important, how well subsequent corrective measures are designed and implemented will dictate the rate at which reliability degrades/grows during production. Specifically, reliability degradation is minimized during manufacturing, and reliability grows as a result of improvements or corrective changes that:

(1) Reduce process-induced defects through

o   accelerated manufacturing learning
o   incorporation of improved processes

(2) Increase inspection efficiency through

o   accelerated inspector learning
o   better inspection procedures
o   incorporation of controlled screening and burn-in tests

As process development and test and inspection efforts progress, problem areas become resolved. As corrective actions are instituted, the outgoing reliability approaches the inherent (design based) value.

The approach to assessing and controlling reliability degradation involves quantifying process-induced defects and determining the effectiveness of the inspections and tests to remove the defects, i.e., estimating the number of defects induced during assembly and subtracting the number estimated to be removed by the quality/reliability inspections and tests. This includes estimating defects attributable to purchased components and materials, as well as those due to faulty workmanship during assembly.

Process-induced defects can be brought about by inadequate production learning or motivation and from fatigue. Quality control inspections and tests are performed to "weed out" these defects. No inspection process, however, can remove all defects. A certain number of defects will escape the production process, be accepted, and the item released to storage or field operation.

More important, these quality defects can be overshadowed by an unknown number of latent defects. These latent defects, which ordinarily pass factory quality inspection, are due to flaws, either inherent to the parts or induced during fabrication, that weaken the fabricated hardware such that it will fail later under the proper condition of stress during field operation. Reliability screen tests are designed to apply a stress during manufacturing at a given magnitude over a specified duration to identify these latent defects. As in the case of conventional quality inspections, screen tests designed to remove latent defects are not 100% effective.

It must be emphasized that reliability prediction and analysis methods, as discussed in Sections 6, 7, and 8, are based primarily on system design characteristics and data emphasizing the attribute characteristics of the constituent parts. Resulting estimates generally reflect the reliability potential of a system during its useful life

period, i.e., during the period after early design when quality defects are dominant and prior to the time when wearout becomes dominant. They represent the inherent reliability, or the reliability potential, of the system as defined by its design configuration, stress and derating factors, application environment, and gross manufacturing and quality factors. A design based reliability estimate does not represent the expected early life performance of the system, particularly as it is initially manufactured.

11.2.2.1 FACTORS CONTRIBUTING TO RELIABILITY DEGRADATION DURING PRODUCTION: INFANT MORTALITY

In order to assess the reliability of a system or equipment item during its initial life period (as well as during wearout), it is necessary to evaluate the components of failure that comprise its overall life characteristics curve. In general, the total distribution of failure over the life span of a large population of a hardware item can be separated into quality, reliability, wearout and design failures as shown in Table 11.2.2.1-1. These failure distributions combine to form the infant mortality, useful life, and wearout periods shown in Figure 11.2.2.1-1. It should be noted that design and reliability defects normally would exhibit an initially high but decreasing failure rate and that in an immature design these defects would dominate all other defects.

TABLE 11.2.2.1-1: FOUR TYPES OF FAILURES

QUALITY	Unrelated to stress	Eliminated by inspection
RELIABILTIY	Stress dependent	Minimized by screening
WEAROUT	Time dependent	Eliminated by replacement
DESIGN	May be stress and/or time dependent	Eliminated by proper application, derating, testing and failure data analysis

As was indicated in earlier sections, the general approach to reliability for electronic equipment/systems is to address only the useful life period, where the sum of the distributions of time-to-failure result in a constant failure rate that can be described by the exponential distribution of time-to-failure. Design action is focused on reducing stress related failures and generally includes efforts to select high quality, long life parts that are adequately derated.

For new items, a design-based approach in itself is not adequate to assure reliability. Examination of Figure 11.2.2.1-1 shows that the infant mortality period is comprised of high but rapidly decreasing quality related failure distribution, a relatively high and decreasing latent stress related (reliability) failure distribution, and a low but

PRODUCT LIFE PERIODS
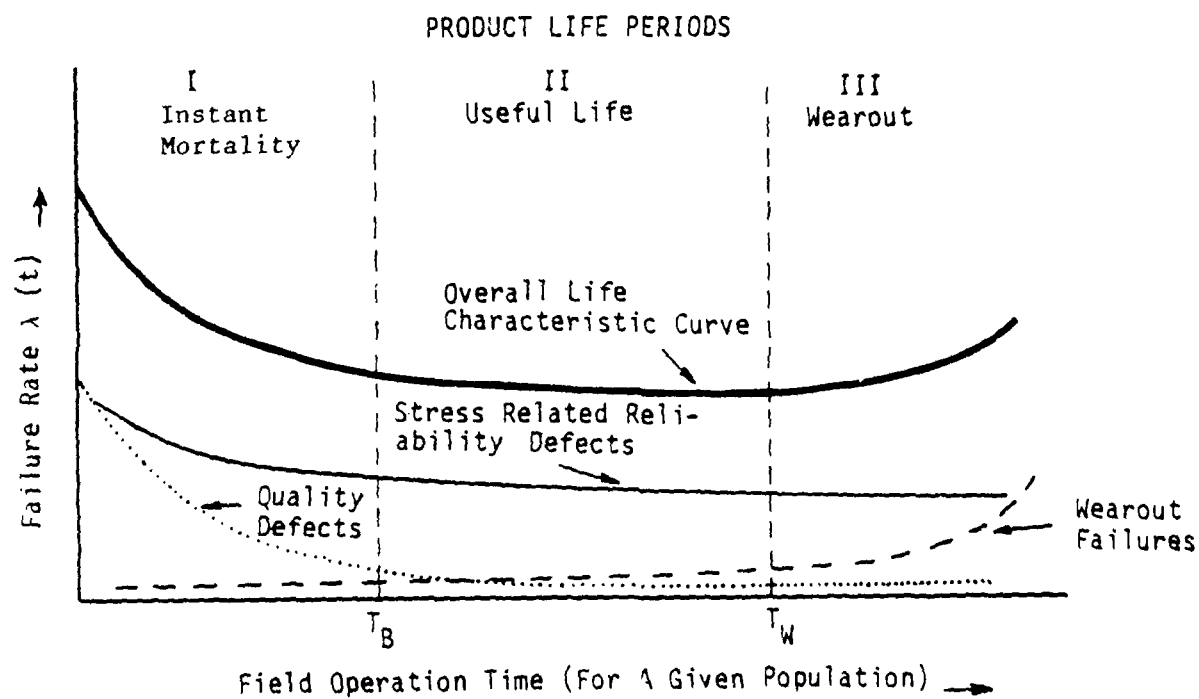
FIGURE 11.2.2.1-1: LIFE CHARACTERISTIC CURVE

slightly increasing wearout related failure distribution. Experience has shown that the infant mortality period can vary from a few hours to well over 1000 hours, although for most well designed, complex equipment it is seldom greater than 100 hours. The duration of this critical phase in reliability growth is dependent on the maturity of the hardware and, if not controlled, would dominate the overall mortality behavior, leaving the item without a significantly high reliability period of useful life. Positive measures must be taken, beginning with design, to achieve a stabilized low level of mortality (failure rate). This includes evaluating the impact of intrinsic part defects and manufacturing process-induced defects, as well as the efficiency of conventional inspections and the strength of reliability screening tests.

The intrinsic defects arise from the basic limitation of the parts that comprise the system or equipment and are a function of the supplier's process maturity, and inspection and test methods. Intrinsic (or inherent) reliability is calculated using design based reliability prediction techniques (e.g., MIL-HDBK-217 methods described in Section 6).

The process-induced defects, as previously discussed, are those which enter or are built into the hardware as a result of faulty workmanship or design, process stresses, handling damage, or test efforts and lead to degradation of the inherent design based reliability. Examples of the types of failures which may occur due to manufacturing deficiencies are poor connections, improper positioning of parts, contamination of surfaces or materials, poor soldering of parts, improper securing of component elements, and bending or deformation of materials.

These defects, as mentioned earlier, whether intrinsic to the parts or introduced during fabrication can be further isolated into quality and reliability defects. Quality defects are not time dependent and are readily removed by conventional quality control measures (i.e., inspections and tests). The more efficient the inspection and test the more defects that are removed. However, since no test or inspection is perfect, some defects will escape to later manufacturing stages and then must be removed at a much higher cost or, more likely, pass through to field use and thus result in lower actual operational reliability with higher maintenance cost.

Stress/time dependent reliability defects cannot generally be detected (and then removed) by conventional QC inspections. These defects can only be detected by the careful and controlled application of stress screen tests. Screen tests consist of a family of techniques in which electrical, thermal, and mechanical stresses are applied to accelerate the occurrence of potential failures. By this means, latent failure producing defects, which are not usually detected during normal quality inspection and testing, are removed from the production stream. Included among these tests are temperature burn-in, temperature cycling, vibration, on/off cycling, power cycling, and various nondestructive tests. Burn-in is a specific subclass of screen which employs stress cycling for a specified period of time. A discussion of screening and burn-in is presented in the next section.

As an example of two types of defects, consider a resistor with the leads bent close to its body. If the stress imposed during bending caused the body to chip, this is a quality defect. However, had the stress been inadequate to chip the body, the defect would go unnoticed by conventional inspection. When the body is cycled through a temperature range, small cracks can develop in the body. This would allow moisture and other gases to contaminate the resistive element, causing resistance changes. This is a reliability defect. Note that this defect can also be a design defect if the design specifications require a right bend to fit the component properly in a board. However, if the improper bend is due to poor workmanship, the defect is classified as a process-induced reliability defect. Consequently, the types of defects to which a system and its subsystems are susceptible are determined by the parts selected and their processing, while the presence of these defects in the finished item is a function of the quality controls, tests and screens that are applied.

Figure 11.2.2.1-2 pictorially shows the reliability impact of the part and process defects. As shown, an upper limit of reliability is established by design based on part derating factors, application environment, quality level, etc. The shaded area indicates that the estimated inherent reliability level may have a relatively broad range depending on the parts that comprise the system and the values for the parameters of the part failure estimating models.

The reliability of initially manufactured units will then be degraded from this upper limit; subsequent improvement and growth is achieved through quality inspections, reliability screening, failure analysis, and corrective action. The extent and rigor with which the tests, failure analysis and corrective actions are performed determine the slope of the reliability improvement curve. As such, process defects, along with the inherent part estimates, must be evaluated in order to accurately estimate reliability, particularly during initial manufacturing.

11.2.2.2 PROCESS RELIABILITY ANALYSIS

The infant mortality period (as was shown in Figure 11.2.2.1-1) is composed of a high but rapidly decreasing quality component, a relatively high and decreasing stress component, and a low but slightly increasing wearout component. Because of this nonconstant failure rate this life period cannot be described simply by the single parameter exponential distribution; computation of reliability during this period is complex. It would require application of the Weibull distribution or some other multiparameter distribution to account for the decreasing failure rate. Controlled life tests would have to be performed or extensive data compiled and statistically evaluated to determine the parameters of the distributions.

A practical approach, however, that would perhaps be useful during preproduction planning or during early production is to compute an average constant failure rate (or MTBF). This average MTBF represents a first approximation of the reliability during this early period. It can be viewed as a form of "step" MTBF, as shown in Figure 11.2.2.2-1 where

Inherent Reliability (R_1)

Includes:

- o Part Derating
  Factors
- o Part Quality
- o Application Factors
- o Operating Environment

Improvement and Growth Brought
About by Screening and Testing

Reliability Level of Initially
Manufactured Items
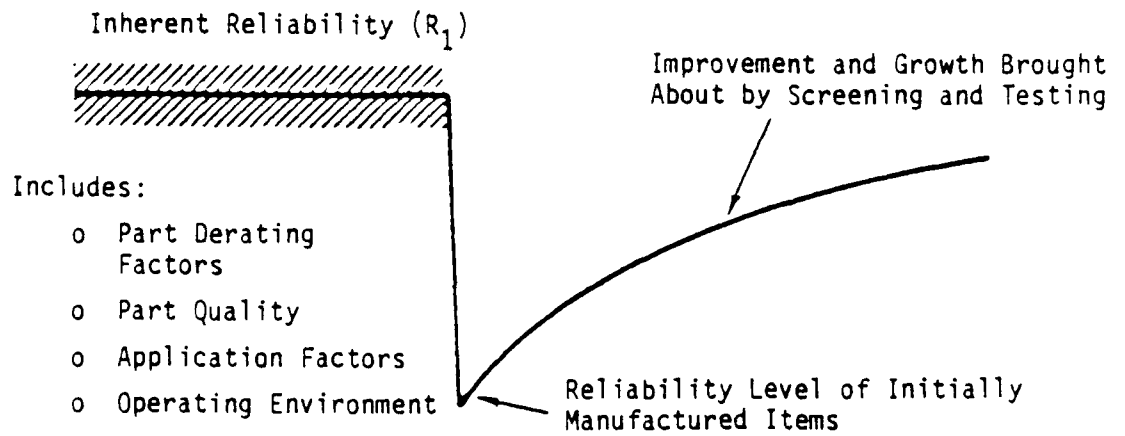
FIGURE 11.2.2.1-2: <u>IMPACT OF DESIGN AND PRODUCTION ACTIVITIES ON EQUIPMENT RELIABILITY</u>

where the "step" MTBF includes both stress and quality failures (defects) at both the part and higher assembly levels, while the inherent MTBF (experienced during the useful life period) includes only stress related failure (defects) at the part level.

A production reliability and inspection analysis can be performed to compute this average "step" MTBF. Such an analysis, in its simplest form, will determine where large degrees of unreliability (defects) are introduced in the manufacturing process and, thus, provides a basis to formulate and implement corrective action in response to the overall improvement process.

This "step" MTBF or outgoing from production MTBF (initial manufacturing) is computed from the following expression:

$$MTBF_a = MTBF_i D_k \qquad (11.1)$$

where

$MTBF_a$ = initial manufacturing MTBF

$MTBF_i$ = the inherent MTBF and is computed from part failure rate models as described in Section 6

D_k = overall degradation factor due to effects of process and inspection efficiency

$$D_k = D_i / D_{out} \qquad (11.2)$$

where

D_i = the inherent defect rate that is computed from $MTBF_i$, i.e,

$$D_i = 1 - e^{t/MTBF_i}$$

and $MTBF_i = 1/\lambda_i$

$\lambda_i = \lambda_{op} d + (1-d) k \lambda_{op}$

λ_{op} = operational failure rate

$\lambda = \lambda_i = 1/MTBF_i$

d = ratio of operational time to total time

k = failure rate reduction factor for nonoperational time

D_o = the outgoing defect rate computed from a detailed reliability process analysis

Figure 11.2.2.2-2 depicts the steps involved in performing a complete reliability analysis leading to an average MTBF ($MTBF_a$) for the early production period of a new hardware item as well as the MTBF ($MTBF_i$) during its useful life period. The analysis involves first evaluating

System Life Periods
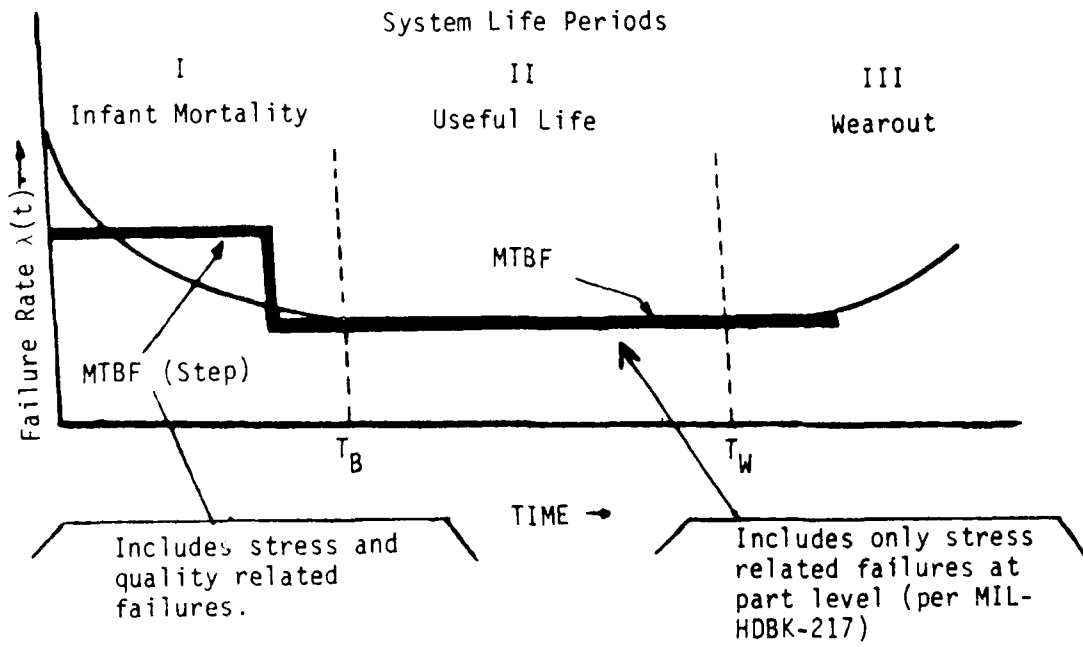
FIGURE 11.2.2.2-1: "Step" MTBF Approximation

Part Failure
Rate Models

Reliability   Part   Part Quality
Block Diagram   Derating   Level
                                    Environmental Factors

STEP 1: Compute Inherent Reliability (MTBF)

Process & Inspection Analysis

STEP 2: Construct Process & Inspection Flow Diagram

STEP 3: Compile and/or Estimate Reject Rate Data

STEP 4: Establish Inspection and Test Efficiency Factors

STEP 5: Compute Outgoing (from Production) Defect Rate, D_{out}

STEP 6: Compute Reliability Degradation, D_k and initial Mfg. MTBF ($MTBF_2$)

FIGURE 11.2.2.2-2: <u>MTBF (OUTGOING FROM PRODUCTION) ESTIMATING PROCESS</u>

the item's design to determine the inherent (design based) $MTBF_i$. Once the design analysis is completed, the process and inspection analysis is performed, as discussed previously, to determine the outgoing (from production) defect rate, D_{out}, and, ultimately, the factor D_k that accounts for degradation in reliability due to initial manufacturing. The output of these two efforts is then combined to yield an MTBF estimate that would account for initial manufacturing induced defects.

The analysis, as depicted in Figure 11.2.2.2-2, involves the following steps:

Step 1 - Compute the reliability of the system or equipment item as it enters the manufacturing process. The initial estimate of reliability is based upon inherent $MTBF_i$ prediction as previously discussed.

Step 2 - Construct a process and inspection flow diagram. The construction of such a flow chart involves first the identification of the various processes, inspection, and tests which take place during manufacturing and second a pictorial presentation describing how each process flows into the next process or inspection point. Figure 11.2.2.2-3 presents a basic and highly simplified process flow diagram to illustrate the technique. Since the analysis may be performed on new equipment prior to production or equipment during production, the process diagram may depict either the planned process or the existing production process.

Step 3 - Establish reject rate data associated with each inspection and test. For analysis performed on planned processes, experience factors are used to estimate the reject rates. The estimated reject rates must take into account historical part/assembly failure modes in light of the characteristics of the test to detect that failure mode. Some of the tests that are used to detect and screen process-induced defects and which aid in this evaluation are discussed in the next section. For analysis performed on existing production processes, actual inspection reject rate data can be collected and utilized.

Step 4 - Establish inspection and test efficiency factors. Efficiency is defined as the ratio of defects removed (or rejects) to the total defects in the fabricated items. Efficiency factors are based on past experience for the same or a similar process, when such data exists. For newly instituted or proposed inspection and screen tests having little or no prior history as to how many defects are found, estimates of inspection and test efficiency must be made. To estimate efficiency, the inspections can be described and characterized relative to such attributes as:

PARTS

Part
Screening → Incoming
Part
Inspection → Assembly → Functional
Test

Screen &
Burn-in Test → Functional
Test → To Final Assembly

(Remove reliability
defects)

- -
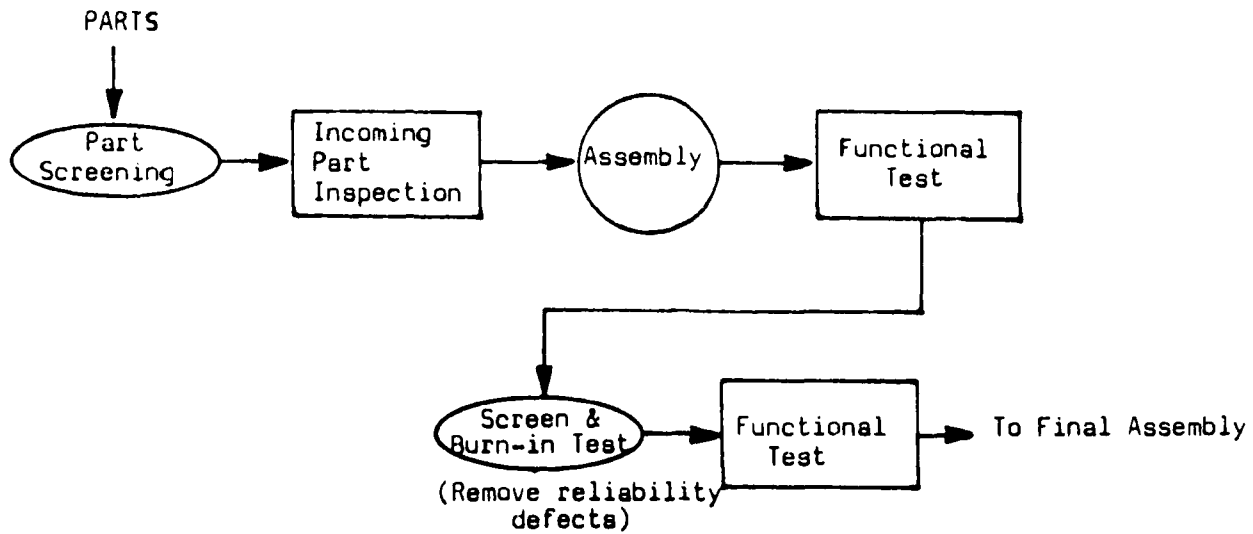
PROCESS ADDED DEFECTS

Defects
Entering
From
Prior
Processes → Defects
Added By
Process → Sum of
Defects
Entering +
Defects Added
By Process
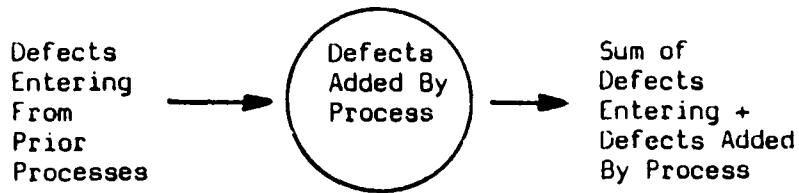
DEFECTS REMOVED BY INSPECTION

Defects
Entering
From Prior
Processes → Probability
of Detection
(E) → Defects
Remaining

$E = \dfrac{\text{defects removed}}{\text{total defects prior to inspection}}$

Defects Removed (rejectS)
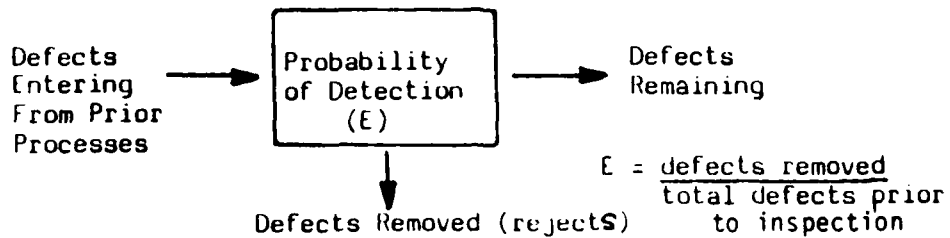
FIGURE 11.2.2.2-3: SAMPLE PROCESS FLOW DIAGRAM

(1) Complexity of part/assembly under test
(e.g., simple part, easy access to measurement)

(2) Measurement equipment
(e.g., ohmmeter for short/open circuit check, visual for component alignment check)

(3) Inspector experience
(e.g., highly qualified, several years in quality control)

(4) Time for inspection
(e.g., production rate allows adequate time for high efficiency)

(5) Sampling plan
(e.g., 100% - all parts are inspected)

Weight factors can be applied to each of the inspection attributes and used to estimate percent efficiency.

Step 5 - Compute outgoing defect rate based on the reject rates (from Step 3) and the efficiency factors (Step 4) using the process flow diagram developed during Step 2. Note that for a given inspection with a predefined efficiency factor, E, the number of defects of a fabricated item prior to its inspection can be estimated from the measured or estimated rejects, i.e., E = reject/total defects (prior to inspection). The number of outgoing defects is simply the difference between the number prior to inspection and that removed by the inspection.

Step 6 - Compute reliability degradation based on the ratio of the inherent design based reliability (Step 1) and the outgoing from manufacturing defect rates (Step 5). Note: Not all defects result in an actual hardware failure. Though a defect may exist, it may not be stressed to the point of failure. Through the reduction of the outgoing defect rates for a production process, field defect rates are reduced and, thus, reliability improved.

Hardware reliability can be improved through successive application of the above analysis. Those processes, wherein large numbers of defects are being introduced, can be isolated and corrected or changed with an improved process or by applying a screen test (or sequence of tests) to remove the defects. The inclusion of a screening test will increase the initial cost of the system, but the cost avoidance due to increased factory productivity (i.e., lower rework, scrap rate, etc.) and, more important, the lower field maintenance and logistics support cost should more than offset the initial cost. To be most cost effective, particularly for large complex systems, the application of the production reliability and inspection analysis should be first applied

to subsystems and equipment designated as critical by methods such as the failure mode and effects analysis procedures described in Section 6.

11.2.3 APPLICATION OF SCREENING AND BURN-IN DURING PRODUCTION TO REDUCE DEGRADATION AND PROMOTE GROWTH

The keystone of an effective production reliability/assessment and control program is the proper use of screening and burn-in procedures. The purpose of reliability screening and burn-in is to compress a system's early mortality period and reduce its failure rate to acceptable levels as quickly as possible. The rigor of the applied tests and subsequent failure analysis and corrective action efforts determines the extent of degradation in reliability and, hence, the degree of improvement. A thorough knowledge of the hardware to be screened and the effectiveness and limitations of the various available screen tests is necessary to plan and implement an optimized production screening and burn-in program.

Screening generally involves the application of stress during hardware tests on a 100 percent basis for the purpose of revealing inherent, as well as workmanship and process induced, defects without weakening or destroying the product. The application of stress serves to reveal defects which ordinarily would not be apparent during normal quality inspection and testing. As previously indicated, there are a large number of tests and test sequences that can be applied to remove defects induced at the various levels of fabricated assembly. Each specific test program must be designed and optimized relative to the individual hardware technology, complexity, and end item application characteristics, as well as the production volume and cost constraints of the particular product being manufactured. Planning a screening test program is an iterative process that involves tradeoff analysis to define the most cost effective program.

Screen tests can be applied at the different levels of part, intermediate, and system assembly. In order to detect and eliminate most of the intrinsic part defects, initial screening is conducted at the part level. Certain part defects, however, are more easily detected as part of an assembly test. This is particularly true of drift measurements and marginal propagation delay problems. Assembly defects, such as cold solder joints, missing solder joints and connector contact defects can be detected only at the assembly or subsystem level. At higher assembly levels, the unit's tolerance for stress is lower and, thus, the stress that can be safely applied is lower. As a general rule, screens for known latent defects should be performed as early in the assembly process as possible. They are most cost effective at this stage. A standard rule of thumb used in most system designs is that the cost of fixing a defect (or failure) rises by an order of magnitude with each assembly level at which it is found. For example, if it costs x dollars to replace a defective part, it will cost 10x to replace that part if the defect is found at the printed circuit board level, 100x if found at the equipment level, etc.

Figure 11.2.3-1 (Reference 1) depicts a typical production process where parts and printed circuit boards (PCBs) or wired chassis comprise assemblies, then manufactured assemblies, purchased assemblies and associated

11-22
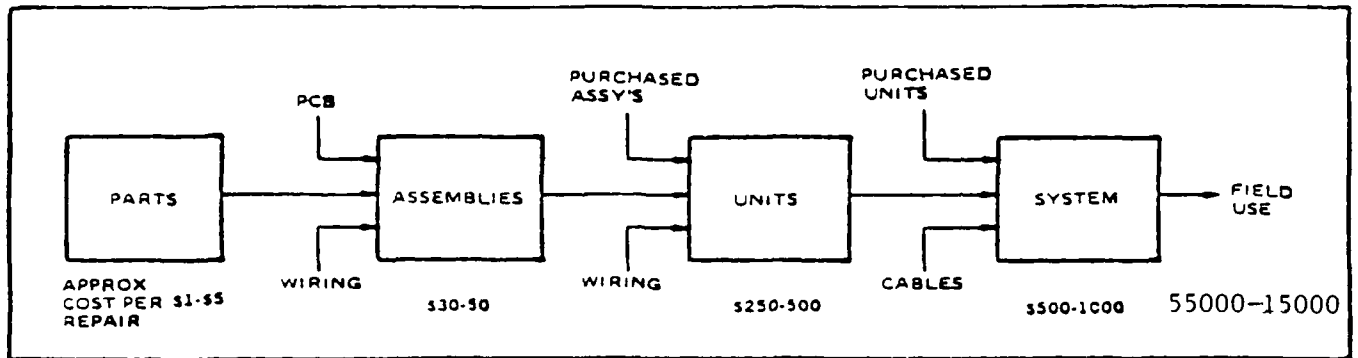
FIGURE 11.2.3-1: A TYPICAL PRODUCTION PROCESS. FINDING DEFECTS AT THE LOWEST LEVEL OF MANUFACTURE IS THE MOST COST-EFFECTIVE

wiring comprise units, and finally the units, other equipmen and inter-
cabling make up the completed system. Latent defects are introduced at
each stage in the process and, if not eliminated, propagate through to
field use. The cost of repair increases with increasing levels of
assembly, being $1 to $5 at the part level and perhaps as high as $1000
at the system level. Field repair cost estimates have been quoted as
high as $15,000. This data would tend to validate the previously
mentioned rule of thumb. Thus, for economic reasons alone, it is
desirable to eliminate latent defects at the lowest possible level of
assembly and certainly prior to field use.

The idealized manufacturing process, depicted in Figure 11.2.3-2, starts
with screened parts procured and received to a predetermined level of
quality. Screen tests are then applied as required at the different
levels of assembly. All screen test rejects are analyzed. The results
of this analysis are used to identify appropriate product design changes
and modifications to the manufacturing process and to reduce, if
possible, the overall test burden. All screen test results, including
reject rates, failure modes, and time-to-failure data are incorporated
into a dynamic real-time database from which the effectiveness of the
screening test program is continuously assessed. The database also
represents a primary experience pool for designing new screen test
programs as new systems are developed and introduced into the
manufacturing stream.

In general, screen and burn-in tests can be applied at the three major
levels of assembly: part, intermediate (i.e., printed circuit board),
and unit/equipment or system. The initial planning and tradeoff studies
should take into account the effectiveness and the economic choices
between part, intermediate, and final equipment/system level screens and
the parameters that must be considered.

11.2.3.1 PART LEVEL SCREEN TESTING

Part level screening is relatively economical and can be incorporated
into supplier specifications. It has the potential for maximum cost
avoidance, particularly when applied to complex microcircuits and other
high technology devices where reliability is largely dependent on
fabrication techniques and process control. Screen stress levels can be
matched to requirements, which, in general, enable the safe application
of higher and more effective stress levels to remove known part defects.
Part level screens offer the advantage of procedural simplicity and the
ability to pass a great deal of the burden for corrective action back to
the part vendors. Low level screens, however, have no impact on the
control of defects introduced during subsequent phases of manufacture
and assembly.

In general, there are two methods for a manufacturer to implement part
level screen tests. The first method is to perform the tests outside of
the manufacturing facilities by either incorporating standard military
requirements (e.g., MIL-STD-883) directly into the procurement
specification or by buying commercially processed parts and having an
independent testing laboratory perform the test. The advantage of this
approach is that no special training, burn-in facilities, or automatic
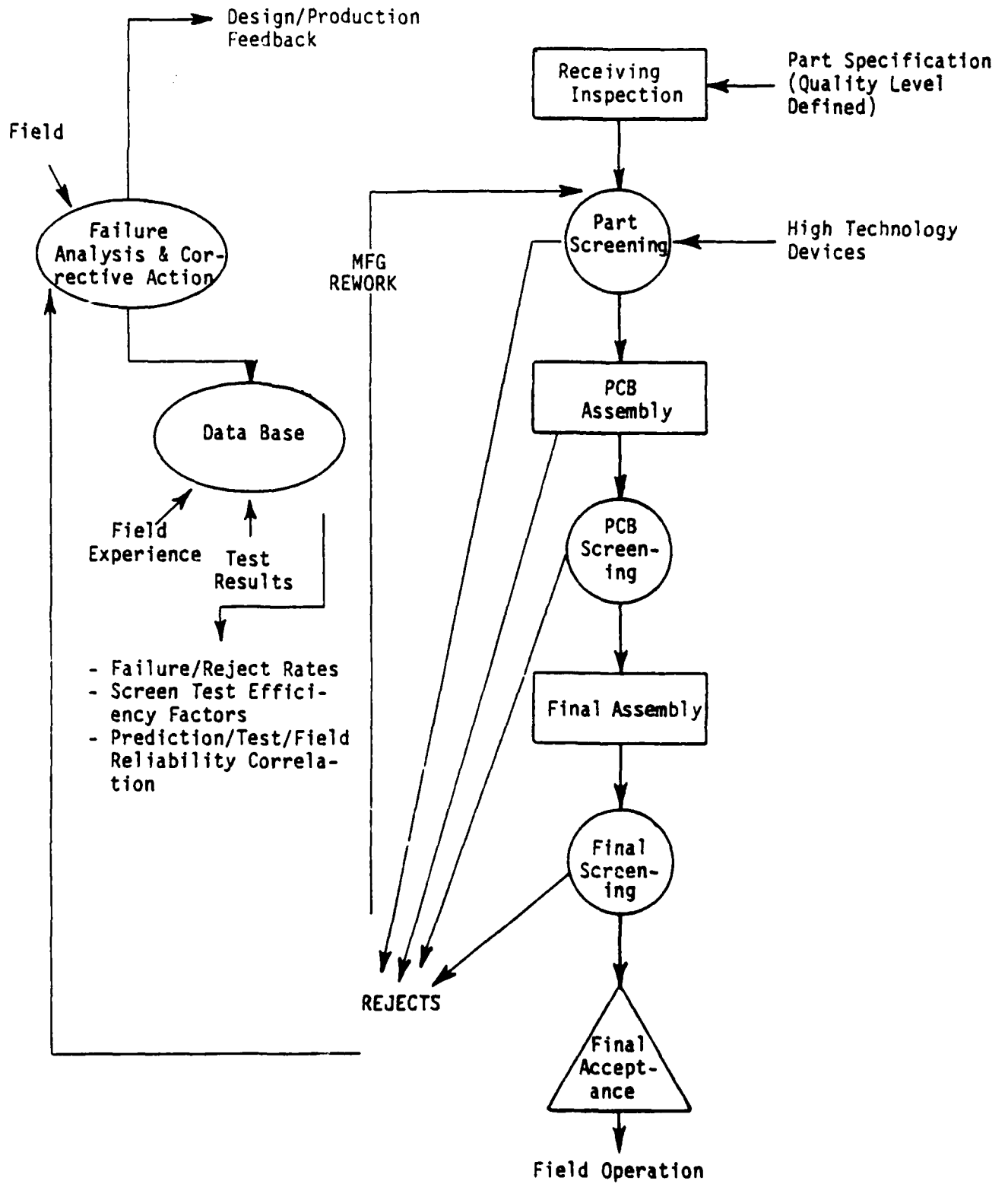
FIGURE 11.2.3-2: APPLICATION OF SCREEN TESTING WITHIN THE MANUFACTURING PROCESS

test equipment are required. The second approach is to perform the screen test with in-house facilities and equipment (generally requiring a capital investment) where flexibility, responsiveness to fabrication demands, and scheduled control can be maximized.

In the case of microcircuits the governing military documents are MIL-M-38510, and MIL-STD-883. The former document details the general requirements for manufacturer certification and qualification; the latter document describes the screening tests and the sequence in which they must be performed in order to obtain a microcircuit of a given reliability/quality level. The reliability/quality levels are Class S (most reliable),and Class B. Class B devices are used for most military applications.

Method 5004 of MIL-STD-883 lists the screening tests required for each class of microcircuits. The MIL-STD also describes in detail each of the test methods and test conditions required to obtain the desired quality level.

Commercial type microcircuits are generally not subjected to special manufacturing procedures, inspections, or burn-in but, as a minimum, generally undergo some form of visual and electrical parameter screening.

In the case of discrete semiconductors, tne governing military documents are MIL-S-19500, and MIL-STD-750. MIL-S-19500 details the general requirements for manufacturer certification and qualification; it also lists the screening tests that must be applied to guarantee a given reliability/quality level. MIL-STD-750 provides details on each test method and test condition.

MIL-S-19500 lists the screening tests required for each reliability/quality class of discrete semiconductors. The classes are: JANS (most reliable), JANTXV (intermediate), and JANTX (least reliable). There is also a fourth class, JAN devices, which although subject to the certification and qualification requirements of MIL-S-19500 are not subjected to 100% screening tests. The basic difference between JANTXV and JANTX devices is the fact that JANTXV devices are subjected to 100% precap visual inspecticn.

Screei.ing and inspection tests for resistors, capacitors and other passive components typically include high temperature conditioning, visual and mechanical inspections, dc resistance mcasurement, low temperature operation, temperature cycling, moisture resistance, short time overload, shock vibration, solderability, and rated power life test.

TABLE 11.2.3.1-1: <u>SUMMARY OF THREE PREVIOUS SURVEYS</u>

Topic	Martin-Marietta Survey (Ref.6)	McDonnell Aircraft Company Survey (Ref.4)	IES Survey (Ref.2)
Thermal Cycle Screening	6-10 cycles. More cycles are required for more complex units & when done at lower assembly levels.	4 and 10 cycles most common. No. of cycles used varies widely (2-70 cycles).	8-12 cycles, independent of unit part count. 20-40 cycles for module-level temp. cycling.
Temperature Range	-54°C to +55°C most common (influence of AGREE testing). Maximum safe range is most effective.	-54°C to +55°C or +71°C (influence of AGREE testing).	Not stated, but stress screening cycles strongly influenced by AGREE testing profiles.
Temperature Rate of Change	10°F to 40°F/min. with higher rates more effective.	3°C to 5°C/min.	5°C/minute. Higher rates (15-20) C/min. at module level more effective.
Power ON vs. OFF	ON, with close monitoring of performance. OFF during cooling down portion.	Not stated, but expected to follow AGREE profile. (ON, except during cool-down portion).	ON, for unit and system-level. Functional testing at both extremes. OFF, for module-level.
Failure-Free Cycles	0-2 cycles FF. 1 FF cycle recommended.	Varies greatly, 0 to 22 FF cycles. 1 FF cycle is most common.	Should be made part of acceptance criteria, separate from stress screening.
Random Vibration	Not addressed.	3-6.2gRMS, 5-10 minutes per axis, 2 or 3 axes.	Various levels. Many are using NAVMAT P-9492, 6gRMS. Recommends tailoring to item being screened. Not effective at module-level.
Degradation	Temperature cycling does not degrade soundly designed hardware.	Not addressed.	Cases noted where high levels of random vibration (6gRMS) cause degradation.

TABLE 11.2.3.1-1: SUMMARY OF THREE PREVIOUS SURVEYS (Cont'd)

Topic	Martin-Marietta Survey (Ref. 6)	McDonnell Aircraft Company Survey (Ref. 4)	IES Survey (Ref. 2)
Distribution of Defects:			Not addressed.
Part-related	62%	46%	
Manufacturing-related	33%	30%	
Design-related	5%	8%	
Other		15%	
Effectiveness of screens other than temperature cycling and random vibration	Low level (2g) fixed sine vibration and temperature soak are not effective screens.	Low level (2g) fixed sine vibration not effective. Opinion mixed on effectiveness of temperature soak.	All screens other than temperature cycling and vibration are less effective substitutes.
Combined Temperature Cycling and Random Vibration	Not addressed, except that AGREE vibration is not an effective screen.	Majority think combining the screens is more effective than applying singly.	Combined testing is no more effective than applying screens singly. Using both temp. cycling and vibration singly is necessary and a synergistic effect is gained.
Sequence of Temperature Cycling and Vibration, when used singly	Not addressed.	Respondents indicated various combinations, vibration before, after and in between temp. cycling, with no concensus opinion on which is most effective.	No preferred sequence. Applying either screen before and after the other screen shows additional fallout.
Reliability Improvement through Stress Screening	Not specifically addressed, but there is general agreement that temp. cycling eliminates incipient defects (and it can be inferred that reliability will thereby improve).	Not specifically addressed, but there is general agreement that temp. cycling eliminates incipient defects (and it can be inferred that reliability will thereby improve).	Equipment reliability can be improved by 25-90% through stress screening.

11.2.3.2 SCREENING AT MODULE AND UNIT/SYSTEM LEVEL

The use of environmental stress screening at the module and equipment level has increased significantly in the past few years among many military electronic equipment manufacturers.

A survey of the current literature (Refs. 1 through 8) has shown that although the use of stress screening is on the increase, there is little general guidance as to how to best plan, monitor and control a stress screening program. The Institute of Environmental Sciences (IES), a professional organization of engineers and scientists, currently has a national program underway to develop a guideline document for Environmental Stress Screening of Electronic Hardware (ESSEH). Results of this effort were published in a guidelines document (Ref. 2).

Because the origin of environmental stress screening was in AGREE (Advisory Group on Reliability of Electronic Equipment) testing (specifically temperature cycling and vibration of avionics "black boxes"), the current general industry consensus is that temperature cycling is the most effective stress screen, followed by random vibration (Ref. 2). The results of this consensus are shown in Figure 11.2.3.2-1. The vibration used in AGREE testing done in the past was single frequency and relatively low level (2.2g). In search of more effective screens, the Grumman experiments (Ref. 8) indicated that random vibration was more effective than either swept-sine or single frequency sine vibration. The results of thermal cycling in eliminating parts and workmanship defects (primarily during AGREE testing) were collected and summarized by Martin-Marietta (Ref. 6). The results of the two studies (Ref. 6, 8) were combined into NAVMAT P-9492 (Ref. 3) to serve as a starting point guideline document with official sanction.

At the module/assembly level, thermal cycling is believed to be an effective screen for both part and workmanship defects. The rate of change of temperature is thought to be an important parameter, with higher rate of change being more effective. Between 20 and 40 temperature cycles are generally recommended. There are two opposing schools of thought on whether power should be applied during the thermal cycling. There also is no general agreement on the efffectiveness of vibration at the module/assembly level (Ref. 2).

At higher levels of assembly (i.e., units, groups) thermal cycling and random vibration are effective screens. Fewer thermal cycles are thought to be necessary at these levels, varying from 4 to 12 cycles. Power "ON" is generally accepted as more effective, and an increasing number of practitioners are recommending a performance verification test (PVT) at each temperature extreme. One report states that 80% of all defects detected during stress screening were found during PVT at the low temperature extreme. Several practitioners using random vibration at these levels cite power "ON" and continuous monitoring as essential to detect intermittents. Low level single frequency vibration is widely accepted as being an ineffective screen.
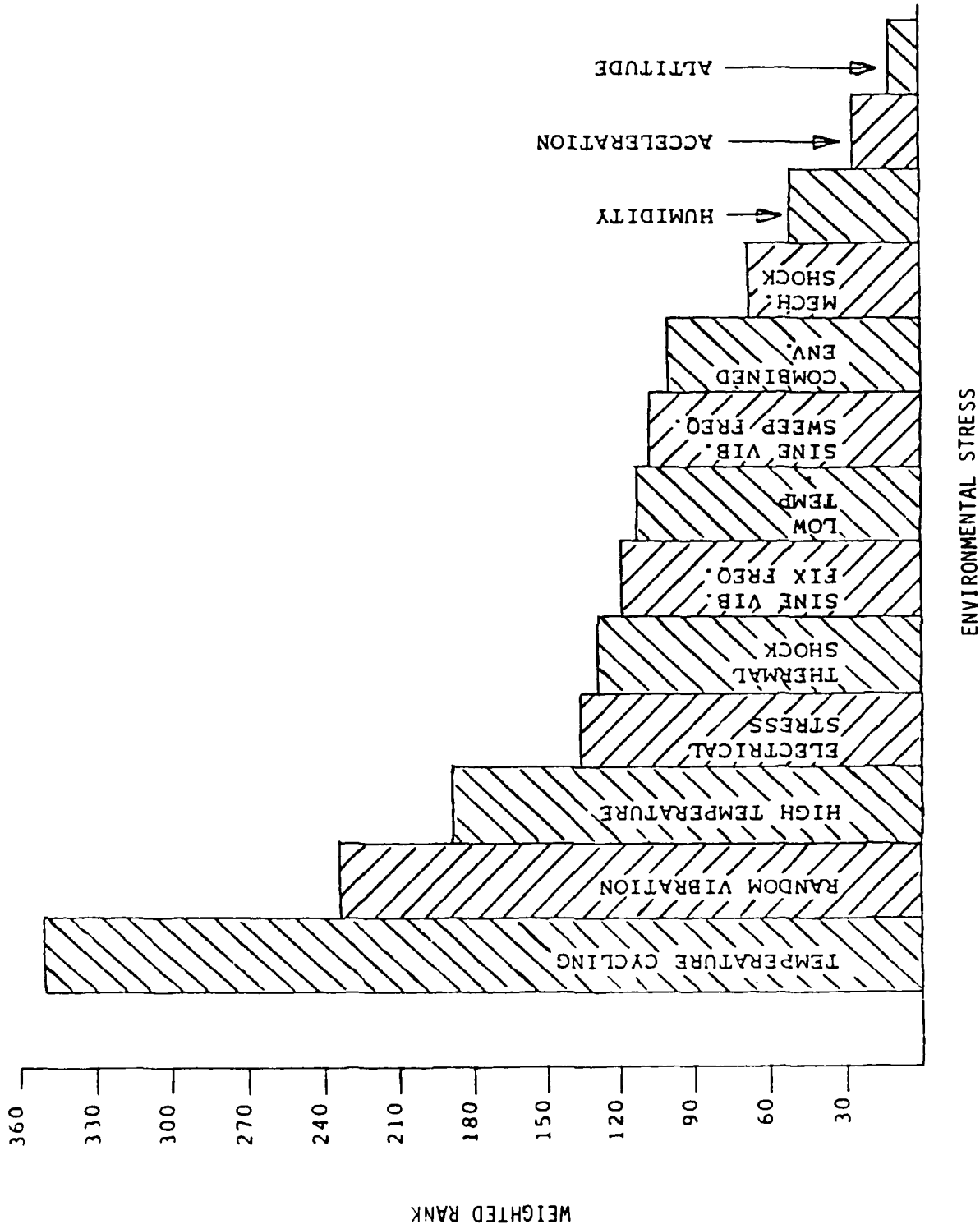
FIGURE 11.2.3.2-1: EFFECTIVENESS OF ENVIRONMENTAL SCREENS

There is some disagreement on the effectiveness of some screens at certain levels of assembly, the source of which may lie in differences in hardware type, construction, part content and degree of design and production maturity. Also, the definitions for the various levels of assembly (subassembly, assembly, module, unit, group, etc.) are not clear descriptions of the items they represent.

The results of three of the recent surveys are summarized in Table 11.2.3.1-1.

More recently, Hughes Aircraft Company prepared a Screening Guidelines document (Ref. 1) under contract with RADC. Two of the more significant outputs of the document are: 1) development of a series of screening strength equations for vibration and temperature cycling and 2) a computerized stress screening model (SSM) which enables one to find an optimum set of screening tests based on inputs of estimated number of initial and process-induced defects and estimated screening costs.

"Screening strength" is defined as the probability that a stress screen will transform a latent defect into a hard failure (given that there is a latent defect present) and that the failure will be detected by the screen. The screening strength equations (and curves) shown in Figures 11.2.3.2-2 through 11.2.3.2-6 were developed for random vibration (Figure 11.2.3.2-2), swept-sine vibration (Figure 11.2.3.2-3), single frequency vibration (Figure 11.2.3.2-4), temperature cycling (Figure 11.2.3.2-5), and constant temperature (Figure 11.2.3.2-6). First, a brief word of explanation of the equations used in the figures. In Figures 11.2.3.2-2 through 11.2.3.2-4, "G" refers to the "g" level of the vibration test; "T" is the vibration time in minutes. In Figures 11.2.3.2-5 and 11.2.3.2-6, LN is, of course, the natural logarithm, dT is the rate of change of temperature in ^{0}C per minute, N_{cy} is the number of cycles, T is the time in hours, and R is the temperature range in ^{0}C.

The screening strength equations and curves can be used to optimize screening tests for a specific application. These equations have been incorporated into the computerized SSM model which utilizes a dynamic programming algorithm to find the optimum solution to either:

(1) the set of screens which achieve a predetermined reduction of latent defects for the least cost, or

(2) the set of screens which achieve the maximum reduction of latent defects for a fixed cost.

11.2.3.2.1 INTERMEDIATE LEVEL SCREENING (E.G., MODULE, PRINTED CIRCUIT BOARD, ASSEMBLY, ETC.)

Intermediate testing is more expensive but can remove defects introduced at the board level as well as those intrinsic to the parts. Because of the several part types incorporated into a board, somewhat lower stress levels must be applied. For example, the maximum test temperature depends upon the part having the lowest maximum temperature rating of all the parts on the board. Generally, special burn-in/temperature cycling facilities are required as well as special automatic test
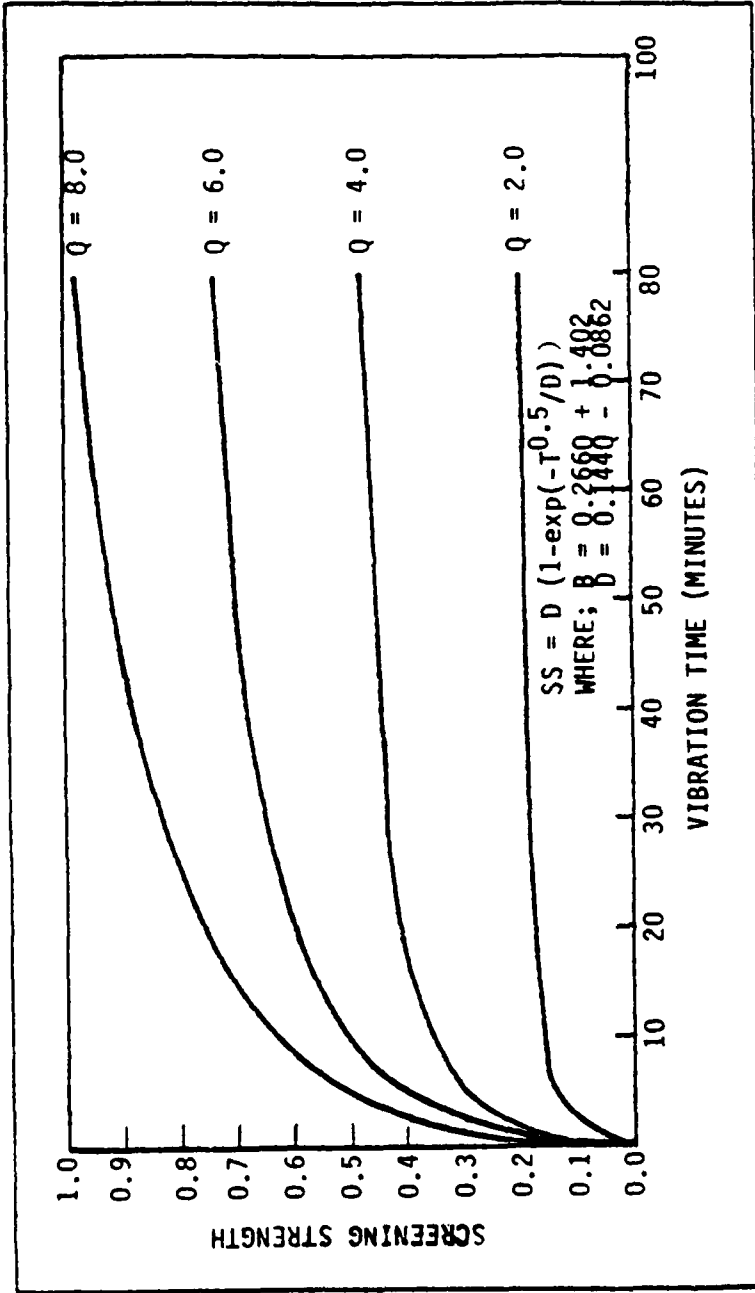
FIGURE 11.2.3.2-2: SCREENING STRENGTH FOR A RANDOM VIBRATION SCREEN

$$SS = D(1-\exp(-T^{0.8}/0))$$
WHERE; $B = 0.0176Q + 7.097$
$D = 0.635Q + 0.1065$
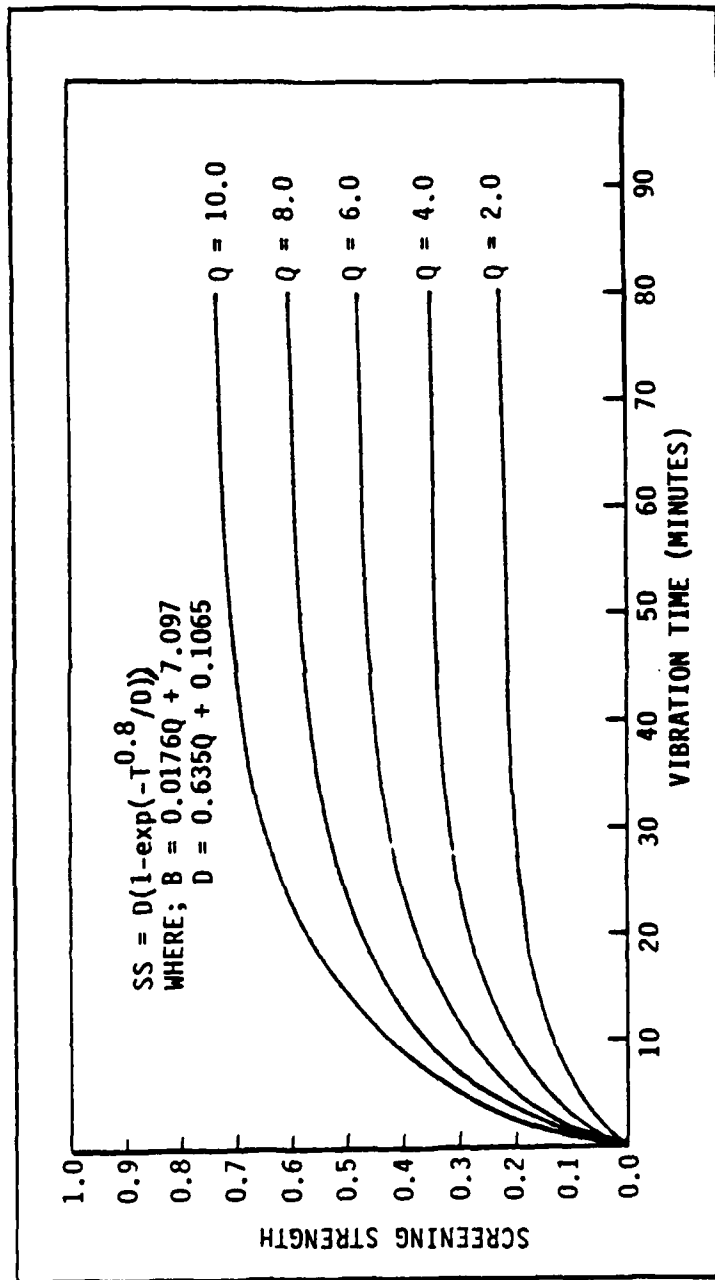
FIGURE 11.2.3.2-3: SCREENING STRENGTH FOR A SWEPT-SINE VIBRATION SCREEN
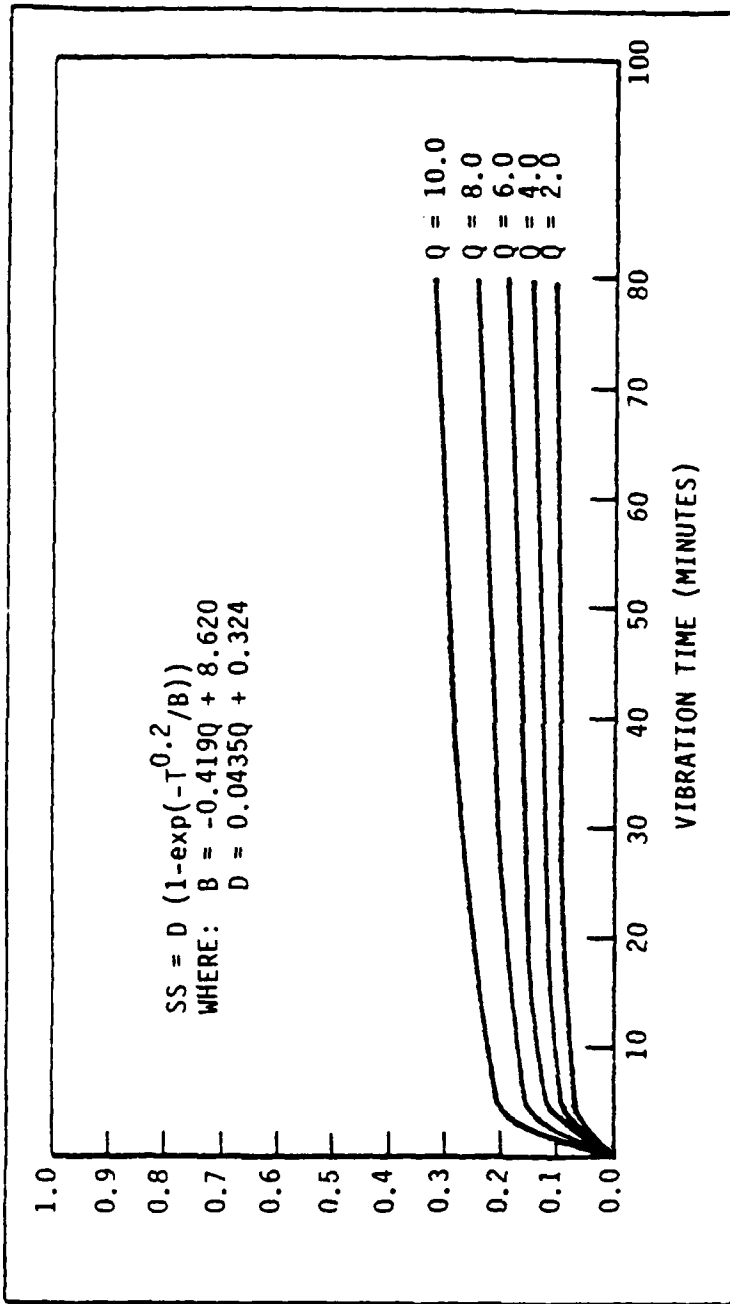
FIGURE 11.2.3.2-4: SCREENING STRENGTH FOR A SINGLE (FIXED) FREQUENCY VIBRATION SCREEN

$SS = D (1-\exp(-T^{0.2}/B))$
WHERE: $B = -0.419Q + 8.620$
$D = 0.0435Q + 0.324$

$Q = 10.0$
$Q = 8.0$
$Q = 6.0$
$Q = 4.0$
$Q = 2.0$

VIBRATION TIME (MINUTES)
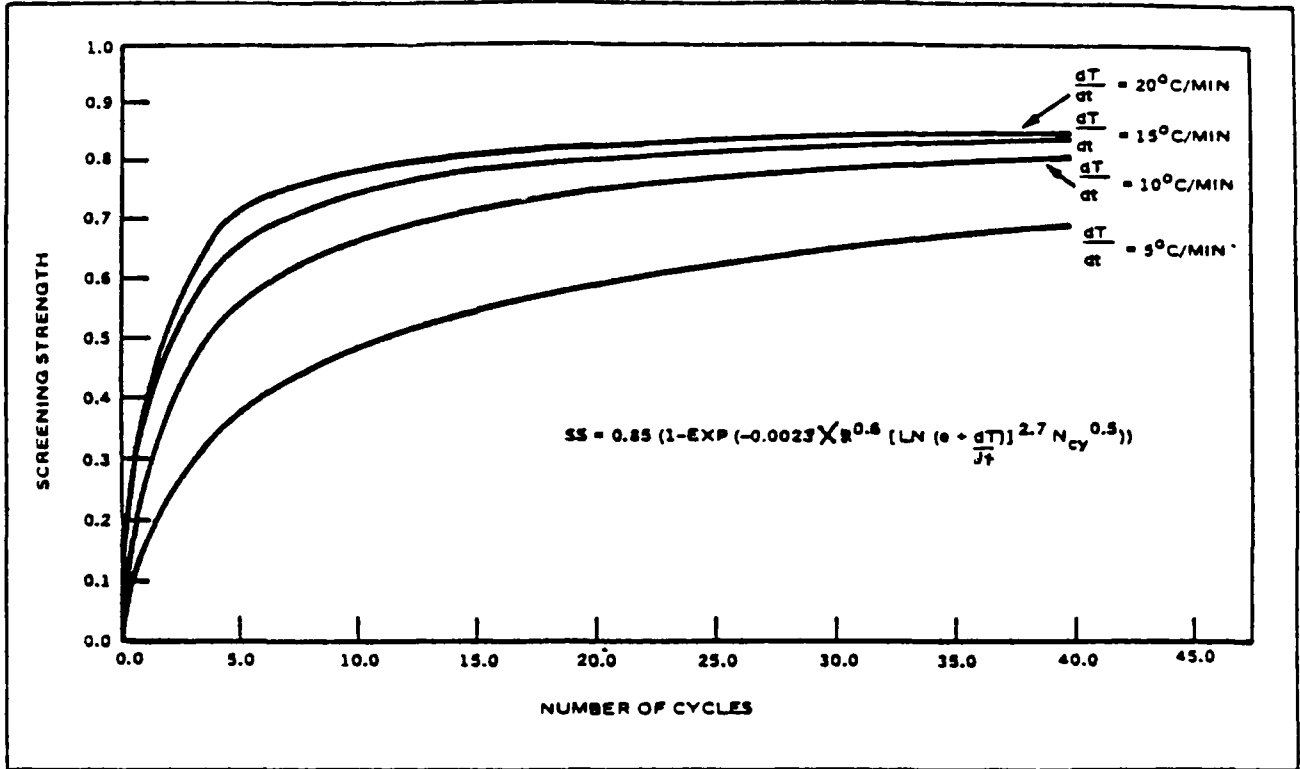
FIGURE 11.2.3.2-5: SCREENING STRENGTH FOR A TEMPERATURE CYCLING SCREEN

$$SS = 0.85 \left(1 - EXP\left(-0.0023 \times R^{0.6}\left[LN\left(e + \frac{dT}{dt}\right)\right]^{2.7} N_{cy}^{0.5}\right)\right)$$
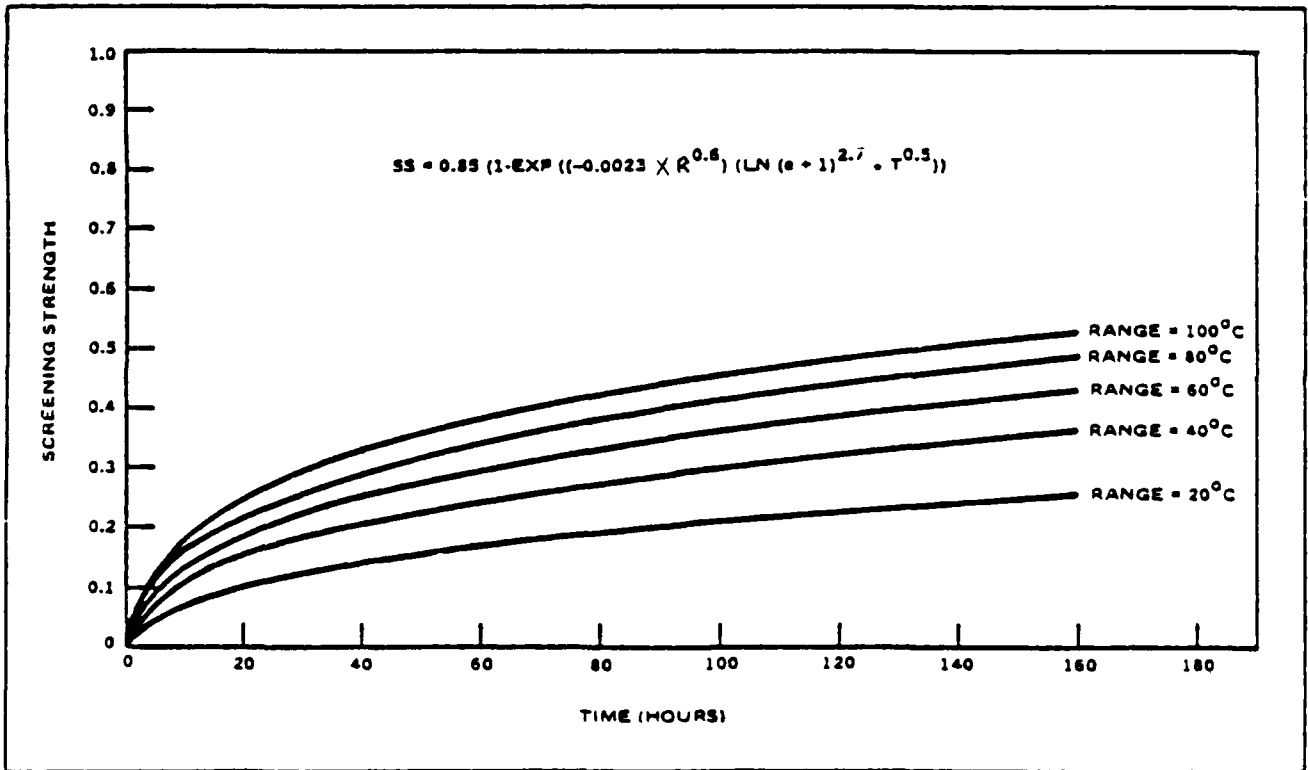
FIGURE 11.2.3.2-6: SCREENING STRENGTH FOR A CONSTANT TEMPERATURE SCREEN

$$SS = 0.85 \left(1 - EXP\left((-0.0023 \times R^{0.6})\left(LN(e + 1)^{2.7} \cdot T^{0.5}\right)\right)\right)$$

equipment (ATE). In general, some amount of ATE is employed in virtually all large scale screening programs. Automatic testing cannot only perform rapid function testing after screening or burn-in of complex boards (or other assemblies) but also is effective in the detection of pervasive faults. The latter consist of marginal performance timing problems and other defects arising from part interactions during operation. The extent of the facilities and equipment is dependent on the test conditions specified. The potential for cost avoidance with intermediate level screens is not as high as for part level screens, and the necessity to employ, generally, a lower stress level reduces their effectiveness to some extent.

Temperature cycling is a highly effective module or printed circuit board stress test which reveals workmanship and process-induced defects as well as those intrinsic parts defects which escaped detection at the part-level screen. Temperature cycling is performed specifically to reveal:

    (1) Assembly defects:

        delamination
        fracture
        insulation cracking

    (2) Part/board bond separating

    (3) Solder problems (cracking opens, etc.)

    (4) Part defects which escaped part manufacturer's screens and receiving inspection tests

    (5) Tolerance drift

The types of latent part defects expected to be present depends on several factors, including:

    (1) types of parts comprising the assembly (i.e., microcircuits, discrete semiconductors, passive parts, low population parts, microwave parts, etc.)

    (2) quality grade of the parts

    (3) extent to which the parts were previously screened (e.g., receiving inspection tests and screens)

    (4) testability of the parts (e.g., microprocessor and other LSI devices are difficult to test completely, and therefore precipitated defects may go undetected).

Figure 11.2.3.2.1-1 illustrates the environmental conditions and profile under which a typical temperature cycling test can be performed. The actual number of cycles employed is dependent upon board density and part technology. For low density/technology boards, three cycles are typical, and for high density/technology boards, ten cycles or more may be applied. As shown in Figure 11.2.3.2.1-1 a functional test can be performed after each cycle at ambient conditions.
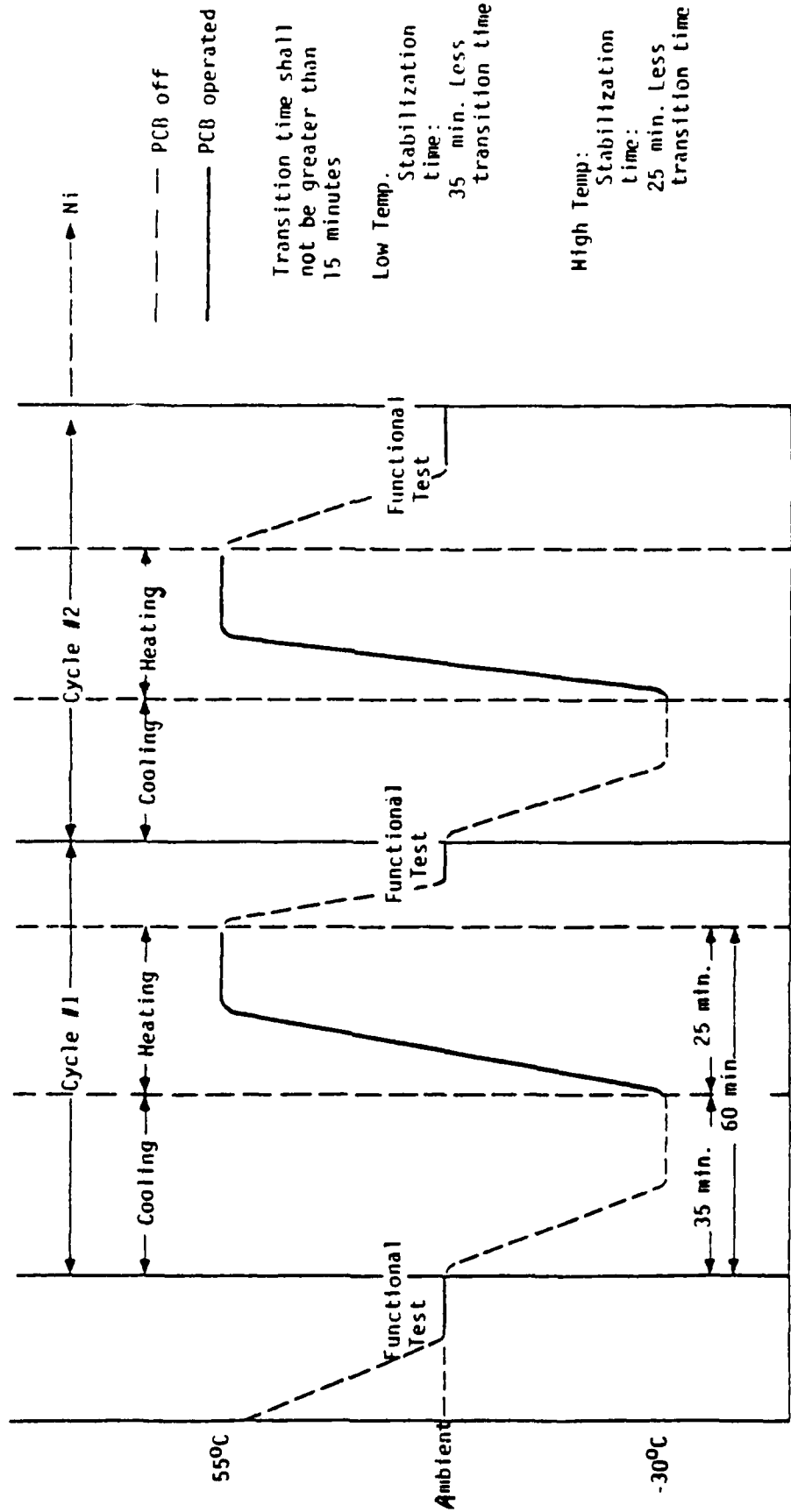
FIGURE 11.2.3.2.1-1: PCB TEMP - CYCLE ENVIRONMENTAL PROFILE

The number of failures should be recorded for each cycle. An analysis is conducted on failed assemblies or boards to determine the underlying failure mechanisms, as well as the possibility of earlier detection and the application of more stringent inspections and screens at the part level. If appropriate, the manufacturing process may be altered as well. Following analysis, repairs are made and the test continued. However, any failure occurring during the last cycle(s) requires repetition and completion of the last cycle(s) following its repair. The number of cycles may be increased beyond those originally set if the repair action is complex or difficult to inspect, if unscreened parts were used as replacements, and, in general, if it is likely that the repair action could induce new defects into the board.

The number of cycles initially applied represents a baseline for designing the temperature cycling screening test. Temperature cycling screening, like any quality inspection test, is considered to be a dynamic test where the number of cycles is adjusted, depending on the results of subsequent higher level tests or field performance. For example, the number of temperature cycles could be increased if a high number of failures is observed and reported in subsequent testing. Conversely, the number of cycles could be decreased if few failures are reported. It must be emphasized, however, that the extent and nature of any changes are determined only through careful review and analyses of the subsequent failures.

If a thermal screen (temperature cycling or constant temperature burn-in) is selected for the assembly level, the following screen parameters must be determined:

(1) <u>Maximum Temperature</u>. The maximum temperature to which the assembly will be exposed should not exceed the lowest of the maximum ratings of any parts or materials comprising the assembly. Nonoperating ratings for parts are higher than the operating ratings.

(2) <u>Minimum Temperature</u>. The minimum temperature to which the assembly will be exposed should not exceed the highest of the minimum ratings of all the parts and materials comprising the assembly.

NOTE: (1) and (2) above must be carefully selected to assure that the maximum screening effectiveness is achieved. Exceeding the maximum ratings may result in damage to nondefective parts or materials which is contrary to the principle of stress screening. If the operating temperature for a power-on screen cannot be readily determined analytically, a thermal survey of the item to be screened should be performed to determine the maximum and minimum screening temperatures.

(3) <u>Temperature Rate of Change</u>. Screening effectiveness increases with increasing temperature rate of change. The maximum rate of change is dependent on the thermal chamber characteristics and the thermal mass of the items to be screened.

(4) <u>Dwell at Temperature Extremes</u>. During a temperature cycle it is sometimes necessary to maintain the chamber temperature constant once it has reached the maximum (or minimum) temperature, sometimes referred to as "dwell." Dwell may be required to allow the item being screened to achieve the chamber temperature. The item thermal lag depends on thermal mass, and most printed wiring assemblies (PWAs) have a low thermal mass.

(5) <u>Number of Cycles</u>. Ref. 2 recommends 20 to 40 thermal cycles for the assembly (module) level. If the computerized SSM is used (Ref. 1), the number of cycles is determined by the required screening strength.

The determination of whether to apply power to assemblies being screened and whether to perform a functional test during the screen requires consideration of the following factors:

(1) <u>Predominant Type of Defect Present</u>. If the predominant type of defect is expected to be a weak interconnection which is transformed to an open circuit by the screen (cold solder joint, weak wire bond), then a post screen test will detect the open circuit and power-on is not required.

If, on the other hand, the predominant type of defect is expected to be of an intermittent nature, then power-on with continuous performance monitoring is necessary.

(2) <u>Economics</u>. A fixture and associated test equipment to house assemblies, apply power, provide stimuli, and monitor assembly performance can be costly. The tradeoff of fixture and test equipment cost and potential benefits may prove difficult.

If the vibration screen is selected for the assembly level, the type of vibration (i.e., random, swept-sine or fixed-sine) must be selected and the following two parameters must be determined:

(1) <u>Vibration Level</u>. Refs. 2 and 3 recommend random vibration and suggest a level of 0.04-0.045 g^2Hz, provided that the assembly can withstand that level without damage. If the assembly dynamic response characteristics to the vibration excitation are not known, a careful vibration survey should be conducted to properly establish the acceleration spectrum and level. Ref. 2 suggests use of swept-sine as a second choice, if random vibration cannot be performed. Single frequency vibration at the assembly level is considered as ineffective.

(2) <u>Vibration Duration</u>. Refs. 2 and 3 suggest 10 minutes per each of three axes. The need for multiaxis excitation may vary from one assembly to another, and therefore it is desirable to determine fallout per axis during initial screens to allow screen adjustments.

Some other factors to consider in determining the desirability of a PWA vibration screen are the PWA size and stiffness. Larger PWAs will flex more and precipitate such latent defects as cracked metal run, cold solder, and embedded conductive debris. Smaller PWAs, particularly if conformally coated, are stiff and not amenable to vibration screening.

Table 11.2.3.2.1-1 indicates the type of module/assembly defects which can be precipitated by thermal and vibration screens.

TABLE 11.2.3.2.1-1: ASSEMBLY LEVEL DEFECT TYPES
PRECIPITATED BY THERMAL AND VIBRATION SCREENS

Defect Type Detected	Thermal Screens	Vibration Screens
Defective part	X	X
Broken part	X	X
Improperly installed part	X	
Solder connection	X	X
PCB etch	X	X
Loose contact		X
Wire insulation	X	
Loose wire termination	X	X
Improper crimp	X	
Contamination	X	
Debris		X
Loose hardware		X
Mechanical flaw		X

11.2.3.2.2 UNIT/EQUIPMENT AND SYSTEM LEVEL SCREENS

Equipment/system level screen testing is expensive but can remove defects introduced at all levels of fabrication. At this point in the manufacturing stream, the potential for cost avoidance is low and the permissible stress level may not adequately exercise certain specific parts. However, these higher level assembly tests are considered important, even if it is thought that the lower level tests may have eliminated all defective parts and board defects. The assembly of the remaining components and the boards into the larger assemblies and into the final item cannot be assumed to be free of failure producing defects. Good parts may be damaged in final assembly, workmanship errors can occur, and product-level design defects may be present.

Unit/equipment level screens, then, are primarily intended to precipitate unit workmanship defects and, secondarily, assembly level escapes. Unit level defect types vary with unit construction but typically include interconnection (defects) such as:

(1) PWA connector (loose, bent, cracked or contaminated contacts, cracked connector)

(2) Backplane wiring (loose connections, bent pins, damaged wire insulation, debris in wiring)

(3) Unit input/output connectors (loose, cracked pins, damaged connector, excessive, inadequate or no solder on wire terminations, inadequate wire stress relief)

11-40

(4) Intra-unit cabling (improperly assembled coax connectors, damaged insulation)

Units may also contain wired assemblies integral to the unit and not previously screened, such as Power Control and BIT Panels, and purchased assemblies, such as modular low voltage power supplies.

The latent defects associated with those assemblies should be considered in the selection of screens. Typical unit/equipment screens include:

(1) Thermal - temperature cycling and/or fixed temperature burn-in
(2) Vibration - sine wave random

Thermal screens are more effective than vibration screens in precipitating latent defective parts. Thermal cycling and vibration screens are both effective in precipitating latent workmanship defects, although each screen may be more effective than the other for certain defect types. The unit composition and knowledge of prior screening will dictate the expected types of defects and aid in screen selection.

If a thermal screen is selected, the same process as described for the assembly must be followed. Differences are outlined as follows:

(1) Units have greater thermal mass, and, therefore, the higher temperature rates of change may be more difficult to achieve. A dwell at temperature extremes is probably required.

(2) Power-on screening is usually easily accomplished and widely recommended. A functional test (PVT) at temperature extremes has been shown in several cases to be effective in detecting defects not detectable at room ambient temperature. As stated previously, one project reported finding 80 percent of the total defects during PVT at low temperature.

(3) Fewer temperature cycles appear to be required at the unit level. A range of 4 to 12 cycles is common.

If a vibration screen is selected, it is very important that competent engineering personnel evaluate the unit to be vibrated to determine the appropriate vibration type, level of excitation, and whether or not a vibration survey should be performed. There is some evidence that for large, massive units, low levels of vibration are effective screens.

If an item is subjected to an unpowered screen, testing subsequent to the screen may reveal part or workmanship defects requiring correction. If the item was not tested prior to entering the screen, it cannot be determined, even if a detailed failure analysis were performed, if the defects found were precipitated by the screen or were present in the item before the screen. If all the necessary information relating to the effectiveness of the screen were known, i.e, the average number of latent defects entering the screen and the average screening strength

in precipitating those defects, it would not be necessary to know the condition of the item prior to screening. However, stress screening has not yet advanced to the point where quantity and type of latent defects can be accurately predicted and screening strengths calculated; therefore, some degree of experimentation is necessary to derive reasonable defect rate and strength estimates. Testing before entering a screen establishes a baseline upon which post-screen testing results can be used to measure the screening strength. The pre-screen testing should be done immediately before the screen to eliminate the uncertainty of latent defect introduction during such processes as cleaning, conformal coating, handling and storage which may follow the initial item testing.

Once the screening effectiveness has been established, the value of both pre-screen and post-screen testing has diminished, and it may prove cost effective to perform only post-screen testing. When major perturbations take place, such as production line changes, fabrication/assembly process changes, personnel changes, or alterations to the stress screening process, it may be advisable to reinstitute pre-screen testing until the process has stabilized.

For long term production programs, the normal learning curves result in process improvements, and the quantity and distribution of latent defects is expected to change accordingly. There will be a predominance of workmanship and manufacturing process related defects in early production, and component related defects dominate mature production. Stress screens have a different degree of effectiveness for different defect types, and, therefore, screens that may have been effective during early production should be periodically reevaluated to assure their continued effectiveness.

11.2.3.3 SCREEN TEST PLANNING AND EFFECTIVENESS

An effective reliability screen test program requires careful planning that starts during early development. Tradeoff studies are performed and a complete test specification is prepared and possibly verified for its effectiveness on prototype hardware.

A key step in specifying an effective screen test program is the identification of the kinds of failure modes that can occur and the assembly level at which they may be induced. The appropriate screen tests are those which are most effective in accelerating the identified modes, whether they are intrinsic to the part or induced by the manufacturing process. Table 11.2.3.3-1 lists some of the more common screens and gives an indication of their effectiveness.

Due to the varied nature of military electronics equipments and their associated design, development and production program elements, it is difficult to "standardize" on a particular screening approach. A tailoring of the screening process to the unique elements of a given program is, therefore, required. As was previously discussed, screening tests such as temperature cycling and random vibration appear to be the most effective tests. In fact, for electronics equipment, temperature cycling was found to be a more effective screen than vibration by a factor of 3 or 4 to 1, with random vibration more effective than swept sine, the latter more effective than fixed sine.

TABLE 11.2.3.3-1: <u>SCREEN TEST EFFECTIVENESS</u>

Temperature Cycling	Extremely effective at all levels of assembly; reveals part/PCB defects, solder problems, bond separations, tolerance drifts, mismatches and changes in electrical characteristics
High Temp Burn-In (Power Cycling)	Effective at all levels of assembly; will reveal time/stress dependent part and process defects
Vibration, Random	Effective primarily at equipment level; reveals solder problems, part/PCB defects, connector contact problems, intermittents, loose hardware and structural problems
High Temp Storage	Relatively inexpensive screen that can be applied at any level of assembly to reveal time/dormant stress (nonelectrical) dependent defects
Thermal Shock	Relatively simple screen that can be applied at the part or module level to reveal cracking, delamination and electrical changes due to moisture or mechanical displacement
Vibration, Sine Fixed Frequency	Applied at final assembly level to reveal loose hardware, connector contact problems and intermittents

However, exposure levels, number of cycles, and test durations differ widely among users. Other, perhaps less costly, tests such as sinusoidal vibration, power cycled burn-in at ambient and temperature soak are also used, but, in general, their effectiveness is believed to be less than the former tests. Precise knowledge of the effectiveness of the various available screening tests is not currently known. Screening tests, therefore, should be selected based upon estimates of cost and test effectiveness, early development program data, equipment design, manufacturing, material and process variables, which at least narrow consideration to the most cost effective choices. The screening process then should be continuously monitored and test results analyzed so that changes in the process can be made as required to optimize the cost effectiveness of the screening program.

As was previously mentioned, two new tools have been recently developed to aid in the planning and optimization of screening tests. These are: 1) the computerized Stress Screening Model (Ref. 1) and MIL-I-45208 the Stress Screening Guidelines Matrix (Ref. 2). They are described in more detail in the following subsections.

11.2.3.3.1 STRESS SCREENING MODEL (SSM)

A simplified flow diagram depicting the SSM and stress screening process is shown in Figure 11.2.3.3.1-1. The figure shows (incoming) the total number of parts and number of defective parts entering a screening process. At level 1, some workmanship defects (ADEF) are introduced, and the screen at level 1 has some screening strength (SS) which acts on the incoming part and workmanship defects to produce an expected fallout of PRT (part defects) and WKM (workmanship defects). The total number of defects entering a level minus the fallout is the number of residual defects passed on to the next level (DEF PASSED). After passing through the three screening levels, there are still some defective parts remaining (DEF P REM) and some workmanship defects remaining (DEF W REM), resulting in some instantaneous outgoing MTBF value. At each level there is an expected fallout, and, because of random variations in defect quantities and screening strengths, a probability interval with upper and lower bounds (UPPR BND, LOWR BND) is computed for monitoring purposes.

Model Options. The SSM has three options as follows:

(1) MTBF Option (Option A). The SSM provides an optimum set of stress screens to precipitate the required number of latent defects to achieve a desired instantaneous MTBF at the termination of the screening.

(2) Cost Option: (Option B). The SSM provides a set of screens to precipitate the maximum number of latent defects for a fixed cost.

(3) Trade-Off Option: (Option C). The SSM provides the capability to evaluate existing screens and to identify equivalent screens for trade-off purposes.

11.2.3.3.2 STRESS SCREENING GUIDELINES MATRIX

The Stress Screening Guidelines Matrix (Table 11.2.3.3.2-1) is a summary of the stress screening guidelines developed from the ESSEH Study (Ref. 2). It is a "working document" that can be used as a quick reference for planning a stress screening program.

Ideally, the parameters of a stress screening program should be optimized for the specific (or similar) equipment on which it is to be implemented, since each equipment has its own population of failure mechanisms peculiar to its parts, processes, packaging, worker skill levels, etc. If preliminary studies for purposes of stress screening planning cannot be performed, these guidelines will prove helpful.
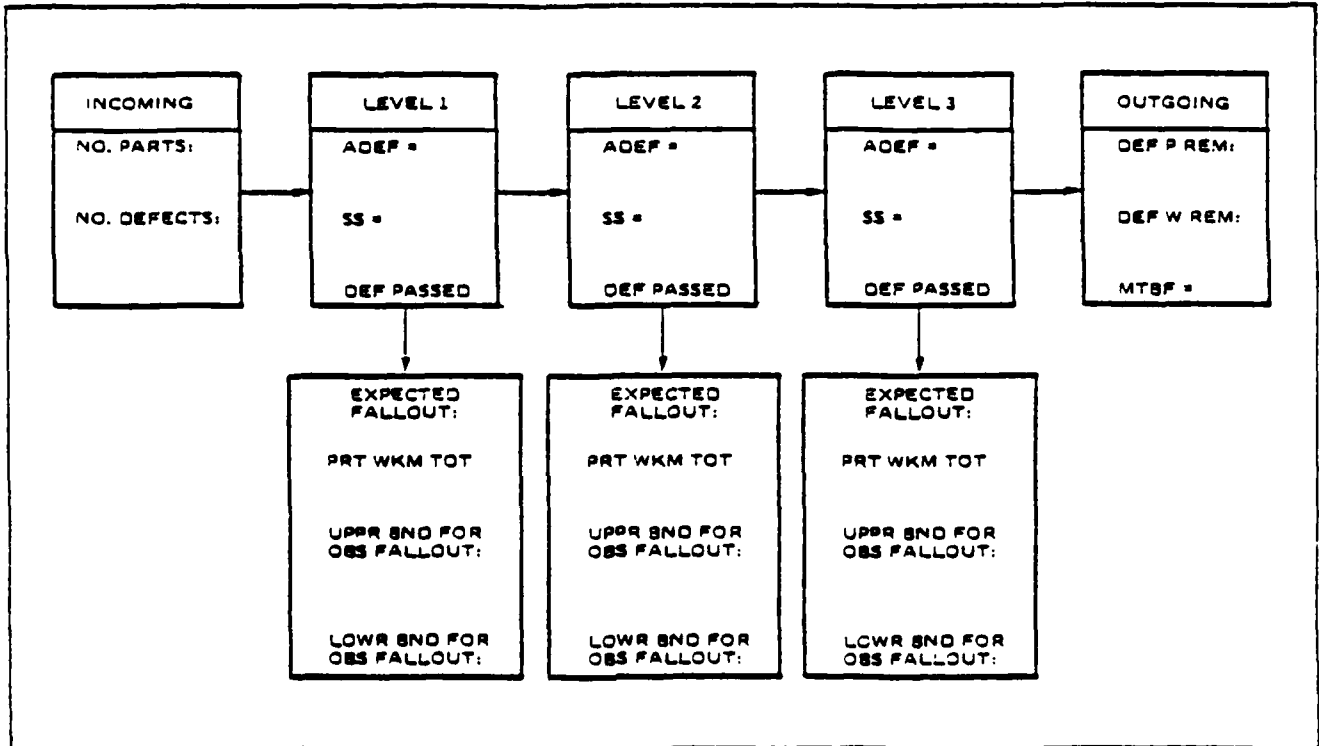
FIGURE 11.2.3.3.1-1: <u>STRESS SCREENING MODEL REPRESENTATION OF THE PRODUCTION FLOW PROCESS.</u>

TABLE 11.2.3.3.2-1: STRESS SCREENING GUIDELINES MATRIX

Stress Environment	Recommended Application	Expected Failure Rate Reduction	Trade-Offs
THERMAL CYCLING, MODULE LEVEL			
o Temp Range	Max: -55 to +125°C (180°C) / Nom: -40 to +95°C (135°C) / Min: -40 to +75°C (115°C)	In-House: 0 to 50% / Field: 20 to 75%	In-house failure rates may in some cases be increased at next assembly level; hence, equipment behavior under proposed stress screening environment should be evaluated prior to implementation.
o Temp Rate	Max: 20°C/min. / Nom: 15°C/min. / Min: 5°C/min.		Temperature rates of change are as measured by thermocouple on components mounted on modules.
o No. of Cycles	Max: 40 / Nom: 30 / Min: 20		Power-ON screening may be continued into early production until latent design problems are exposed and production processes and test procedures are proven.
o Power	Power ON (Devel. Phase) / Power OFF (Produc'n Phase)		Power-OFF screening is considerably cheaper and is effective on mature production hardware.
THERMAL CYCLING UNIT AND SYSTEM LEVEL			
o Temp Range	Max: -55 to +125°C (180°C) / Nom: -40 to 95°C (135°C) / Min: -40 to 75°C (115°C0)	In-House: 0 to 75% / Field: 20 to 90%	In-house failure rate may in some cases be increased at next assembly level; hence, equipment behavior under proposed stress screening environment should be evaluated prior to implementation.
o Temp Rate	Max: 20°C/min. / Nom: 15°C/min. / Min: 5°C/min.		Higher temperature rates may require open-unit exposure with higher air flow rate to overcome slower temperature response of higher mass.
o No. Cycles	Max: 12 / Nom: 10 / Min: 8		Functional testing at high and low temperature increases failures detectability.
o Power	Power ON		

TABLE 1₄.2.3.3.2-1: STRESS SCREENING GUIDELINES MATRIX (Cont'd)

Stress Environment	Recommended Application	Expected Failure Rate Reduction	Trade-Offs
VIBRATION, MODULE LEVEL	Not recommended for non-complex modules		Marginal payoff for non-complex modules whose configurations are not susceptible to vibration environment screening.
	For complex modules, use recommendations for unit and system level.	(See Vibration, Unit and System Level)	For complex modules, refer to unit and system level trade-offs.
VIBRATION UNIT AND SYSTEM LEVEL			
o Vibration Type	Random Preferred	In-House: 0 to 25% Field: 10 to 30%	Techniques for simulationg random vibration may be considered, such as two exciters to produce diagonal force vector excitation or use of pneumatic vibration methods to provide excitation in three axes.
o Vibration Type	Random (Preferred) Swept Sine (Acceptable)		
o Vibration Level and Spectrum (Random)	Spectrum and level - itomized for specific equipment; .045 g²/Hz recommended initial starting level with scaling up and down depending on structural response of test specimen; frequency range approximately 100 to 1000 Hz.		Generalized envelope provides guideline boundaries for acceleration spectra; (see Figure 5-1); for large mass, frequencies below 500 Hz disclose large number of defects; for stiff hardware with low resonant frequency modes above 500 Hz, upper frequency limit may approach 1000 Hz.
			Hardware responses must be large enough for screening to be effective while not exceeding hardware capability; initial response survey required.
			For some equipment, higher levels of random vibration (e.g., 6 g's RMS) may introduce degradation.
o Vibration Level and Spectrum (Swept Sine)	Spectrum and level customized for specific equipment.	In-House: 0 to 15% Field: 10 to 20%	See Figure 5-2 for recommended spectrum for swept sine vibration.

TABLE 11.2.3.3.2-1: STRESS SCREENING GUIDELINES MATRIX (Cont'd)

Stress Environment	Recommended Application	Expected Failure Rate Reduction	Trade-Offs
VIBRATION, UNIT AND SYSTEM LEVEL (Cont'd)			
o Vibration Duration and Number of Axes	10 minutes per axis, 3 axes.		If a particular preference of the equipment for failure modes in one or two axes can be defined, 3 axes may not be required; vibration survey results may be useful in such identification.
THERMAL CYCLING AND VIBRATION COMBINED			
o Applied independently or simultaneously	Use optimized parameters presented above for thermal cycling and vibration.	In-House: 0 to 75% Field: 20 to 90%	Independent application of thermal cycling and vibration will result in effective screening; order of application not found significant insofar as screening effectiveness; screening time may be reduced with simultaneous application; some failure mechanism types may be more sensitive to simultaneous application of the two environments.
Applied Level For Screening	Recommended Application	Expected Failure Rate Reduction	Trade-Offs
o Module	See Trade-offs	In-House: 0 to 50% Field: 20 to 75%	Trade-off factors include: a. level at which failure mechanisms are detectable
o Unit		In-House: 0 to 75% Field: 20 to 90%	b. % of defects detectable at a specific level
o System		In-House: 0 to 75% Field: 20 to 90%	c. feasibility of implementing screening at a specific level d. achievable failure rate reduction versus reliability requirements e. comparative cost savings

The following is a list of the stress screening parameters covered in the Matrix:

    Thermal Cycling
        Temperature Range
        Temperature Rate of Change
        Number of Cycles
        Operating Versus Nonoperating
    Vibration
        Type of Vibration (Sine, Random, etc.)
        Vibration Level (g's)/Spectrum
        Duration
        Number of Axes
    Thermal Cycling and Vibration Combined
        Applied Sequentially
        Applied Simultaneously
    Assembly Level of Screening
        Module
        Unit
        System

For each parameter above, the Matrix contains the following information:

(1) Recommended Application - A brief statement of the form, level, etc., of the parameter found to have provided optimum screening effectiveness

(2) Expected Reduction in Failure Rate - A statement of expected reduction in failure rates achievable in-house or in the field contingent upon performing the screen as recommended

(3) Trade-off Considerations - Identification and brief discussion of implementation and cost trade-offs as related to optimizing the screening factor per the recommendations

The Guidelines are applicable to both the development and production phases, preferred approach being to:

(1) implement a screening program based on the Guidelines during development
(2) refine the screening program parameters during the development phase for use in production
(3) monitor the screening program effectiveness during production and make adjustments as needed to tighten where more effective screening is needed or to reduce when warranted by maturing of system reliability

After evaluating the various options, applying the previously discussed tools and guidelines, and establishing the type and level of tests to be performed, a complete screen test specification should be prepared encompassing the following:

(1) Test sequence and application levels

(2) Test conditions including test duration, number of cycles, failure free criteria, cumulative operating time, and critical electrical parameters
(3) Expected reject or fall-out rates
(4) Test facilities
(5) Special automatic test equipment (ATE)
(6) Data recording requirements and methods
(7) Failure reporting analysis and corrective action procedures
(8) Manpower and training requirements

In addition, if possible, provisions should be included for studies or experiments during the development phase so that the production stress screening plan can be based on established behavior of the specific hardware. The failure free criteria should be made part of acceptance rather than stress screening criteria, and the opportunity should be provided to the contractor to perform preliminary stress screening studies to determine costs related to the requirement. Finally, the data system, supported by failure analysis and corrective action, is important in order to maintain visibility over the effectiveness of the overall plan and of each screen so that adjustments may be made in the plan as necessary to minimize costs and maximize screening effectiveness.

11.2.4 PRODUCTION RELIABILITY ACCEPTANCE TESTING (MIL-STD-781 and MIL-HDBK-781)

Reliability acceptance testing is performed on production hardware to determine compliance to specified reliability requirements. MIL-STD-781 and MIL-HDBK-781 contain all the essential procedures and requirements for specifying an acceptance test plan for equipment that experiences a distribution of times-to-failure that is exponential. This is normally the case for electronic equipment/systems. It defines test conditions, procedures and various test plans, and respective accept/reject criteria.

This standard has recently been completely revised to include detailed information for test planning and evaluation of data. The latest revision has been restructured to make extensive use of appendices to expand and clarify the various sections of the standard. It clarifies the definition of mean-time-between-failures (MTBF) and the use of θ_0 (upper test MTBF) and θ_1 (lower test MTBF), which are test planning parameters, and specifies the use of combined environmental test conditions (temperature, vibration and moisture)* based on the actual mission profile environments encountered during the equipment's useful life.

MIL-STD-781 and MIL-HDBK-781 are not to be invoked on a blanket basis but each requirement shall be assessed in terms of the need and mission profile. Appendices are designed so that the procuring activity may reference them with specific parts of the standard and invoke them in the equipment specification.

*Altitude may be included if the procuring activity determines that it is cost effective, but the cost of test facilities for combining altitude with the other environments would probably not be cost effective.

MIL-HDBK-338-IA

MIL-STD-781 and MIL-HDBK-781 cover requirements for preproduction qualification tests as well as production acceptance tests. Qualification tests are normally conducted after growth tests in the development cycle, using initial production hardware to make a production release decision. It should be emphasized that qualification testing, conducted per MIL-STD-781 and MIL-HDBK-781, is to demonstrate reliability with statistical confidence, whereas reliability growth testing is performed to improve reliability. Depending on program requirements, funding, and other constraints, preproduction testing may maximize growth testing and minimize statistical testing (resulting in a high MTBF at a low confidence) or may minimize growth and maximize demonstration (resulting in a lower MTBF at a high confidence). Preproduction testing, including both reliability growth and qualification, was discussed in detail in Section 8.

Production reliability acceptance tests per MIL-STD-781 and MIL-HDBK-781 are described as "a periodic series of tests to indicate continuing production of acceptable equipment" and are used to indicate individual item compliance to reliability criteria. The tests are intended to simulate in-service evaluation of the delivered item or production lot and to provide verification of the inherent reliability parameters as demonstrated by the preproduction qualification tests.

Therefore, an equipment would undergo qualification testing on preproduction hardware. Once the specified reliability has been demonstrated, then, after production begins, the lots produced would undergo reliability acceptance testing, usually at a level less stringent than the demonstration test level, to indicate continuing fulfillment of reliability requirements.

Production Reliability Acceptance testing per MIL-STD-781 and MIL-HDBK-781 can be performed based on sampling an equipment from each lot produced as well as on all equipment produced. The test conditions, or stress profile, applied during the test should be measured (preferred) or estimated by the procuring activity and incorporated into the equipment specification. However, when the stress types and levels are not specified by the procuring activity and when measured environmental stresses for the proposed application or a similar application are not available for estimating, then the stress types and levels given in Table 11.2.4-1, taken from MIL-STD-781 and MIL-HDBK-781, should be applied. Table 11.2.4-1 provides a summary of combined environmental test condition requirements applicable to the following categories of equipment classification:

Category 1	Fixed ground equipment
Category 2	Mobile ground vehicle equipment
Category 3	Shipboard equipment -sheltered -unsheltered
Category 4	Equipment for jet aircraft
Category 5	Turbo-prop aircraft and helicopter equipment
Category 6	Air-launched weapons and assembled external stores

Figure 11.2.4-1, also taken from MIL-STD-781 and MIL-HDBK-781, illustrates a typical test cycle that shows the timing of the various conditions. MIL-STD-781 and MIL-HDBK-781 describe standard statistical test plans covering:

11-51

TABLE 11.2.4-1: TEST CONDITIONS MATRIX
(Taken from MIL-STD-781 and MIL-HDBK-781)

Summary of Combined Environmental Test Condition Requirements

	FIXED GROUND	GROUND VEHICLE	SHIPBOARD SHELTERED	SHIPBOARD UNSHELTERED
ELECTRICAL STRESS				
Input voltage	Nominal + 5%-2%	Nominal ± 10%	Nominal ± 7%*	Nominal ± 7%*
Voltage cycle	high, nominal and → one per test cycle ————————————————→			
	low			
VIBRATION STRESS				
Type vibration	sinewave	swept-sine	swept-sine**	swept-sine**
	single frequency	log sweep	continuous	continuous
Amplitude	(See APPENDIX B for stress levels)			
Frequency range***	20 to 60 Hz	5 to 500 Hz		
Application	20 minimum per	sweep rate	(See APPENDIX B ————————→)	
	equipment	15 minimum once/hr		
THERMAL STRESS (°C)	A B C ****	LOW HIGH	LOW HIGH	LOW HIGH
Storage temperature	- - -	-54 85	-62 71	-62 71
Operating temperature	20 40 60	-40 TO 55	0 TO 50 (CONTROLLED)	-28 65
Rate of change	- - -	5°/min.	5°/min.	5°/min.
Maximum rate of change	- - -	10°/min.	10°/min.	10°/min.
MOISTURE STRESS				
Condensation	none	1/test cycle	See APPENDIX B	1/test cycle
Frost/freeze		1/test cycle		1/test cycle

	AIRCRAFT FIGHTER	AIRCRAFT TRANSPORT, BOMBER	AIRCRAFT HELICOPTER	AIRCRAFT TURBO-PROP	AIR-LAUNCHED WEAPONS AND ASSEMBLED EXTERNAL STORES
ELECTRICAL STRESS					
Input voltage range	nominal ± 10%	± 10%	± 10%	± 10%	± 10%
Voltage cycle	(nominal, high and low voltage, one cycle/thermal cycle or per APPENDIX B)				
VIBRATION STRESS					
Type vibration	random	random	swept-sine log sweep	swept-sine	swept-sine*** and random
Amplitude	(◄——————— SEE APPENDIX B ————————————————————→)				
Frequency range	20-2000 Hz	20-2000 Hz	5-2000 Hz****	10-2000 Hz	20-2000 Hz
Application	continuous	continuous	sweep rate 15 min, one/hr	continuous (see APPENDIX B)	continuous (see MIL-STD-1670)
THERMAL STRESS (°C)	LOW HIGH	LOW HIGH	LOW HIGH	LOW HIGH	LOW HIGH
Storage temperature (non-oper.)	-54 +71	-54 +71	-54 +71	-54 +71	-65 +71
Operating temperature range	(◄——————— See APPENDIX B ————————————————————→)				
Rate of change (min.)	5°/min.	5°/min.	5°/min.	5°/min.	5°/min.
Duration (nominal)	3 1/2 hours	3 1/2 hours	3 1/2 hours	3 1/2 hours	3 1/2 hours
MOISTURE STRESS					
Condensation	(1/test cycle -)				
Frost/freeze	(1/test cycle -)				

See MIL-STD-1399
See MIL-STD-167-1
*Frequency tolerance ± 2 percent or ± 0.5 Hz for frequencies below 25 Hz.
See 50.1.4 of Appendix B
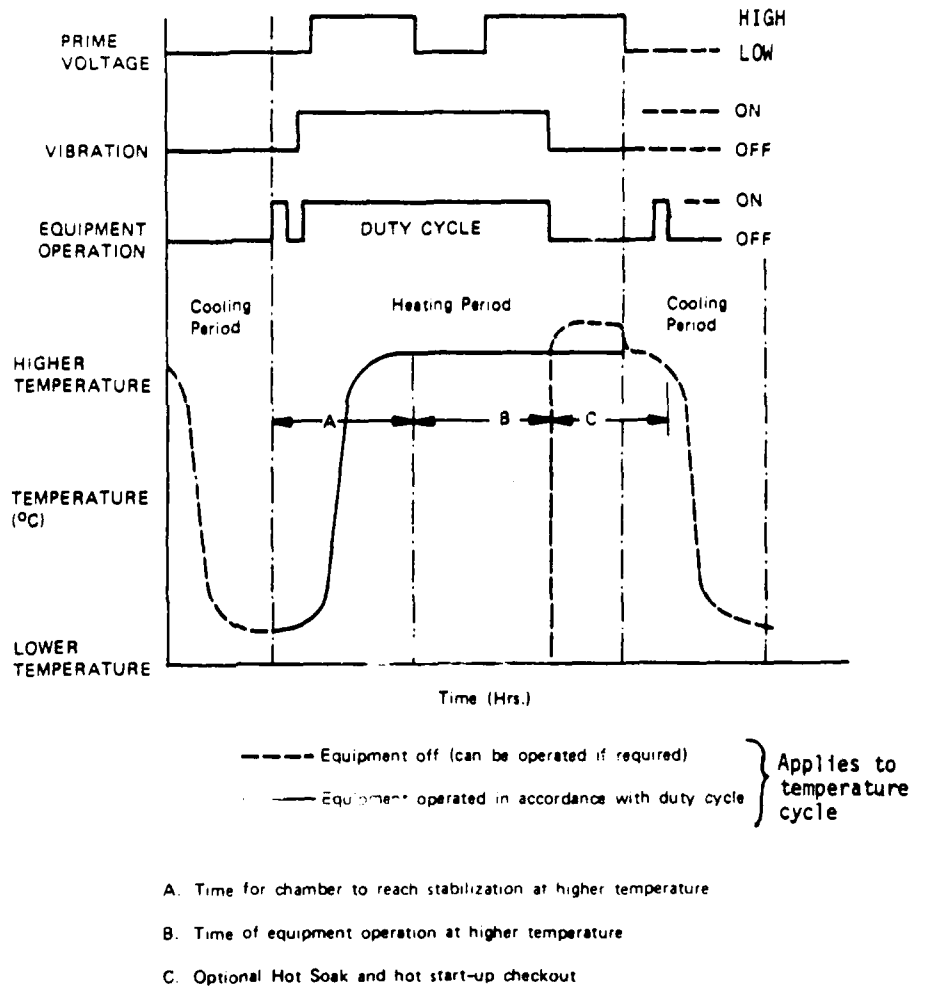
FIGURE 11.2.4-1:   SAMPLE ENVIRONMENTAL TEST CYCLE

(1) Fixed length test plans (Test Plans IXC **through** XVIIC and XIXC *through XXIC*)

(2) Probability ratio sequential tests **(PRST)**, **(Test Plans IC** through VIC)

(3) Short run high risk PRST plans (Test Plan VIIC and VIIIC)

(4) All equipment reliability test (Test Plan XVIIIC)

Accept/reject criteria are established on θ_1 and θ_0, where θ_1, the lower test MTBF, is an unacceptable MTBF based on minimum requirements. θ_0 is the upper test MTBF, or the acceptable MTBF. The ratio θ_0/θ_1 is defined as the discrimination ratio. Specifying any two of these three parameters, given the desired producer and consumer decision risks, determines the test plan to be utilized.

Test Plan XVIIIC, shown in Figure 11.2.4-2, can be used for 100% production reliability acceptance testing. This test plan shall be used when each unit of production (or preproduction equipment if approved by the procuring activity) equipment is to be given a reliability acceptance test. The plan consists of a reject line and a boundary line. The reject and boundary lines are extended as far as necessary to cover the total test time required for production run. The equation of the reject line is $f_R = 0.72T + 2.50$ where T is cumulative test time in multiples of θ_1, f_R is cumulative number of failures. The plotting ordinate is failures and the abscissa is in multiples of θ_1, the lower test MTBF. The boundary line is 5.67 failures below and parallel to the rejection line. Its equation is $f_B = 0.72T - 3.17$.

The test duration for each equipment shall be specified in the test procedure as approved by the procuring activity. The maximum duration may be 50 hours and the minimum 20 hours to the next higher integral number of complete test cycles. If a failure occurs in the last test cycle, the unit shall be repaired and another complete test cycle run to verify repair.

An optional nonstatistical plan can also be used for production reliability acceptance testing. Its purpose is to verify that production workmanship, manufacturing processes, quality control procedures, and the assimilation of production engineering changes do not degrade the reliability, which was found to be acceptable by the reliability qualification test. The test is to be applied to all production items with the item operating (power applied). The required test duration and number of consecutive, failure free, thermal test cycles (minimum of two) which each deliverable item must exhibit is specified by the procuring activity. The vibration, temperature cycling, and moisture environments together with any others which are deemed necessary may be applied sequentially. The equipment duty cycle and the sequence, duration, levels of the environments, and the vibration option to be used in this test require approval of the procuring activity and are submitted in accordance with the test program requirements.

TEST TIME (IN MULTIPLES OF LOWER TEST MTBF, θ_1)
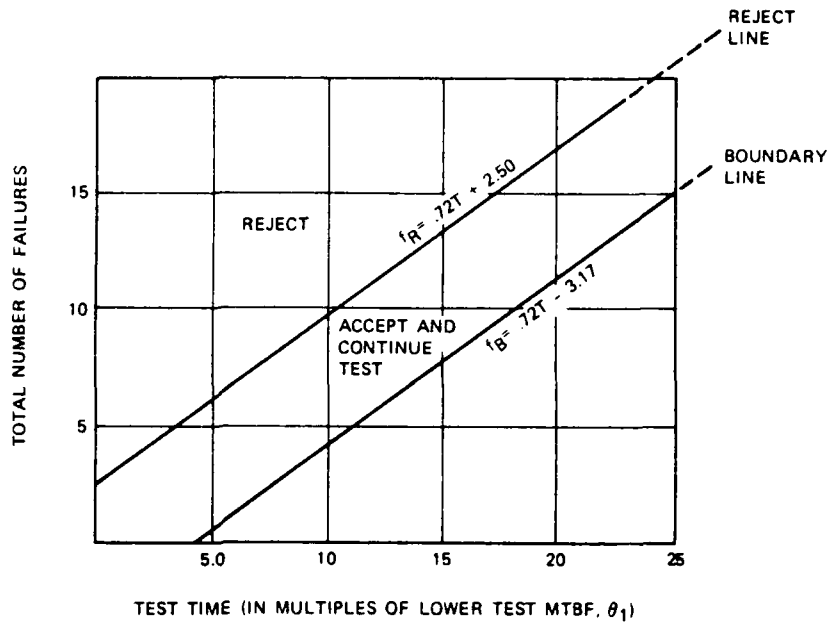
Total Test Time*				Total Test Time*		
Number of Failures	Reject (Equal or less)	Boundary Line		Number of Failures	Reject (Equal or less)	Boundary Line
0	N/A	4.40		9	9.02	16.88
1	N/A	5.79		10	10.40	18.26
2	N/A	7.18		11	11.79	19.65
3	.70	8.56		12	13.18	21.0.
4	2.08	9.94		13	14.56	22.42
5	3.48	11.34		14	ETC	ETC
6	4.86	12.72		15	.	.
7	6.24	14.:0		16	.	.
8	7.63	15.49		.	.	.

* Total test time is total unit hours of equipment on time and is expressed in multiples of the lower test MTBF
Refer to 4.5.2.4 for minimum test time per equipment.

FIGURE 11.2.4-2: **REJECT-ACCEPT CRITERIA FOR TEST PLAN XVIIIC**

MIL-STD-785, incorporates the requirements of MIL-STD-781 and MIL-HDBK-781. It must be emphasized that test criteria, including confidence level or decision risk, should be carefully selected and tailored from 781 to avoid driving cost or schedule without improving reliability. Appendix A to MIL-STD-785 provides the following general guidelines for planning and implementing production reliability acceptance testing:

"Production reliability acceptance testing must be operationally realistic, and may be required to provide estimates of demonstrated reliability.

The statistical test plan must predefine criteria of compliance ("accept") which limit the probability that the item tested, and the lot it represents, may have a true reliability less than the minimum acceptable reliability, and these criteria must be tailored for cost and schedule efficiency.

Production reliability acceptance testing may be required to provide a basis for positive and negative financial feedback to the contractor, in lieu of an in-service warranty.

Because it must simulate the item life profile and operational environment, production reliability acceptance testing may require rather expensive test facilities; therefore, all equipment production reliability acceptance testing (100% sampling) is not recommended.

Because it must provide a basis for determining contractual compliance, and because it applies to the items actually delivered to operational forces, production reliability acceptance testing must be independent of the supplier, if at all possible.

Finally, even though sampling frequency should be reduced after a production run is well established, the protection that production reliability acceptance testing provides for the government (and the motivation it provides for the contractor's quality control program) should not be discarded by complete waiver of the production reliability acceptance testing requirement."

Plans for performing production reliability acceptance testing are prepared and incorporated into the overall reliability test plan document. The plans encompass the following considerations:

(see Task 304, MIL-STD-785):

(1) Tests to be conducted per MIL-STD-781 and MIL-HDBK-781.

(2) Reliability level (i.e., MTBF) to be demonstrated and the associated confidence level, and the relationship between demonstrated MTBF, confidence, test time, etc.

(3) Representative mission/environmental profile.

(4) The number of units for test, expected test time, calendar time factors, and scheduling of effort.

(5) The kinds of data to be gathered during the test.

(6) Definition of failure (relevant, nonrelevant).

(7) Authorized replacement and adjustment actions.

(8) Logs/data forms to be maintained that record number of units on test, test time accumulated, failures, corrective actions, statistical decision factors, and accept/reject criteria.

11.2.5 DATA COLLECTION AND ANALYSIS (DURING PRODUCTION)

The production reliability test and control program once implemented in the factory should continually be challenged relative to the effectiveness of the overall program, as well as that of the individual tests. Production screening and acceptance testing is a dynamic process which must be continually modified in response to experience. Test results and field experience data are monitored to determine the need to modify individual test criteria and conditions to reduce the sampling frequency of acceptance tests and to identify the possibility of applying earlier screen tests where the test costs are less and the potential for cost avoidance is higher. It should be emphasized that the production program, as initially planned, represents a baseline for applying the tests. A production screen test, for example, like any quality inspection must be adjusted depending on the results of subsequent higher level tests or field performance. However, the extent and nature of any changes should be determined only through careful review and analysis of the subsequent failures.

A data system supported by failure analysis and corrective action is established to maintain visibility over the effectiveness of the production test program as well as all tests including development, qualification, and production. The data system is designed to compile test and failure data and to provide information that would provide a basis to change the test program as necessary to minimize cost and maximize effectiveness. A failure reporting, analysis and corrective action system (FRACAS) is an essential element of the production test program as well as the overall reliability control program. It must meet the requirements of MIL-STD-785 and in particular the failure recording and analysis requirements of MIL-STD-781 and MIL-HDBK-781 to the extent specified in the applicable program and/or test plan. A well designed FRACAS system will provide a uniform mechanism for reporting failures, determining causes and remedies, and making these findings known to the appropriate engineers and designers to enable them to formulate and implement corrective action and, specifically, to ascertain whether or not to design and implement improved inspection, screening and acceptance tests.

Section 8 of the handbook describes failure reporting, analysis, corrective action, and the provisions necessary to assure that failures are accurately reported, thoroughly analyzed, and that corrective actions are taken on a timely basis to reduce or prevent recurrence.

The results of production acceptance test, screening and inspection results, as well as failure reports and analyses from the FRACAS program, are compiled and incorporated into the data system. Maintaining accurate and up-to-date records through a formal data recording and analysis system is particularly essential in tracking and assessing field reliability performance. Comparative evaluation between predicted reliability estimates and actual field reliability provides criteria for improving production acceptance testing (including the screening and burn-in testing procedures) to assure that the most cost effective test program is developed and applied. This is especially important for new systems where changing performance and reliability characteristics would be expected as a result of design and manufacturing improvements.

A properly designed and operating data system would provide the following information as it pertains to production testing:

    (1) Identification of hardware subjected to production tests
    (2) Total cumulative operating time for each hardware item including the last operating time interval of failure free operation and acceptance test completion dates
    (3) Sampling frequency of reliability acceptance tests
    (4) Failure reports of hardware discrepancies including description of failure effects and accumulated operating hours to time of failure
    (5) Failure analysis reports of hardware discrepancies including cause and type of failure modes

Also, cumulative plots of screening and burn-in failure events versus time can be prepared and maintained and periodic summary reports submitted to engineering and management activities that provide:

    (1) Failure/reject rates by test type and level
    (2) Screen test efficiency factors
    (3) Responsible failure mechanisms
    (4) Recommended or accomplished corrective actions
    (5) General product reliability analysis that correlates design predictions with test results and field experience

11.3 PRODUCTION MAINTAINABILITY CONTROL

11.3.1 INTRODUCTION

As was previously indicated for reliability, the inherent design maintainability of an equipment/system can be degraded during production unless adequate controls are specified and applied to prevent this degradation.

It is the responsibility of the procuring activity to insure that the production contractor is made responsible for reproducing and upholding the level of inherent design maintainability represented by the specifications and drawings released with the production contract. This responsibility includes: definition and maintainability control criteria; design and application of control procedures; collection, analysis, and feedback of production test results and maintenance data

for discrepancy recurrence control; and integration of these functions into the contractor's overall plans for configuration management, quality control, test and evaluation, and logistic support. It is the function of the contractor's maintainability assurance engineering staff to translate maintainability features of the design into control criteria adaptable to these production activities.

11.3.2 MAINTAINABILITY DESIGN ATTRIBUTES

Inherent maintainability in a given design is achieved by careful consideration and optimum balance among the following factors. Preservation of this balance in production can be assured only when each attribute is described in production specifications and drawings to establish the product baseline maintainability configuration.

    (a) Basic physical configuration and layout of the design for quick and easy access for maintenance

    (b) Test provisions for quick and accurate fault localization and failure isolation to the replaceable item level

    (c) Use of methods for quick disconnecting, interconnecting, connecting, and hold-down of replaceable items for easy removal and replacement

    (d) Interchangeability of replaceable items for minimum adjustment and alignment during or following replacement

    (e) Provisions for rapid post-maintenance checkout to verify restoration to specified performance levels

    (f) Utility of standard test equipment and tools for maintenance

    (g) Adequacy, clarity, and simplicity of maintenance procedures, instructions, and documentation

    (h) Compatibility of available skill levels and technician training to perform the maintenance tasks unique to the design

11.3.3 MAINTAINABILITY CONTROL PARAMETERS

The following procedures are applicable for the identification and definition of equipment design attributes whose control is critical to the preservation of achieved maintainability. The procedures should be used by the production contractor when production specifications and drawings or supplemental maintainability assurance provisions do not reflect complete evaluation and adequate translation of maintainability design attributes into quality assurance requirements.

Step I Identify Primary Sources of Maintenance Downtime

Maintenance downtime attributable to time required to gain access to failure, physically replace the faulty item, reassemble equipment following repair, and adjust and align the repaired equipment to the specified level of performance is usually related in a direct way to

physical functional, or interface characteristics of equipment and replaceable item design. As the starting point for the design and application of suitable production controls, the maintenance task time analysis performed in prediction studies or test data analysis should be reviewed to identify the sources of maintenance downtime attributable to these manual and manipulative tasks.

Consider as a simplified example the maintenance tasks associated with replacement of a hypothetical hydraulic pump, depicted in Figure 11.3.3-1. As indicated in the figure, replacement involves the following manual tasks: (1) remove four hold-down stud bolts which fasten the pump to the hydraulic servo assembly; (2) disconnect two stainless steel hydraulic lines; (3) loosen two allen-head set screws in the motor-to-pump shaft coupling; (4) pull the pump away from the drive motor to disengage the pump shaft from the coupling. Install the replacement pump by reversal of these steps.

The distribution of maintenance task times for the example pump replacement action is summarized in Figure 11.3.3-2. On the average, over half of the maintenance downtime in this action is in the replacement task itself.

Step 2 Define Quantitative Inspection Criteria for Production Control

The physical characteristics, functional parameters, and interface tolerances related to primary sources of downtime identified in Step 1 should be determined. A sensitivity analysis of the test data should be made when a cause-effect relationship cannot be established between critical parameter variation and maintenance task time variation.

Assume, for example, that the major portion of repair time in the pump example is attributable to the pump shaft binding in the drive motor coupling, making Task 4 (pump shaft removal) difficult and time consuming. For the same reason, installation of a new replacement pump is difficult in that the shaft-to-coupling interface tolerances on diameter are not satisfied. Test data reveals that control of pump shaft outside diameter and shaft coupling inside diameter to the limits shown in Figure 11.3.3-3 will reduce pump replacement mean time from 36 minutes to 10 minutes.

11.3.4 MAINTAINABILITY ASSURANCE TASKS IN THE PRODUCTION PHASE

The ideal production phase starts with the release of an adequate procurement package consisting of detailed specifications and drawings for hardware production. In the ideal situation, development models of the equipment will have demonstrated conformance to specified maintainability and other operational requirements established in the production baseline specification and drawing package.

The production phase is initiated with a preproduction period in which the contractor develops, applies, and refines his fabrication and assembly techniques, process and workmanship instructions, configuration and change control procedures, parts and materials inspection and testing procedures, and maintainability control procedures and criteria. During this preproduction period, a limited number of equipments are produced for test and evaluation before full-scale production begins.
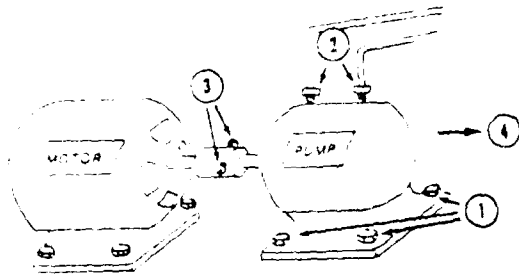
FIGURE 11.3.3-1: MAINTENANCE STEPS IN EXAMPLE REPLACEMENT ACTION

Maintenance Task	Observed Range of M_{ct_i} (Min)	$\overline{M}_{ct_i}$
Fault Detection	5 - 10	7
Fault Isolation	3 - 5	4
Gaining Access	7 - 12	8
Pump Replacement	20 - 60	36
Reassembly	8 - 15	10
Adjustment and Alignment	0 - 2	1
Checkout	2 - 5	4
Mean Corrective Time		70

FIGURE 11.3.3-2: DISTRIBUTION OF MAINTENANCE TASK STEPS
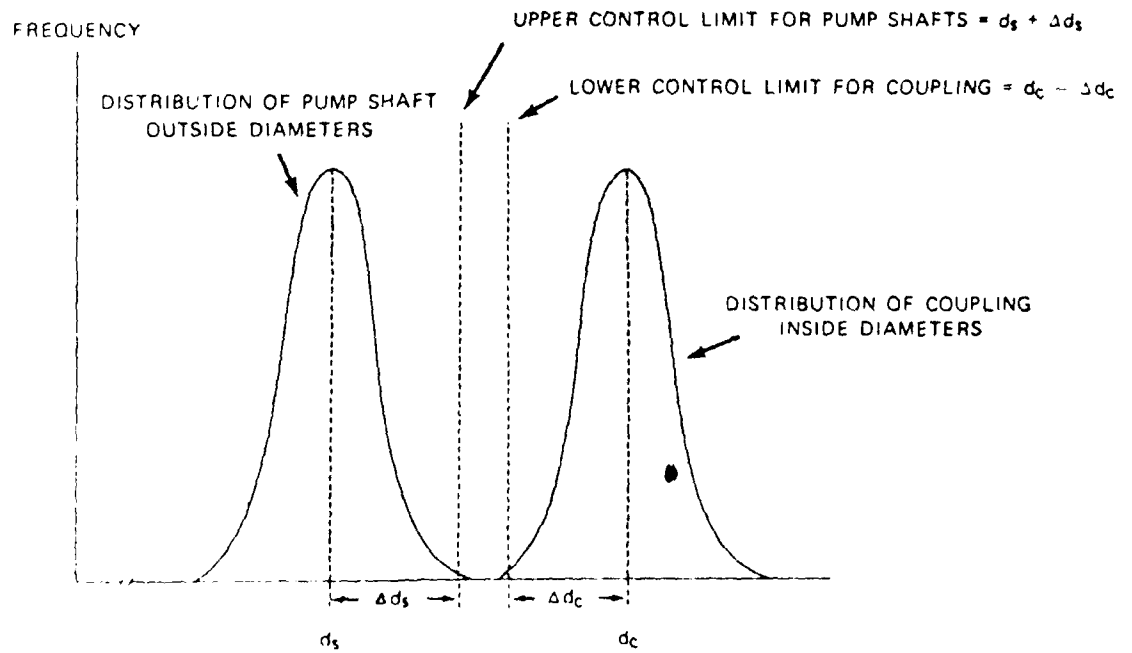
FIGURE 11.3.3-3: DERIVATION OF CONTROL LIMITS FOR INTERFACING PARAMETERS

11-61

These first articles are inspected and tested to ensure that operational features (including maintainability) of the equipment design have been reproduced and to verify adequacy of manufacturing controls to prevent degradation of these design features in full scale production. Tests of preproduction units usually include operational evaluation conducted in a preplanned operational environment to verify suitability of the equipment for deployment. Deficiencies found during the test are corrected by engineering changes whose effect on maintainability is evaluated in the engineering change proposal (ECP) phase prior to their incorporation in follow-on production.

As full scale production is implemented, the first items produced are again inspected and tested to ensure that maintainability features of the pilot models, including changes thereto, have been successfully reproduced in the production model. Maintainability controls are applied at inspection and test stations throughout the production flow, and maintainability criteria are integrated into Government acceptance tests. Deficiencies in maintainability control noted during these tests are corrected through appropriate changes in production techniques, process controls, workmanship standards, tooling, etc.

Data subsequently collected by the maintenance data collection system from deployed units is analyzed and applied to identify and correct maintainability problem areas attributable to inadequate production methods or control procedures. Design deficiencies are also identified in the data analysis for corrective action decisions by the procuring activity. All approved changes are appropriately documented to maintain the production data package up-to-date with the current approved configuration.

Review of the idealized production cycle identifies certain primary maintainability assurance tasks which must be formally assigned and diligently executed to provide effective control of maintainability in production:

(1) Definition of Control Requirements. Translate maintainability features and critical areas of the design into measurable parameters and inspection and test criteria amenable to control by inspection and test procedures applied in the production line.

(2) Test Design. Define inspection and test requirements, procedures, conditions, instrumentation, etc., for control of these maintainability dependent parameters.

(3) Inspection and Test. Incorporate inspection and test criteria in applicable work instructions, incoming inspection procedures, etc.; perform inspection and test of parts and materials, manufacturing processes and fabrication workmanship, handling, packing, shipping, etc., to verify conformance to maintainability criteria incorporated in work instructions.

(4) Acceptance Test. Incorporate maintainability acceptance criteria into Government acceptance tests for the product, and perform these tests in accordance with contract requirements.

(5) Maintenance Data Reporting. Establish (or integrate into existing R&QA reporting system) provisions and procedures for recording, reporting, storage and retrieval, and computer processing of performance data from production tests, acceptance tests, and fleet experience. This data reporting system should become the nerve center of the production maintainability control program.

(6) Data Analysis. Perform statistical analysis and engineering evaluation of production test and inspection data, acceptance test results, and field experience data to verify adequacy of maintainability control procedures. Identify and describe problem areas, and prescribe appropriate corrective action and recurrence control measures.

(7) Engineering Evaluation. Make engineering investigation of maintainability problems attributable to design, support equipment, maintenance procedures, manuals, training, logistics, and other nonproduction oriented causes. Provide maintainability engineering support in the evaluation of improvement alternatives and tradeoffs and in the preparation of engineering changes which would solve these problems.

(8) Change Proposal Review. Provide support to configuration management and change control activity by reviewing proposed changes to production processes and manufacturing methods, engineering change proposals, proposed changes to production plan and control procedures, etc., to evaluate probable impact of these changes on maintainability.

(9) Maintainability Status Reporting. Prepare production maintainability reports describing results of the foregoing tasks and statistical trends in control data to provide a basis for management decision and overall direction.

11.3.5 RELATIONSHIP OF MAINTAINABILITY ASSURANCE TO THE QUALITY PROGRAM

In Section 11.2.1, the importance of quality control was discussed in terms of its applicability to minimizing reliability degradation during production. The same relationship holds for maintainability control during production. Inspection and test criteria for production maintainability control for the most part can be defined in quality terminology and integrated with quality control inspection and quality conformance procedures.

Provisions of MIL-Q-9858 are outlined in the paragraphs which follow to show how with maintainability engineering support the actual execution of maintainability assurance tasks defined in the previous section can be integrated into the contractor's quality program.

Initial Quality Planning for Maintainability. MIL-Q-9858 requires the contractor to identify and provide the special controls, processes, test equipment fixtures, tooling, and skills needed for assuring product quality where maintainability is defined as a quality attribute. Under this provision and with maintainability engineering support, requirements for maintainability testing (including test equipment, test procedures, test conditions, etc.) can be planned as part of the quality program prior to initiation of production.

Integration of Maintainability Criteria into Work Instructions. With maintainability engineering support, the MIL-Q-9858 quality program can assure that all work affecting maintainability is properly described and documented in work instructions and manufacturing control documents. These instructions are thus made to include provisions for supervising and inspecting the manufacturing work operations affecting maintainability. Work instructions must be kept current and complete and must be updated as necessary with each engineering change. The maintainability engineering activity must distinguish those work instructions affecting maintainability from those involving safety and other parameters and must periodically verify that they are being carried out and that they are not depreciated in the conduct of the quality program.

Data Reporting. When maintainability assurance requirements are translated into quality criteria, maintainability data is automatically included in the contractor's quality program data reporting system. The reporting system is a major operation for a production contractor. It often includes a data center together with an automated process for data storage and retrieval and provides for the analysis and use of the data as a basis for corrective action. Maintainability data for a repair operation in the field can be checked against factory records relating to the particular item to identify discrepancies in production processes or quality control procedures. Data reported into the system include the following:

(1) Records of inspections and tests, including verification of independent examinations by subcontractors and suppliers

(2) Records of work accomplished, including compliance or noncompliance with instructions

(3) Records of changes in suppliers and the level of quality attained by each

(4) Records of customer returns

(5) Field complaints, including failures in use, etc.

Corrective Action. MIL-Q-9858 specifies that the quality program must correct conditions adverse to quality (including maintainability). Corrective action is extended to the performance of suppliers and vendors and includes examination of the product or material involved, analysis of data, analysis of trends relating to nonconforming products or

processes, and the introduction of fundamental improvements. Corrective action is applied by the quality program to out-of-control processes, workmanship errors, inspection discrepancies, and other quality control problems. Corrective action for maintainability problems attributable to design deficiencies and other non-QA sources is referred to the maintainability engineering activity for investigation.

Drawings, Documentation, and Changes Which Affect Maintainability. MIL-Q-9858 requires the contractor to assure adequacy and currency of specifications and drawings. His configuration and change control procedure must ensure that approved changes are incorporated in these documents and that obsolete drawings are removed from all points of issue and use. Supplementary documents must also be closely controlled under the contractor's change control procedures. These include work instructions and documents for fabrication, service, inspection, test, packaging, identification, etc., and maintenance handbooks and general service instructions, preparation and control of which require support of the contractor's maintainability engineering activity.

Maintainability Measuring and Testing Equipment. MIL-Q-9858 requires that the contractor's quality program provide for maintenance of gauges and other measuring and testing devices necessary to ensure that supplies conform to specified requirements. The specification also requires that the devices be calibrated against prescribed standards at specified periods. The contractor's metrology facility must be adequate to maintain test equipment accuracy consistent with the requirements of the materials and equipment being measured. All test facilities and measurement equipment used in the testing and control of specified maintainability parameters are included in this general system of equipment control.

Control of Subcontractors and Vendors. The contractor's quality program is responsible, under provisions of MIL-Q-9858, for ensuring that supplies and services procured from subcontractors and vendors conform to contractor requirements. He must develop and apply procedures for selecting sources properly qualified for supplying parts and materials, both for equipment production and for necessary spares. The contractor is also required to establish procedures for assuring that parts and materials produced by the suppliers continuously meet specified requirements, including those related to equipment maintainability. This task will usually be accomplished by means of acceptance sampling in accordance with MIL-STD-105 or MIL-STD-414, as appropriate, either conducted by the contractor's incoming inspection department or conducted by the supplier and verified by the contractor. The quality program must also ensure that test data from subcontractor and vendor products is accumulated and recorded to provide traceability in the event of a production problem involving these products.

Manufacturing Control of Maintainability. When maintainability is defined as a quality attribute and expressed in terms amenable to control by quality control procedures, the quality program under MIL-Q-9858 ensures that all manufacturing operations affecting maintainability

are properly controlled. This includes handling of materials; are properly controlled. This includes handling of materials; processing and assembly operations; inspection and testing; handling, storage and delivery of the completed equipment; and provisions for maintenance during production, prior to delivery.

11.4 RELIABILITY AND QUALITY DURING SHIPMENT AND STORAGE

Electronic components and equipment are subject to change, deterioration and performance degradation during shipment and while in storage. Consequently, the identification of significant defects, the quantification of the rate of defects, and the analysis of deterioration influenced by shipment and storage environments, dormancy, storage testing, and environmental cycling effects are essential to minimize performance degradation and to assure the designed hardware reliability. Specific inspections and analyses to predict the effects of shipment and storage, to assess the in-storage functional status of component and equipment items, and to control deterioration mechanisms are performed as part of the overall life-cycle reliability program. Included are efforts applicable to:

(1) New Items -- determine the effects of shipment, storage and handling on reliability per Task 209 of MIL-STD-785

(2) Items in Storage -- generate storage reliability control techniques covering receipt, storage and prior-to-issue phases of material and equipment items

The control efforts include identifying components and equipment (and their major or critical characteristics) which deteriorate during shipment and with storage age and preparing procedures for in-storage cycling inspection to assure reliability and readiness. The inspection procedures are to identify the quantity of items for test and the acceptable levels of performance for the parameters under test. Results of these efforts are used to support long term failure rate predictions, design trade-offs, definition of allowable test exposures, retest after storage decisions, packaging, handling, or storage requirements, and refurbishment plans.

11.4.1 FACTORS CONTRIBUTING TO RELIABILITY DEGRADATION DURING SHIPMENT & STORAGE

Defects can be induced during shipment because (1) the packing protection was not compatible with the mode of transportation, (2) container or other packaging material did not meet specification requirements, or (3) the equipment was roughly handled or improperly loaded. Electronic components age and deteriorate over long storage periods due to numerous failure mechanisms. In particular, the electrical contacts of relays, switches, and connectors are susceptible to the formation of oxide or contaminant films or to the attraction of particulate matter that adheres to the contact surface, even during normal operation. During active use, the mechanical sliding or wiping action of the contacts is effective in rupturing the films or dislodging the foreign particles in a manner which produces a generally stable, low resistance contact closure. However, after long periods of dormant

storage, the contaminant films and/or the diversity of foreign particles may have increased to such an extent that the mechanical wiping forces are insufficient for producing a low resistance contact.

The formation of contaminant films on contact surfaces is dependent on the reactivity of the control material, its history, and the mechanical and chemical properties of the surface regions of the material. Gold is normally used whenever maximum reliability is required, primarily because gold is almost completely free of contaminant oxide films. Even gold, however, is susceptible to the formation of contaminant films by simple condensation of organic vapors and the deposition of particulate matter. Silver is highly susceptible to the sulfide contaminants that abound in the atmosphere, as are alloys of copper and nickel. Shipping and storage of these systems in paper boxes should be avoided because of the effects of sulfur containing paper. Particulate contamination can also lead to corrosive wear of the contact surfaces when the particle is hygroscopic. With this condition, water will be attracted to the contact surface and can lead to deterioration through corrosive solutions or localized galvanic action. The source of such particles can be directly deposited airborne dust or wear debris from previous operations.

Another failure mode which may become significant after long term storage is the deterioration of lubricants used on the bearing surfaces of relays, solenoids, and motors. Lubricants can oxidize and form contamination products. Similarly, lubricants can also attract foreign particles, particularly when exposed to airborne dust, and can lead to lubrication failures and excessive wear.

Over a period of time, many plastics (such as those used in the fabrication of electronic components, i.e., integrated circuits, capacitors, resistors, transistors, etc.) lose plasticizers or other constituents which may evaporate from the plastic, causing it to become brittle and possibly shrink. This can cause seals to leak, insulation to break down under electrical/mechanical stress, and other changes conducive to fatigue and failures. Additionally, plastics may continue to polymerize after manufacture. That is, the structure of the molecules may change without any accompanying change in chemical composition. This will result in change in characteristics and physical properties.

Many materials slowly oxidize, combine with sulfur or other chemicals, or break down chemically over a period of time. These changes may affect electrical resistivity, strength, etc. In addition, many of these materials when exposed to condensed moisture or high humidity conditions may through a leaching process lose essential ingredients such as fire retardant additives, thereby causing a hazard to slowly develop.

Many component parts and assemblies are sensitive to contaminants and, thus, are sealed during manufacture. These seals will often leak, partly as a result of flexing due to changing temperature and atmospheric pressure, allowing air, moisture or other contaminants to reach the active portions of the component. This leakage can be so slow that the effects may not be discernible for years, but ultimately significant changes can occur.

Finally, the methods/materials of preservation, packaging, and packing (PP&P) used in the storage of components and equipment, i.e., cardboards, plastic bags, polystyrenes, etc., themselves may react with the items of storage and cause decomposition and deterioration when left dormant for long durations.

Rough handling during shipment and depot operations, aging, and deterioration mechanisms as discussed above can, if uncontrolled, lead to a variety of component and equipment failure modes. A summary of some of the failure modes encountered with electronic components during storage is given in Table 11.4.1-1. Protective measures must be applied to isolate the components from the deteriorative influences in order to eliminate or reduce failure modes such as those listed in Table 11.4.1-1 and others that can be induced during shipment and storage.

11.4.2 PROTECTION METHODS

Proper protection against damage and deterioration to components and equipment during shipment and storage involves the evaluation of a large number of interactive factors and the use of tradeoff analysis to arrive at a cost effective combination of protective controls. These factors can be grouped into three major control parameters: (1) the level of preservation, packaging and packing (PP&P) applied during the preparation of material items for shipment and storage; (2) the actual storage environment; and (3) the need and frequency of in-storage cyclic inspection. These parameters, as depicted in Figure 11.4.2-1 (circled numbers), must be evaluated and balanced to meet the specific characteristics of the individual equipment and materiel items. The significance of each of the three parameters is as follows:

(1) Preservation, packaging and packing (PP&P) is the protection provided in the preparation of materiel items for shipment and long term storage. Preservation is the process of treating the corrosible surfaces of a material with an unbroken film of oil, grease, or plastic to exclude moisture. Packaging provides physical protection and safeguards the preservative. In general, sealed packaging should be provided for equipment, spare parts, and replacement units shipped and placed in storage. Packing is the process of using the proper exterior container to ensure safe transportation and storage.

Various levels of PP&P can be applied, ranging from complete protection against direct exposure to all extremes of climatic, terrain, operational, and transportation environments (without protection other than that provided by the PP&P) to protection against damage only under favorable conditions of shipment, handling and storage. A military package as defined per MIL-E-17555 is the degree of preservation and packing which will afford adequate protection against corrosion, deterioration, and physical damage during shipment, handling, indeterminate storage, and worldwide redistribution. A minimum military package is the degree of preservation and packaging which will afford adequate protection against corrosion, deterioration and physical damage during shipment from supply source to the first receiving activity, for immediate use or controlled humidity storage. Many times a minimum military package conforms to the supplier's commercial practice.

TABLE 11.4.1-1: FAILURE MODES ENCOUNTERED WITH
ELECTRONIC COMPONENTS DURING STORAGE

COMPONENT	FAILURE MODES
Batteries	Dry batteries have limited shelf life. They become unusable at low temperatures and deteriorate rapidly at temperatures above $35^{\circ}C$. The output of storage batteries drops as low as 10 percent at very low temperatures.
Capacitors	Moisture permeates solid dielectrics and increases losses which may lead to breakdown. Moisture on plates of an air capacitor changes the capacitance.
Coils	Moisture causes changes in inductance and loss in Q. Moisture swells phenolic forms. Wax coverings soften at high temperatures.
Connectors	Corrosion causes poor electrical contact and seizure of mating members. Moisture causes shorting at the ends.
Relays and Solenoids	Corrosion of metal parts causes malfunctioning. Dust and sand damage the contacts. Fungi grow on coils.
Resistors	The values of composition-type fixed resistors drift, and these resistors are not suitable at temperatures above $85^{\circ}C$. Enameled and cement-coated resistors have small pinholes which bleed moisture, accounting for eventual breakdown. Precision wire-wound fixed resistors fail rapidly when exposed to high humidities and to temperatures at about $125^{\circ}C$.
Semiconductors, Diodes, Transistors, Microcircuits	Plastic encapsulated devices offer poor hermetic seal, resulting in shorts or opens caused by chemical corrosion or moisture.
Motors, Blowers, and Dynamotors	Swelling and rupture of plastic parts and corrosion of metal parts. Moisture absorption and fungus growth on coils. Sealed bearings are subject to failure.
Plugs, Jacks, Dial-Lamp Sockets, etc.	Corrosion and dirt produce high resistance contacts. Plastic insulation absorbs moisture.
Switches	Metal parts corrode and plastic bodies and wafers warp due to moisture absorption.
Transformers	Windings corrode, causing short or open circuiting.

New Components
& Material Items

Field
Returns

From
Maintenance

Transfers
(Other Depots)

① Protective PP&P
Military,Commerical,etc

Ship-
ment to
Depot

Receiving
Inspection

Trade-off
Analysis

② Storage Space

Controlled Heated Unheated Shed Open

Depot
Handling
and
Inspection
Flow

③ Instorage Cyclic Inspection
• Frequency (6-60 months)
• Type
  - Visual
  - Functional

Withdrawal
(from storage)

Inspection
Prior to Issue

① Protective PP&P
if req'd

Ship-
ment to
Field

FIGURE 11.4.2-1: PROTECTIVE CONTROL DURING SHIPMENT AND STORAGE

(2) The storage environment can vary widely in terms of protection afforded. However, whenever possible electronic hardware should be stored in dry, well ventilated warehouses, where the temperature of the air surrounding the equipment can be regulated so that it does not fall to dewpoint values at night. Storage in controlled temperature/humidity buildings is of course, ideal. If equipment is stored in bins, it is important that it be placed above floor level. The military has several types of storage areas. These include warehouse space with complete temperature and humidity control, warehouse space with no humidity and temperature control, sheds, and open ground areas that are simply designated for storage.

(3) In-storage scheduled cyclic inspection is the key to assuring the actual reliability of components and equipment during storage. In-storage cycling inspections are designed to detect performance degradation, deterioration, and other deficiencies caused by extended periods of storage and improper storage methods. The inspections are to identify those items which require corrective packaging (or further storage control) or condition reclassification to a lesser degree of serviceability. The inspections are performed at intervals derived from shelf life periods and the level of protective packaging and storage afforded the material items. It should be noted that all items when originally placed in storage are ready for issue and that all applicable preservation, packaging and packing (PP&P) requirements have been met. In-storage cycling inspection is part of the depot's overall inspection system (see Figure 11.4.2-1) that includes inspection of items at receipt as well as prior to issue.

In general, shipment and storage degradation can be controlled in terms of the above mentioned three parameters. The planning and specification of shipment and storage requirements for new component and equipment items (as well as the reestablishment of requirements for existing items in storage) must take into account economic choices between the various factors within these parameters to arrive at the most cost effective balance that meets reliability and readiness objectives.

11.4.3 SHIPMENT AND STORAGE DEGRADATION CONTROL (STORAGE SERVICEABILITY STANDARDS)

Since electronic components and equipment are subject to damage, deterioration and performance degradation if unprotected during shipment and left uncontrolled for long periods of dormant storage, organizations have established programs to control the parameters defined above. The Army, for example, has established the Care of Supplies in Storage (COSIS) program (Ref. 9). The program assures that material is maintained in a condition to meet supply demands at a minimum cost in funds, manpower, facilities, equipment, and materials. COSIS by definition is "a Department of the Army (DA) program to perform specific

tasks to assure that the true condition of material in storage is known, properly recorded, and the materiel is provided adequate protection to prevent deterioration. The distinction between COSIS-related actions and actions that might otherwise fall into the broad category of care given materiel in storage is that COSIS concerns itself with the in-storage inspection, minor repair, testing, exercising of materiel and the preservation, packaging and packing (PP&P) aspects of the efforts."

A major and most significant element within the COSIS program is the Storage Serviceability Standards (SSS) documents controlled by participating Army commodity commands as required by DARCOM-R 702-23, "Product Assurance - Storage Serviceability Standards (SSSs)," (Ref. 10). The SSS documents consolidate and establish the depot quality control and reliability management procedure for assuring materiel readiness. They contain mandatory instructions for the inspection, testing, and/or restoration of items in storage. They encompass preservation, packaging, packing (PP&P) requirements, storage environment criteria, as well as inspection requirements during the storage cycle to determine materiel serviceability and the degree of degradation that has occurred. They are applicable to shelf life items as well as all items that are considered sensitive to shipment and storage deterioration. In the case of shelf life items, specifically those items whose shelf life is considered extendible, the standards are used to determine if the items have retained their original characteristics and are of quality level which warrants extension of their assigned time period.

Figure 11.4.3-1 illustrates conceptually the basic technical approach in the preparation of the standards. The figure shows that the storage serviceability standards are formatted into two documents (per Ref. 10). The first, which is based on Appendix A of Ref. 10, specifies PP&P levels, storage type and those tests, criteria and other provisions that can be coded easily into a computerized format. The second, which is based on Appendix B of Ref. 10, specifies applicable supplementary tests including functional/performance, detailed visual and other special tests that cannot be coded easily into a computerized format but are necessary to assess the readiness of the stored items.

The form for the storage serviceability standards (see Figure 11.4.3-1 - Appendix A of DARCOM-R 702-23) contains in coded format the following data:

Federal Stock Number (FSN) - the federally assigned stock number for the item.

Item Name - provides a brief description of the item.

Quality Defect for Inspection (QDC) - defines potential storage-induced defects. The assigned defect codes cover preservation, packaging, marking, and storage as well as material deficiencies. Cyclic inspections are performed to accept or reject material relative to the defects identified by this code. A three digit code is used, where the first digit identifies the severity of the defect (critical 0, major 1, or minor 2), and the second and third digits (see Table 11.4.3-1) identify
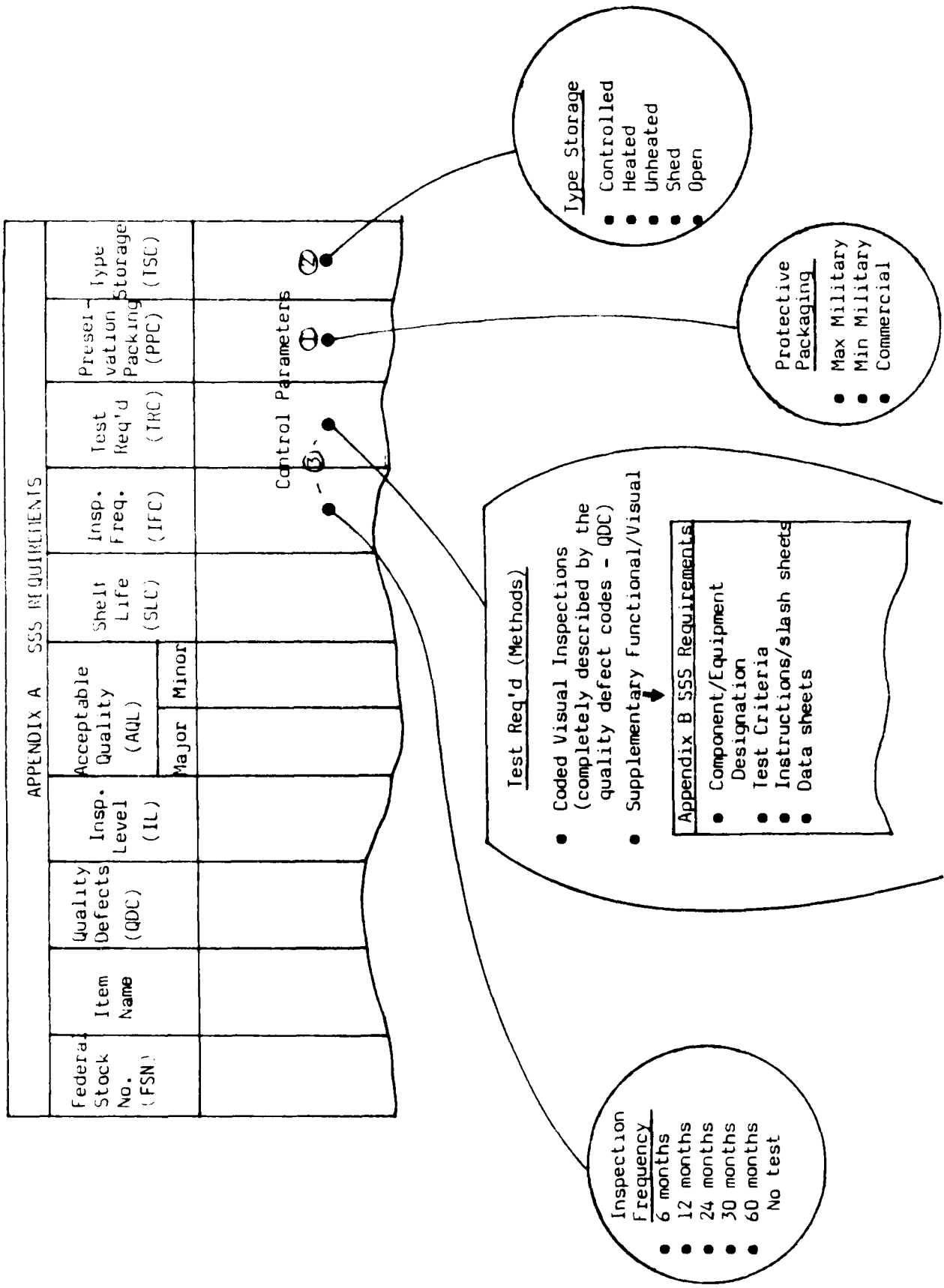
FIGURE 11.4.3-1: TECHNICAL APPROACH TO STORAGE SERVICEABILITY STANDARDS

TABLE 11.4.3-1: <u>STORAGE-INDUCED QUALITY DEFECTS</u>

<u>Category</u>	<u>Second & Third Digit (QDC)</u>
Preservation Inadequate	02
Container Damaged or Deteriorated	13
Containers, Boxes, Crates, or Pallets Damaged or Deteriorated	23
Markings Illegible	33
Loose or Frozen Parts (out of adjustment)	40
Damaged Parts (cracked, chipped, torn)	41
Leakage (liquid)	45
Bonding Deterioration (soldering, welding, etc.)	48
Contamination (dirt, sludge, moisture, foreign matter)	50
Excessive Moisture (fungus, mildew, rot)	51
Shelf-life Data Exceeded	55
Failed Test Requirements (failed supplementary tests functional/visual)	62
Improper Storage Space	86
Corrosion, Stage 1 (or more)	90

a specific class of defects. For example, the code 1 2 3 would indicate a major defect (1) due to (2 3) container damaged or deteriorated. Complete definitions for quality defect codes applicable to the acceptance/rejection of material items inspected during the various depot inspection and testing phases (i.e., on receipt, audit, scheduled cyclic, special, etc.) are provided in AMCR 702-7 (Ref. 11).

Inspection Level (IL) - determines the relationship between item lot or batch size and sample for inspection. The inspection level is used in conjunction with the acceptable quality level (AQL) to form the sampling plan. (The sampling plan provides accept/reject criteria for individual item inspections. Complete instructions for determination and use of sampling plans is found in MIL-STD-105.)

Acceptable Quality Level (AQL) - the maximum percent defective (or the maximum number of defects per hundred units) that for purposes of sampling inspection can be considered satisfactory. MIL-STD-105 provides specific accept/reject criteria for designated sample size and acceptable quality levels.

Shelf Life (SLC) - describes deterioration characteristics versus time. Shelf life periods for deteriorative material range from 1 month to 60 months. The condition of a shelf-life item is evaluated during cyclic inspection in terms of time remaining and downgraded if necessary.

Inspection Frequency (IFC) - defines the elapsed time between cyclic inspections. Inspection periods range from 6 months to 60 months.

Test Required (TRC) - describes the method by which an item is to be inspected or tested.

Preservation Packaging (PPC) - describes the preferred level and/or most cost effective level of protection for each item. After an item has been inspected and accepted, the packaging/preservation is to be restored to its preinspection level. Further, the date of repackaging as well as the date of original packaging is stamped on the package.

Type Storage (TSC) - indicates the preferred or most cost effective storage condition.

In order to prepare standards for new or existing material items, criteria for specifying cost effective tests and control provisions are first established. The criteria (and the subsequent standards) should provide for the inspections to be performed frequently enough to detect potential problems but not so often as to dilute the total depot inspection effort and compromise other items in storage which may be more critical and require higher inspection frequencies. To be effective, the criteria must take into account:

    (1) Material deterioration
    (2) Application risk criticality
    (3) Cost
    (4) Material complexity
    (5) Preservation/packing and packaging (PP&P)
    (6) Storage environment

The Army has developed general criteria and a materiel weighting factor technique as part of a complete standard preparation process that takes into account these factors (Ref. 12). The process, which is illustrated in Figure 11.4.3-2, focuses on the three major control parameters: (1) protective packaging level, (2) storage type, and (3) cyclic inspection (frequency and method). The process involves first defining the level of packaging and storage (preferred) from a review of material deterioration properties and then determining inspection frequency by evaluating deterioration, application risk, criticality and other factors in light of the defined packaging and storage environment levels. It is an iterative process that involves tradeoff analysis to define an optimum set of requirements. It emphasizes and uses to the maximum extent the visual coded inspection criteria, i.e., (QDC), to detect materiel failure and/or defects due to corrosion, erosion, and other deficiencies resulting from improper storage methods, extended periods of storage, and the inherent deterioration characteristics of the materiel item. The technique is sufficiently flexible to make allowances for available storage facilities if they differ from the preferred through the adjustment of inspection frequency.

In the initial preparation of the standards, the type and level of storage space and packaging methods are considered as fixed parameters (although iterative) where the preferred levels are defined based on material deterioration properties. Therefore, the element which provides the overall stimulus for the control and assurance of the readiness of stored components and equipment is the type and frequency of inspection. A ranking is assigned to each item that accounts for materiel deterioration and the other factors depicted in Figure 11.4.3-2 and is used as the basis to determine first the need for inspection and then, if needed, the frequency and type of inspection.

To effectively manage the depot cyclic inspection program, priorities are established as indicated in Figure 11.4.3-2. Items classified as definite shelf-life are given priority and subjected to cyclic inspection. Other indefinite shelf-life items that are considered particularly sensitive to deterioration are also subject to cyclic inspection. Definite shelf-life items are those possessing intrinsic deterioration characteristics that cannot be eliminated (or minimized) by storage and packaging controls. They are further classified into nonextendible (Type I) and extendible (Type II) materials. Indefinite shelf-life items, on the other hand, include items that do not deteriorate with storage time, as well as items that are sensitive to deterioration as a result of induced external failure mechanisms. The relationship between these types of materiel item classification and their relative deterioration level is illustrated in Figure 11.4.3-3. Figure 11.4.3-3 shows the nonextendible life characteristic of Type I materiel, the extendible shelf-life characteristic of Type II materiel, and the relative indefinite shelf-life characteristic of all other stored materiel.

Figure 11.4.3-4 presents a matrix that can be used to determine inspection frequency (IFC) and to optimize in-storage inspection coverage. The matrix includes:
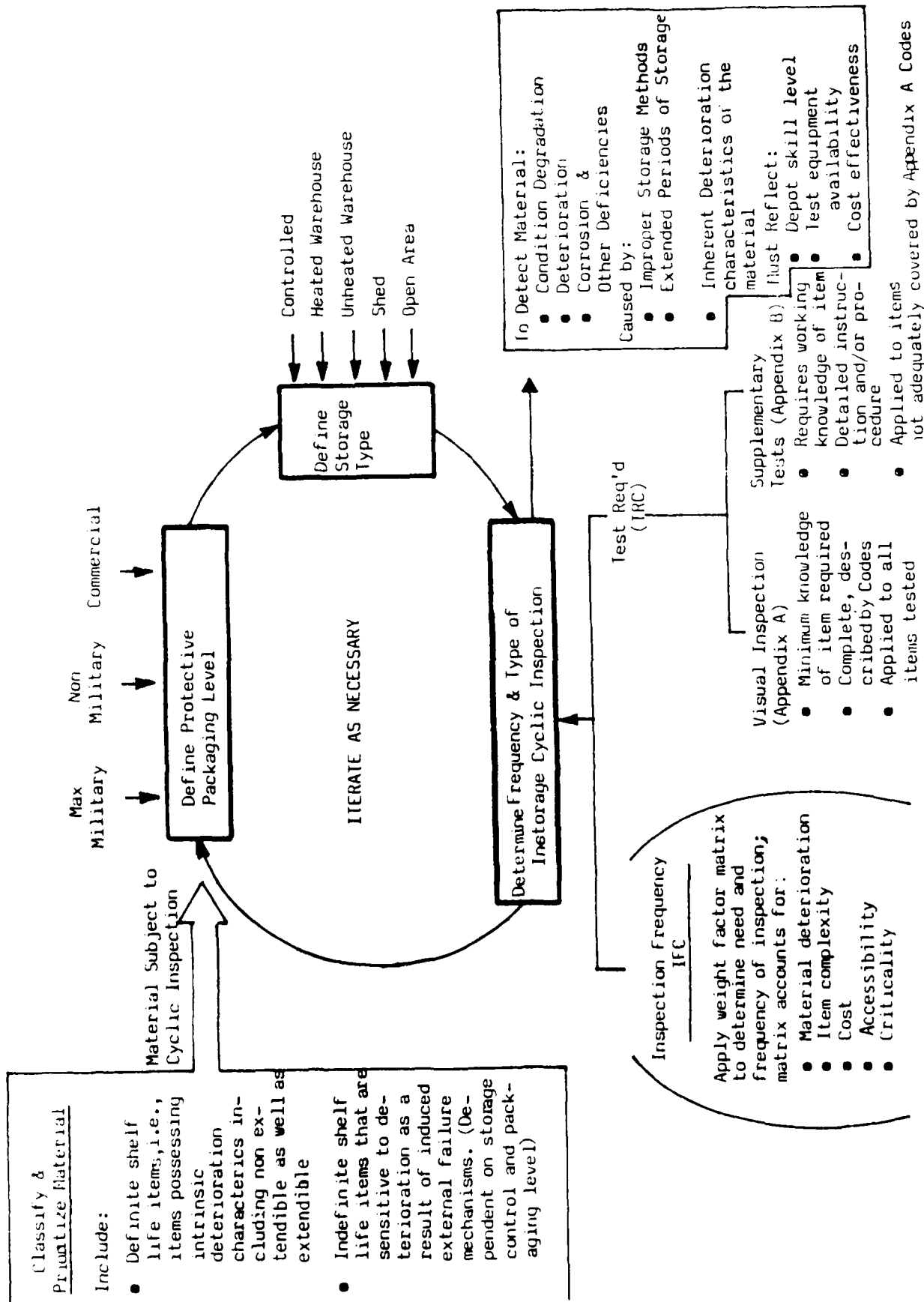
FIGURE 11.4.3-2: STORAGE SERVICEABILITY STANDARD PREPARATION PROCESS
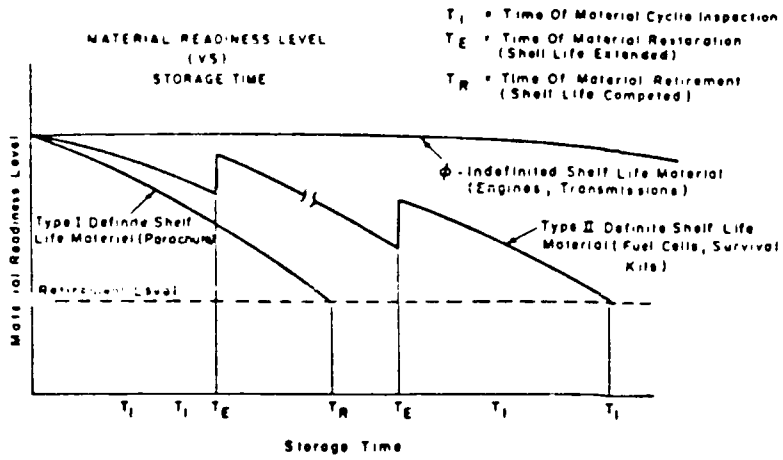
FIGURE 11.4.3-3: DETERIORATION CLASSIFICATION OF MATERIAL

WEIGHT FACTOR

	WEIGHT FACTOR
DETERIORATION	
LOW	0
MODERATE	1
HIGH	2
COMPLEXITY	
LOW	0
HIGH	1
ITEM COST	
LOW	0
MEDIUM	1
HIGH	2
ACCESSIBILITY (IMPACT ON SYSTEM REPAIR TIME)	
- NO MAJOR EFFECT, SIMPLE SUBSTITUTION OF REPLACEABLE ITEM (I.E. EASILY ACCESSIBLE)	0
- NOT READILY ACCESSIBLE, REPAIR TIME INVOLVED, REQUIRES SOME SYSTEM TEARDOWN	1
- NOT ACCESSIBLE, REPAIR TIME IS SUBSTANTIAL, REQUIRES MAJOR SYSTEM TEARDOWN	2
CRITICALITY	
LOW	0
MEDIUM	2
HIGH	5

Inspection Frequency Matrix (Material Weight Factor →)

STORAGE PROTECTION (Storage Environment)	PACKING LEVEL	0-1	2-3	4-5	6-7	8-10	11-12
CONTROLLED HUMIDITY	CONTAINERIZED	6	6	6	5	3	2
HEATED	CONTAINERIZED	6	6	6	5	3	2
UNHEATED	CONTAINERIZED	6	6	6	5	3	2
SHED	CONTAINERIZED	6	6	6	5	3	2
OPEN	CONTAINERIZED	6	6	6	5	3	2
CONTROLLED HUMIDITY	"A" MAX. MIL.	6	6	6	5	3	2
HEATED	"A" MAX. MIL.	6	6	5	4	2	2
CONTROLLED HUMIDITY	"B" MIN. MIL.	6	5	5	4	2	2
UNHEATED	"A" MAX. MIL.	6	5	4	3	2	1
HEATED	"B" MIN. MIL.	6	5	4	3	2	1
CONTROLLED HUMIDITY	COMMERCIAL	6	5	4	3	2	1
SHED	"A" MAX. MIL.	6	5	3	3	2	1
UNHEATED	"B" MIN. MIL.	6	5	3	3	2	1
HEATED	COMMERCIAL	6	5	3	3	2	1
OPEN	"A" MAX. MIL.	6	4	2	2	1	1
SHED	"B" MIN. MIL.	6	4	2	2	1	1
UNHEATED	COMMERCIAL	6	4	2	2	1	1
OPEN	"B" MIN. MIL.	6	3	2	2	1	1
SHED	COMMERCIAL	6	3	2	2	1	1
OPEN	COMMERCIAL	6	3	2	2	1	1

TEST FREQUENCY

6 Months	-1
12 Months	-2
24 Months	-3
30 Months	-4
60 Months	-5
No Test	-6

FIGURE 11.4.3-4: INSPECTION FREQUENCY MATRIX

(1) The most deteriorative items to the least deteriorative in terms of a total ranking factor that accounts for deterioration, complexity, cost, accessibility and criticality

(2) All combinations of depot storage and packaging conditi, ranging from the most protective (containerized package and a controlled humidity environment) to the least protective (commercial package and an open area)

Application of the matrix to a given materiel item involves assigning appropriate values to each of the weight factors depicted in Figure 11.4.3-4 in order to arrive at a total ranking. This ranking represents a rough measure of the overall deterioration/cost sensitivity of the item to the storage environment. The ranking is then inputted at the proper weight column of the matrix to determine inspection frequency for any desired combination of packaging and depot storage protection level.

For new items, the matrix allows broad tradeoffs to be made to arrive at the optimum balance of packaging, storage, and inspection requirements. Also, the combining of deterioration with cost and the other weight factors via the matrix approach allows the specification of cost effective inspection periods. This cost effectiveness is illustrated by considering two items where one exhibits low deterioration properties but cost and the other factors are high and the other exhibits high deterioration properties but the total of the other factors is low. A relatively low cost or nominal test inspection frequency may be computed for both items that reflects an effective balance of all factors; whereas, if only deterioration was considered in computing the test periods, over inspection (excessive cost) of the high deterioration item and under inspection (low readiness assurance) of the low deterioration items would most likely result. Of course, for those items where all factors including deterioration and cost are high, frequent inspection would be required to assure materiel readiness, and for those items where deterioration and the other factors are low less frequent inspections would be required.

The matrix approach also provides flexibility for regulating the number and type of items subjected to cyclic inspections by adjustment of the weight assigned to the factors that relate the materiel to the storage environment.

As previously indicated, an inspection time period is originally set based upon preferred storage environment and packaging methods specified in the TSC and PPC columns of Figure 11.4.3-1. However, many times an item will be stored and packaged at a different level. In that case an adjustment is made to its inspection time periods to maintain the same state of readiness based on the data provided in the inspection frequency matrix.

11.4.3.1 APPLICATION OF CYCLIC INSPECTION DURING STORAGE TO ASSURE RELIABILITY AND MATERIEL READINESS

Critical to the control of reliability during storage is the proper application of cyclic inspections and tests. The purpose of in-storage cyclic inspection is to assess component/equipment reliability and readiness for use, to detect deterioration while in storage, and to furnish data for any necessary condition reclassification action. A knowledge of the component or equipment item, particularly its deterioration properties and risk attributes, is necessary to plan and specify optimum in-storage cyclic inspection requirements. The inspections must be practical and maintain an overall cost effective posture that reflects readily available depot test equipment and skills.

In-storage cyclic inspection generally includes two basic types as indicated in the previous subsection. The first type is based on subjected visual inspections where material acceptance is completely described by codes covering quality defects (and included in the QDC column of the Storage Serviceability Standard). A minimum knowledge of the items is required to specify the criteria and perform the inspections. These coded requirements apply to all items tested. Figure 11.4.3.1-1 illustrates some of the quality defect codes and shows that the assigned codes cover preservation, packing, marking and storage, as well as materiel deficiencies. The figure indicates that there are basically three levels of inspection corresponding to (1) the outer package or container, (2) the inner packing, and (3) the item itself. If a defect is not considered critical, major, or minor at the time of inspection but (due to inspector experience) is expected to become critical, major or minor prior to the next cyclic inspection, it is identified as such, considered as a cause for rejection, and counted relative to the item's sampling plan criteria. Defects of a trivial nature are not considered as cause for rejection of a lot, unless some reduction in usability or function of items is expected prior to the next scheduled inspection. For example, nicks, dents, or scratches that do not break coatings or paint films are considered trivial deficiencies.

The second type of in-storage inspection involves supplementary requirements that are applied to items that cannot adequately be inspected by the visual coded requirements. They generally include functional tests (derived from technical manuals) and/or special, more detailed visual inspections. Special test and/or inspection procedures complete with acceptance criteria are prepared for these items and included in Appendix B to the SSS. Emphasis is placed on defining viable test or checkout procedures that can be applied simply and quickly to the stored material items to assure that they perform satisfactorily with only a minimal level of evaluation, support, and guidance. These supplementary tests can be applicable to parts, material, equipment, or complete systems, including shelf-life items as well as other items that are storage sensitive.

The supplementary tests are not intended to represent a complete and detailed inspection or checkout of the item to determine compliance to specified requirements. The tests are designed to verify operability

INSPECT OUTER PACKAGE
OR CONTAINER AND
STORAGE METHODS

- CONTAINERS, BOXES, CRATES
  OR PALLETS DAMAGED OR
  DETERIORATED
- MARKINGS ILLEGIBLE
- SHELF LIFE EXCEEDED
- IMPROPER STORAGE SPACE

REJECT

ACCEPT

INSPECT INNER PACKAGING

- PRESERVATION INADEQUATE

- INNER CONTAINER OR
  PACKAGING DAMAGED OR
  DETERIORATED

RECLASSIFIED
TO APPROPRIATE
CONDITION
CODE

REJECT

ACCEPT

INSPECT MATERIAL ITEMS

- LOOSE OR FROZEN PARTS,
  OUT OF ADJUSTMENT

- DAMAGED PARTS.
- BONDING DETERIORATION
- CONTAMINATION
- EXCESSIVE MOISTURE
- FAILED TEST REQUIREMENTS
  (SUPPLEMENTARY FUNCTIONAL/
  VISUAL
- CORROSION
- Leakage

REJECT

MATERIAL ACCEPTED

FIGURE 11.4.3.1-1: CODED QUALITY INSPECTION LEVELS

and are to be based on a "go/no-go" concept, fully utilizing end item functions to indicate functional readiness for service and issuance.

The functional tests are designed such that they do not require external and specialized test equipment except common and readily available equipment found at the depots and other installations (power supplies, volt-ohmmeters, etc.). The functional tests in general involve first checking the operational mode of all indicators such as dial lamps, power lights, meters, and fault lights as applicable and then applying a simple procedure that exercises some or all of its functions to verify operational status. Many times the equipment can be tested as part of a system. For example, two radio (receiver/transmitter) sets could be tested as a system pair by positioning the sets a certain distance apart (e.g., 25 feet). One is placed in the receive mode and the other in the transmit mode, and all associated hardware and interconnecting cables are attached. An audio (spoken word) input is applied to the set in the transmitting mode, and the set in the receive mode is checked for reception. The process is repeated with the transmitter/receive modes reversed.

The functional test procedures for a given equipment item can be derived from a review of the equipment's maintenance and/or operating manuals. These manuals describe the operational sequence, the turn-on and shut-down procedure, and the equipment operational test and checkout procedure necessary for complete verification of equipment operational status. Consequently, they provide a sound basis for deriving a simplified and cost effective functional test that is suitable for assessing reliability during storage.

11.4.4 DATA COLLECTION AND ANALYSIS (DURING STORAGE)

The shipment/storage test and control program, like the production test program, must be continually challenged relative to the effectiveness of the overall program as well as the individual tests. In-storage cyclic inspection must also be considered as a dynamic test where the test methods, frequencies, and criteria are adjusted to reflect actual depot and field experience. In-storage data (reject rate, quality discrepancy reports, causal data, etc.) generated during the implementation of the cyclic inspections should be compiled, reduced, thoroughly analyzed, and fed back to item management and engineering activities in a form that will provide a basis to:

(1) determine the effectiveness of the shipment/storage degradation control program to meet reliability and readiness objectives

(2) eliminate the causes for deficiencies

(3) revise item inspection or protective packaging and storage level requirements, if necessary

11.5 OPERATIONAL R&M ASSESSMENT AND IMPROVEMENT

Electronic systems are also subject to damage and performance degradation during operation and maintenance. Consequently, operational

systems are continually assessed to assure that they are performing in accordance with expectation and to identify areas where improvements can be incorporated to minimize degradation, improve R&M, and reduce life cycle costs. This time period is most significant because it is here that the true cost effectiveness of the system and its logistic support are demonstrated and historical R&M data is gathered and recorded for use on future products. The effort includes:

(1) assessing R&M performance from an analysis of operation/failure data, identifying operation/maintenance degradation factors, and comparing actual R&M with that predicted and demonstrated during acquisition

(2) identifying systems, equipment and other hardware items that exhibit poor reliability, require extensive maintenance and are prime candidates for cost effective improvements

(3) evaluating the impact on R&M of system changes and corrective action implemented in response to operational failures

11.5.1 FACTORS CONTRIBUTING TO R&M DEGRADATION DURING FIELD OPERATION

Degradation in reliability can occur as a result of wearout, with aging as the dominant failure mechanism. Defects can also be induced into a system during field operation and maintenance. Operators will many times stress a system beyond its design limit either to meet a current operational need or constraint or inadvertently through neglect, unfamiliarity with the equipment, or carelessness. Situations occur in which a military system may be called upon to operate beyond its design capabilities because of an unusual mission requirement. These situations can cause degradation in inherent R&M parameters. Operational abuses due to rough handling, extended duty cycles, or neglected maintenance can contribute materially to R&M degradation during field operation. The degradation is usually the result of the interaction of man, machine and environment. The translation of the factors which influence operational R&M degradation into corrective procedures requires a complete analysis of functions performed by man and machine plus environmental and/or other stress conditions which degrade operator and/or system performance.

Degradation in inherent R&M can also occur as a result of poor maintenance practices. Studies (Ref. 13) have shown that excessive handling brought about by frequent preventive maintenance or poorly executed corrective maintenance (e.g., installation errors) have resulted in defects introduced in the system, with resultant degradation of R&M. Some examples of defects resulting from field maintenance, depot overhaul, or reconditioning are due to:

(1) foreign objects left in an assembly
(2) bolts not tightened sufficiently or overtightened
(3) dirt injection
(4) parts replaced improperly
(5) improper lubricant installed

Also, during unscheduled maintenance, good parts are replaced in an effort to locate the faulty parts. In many cases, the good parts are written up as defective instead of being reinstalled. These parts often are returned to the depot for repair or discarded, resulting in a reported field failure rate that is higher than is actually occurring.

Several trends in system design have reduced the need to perform adjustments or make continual measurements to verify peak performance. Extensive replacement of analog with digital circuitry, inclusion of more built-in test equipment, and use of fault-tolerant circuitry are indicative of these trends. These factors, along with greater awareness of the cost of maintenance, have brought changes for ease of maintenance whose by-product has increased system R&M. In spite of these trends, the maintenance technician remains a primary cause of R&M degradation. The effects of poorly trained, poorly supported or poorly motivated maintenance technicians on R&M degradation require careful assessment and quantification.

The operation and maintenance induced defects are factors that must be carefully considered and taken into account in the assessment and control of operational R&M. In general, the environmental factors considered in prediction techniques account for the added stress provided by operation within that environment. However, the environmental stresses imposed during field maintenance may be other than what was anticipated during the original prediction. For instance, a subassembly removed for repair in a desert area may be placed in direct sunlight while awaiting transfer. Component temperatures may exceed those experienced during normal operation for an extended period, thus reducing their life expectancy. Mechanical stresses imposed on components during removal, repair, and reinsertion may exceed that designed for a given environment. Therefore, field and depot requirements and procedures must include criteria for controlling the reliability and quality of the repair/overhaul action to minimize potential maintenance induced defects in order to achieve an actual field R&M that approaches that predicted and demonstrated during acquisition.

11.5.2 MAINTENANCE DEGRADATION CONTROL (DURING DEPOT OPERATIONS)

Depot maintenance activities include complete overhauling, partial rebuilding, product improvement and retrofit, calibration, and the performance of highly complex repair actions. In addition, the depot normally stores and maintains the supply inventory. Physically, depots are specialized fixed installations that contain complex and bulky production and test equipment, and large quantities of spares under environmental storage control. Depot facilities maintain high volume potential and use assembly line techniques with relatively unskilled specialists in key areas such as condition evaluation, fault diagnosis, and quality control and inspection.

Since the R&M of hardware items can be materially degraded during maintenance and depot operations, engineering plans and analyses are performed and R&M controls implemented to assure performance and to eliminate defects due to workmanship and the various other factors that would, if uncontrolled, lead to poor quality and R&M degradation.

Control efforts for a given hardware item start with the preparation of a Maintenance Plan during development as part of logistic support analysis (LSA); they continue into the operational and maintenance phase with the establishment of specific criteria and special maintenance and restoration procedures which must be followed to avoid R&M degradation and to retain the inherent R&M of the item. Possible deviations from the Maintenance Plan are described and related to their potential effect on operational R&M. Specifications are prepared and incorporated into a maintenance/depot requirement document including provisions covering:

(1) Life cycle reconditioning performance/quality parameters and acceptance criteria

(2) Types and kinds of material approved for use during overhaul, repair, and reconditioning

(3) Acceptable workmanship standards and techniques

(4) Quality and reliability assurance inspection, tests, analysis methods, and controls

The intent of the maintenance requirement document is to assure that quality and R&M measures reflect adequate, viable, and practical acceptance criteria and procedures that can be implemented most cost effectively by depot personnel during the repair, overhaul, or reconditioning of the hardware items.

Some of the areas that are evaluated, controlled and reflected into the maintenance documentation from a reliability and quality standpoint are listed in Table 11.5.2-1. This includes reviewing the technical accuracy and adequacy of instructions covering equipment checkout, calibration, alignment, and scheduled removal and replacement. In addition, all dis-assembly, cleaning, inspection, testing, repair, replacement, reassembly, troubleshooting, preventive maintenance checks and services, and maintenance processes and procedures are evaluated.

Criteria are also established that recognize the fact that hardware in field use (as well as during storage) deteriorates due to age, environment, and storage conditions. When deterioration begins to take effect, the quality level of the material will decline below that which was initially specified during procurement. Although the effectiveness and adequacy of the reconditioning operations and controls will minimize the decline, the resultant quality level of the reconditioned material will usually be lower than that initially specified. The depot requirements include maintenance quality level requirements that reflect:

(1) Minimum deterioration, which is lower than the initially specified value

(2) Criteria that indicate the quality limits beyond which repair is not economically achievable

(3) Acceptance criteria for reconditioning cycles(s) at predeter-mined storage and use milestones

TABLE 11.5.2-1: DEPOT MAINTENANCE REQUIREMENT AREAS

Inspection and Test Equipment. The test equipment used to determine performance of depot maintenance specifications and requirements.

Material Quality. The quality level of parts and material used for replacement, repair or modification.

Preshop Analysis. The extent of overhaul required. Included in the analysis would be procedural instructions as well as a detailed checklist to aid in the evaluation of the items for determining extent of cleaning, repair, modification or replacement.

In-Process Inspection. The in-process inspection requirements, including procedural as well as accept/reject criteria associated with each overhaul operation such as disassembly, cleaning, repair, replacement and modification, as applicable.

Diagnostic and Automated Test Equipment. The diagnostic and automated equipment (such as NDT, magnetic particle, dye penetration, etc.) used to determine the adequacy of repair, overhaul or reconditioning.

Repair. The total sequential, step-by-step instructions and specifications used for repair, replacement, reclamation, rework or adjustment for hardware items.

Assembly. The total step-by-step instructions used to assemble the hardware item.

Calibration. The level and method of calibration for all equipment and instrumentation.

Final Performance Check. The techniques and methods to assure total satisfactory performance of the hardware item in accordance with the established criteria.

In addition, a process analysis similar to that described in Sections 11.2 and 11.3 to determine and control R&M degradation introduced by manufacturing can also be applied to determine and control degradation introduced by the reconditioning and overhaul process. This analysis would identify processing and inspection steps that can be improved to reduce R&M degradation and determine the need to incorporate controlled screening and burn-in tests as described in Section 11.2.

11.5.3 IMPORTANCE OF A MAINTENANCE PLAN FOR DEGRADATION CONTROL

Critical to R&M degradation control, particularly for large complex weapon systems and equipment, is the development of the Maintenance Plan. The Maintenance Plan for an equipment/system is a document that describes the requirements and tasks to be accomplished for achieving,

restoring, or maintaining the operational capability of the equipment/system. The Maintenance Plan evolves from logistic analyses during development to identify the maintenance concept, reliability and maintainability parameters and requirements, maintenance tasks, descriptions of maintenance organizations, support and test equipment requirements, maintenance standards, supply support requirements, and facility requirements.

The final plan includes the target operational readiness date and specific requirements for personnel, technical publications, facilities, repair parts, special tools, test and support equipment, technical assistance, and related maintenance materials for maintenance support. The plan also allocates the maintenance tasks to the appropriate maintenance levels, i.e., organizational, field or intermediate, depot, or contractor facilities.

From the allocation of maintenance responsibilities, affected organizations develop progressively more detailed schedules for maintenance of each maintenance significant item in order to control the accomplishment of all known tasks in accordance with established priorities. These schedules can be relatively firm for preventive maintenance activities accomplished on a periodic basis, needing adjustment only for variations caused by operational requirements and immediate workloads. Corrective maintenance schedules must be developed on the basis of reliability data, actual or estimated, with anticipated failures prorated over a period of time on the basis of previous experience and the best judgment of material maintenance specialists. The schedules for organizational level maintenance, primarily, will concern preventive maintenance and corrective maintenance resulting from periodic tests/inspections and operational failures. Field level maintenance schedules are a combination of preventive maintenance beyond the capability of the organization level maintenance personnel and corrective maintenance by repair of designated items. Depot level maintenance schedules, primarily, are concerned with corrective maintenance by repair of failed items, although overhaul items removed because of life limitations may be considered preventive.

An example of this allocation for a representative electronic equipment is shown in Figure 11.5.3-1.

11.5.3.1 MAINTENANCE DOCUMENTATION REQUIREMENTS

An important factor in controlling R&M degradation during deployment is the availability of adequate maintenance documentation for the equipment/system. System maintenance documentation includes the written, graphical, and pictorial data which should be supplied with the system for use by operators and maintenance personnel to accomplish both the routine preventive maintenance tasks and the corrective repair procedures identified in the Maintenance Plan for the system. This documentation should reflect the maintenance concept and repair policies established for the system. In general, system operation and maintenance documentation should be a completely integrated package providing clear cut direction leading from failure detection to fault

TRANSMITTER UNIT GROUP	ORGANIZATIONAL LEVEL	INTERMEDIATE LEVEL	DEPOT LEVEL	CONTRACTOR
Unit a Cooling System	Fault Isolation → Repair In Place → Spares	Diagnostic Checks → Component Repair → Supply		
Unit b Power Supply	Fault Isolation → Repair by Subassembly Replacement → Spares	Diagnostic Checks → Repair by Part Replacement → Supply	Diagnostic Checks → Overhaul → Ready for Issue	
Unit c Automatic Test & Monitoring Equipment	Fault Isolation → Switch to Alternate mode → Diagnostic Checks → Repair in Place → Spares	Diagnostic Checks → Repair → Supply	Diagnostic Checks / Disposition Instruction → Ready for Issue	Diagnostic Checks → Repair → DD 250
Unit d Modulator/ Amplifier	Fault Isolation → Repair by Unit Replacement → Repair Units by Module Replacement → Spares	Diagnostic Checks → Repair by Module Replacement → Supply	Diagnostic Checks → Module Repair → Ready for Issue	Diagnostic Checks → Repair or Replace → DD 250 or Warranty Replacement

FIGURE 11.5.3-1: EXAMPLE OF MAINTENANCE RESPONSIBILITY FLOW CHART

isolation and repair procedures and should be presented in a format and style designed for ready access and updating as changes are introduced.

Four types of data represent the minimum package which should be provided with an operating system if it is to be successfully operated and maintained in accordance with the Maintenance Plan. These working documents should be instructional and factual. The four categories of maintenance documentation required to successfully implement the Maintenance Plan are described as follows:

(1) Functional Description and Operating Instructions for Each System. Data in this category includes: a description of the capabilities and limitations of the installed system; a technical description of system operation, including its operating modes and alternate modes; step-by-step turn-on and manual operating procedures; "confidence" checks normally employed to verify that equipment is performing satisfactorily.

(2) Equipment and Installation Description. Data in this category must provide an accurate, up-to-date description of the hardware as it is installed in the weapons system. Minimally, it should consist of: complete set of functional flow or logic diagrams; complete set of schematic diagrams for electrical layout, electronics, hydraulics, pneumatics, etc.; parts data containing reference information in sufficient detail to permit reordering or fabrication of the individual parts within the system; and the necessary instructions for installing and checking out installed/retrofitted equipment.

(3) Maintenance Aids (Troubleshooting). This category presents the specific data required by the technician for localizing a fault to a replaceable item and for checking out the system after repair. Included are:

(a) Methods for system-level fault isolation when the system is "up" but operating in a degraded mode -- use and interpretation of system readiness test results

(b) Method of system level fault isolation when the system is totally down -- use and interpretation of fault isolation tests and monitor console displays

(c) Procedures for functional equipment level fault isolation -- based on fault sensing indicators supplemented as required by test point measurements using built-in test equipment

(d) Equipment level isolation techniques which will permit identification of the problem area to a single module or replaceable part

(e) Routine tests, adjustments, alignment, and other "preventive" procedures which are performed at periodic intervals

(4) <u>Ready Reference Documentation</u>. This documentation is limited to that information routinely required by the technician in a given equipment repair area. The documentation should be easily usable in the work area -- i.e., capable of being held with one hand, remaining open to a given section, permitting easy replacement or additions, and suitable for storage in the work area. It should contain only routine checkout, alignment, and preventive maintenance procedures; fault monitoring interpretation and replacement data; supplemental trouble shooting techniques required to complement the automatic fault detection and isolation system; and item and unit spare parts ordering data keyed to system identity codes.

11.5.3.2 RELIABILITY CENTERED MAINTENANCE CONCEPT

A relatively new program initiated by the Army for deriving an optimum Maintenance Plan is the application of Reliability Centered Maintenance (RCM) principles to maintenance-significant equipment. RCM is a precept which uses an analytical methodology, or logic, for influencing design maintainability and reliability, and for establishing specific maintenance tasks for complex systems or equipment. Detailed instructions for application of RCM principles is provided in AMCP 750-16, "AMC Guide to Logistic Support Analysis," (Ref. 14).

Intrinsic to RCM is the identification of critical failure modes through engineering analyses and/or field experience, determination of the related consequences, analysis of the interaction between failure probability and a maintenance task to detect the incipient condition of failure, and determination of the most effective apportionment of maintenance activities. Noncritical tasks are included only when performance of the task produces cost effective results.

An important step in the evaluation of the RCM Maintenance Plan is the segregation of the maintenance requirements into the following three categories:

(1) On-condition maintenance requirements -- scheduled inspections or tests designed to measure deterioration of an item; based on the deterioration of the item, either corrective maintenance is performed or the item remains in service

(2) Hardtime maintenance requirements -- scheduled removal tasks at predetermined fixed intervals of age or usage

(3) Condition monitoring maintenance requirements -- unscheduled tasks on components which are allowed to fail or are components where impending failure can be detected through routine monitoring during normal operations

The segregation of maintenance into these three categories will determine the scheduled maintenance burden on the field, impact on the operating and support cost incurred by the system, and impact on the operational readiness characteristics of the equipment/system. The

the development of the Maintenance Plan is to reduce the scheduled maintenance burden and support cost incurred by the system while maintaining the necessary readiness state.

RCM provides the detailed logic process to segregate maintenance requirements into the on-conditions, hard time, and condition monitoring categories. As an integral part of the logistic analysis process, application of RCM requires input from other system engineering programs such as reliability, maintainability, and safety, and it provides data to other logistic analyses such as level of repair analysis, detailed maintenance task analysis, and tradeoff analyses with the design engineering function.

The overall objective of the RCM program is to arrive at the precise amount of maintenance which is essential for restoring and preserving inherent system reliability, meeting safety standards, and minimizing the likelihood of a mission abort. The program is designed to accomplish the following:

(1)   By using data from the system safety and reliability programs, identify components in equipment/system which are critical in terms of mission and/or operating safety

(2)   Provide a logical analysis process to determine the feasibility and desirability of scheduled maintenance task requirements

(3)   Highlight maintenance problem areas for design review consideration

(4)   Provide the supporting justification for scheduled maintenance task requirements

The logic process is based upon the following criteria:

(1)   Scheduled maintenance tasks should be performed on noncritical components only when performance of the scheduled task will reduce the life cycle cost of ownership of the equipment/system.

(2)   Scheduled maintenance tasks should be performed on critical components only when such tasks will prevent a decrease in reliability and/or deterioration of safety to unacceptable levels or when the task will reduce the life cycle cost of ownership of the equipment/system.

The RCM logic is intended for application once a component's failure modes, effects, and criticality have been identified. As with other reliability and logistic analyses and tasks, the logic process is reapplied as available data moves from a predicted state to measured values with a higher degree of certainty and as design changes are made. In addition, once all components have been subjected to the logic process, an overall system analysis is required to arrive at the overall maintenance plan. This system analysis merges individual component

requirements into a System Maintenance Plan by optimizing the frequency of scheduled maintenance requirements and the sequence of performance of individual scheduled tasks.

The RCM logic is applied to each repairable item in the equipment/system. The maintenance task requirements are identified against the repairable components; however, individual failure modes must be addressed during the application of the RCM logic. Thus, for a given component, different scheduled tasks could be the results, due to the different failure modes and their characteristics. As an example, a given component might undergo condition monitoring during normal operations to detect the majority of predicted failure modes for the component while still having an on-condition or hardtime requirement due to a failure mode that is not detectable during routine operator monitoring.

In addition to the scheduled maintenance task requirements identified during application of the RCM logic, any scheduled tasks that were assumed in establishing the reliability characteristics of the equipment/system under the reliability program must either be included in the maintenance plan or identified as being omitted from the maintenance plan. Inherent failure rates and failure modes and effects might need adjusting if an assumed scheduled maintenance action is omitted from the Maintenance Plan after application of the RCM logic.

11.5.4   DATA COLLECTION AND ANALYSIS (DURING FIELD DEPLOYMENT)

A new system or equipment begins to accrue valuable experience data with its initial introduction into the field. This data, accurately recorded and consistently reported, provides the final basis for judging suitability of the system for continuing deployment. Thereafter, the reporting system can become the essential basis for an effective R&M feedback loop if provisions are made for continuous reporting and periodic analysis of maintenance experience data throughout the deployment phase and if formal procedures are established for progressive correction of discrepancies revealed by the analysis. On the other hand, if the reporting system is not fully exploited analytically and applied dynamically in a formal corrective action program, the R&M feedback loop is short circuited and serves no purpose other than logistic surveillance.

Data required to effectively assess, monitor, control and improve the R&M of fielded systems and equipment items includes hours of operation (and appropriate data on operating characteristics), performance measures and assessments, application environmental factors, and, most important, failure and maintenance data. The feedback of information obtained from the analysis of failure during actual use is essential to reliability growth.

Development of a formal and well documented field data recovery, analysis and feedback system is a key element in an effective R&M program. The data recovery and feedback program is designed to be compatible with and incorporate data from other data collection efforts

during acquisition and storage. An effective data system provides output information that can be used for:

(1) R&M assessments
(2) R&M tracking
(3) comparative analysis and assessments
(4) determination of the effectiveness of R&M tasks and management concepts
(5) identification of critical equipment, components and problem areas
(6) compilation of historical component failure rates for design predictions

Plans are prepared that describe the specific mechanisms for collecting operation, maintenance and installation data at field sites, depots, and disposal areas as well as during factory test for feedback. Included are detailed instructions, document forms, and the delineation of responsibilities for implementation.

Furthermore, the system must be planned such that it is compatible with standard military data systems. It should be noted that during acquisition the data system is primarily the responsibility of the system equipment developer where control by the military is established through reporting of summary data and deliverable data items. During operation, military maintenance data collection systems are used to record and accumulate ongoing data. These programs, including the Army's TAMMS (The Army Maintenance Management System), the Navy's 3M and the Air Force's 66-1 system, are primarily maintenance oriented. Maintenance actions are reported and processed in a computer data bank at three levels: equipment, assembly board, and piece part. For each entry, the failure indicator is reported along with codes identifying such things as the base command and the equipment nomenclature. They do not, however, report operating time. Moreover, the field use environment and the field maintenance environment are not adequately quantified to insure consistent interpretation of field data. Thus, field reliability cannot be assessed via the military data systems alone. In order to assess reliability and to compare the attained field reliability with that specified and estimated during acquisition, both equipment/system failure (or maintenance) data and their associated operating time(s) are required. The associated equipment/system operating time must be estimated or obtained directly from the operational units themselves. Operating times are recorded in station logs and the equipment inventory, with associated records of uptime, storage time and maintenance times by month.

In addition to the previously mentioned maintenance data collection systems, the Department of Defense has instituted the Reliability Analysis Center (RAC), a DoD Information Analysis Center, which functions as a focal point for the recovery of reliability test data and experience information on microcircuit, discrete semiconductor, electrical/electromechanical components, and R&M data on the equipments/systems in which these components are used. Reliability experience information is disseminated by the RAC through reliability data compilations, handbooks and appropriate special publications to upgrade and support system reliability and maintainability.

These publications cover the following:

(1) Microcircuit Device Reliability

- Digital Failure Rate Data
- Digital Evaluation and Failure Analysis Data
- Linear/Interface Data
- Memory/LSI Data
- Hybrid Circuit Data

(2) Discrete Semiconductor Reliability

- Transistor/Diode Data

(3) Nonelectronic Component Reliability

- Nonelectronic Parts Reliability Data

(4) Electronic Equipment Reliability and Maintainability Data

- Electronic Equipment Reliability Data
- Electronic Equipment Maintainability Data

Each of these publications provides summary tables, charts and graphs in addition to detailed screen/burn-in, environmental and failure rate data. The publications are updated and reissued annually, deleting outdated data entries and incorporating new acquisitions from the latest technologies and device processes, configurations, and applications. For additional information on the RAC, as well as other specialized DoD Information Analysis Centers, see Reference 15.

11.5.5 SYSTEM R&M ASSESSMENT

Once an equipment/system is deployed, its R&M performance is periodically assessed based on the analysis of collected field operational/failure data as described in the previous section, as well as information derived from other sources. Programs have been established to assess R&M in a manner so as to yield consistent and accurate data and information that can be fed back into the product improvement process as well as to provide a "lessons learned" information base for subsequent acquisitions. The programs are designed to provide data and information that can be used to:

(1) Uncover problem areas, effect timely corrective action, and provide a solid basis for system R&M improvement programs

(2) Determine the effectiveness of design, test and program concepts applied during system acquisition

(3) Track the performance and, in particular, the R&M of the fielded system

Application of the feedback loop to service evaluation of R&M and correction of R&M problems is accomplished in five major steps, the last of which becomes the first step in a repetition of the cycle:

(1) Acquisition of Required Data. Use the data collection and reporting system to acquire the basic service use experience data, supplemented as necessary by system configuration and engineering data and operational information to ensure correlation between reported maintainability experience and the conditions under which the experience data was accrued.

(2) R&M Assessment. Analyze the reported experience data to derive a measure of the R&M parameters (e.g., failure rate, MTBF, mean corrective maintenance time ($\overline{M}_{ct}$), maximum corrective maintenance time ($M_{max_{ct}}$), maintenance manhours per operate hour, logistics delay time, etc.) at system, subsystem, equipment, major component, and lower levels, corresponding to the levels to which R&M was allocated, specified, and demonstrated during the development phase.

(3) Problem Definition. Identify, investigate, and describe the underlying problems which account for major discrepancies or deficiencies noted in the analysis of (2) above in terms amenable to translation into corrective action as design changes, documentation changes, maintenance or logistics procedural changes, etc., as appropriate. Introduce on a limited sampling basis such supplementary data recording forms, time clocks, instrumentation, and reporting instructions as required for the assessment of R&M where the field values greatly exceed predicted or demonstrated values.

(4) Corrective Action Assignment. Formally assign corrective action responsibility accompanied by problem descriptions developed under (3) above with specified criteria for verifying achievement of corrective action objectives.

(5) Follow-Through. Reassess R&M as in (2) above to evaluate effectiveness of corrective actions, to compare R&M trends relative to established improvement objectives, and to reevaluate problems identified in earlier assessments. This step begins the assessment cycle all over again.

DARCOM Regulation 709-2 (Ref. 16) defines the policies and procedures of a formal R&M System Assessment Program established by the Army. This regulation requires that assessments be performed in order to determine whether the fielded system has satisfied user needs for mission performance and logistic support. They are conducted in order to identify and take corrective action on problems which are degrading user satisfaction, operational readiness, and life cycle cost. Through the performance of such assessments the Army determines how a system is operating, uncovers and corrects problems in system operation and support, and thus helps achieve complete user satisfaction.

As presently structured, the System Assessment Program includes the assessment of all aspects of fielded system operations including:

(1)	Technical	- A narrative description of the system and its support equipment - Original design objectives - The results of development and operational tests - Corrective action results
(2)	Operational	- Initial field performance parameter values - Changes incorporated into the fielded system (e.g., payload, accuracy, reliability, availability, and maintainability) - Present field performance parameter values
(3)	Environmental	- Individual component shelf-life values - The reliability of components which require storage stockpile testing - The effect stored components are having on overall system reliability
(4)	Human Factors	- The user's opinion of the adequacy of the system - The quantity of personnel, by military occupational specialty - The quality of personnel, by military occupational specialty
(5)	Support	- Current problems - Development initiatives for replacement - Effectiveness of the present logistic support system - Improvement actions required - System improvement plans

DARCOM Regulation 702-9 states that maximum use will be made of existing field data to assess these areas. Other data sources include:

(1) Sample data collection programs
(2) Field visits and surveys
(3) User questionnaires
(4) User conferences
(5) Logistic personnel and field maintenance technicians

11.5.6 SYSTEM R&M IMPROVEMENT

In addition to optimizing R&M during acquisition through aggressive design, development, and production programs, substantial R&M growth potential exists during deployment. Some of this growth occurs naturally as the operations and maintenance personnel become more familiar with the equipment. However, to accelerate the growth rate and achieve significant increases in operational R&M requires the

application of a closed-up process of positive corrective action based on analysis and assessment of field R&M data. For newly deployed equipment, this closed-loop process can achieve significant reliability improvement, especially when used within the context of a total, disciplined system assessment program as discussed in the previous subsection. Reliability growth is based upon the iterative process of monitoring system operation to identify actual or potential sources of failures, to redesign out the failure source, and to fabricate and apply changes which improve system reliability. As such, reliability growth can be applied during development, production, or during operation. For fielded systems, the reliability growth process is a valuable tool to attain reliability improvements and achieve savings that could more than offset the cost of the reliability improvement program. The process is also performed during field deployment to eliminate problem areas not evident during the development phase.

In recognition of field R&M growth potential, each of the military services has formal product improvement programs. Examples are:

(1) Air Force - Productivity, Reliability, Availability, Maintainability (PRAM)
(2) Army - Reliability Improvement of Selected Equipment(RISE)
(3) Navy - Fleet Reliability Assessment Program (FRAP)

Application of these programs to selected systems has resulted in significant reduction in failure rates and maintenance and logistics support cost.

Each of the programs is similar in nature and charter in that they are concerned with "front end" studies of efforts leading to:

(1) reduced operating and support costs of in-service weapon systems and equipment
(2) increased efficiency in maintenance procedures
(3) improved standards and specifications for developing, procuring, and testing systems
(4) adaptation of existing equipment to broaden application
(5) operational readiness improvements

The R&M improvement program must work in conjunction with the data collection and assessment programs (as discussed in the previous section) in a total integrated process consisting of data collection, system assessment and improvement selection, development, and implementation to achieve reliability growth in the field.

As described in more detail in the previous section, the program is an iterative feedback process consisting of the following steps:

(1) acquisition of required data
(2) R&M assessment
(3) problem definition
(4) corrective action assignment
(5) follow through to evaluate effectiveness of corrective action(s)

Improving system reliability (MTBF) action involves a systematic review of several concepts which appear from the backup data to be most useful for reliability cost tradeoff considerations, among which are the following:

(1) The reduction of failure rates by operating components at reduced (derated) stress levels, accomplished by selecting components which have ratings well in excess of those required for their system application

(2) The use of improved components for which reliability has been significantly increased through special manufacturing techniques, quality control procedures, and testing methods

(3) Design simplification to eliminate parts or components

(4) The substitution of functionally equivalent items with higher reliability

(5) The overall reduction of failure rate through increased control of the internal system environment, e.g., through reduction of ambient temperature, isolation from handling effects, and protection from dust

(6) The provision of design features which enable prediction of incipient failures and permit remedial action to be taken before an operational failure occurs

(7) The provision of design features which reduce the probability of human-initiated errors

(8) The provision of multiple identical parts, paths or higher functional levels (redundancy) in order to prevent a system failure in the event that one element fails

(9) The reduction of failure rate through increased control of the environment external to the equipment, as through reduction of ambient temperature, isolation from handling effects, isolation of operator from ambient noise, and protection of equipment from dust

(10) The implementation of controlled screening and burn-in tests for the purpose of significantly reducing incipient failures due to undetected defects in workmanship or components

Similarly, maintainability (MTTR) can be improved by incorporating improved use of maintenance practices, providing higher quality technical manuals and maintenance aids or possibly better training to improve the skill level of the technicians.

Computing the impact of the improvement recommendations which appear most useful for cost tradeoff consideration on MTBF, MTTR, overall downtime and system performance, using the methods and techniques previously described, and determining the total cost for their implementation is an essential step in evaluating the effectiveness of the improvement.

Critical to the analysis process is the ability to assess quantitatively the cost effects of reliability and maintainability. The cost of each recommended change must take into account total cost throughout the life cycle of the system and accordingly must include cost elements associated with design, manufacture, procurement, installation, and field use (i.e., operation, maintenance, and logistics).

The final step is to compute cost/benefit factors, i.e., develop a numeric for each R&M recommendation which reflects the total cost of the change, its impact on system performance, and the cost avoidance to be realized over a given time period by their implementation. This will allow the determination of those change recommendations which have maximum cost effectiveness. The recommended changes can then be presented in an improvement plan in prioritized order of cost effectiveness, as defined by the computed cost/benefit factors.

REFERENCES

1. Schafer, R.E., A.E. Sari and S.J. Van DenBerg, <u>Stress Screening of Electronic Hardware</u>, RADC Final Report, RADC-TR-82-87 (AD-A118261), May 1982.

2. "Environmental Stress Screening Guidelines," The Institute of Environmental Sciences, Library of Congress Catalog Card No. 62-38584, 1981.

3. "Navy Manufacturing Screening Program," NAVMAT P-9492, Naval Material Command, May 1979.

4. Anderson, J.R., "Environmental Burn-In Effectiveness," McDonnell Douglas Aircraft Company, St. Louis, MO, AFWAL TR-80-3086, August 1980.

5. Schafer, R.E., L.E. James, et al., "Electronic Equipment Screening and Debugging Techniques," RADC-TR-78-55 (AD-A053561), March 1978.

6. Burrows, R.W., "Long Life Assurance Study for Manned Spacecraft Long Life Hardware," Vols. 1-5, Martin Marietta Corp., Denver CO, December 1972.

7. "Optimum Burn-In Determination," Tracor Sciences and Systems, Arlington, VA, Document No. 9229, November 1979, Contract No. DAAB07-78-C-2965.

8. Kube, F., and G. Hirschberger, "An Investigation to Determine Effective Equipment Environmental Acceptance Test Methods," Grumman Aerospace Corporation, Report No. ADR 14-04-73.2, April 1973.

9. Army Regulation AR 740-3, "Care of Supplies in Storage (COSIS)."

10. Army Regulation DARCOM-R 702-23, "Product Assurance - Storage Serviceability Standards (SSSs)."

11. Army Regulation AMC-R 702-7, "Product Assurance Depot Quality Assurance System."

12. Army Supply Bulletin SB740-99-1, "Storage Serviceability Standard for TSARCOM Materiel."

13. "Research Study of Radar Reliability and Its Impact on Life Cycle Costs for the AN/APQ113, 114, 120 and 144 Radar Systems," General Electric Co., Aerospace Electronic Systems Dept., Utica, NY, August 1972.

14. AMCP 750-16, "Maintenance of Supplies and Equipment, AMC Guide to Logistics Support Analysis," Headquarters, Army Materiel Command, January 1978.

15. "Information Analysis Centers Profile for Specialized Technical Information," Defense Technical Information Center, Defense Logistics Agency, Cameron Station, Alexandria, VA 22314.

16. DARCOM Regulation 702-9, Department of the Army, September 1977.

12.0 R&M MANAGEMENT CONSIDERATIONS

12.1 INTRODUCTION

The successful development and fielding of highly reliable and maintainable equipment and systems require the combined application of technical and management disciplines. Previous sections of this handbook have been devoted to the technical aspects of the design and development process, e.g., mathematical modeling, design and analysis methodologies, prediction and allocation methods, test procedures, etc. This section will concentrate on the management aspects of the process, e.g., planning, organizing, staffing, directing, and controlling.

In general, management and control of system reliability and maintainability must be based on recognition of the system's life cycle. Appropriate R&M management and engineering tasks must be performed during all life cycle phases.

The successful management of R&M during the system life cycle assumes the following premises:

(1) There are five definable phases in the creation of a military electronic system, namely: conceptual (CONCEPT), demonstration and validation (VALID), full scale engineering development (FSED), production (PROD), and deployment (DEPLOY), as shown in Figure 12.1-1. These are defined as follows:

    (a) Conceptual Phase - is the period where alternative solutions are explored and identified as meeting a validated need.

    (b) Demonstration and Validation Phase - is the period when selected candidate solutions are subjected to extensive study and analyses; hardware developed if appropriate, tested, and evaluated.

    (c) Full Scale Engineering Development Phase - is the period when the system and principal items necessary for support are designed, fabricated, tested and evaluated.

    (d) Production Phase - is the period from production approval until the last system is delivered and accepted.

    (e) Deployment Phase - is the period wherein the equipment is operated in the field throughout its useful life.

(2) There is a special R&M role in each of these phases. To achieve the R&M goals in the deployment phase requires planned actions in all previous phases.

(3) To assemble and execute an effective R&M program during any of the five life cycle phases requires not only a knowledge of R&M principles but also an understanding of the system itself and its associated technology.
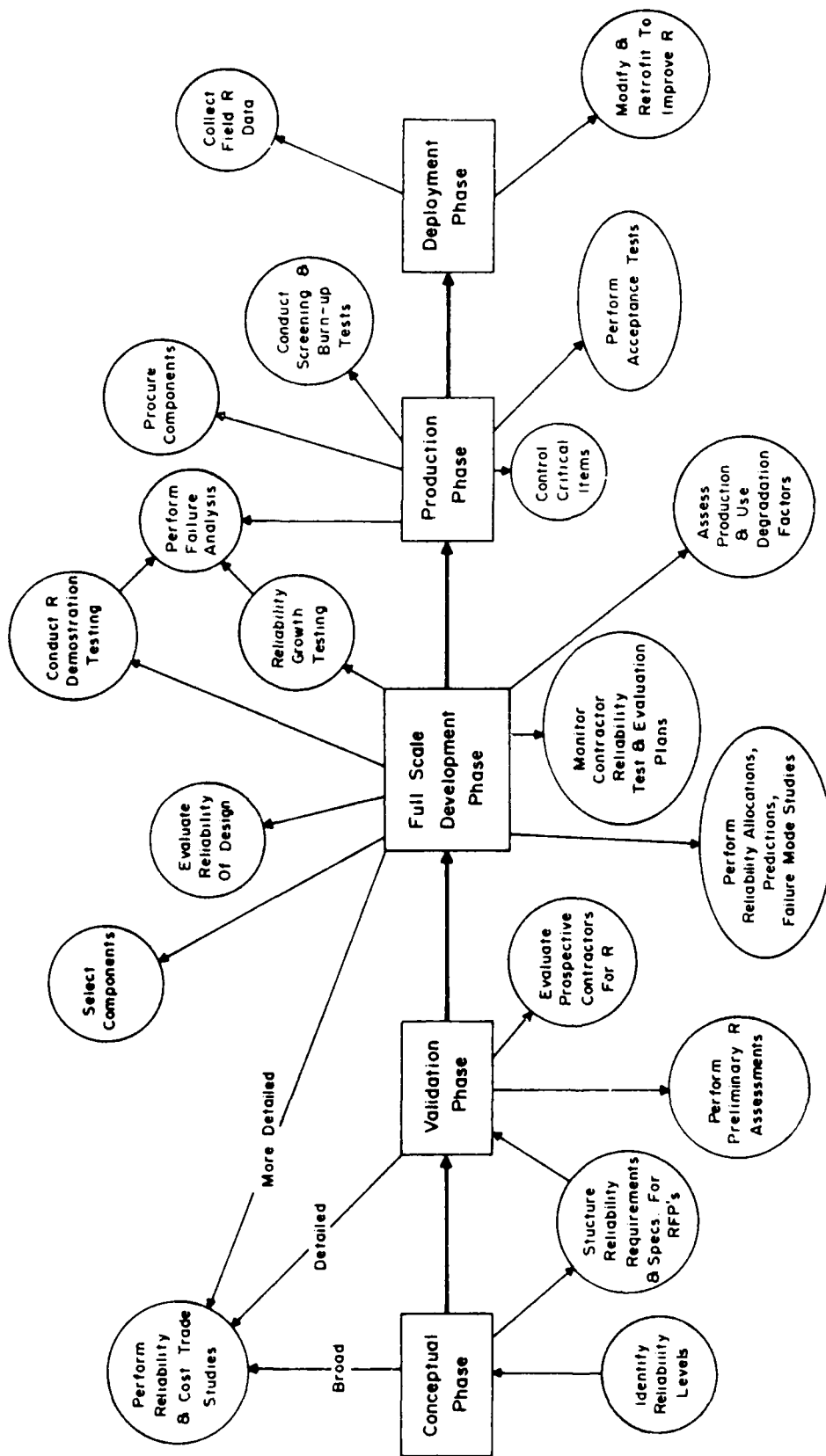
FIGURE 12.1-1: R&M ACTIVITIES SYSTEM LIFE CYCLE

(4) Quality/reliability control programs are essential during the production phase if the desired level of R&M is to be achieved in the deployment phase.

(5) More effective results will be achieved if R&M activities are managed as part of the system program, and not as separate activities.

As was shown in Figure 12.1-1 the achievement of R&M during deployment requires a coordinated performance of a series of tasks by managers and technical specialists. This series begins with the first conceptual studies of the new system, continues through production, and ends only when the system is phased out of use. The procuring activity (acquisition command), the manufacturer (contractor), the user (operational command) and the support activity (logistics) each has responsibilities in the chain of events.

The acquisition manager needs to have an understanding of these R&M engineering and management tasks, their timing, and the persons/groups responsible for their implementation. The manager must know how and when to specify, evaluate, and track R&M activities during each of the life cycle phases. He must understand the relative importance of each of the activities and the possible consequences of omitting or curtailing them. The manager should be knowledgeable as to the corresponding costs and risks involved with each decision element, so that they can be factored into a rational procedure for arriving at a final decision. It is the intent of this section to provide the manager with such information.

This section is structured as follows:

Section 12.2   provides an overview of life cycle R&M management considerations, guidelines and guidelines for minimizing life cycle costs and performing tradeoff analyses

Section 12.3   discusses methods of specifying, managing, and controlling reliability programs to achieve the desired reliability

Section 12.4   same as 12.3, but applied to maintainability

Section 12.5   same as 12.3, but applied to software

Section 12.6   discusses R&M data items which are the deliverable documents inserted into contracts, and used to manage R&M programs

Section 12.7   describes how to selectively apply and specify R&M program elements, depending upon the type of procurement, e.g., existing commercial equipment, modified commercial equipment, equipment meeting full military requirements

Section 12.8   provides guidelines for R&M program evaluation and surveillance

12.2 R&M PLANNING AND BUDGETING

The most basic of management functions is planning. Planning is deciding in advance what to do, how to do it, when to do it, and who is to do it. Budgeting, which goes hand in hand with planning, involves insuring that adequate resources, financial or otherwise, are available to carry out the plan to achieve the desired goal.

R&M planning cannot be done in a vacuum; it is an effort that must be dovetailed into the overall system program development plan. In the conceptual phase, for example, the choice of system design alternatives must include R&M estimates and projected costs in order to select the most cost effective system. In later development stages, R&M estimates are needed for system support planning for spare parts, repair and rework facilities, and personnel training. Hence, R&M is a key element in overall program planning, and from this planning should emerge a set of realistic, cost effective, R&M objectives.

Of course, planning includes the budgeting process of allocating the necessary resources to implement the plan. Without proper budgeting, R&M planning is an empty exercise. Accordingly, in the following discussions, planning assumes proper budgeting.

12.2.1 CONCEPTUAL PHASE PLANNING

In this phase, system R&M estimates are necessary to identify the best possible system alternative and to provide a valid picture of the cost effectiveness of the proposed system for comparison with other system alternatives. R&M estimates in the conceptual phase must necessarily be based on historical data.

R&M planning in the concept phase should include the following:

(1) Definition and refinement of realistic R&M requirements to be finally demonstrated during FSED tests.

(2) Parts selection criteria using military standard parts to the maximum extent possible. In particular, critical parts in terms of technology and/or reliability must be identified so that the program provides for the procurement of these special parts in a timely manner.

(3) Planning for tracking R&M progress through the development life cycle to provide a continual measure of achieved versus required R&M.

(4) A planned period of R&M growth, if required, during the validation and FSED using all available failure and maintenance data for R&M problem analyses and correction.

(5) Identification of program review milestones for assessing R&M progress.

(6) Adequate manning and budgeting to insure competent R&M planning and surveillance of the contractor's efforts, and the possible need to use outside activities for R&M support.

(7) Interfacing with eventual user and support commands on R&M plans and requirements.

12.2.2 VALIDATION PHASE PLANNING

In the validation phase, hardware will be developed, perhaps by competing contractors, and R&M planning will focus on contractual requirements. The statement of work (SOW) prepared by the acquisition activity will be using basic Service and Command guidance documents in the preparation of the SOW. The following are therefore considered critical inclusions in the SOW for implementation.

(1) Quantitative R&M requirements must be specified and defined. The hardware must be inherently capable of achieving the required R&M, and R&M predictions should substantiate this capability.

(2) R&M testing must be included as a requirement, executed by evaluation testing or demonstration testing or both. The extent of the R&M testing program, its intent, and, wherever possible, the acceptance criteria must be clearly identified.

(3) Fundamental design features which will affect maintainability must be stated. For example, built-in test provisions must be included in the validation phase equipment in order to evaluate its functional effectiveness even though the exact physical makeup of the hardware may not correspond to operational standards.

(4) Parts selection must be controlled. However, because of difficulties in obtaining preferred military quality parts in small quantities it may not be practical to employ them fully in the validation hardware. All substitute parts should be identical in form, fit, and function to the preferred parts to preclude difficulty with including preferred parts in later systems.

(5) R&M design tradeoff studies must be performed to include design for reliability and maintainability, redundancy options, optimum repair level analysis, failure mode analysis, and any other analyses required to optimize the design, or to provide input for other plans such as the detailed Maintenance Plan or Integrated Logistics Support Plan.

(6) R&M predictions must be performed and continually refined as the design matures to provide an indication of potential R&M of the system for use in making an FSED decision.

(7) A closed loop data system is required to obtain R&M data from all tests performed. The data will be used to determine the cause of R&M problems and to formulate corrective actions required.

(8) Program and design reviews are essential for control and motivation of the entire R&M program and to insure that detailed R&M design effort is progressing according to plan.

(9) Appropriate deliverable data items must be called out to provide the program office with visibility into the above stated activities and to document the ensuing results.

By the completion of the validation phase the program office must have the following R&M outputs in hand in order to m ke decisions and plans for the follow-on FSED phase:

(1) Predictions of the potential R&M capabilities of the system must be up-to-date. These must be realistically derived, commensurate with the expected operational environment and selected parts quality.

(2) Data on achieved R&M performance of the validation hardware should be in hand. The program manager must have available a track record of the R&M growth experienced during validation and sound engineering solutions to all R&M problems uncovered.

(3) System design tradeoff studies should be complete, using realistic R&M inputs to define the most cost effective system configuration.

(4) System design specifications intended for FSED must be completed. These must incorporate quantitative R&M requirements, clearly defined, and all corresponding R&M design requirements necessary for their achievement, i.e., parts selection criteria, built-in test features, modular configuration, environmental criteria, etc.

(5) System acceptance specifications must be completed defining R&M demonstration tests to be performed in FSED and production including test plans and test levels, system burn-in requirements, ground rules for classification and failures. Environmental qualification tests must also be defined.

(6) The R&M program plans for FSED must be completed.

Approval to proceed into FSED will be based on assurance that systems tradeoffs have produced a balanced and realistic set of performance parameters, risk areas identified and reduced to acceptable levels, and that cost and schedules for FSED are acceptable.

12.2.3 FULL SCALE ENGINEERING DEVELOPMENT PHASE PLANNING

Essential differences between the validation and FSED phases are:

(1) During validation, the realism of R&M requirements must be established, system tradeoffs made, and R&M problems identified and eliminated.

(2) During FSED, the requirements are firm, and the program geared toward implementing final design decisions and providing adequate demonstration tests to insure that R&M requirements will be met.

During the early part of FSED, the contractor must prepare R&M test plans which are important key program documents. The R&M test plans provide the execution details of the R&M demonstration tests. Next to unambiguous requirements, the R&M tests are the most essential elements during the FSED phase.

During FSED, a final Integrated Logistics Support Plan must be prepared utilizing R&M inputs from the Detail Maintenance Plan.

It is essential that, during FSED, adequate budgeting be provided for both the government and contractor to perform the necessary R&M program functions. All too often, budgeting for these activities is not given proper priority in the total program budget estimates.

12.2.4 PRODUCTION PHASE PLANNING

In the Production Phase R&M activities will be concerned with:

(1) Finding and fixing problems arising during production. These will be primarily workmanship and parts defects, since most design problems will have been resolved in previous phases.

(2) Performing stress, screening, and periodic verification tests to identify and correct reliability degradation during production runs.

(3) Insuring that quality/reliability control procedures are given required attention.

(4) Evaluating engineering change proposals (ECPs) for their effects on R&M.

12.2.5 DEPLOYMENT PHASE PLANNING

During deployment R&M activities will be concerned with:

(1) Data collection to track field R&M performance

(2) Establishment of test criteria and controls (and analyses of storage data) to assure the readiness of equipment and material items during storage.

(3) Analyses of field data to determine fruitful areas for R&M improvement.

12.2.6 COST FACTORS AND GUIDELINES

Most military equipment/system acquisition managers must cope with four basic, usually conflicting, criteria:

o performance
o cost
o schedule
o risk

The goal is to balance these criteria so as to obtain the "best" system. With the increasingly high costs of buying, operating, and maintaining weapon systems, further exacerbated by the high inflation rates of recent years, the term "best" has come to mean developing a system with minimum life cycle costs (LCC) consistent with required performance.

This balanced design approach is shown in Figure 12.2.6 in which design engineers and acquisition managers must balance performance, R&M, and unit production costs equally against the overall objective of minimizing the cost of ownership or LCC.
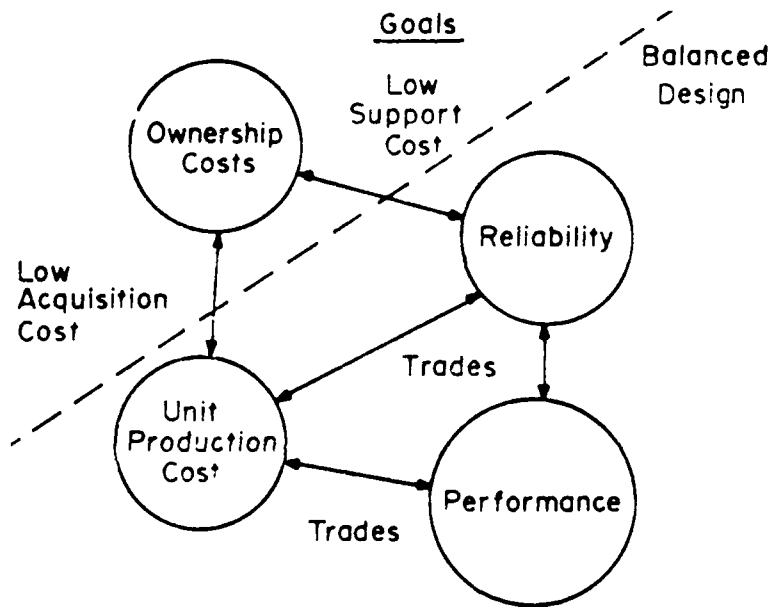
FIGURE 12.2.6-1: **BALANCED DESIGN APPROACH**

An important fact that the manager must keep in mind is that early design decisions "lock-in" a major portion of the life cycle costs. This is shown graphically in Figures 12.2.6-2 and 12.2.6-3 (Ref. 1).
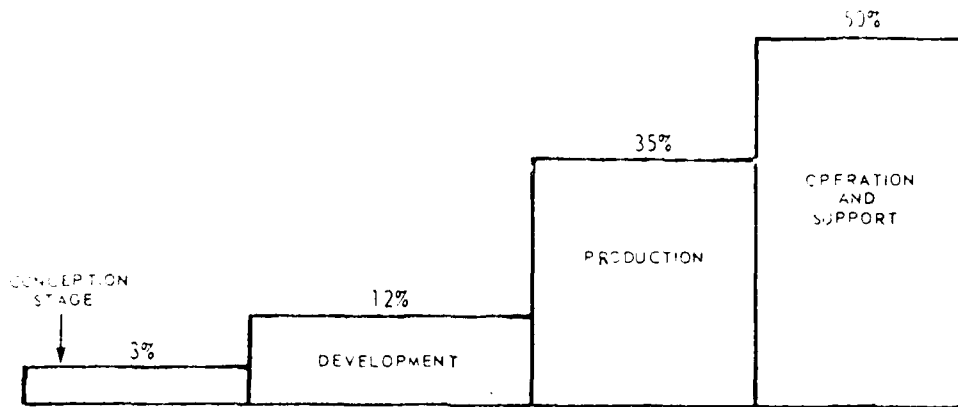
FIGURE 12.2.6-2: EXPENDITURES DURING LIFE CYCLE
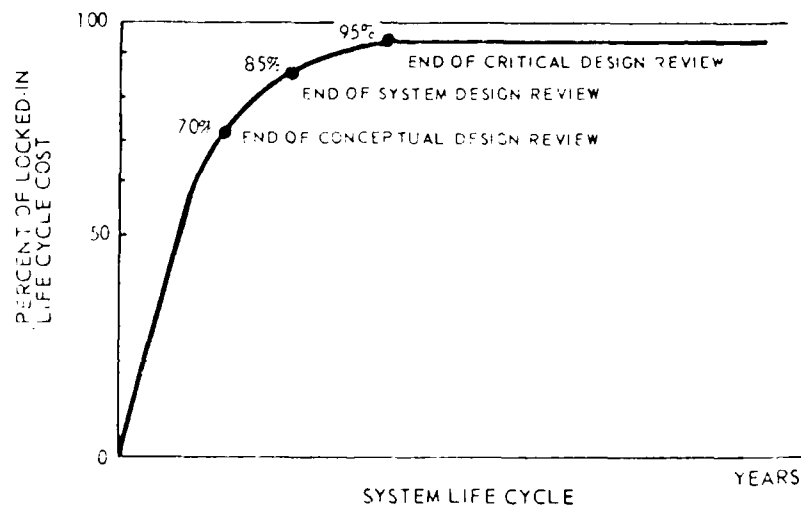
FIGURE 12.2.6-3: EFFECT OF EARLY DECISION ON LIFE CYCLE COST

These figures relate dollar expenditures and percent of locked-in life cycle costs to the life cycle of a project. These figures are held as being representative for the U.S. Department of Defense. Figure 12.2.6-2 shows that the design and development phase of a project consumed only 15% of the cost of a typical project, as opposed to 35% for the production phase and 50% for the in-service phase. Although only 15% of the expenditures were made prior to production, Figure 12.2.6-3 shows that about 90-95% of the life cycle costs were determined. The design specifications that were approved prior to production determined how it would proceed and, therefore, determined the costs to be incurred in that phase. Similarly, the detailed specifications were produced based upon a certain operational, maintenance and supply support policy. These policies and the design dictate such in-service variables as manpower, consumables and spares levels.

The significance of these figures should be kept in mind by the acquisition manager. Prior to the conceptual design review, 100% of the design can be altered and 100% of the life cycle cost can be affected. Completion of the conceptual design review gives approval for the basic framework of the design. The concepts approved, although not a written set of specifications, place constraints on the design team, narrow their decision horizon and fix a certain level of the life cycle cost on the project. As time progresses, the decision horizon narrows and a greater percentage of life cycle costs become determined. It has been estimated that by the time 15% of a typical system's life cycle has expired, 90% of the life cycle costs have been determined. Thus, a manager needs to be familiar with the available tools to enable him to make timely decisions to minimize LCC.

R&M decisions have a great impact on LCC. The frequency of failures and the time to repair them determine the resources, manpower, and material needed to maintain the system in the field.

The principal difficulty which confronts the acquisition manager in making R&M decisions is the complexity of the problem. The equipment R&M requirements defined in the development specification establish the objectives of the design. As shown in Figure 12.2.6-4 however, these must be considered in conjunction with numerous other requirements and constraints, all of which influence operations and support costs.
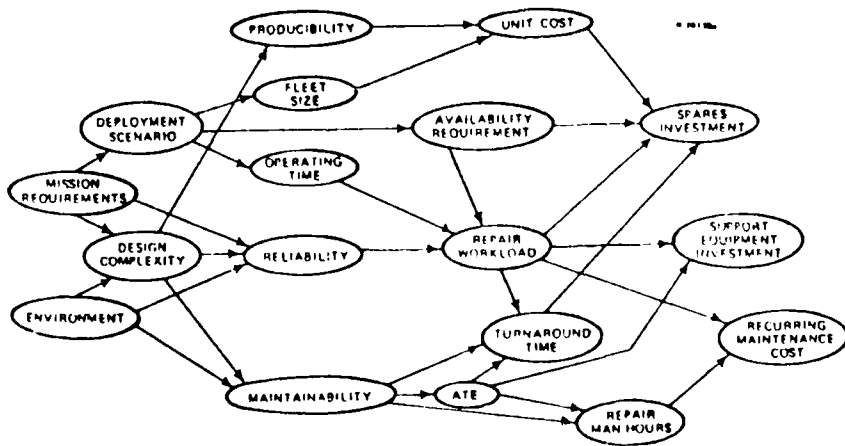
FIGURE 12.2.6-4:   INTER-RELATIONSHIP OF REQUIREMENTS & CONSTRAINTS

Despite the complexity of the problem, systematic analysis procedures can be employed during early stages of a program which can help in the decision making process (Ref. 2). Some examples are:

o identification of principal cost drivers (focuses attention on high cost areas)

o logistic support tradeoff analysis (e.g., comparison of alternative maintenance policies)

o assessment of cost sensitivities to uncertain parameters such as mean-time-between-failure (MTBF), mean-time-to-repair (MTTR), resupply time, etc.

o acquisition versus support cost tradeoff analyses (i.e., tradeoff between higher reliability and, hence, higher unit cost and lower support costs)

The utility of such analyses lies in the insights regarding where planning and design emphasis must be placed. As was shown previously, the earlier these insights are gained the easier it is to influence LCC.

Additionally, the acquisition manager has at his disposal a number of management tools and contractual mechanisms which can aid in the development of minimum LCC systems. Some examples are:

o design-to-cost procedures
o life cycle cost concepts
o product performance agreements

12.2.6.1 DESIGN-TO-COST PROCEDURES

Design-to-cost goals are used in contracts to seek the best balance between performance and acquisition cost in a system development program. The original intent of the use of design-to-cost procedures was to slow the trend of continually increasing acquisition costs due to emphasis on achieving the ultimate in system performance.

Design-to-cost (DTC) can take different emphases dependent on the type of development program. Four programs with varying design-to-cost emphasis are shown in Table 12.2.6.1-1. As seen in the table, "Design-to-Unit-Production-Cost" (DTUPC) has been emphasized in most major military programs. DTUPC can determine the number of aircraft or equipment that the DOD can "afford."

DTC policies and objectives are delineated in DOD Directive 5000.28 (Ref. 3). Also, a design-to-cost guide has been jointly published by each of the military services (Ref. 4).

TABLE 12.2.6.1-1: TYPES OF DESIGN-TO-COST PROGRAMS

Design-to-Cost Programs	Program Characteristics	Program Examples
Production Unit Price	Large Quantity Procurements	o Close Support Aircraft A-10 o Lightweight Fighter
Total Program Costs	o Complex Equipment o Small Buys o High Development Cost	o AWACS o Advanced Airborne Command Post
Production Unit Cost and Installation Cost	o Large Quantity Procurement of Subsystems	o Airborne Radar o Avionic Equipment o TACAN o Gyroscope
Development and Operating Costs	Facilities and Construction Programs	o Ground Radar Installations

As is shown in Table 12.2.6.1-1, most DTC contractual requirements have emphasized unit production cost. However, the ultimate goal is to minimize the cost of ownership or LCC. Minimizing unit production cost is only one step toward achieving the ultimate goal. Emphasizing this step and ignoring the ultimate goal could conceivably result in compromising R&M requirements, thus resulting in increased support costs. This means that one should strive for a design which will:

o   maximize performance within unit cost goals, and
o   minimize support cost to minimize LCC.

In other words, DTC and LCC must be jointly considered.

12.2.6.2 LIFE CYCLE COST (LCC) CONCEPTS

LCC is defined as the total cost to the government of acquisition and ownership of a system over its full life. It includes the cost of development, acquisition, operation, support, and eventual disposal. Figure 12.2.6.2-1 is provided as a guide for the acquisition manager in terms of the activities that should be performed at each phase of a system's life cycle in order to minimize LCC. They are quite self explanatory, and, for the interested reader, are treated in greater detail in Section 10.

Conceptual Phase	Validation Phase	Full Scale Development Phase	Production Phase	Operational Phase
a Identify LCC cost drivers	a Refine R&M cost tradeoff analysis	a Review contractor LCC provision/ goals	a Perform Engr Change Proposal (ECP) reviews	a Collect field cost data – operation – support
b Perform sensitivity performance level cost trade studies	b Perform cost of ownership assessment – operation – support	b Define LCC procurement requirements	b Develop warranty/ guarantee selection guidelines	b Perform cost comparison studies
c Identify optimum R&M levels	c Review LCC procurement requests	c Conduct detailed cost of ownership analysis	c Conduct LCC achievement test	c Perform update studies, modify and retrofit to reduce cost
d Develop LCC procurement approaches	d Conduct source selection	d Prepare LCC achievement test plan/ procedure		
e Define design to cost (DTC) requirements	e Develop LCC provisions (DTC, RIW)	e Monitor contractor LCC plans and achievement of goals		
f Review LCC Provisions including DTC/RIW	f Initiate development cost monitoring plan	f Establish "cost of change" review guidelines		
g Perform cost of ownership assessment – operation – support	g Initiate LCC guidelines for RFP and source selection			
h Conduct comparison cost studies of current systems/equipments				
i Review LCC provisions – DTC – RIW				

FIGURE 12.2.6.2-1: LIFE CYCLE COST ACTIVITIES

From a managerial point of view, for LCC to be successful it must be an explicit part of the original contract competition. Competition in system development and production serves to place a "downward pressure" on the estimates of equipment production costs proposed by competing suppliers. Recognizing that competition will almost certainly cease to exist at entry into the production phase of a program, the objective of LCC competition is to obtain as much assurance as possible prior to production that the selected equipment will satisfy the requirement for lowest practical life-cycle cost. To accomplish this, the competitive phases of an LCC program are structured with emphasis on identifying and reducing the life-cycle cost drivers. In addition, in a properly planned development program where the participating contractors are thoroughly briefed on the importance of LCC and where provisions exist for extensive development testing to validate cost related parameters (e.g., reliability), competition serves to induce each contractor to address cost-risk design problems which would otherwise not be encountered until after production was underway.

12.2.6.3 PRODUCT PERFORMANCE AGREEMENTS

During the past decade, one of the relatively new tools applied to reduce life cycle costs of DOD equipment/systems has been the use of Product Performance Agreements (PPAs) in the form of warranties/guarantees.

These procedures were adapted from standard commercial practices which have been used in the US for years. Their purpose is to extend the contractor's responsibility for his equipment for a long period of time beyond delivery. He must not only consider design, development, and production costs, but also long term support costs. He is, thus, strongly motivated to build more reliability and maintainability into his equipment to reduce support costs, minimize the sum of production and support costs, and maximize profit.

The initial impetus for the use of warranties was provided by the airline industry, which has been using them successfully for years. One of the first DOD warranty studies was done by the Rome Air Development Center in 1969 entitled "Airborne, Electronic Equipment Lifetime Guarantee." Another study (Ref. 5), "The Use of Warranties for Defense Avionic Procurement," issued in 1973, sought to determine the basic feasibility and utility of the warranty concept for DOD application. Results of this study formed the basis for the Air Force's "Interim Guidelines Reliability Improvement Warranty" (Ref. 6) issued by Hq USAF AF/LGP in July 1974. A follow on effort (Ref. 7) entitled "Guidelines for Application of Warranties to Air Force Electronic Systems," published in 1976, developed criteria which can be used in the selection of candidates for warranty application, provided sample contractual terms and conditions, and provided a computer based cost estimating model for use in Warranty vs. Nonwarranty LCC evaluations. Another RADC study (Ref. 8) investigated the application of Warranty/Guarantee concepts in the fixed ground maintenance environment. The study provided guidelines for the use of warranty plans containing incentive features on other than reliability alone (e.g.,availability).

Most recently (Ref. 9) the Air Force published a "Product Performance Agreement Guide," which expands the warranty concept to areas such as software, repair/exchange agreements, logistics support, etc.

12.2.6.3.1 TYPES OF PRODUCT PERFORMANCE AGREEMENTS

Following are brief descriptions of a number of Product Performance Agreements that may be appropriate for use in DOD contracts.

Inspection

This agreement is applicable to fixed price contracts. It provides for a preacceptance inspection of supplies by the Government and its use is intended to ensure that all delivered supplies conform to contract requirements at time of delivery.

Inspection of Supplies and Correction of Defects

This agreement is applicable to cost type contracts. It provides a mechanism to obtain correction any nonconformance discovered by the Government in all work performed under the contract.

Warranty of Supplies

This agreement is applicable to fixed price contracts. It extends the contractor's responsibility for materials, workmanship, and specification conformance beyond the period of acceptance of supplies.

Correction of Deficiencies

This agreement is applicable to fixed price contracts. It applies to deficiencies in design as well as materials and workmanship. The contractor is responsible to repair or replace deficient items and to make design changes necessary to satisfy performance requirements.

Warranty of Technical Data

This agreement is applicable to either cost reimbursement or fixed price contracts. It provides for correction or replacement of deficient data for a specified time after delivery and inspection.

Rewarranty of Repaired/Overhauled Equipment

This warranty applies to the results of repair or overhaul efforts. The contractor agrees to warrant that the repaired or replacement parts and/or materials are free from any further defect in material or workmanship for a specified period.

Repair/Exchange Areements

When the volume of repair activity for an item being introduced into the DOD inventory is expected to be too low to justify organic support, the repair/exchange agreement can provide an alternate approach. The

contractor must establish the capability to exchange complete items or to repair parts returned to his facility within agreed upon turnaround times.

Reliability Guarantee

The contractor agrees to maintenance/overhaul intervals for components and/or subsystems. When specific types of failures occur between overhaul intervals in covered items, the contractor is responsible to supply a specified combination of labor, material, or replacement items.

Reliability Improvement Warranty (RIW)

Under RIW, the contractor agrees to repair all covered failures for a specified period at no additional expense to the Government. This warranty is designed to increase equipment reliability and reduce repair costs.

Mean-Time Between Failure-Verification Test (MTBF-VT)

The MTBF-VT can be used to achieve improvement in operational reliability. The MTBF-VT can be applied at the "black-box" or subsystem level or components from several subsystems can be aggregated to system level commitment. The test of compliance would normally be scheduled for the first deployed unit. Deviations between MTBF targets and measured performance form the basis for rewards or corrective action.

Availability Guarantee

The Availability Guarantee can be used to reduce downtime for systems or equipments which operate in a continuous mode or with dormant systems where readiness upon random demand is a critical requirement. The equipment should provide a positive indication of operability either through continuous performance checks or, in the case of dormant systems, through go/no-go checks.

Logistics Support Cost Guarantee (LSCG)

The LSCG is used to control and reduce selected aspects of life cycle cost and to improve equipment supportability in operational use. The LSCG uses a cost model which describes the effect that system design, operating, and logistics characteristics have on potential support costs. The model addresses those features of the equipment which impact support investment and recurring operations and support costs. Deviations between target logistics parameters and measured performance form the basis for rewards or corrective action.

Maximum Parts Cost Guarantee

The Maximum Parts Cost Guarantee can be applied to equipments when repair costs are critical. The contract specifies an average repair cost (which can include parts and labor) for the system or critical portions thereof. "Actual" average repair cost is then compared with the specified average to determine what remedy or consideration is applicable.

Utility Functions

Utility function agreements can be applied to consumable items. The DoD establishes a utility function for the item being procured (e.g., landings per tire or set of brakes or starts per battery). The contractor specifies a value for this function. A demonstration is performed to develop an "actual" value of the utility function. The "actual" and "specified" values are compared to determine what remedy or consideration is applicable. This type agreement is often incorporated as the basis of life cycle cost procurement actions for consumable items.

Reliability Improvement Warranty (RIW) With a Mean Time Between Failure (MTBF) Guarantee

The MTBF guarantee can be applied to systems where the objective is to achieve substantial reliability growth. An increasing series of target values is specified over consecutive time periods of the guarantee. Failure to meet target values results in contractor corrective action. Exceeding targets could result in incentive awards.

Chronic Line Replaceable Unit (LRU) Guarantee

A Chronic LRU Guarantee can be applied to LRUs where mean time between removals (MTBR), mean time between failure (MTBF) or similar reliability criteria are an important consideration. During the period of the guarantee, any LRU which experiences an extraordinary number of consecutive removals is designated a "chronic LRU." The contractor is required to replace chronic LRU's and chronic LRU's are not counted in calculating actual MTBR or MTBF results.

Mean Time to Repair (MTTR) and Mean Time Between Unscheduled Removals (MTBUR) Guarantees

MTTR and MTBUR Guarantees can be used on systems and subsystems where downtime or frequency of maintenance are critical to equipment performance. Measurements of achievement under operational conditions will be made over a series of specified intervals. When measured achievements fall outside of acceptable limits, a specified remedy is required.

Ultimate Life Guarantee

The Ultimate Life Guarantee can be applied to basic elements of a system such as aircraft structure, engines, and landing gear. A value is established for the life of the item and a remedy identified if failures occur.

Commercial Service Life Guarantee

A Commercial Service Life Guarantee can be used to extend limited term warranty coverage to the service life of the item.

Software Design Guarantee

This guarantee may be applied prior to a production contract award since its purpose is to provide contractors with an incentive to develop software packages with inherently high quality, low maintenance and update costs. As part of a development contract, quantitative targets for parameters such as modularization, documentation, testability, and transportability are established for software and demonstration requirements.

Software Configuration Guarantee for an LRU

This guarantee may be applied to software packages associated with a system or other specific set of LRUs. The contractor agrees to be responsible, at no additional cost, for software changes due to associated changes that are the contractor's responsibility. The contractor is also responsible to maintain software configuration and documentation.

Test and Repair Improvement Guarantee

This guarantee may applied to the test equipment and test procedures that are developed for a system. The contractor guarantees that his test equipment and procedures, when applied in accordance with applicable documentation, will demonstrate MTBR (or MTBF) characteristic of systems in field operation. When comparisons between operational and test results fall outside specified boundaries, the contractor is responsible to make changes to the test equipment or procedures.

Method of Test Guarantee

This guarantee is intended to ensure that the unique test equipment and test methods used for specified LRUs will accurately verify the performance of the LRU's during an agreed upon period of time. The contractor at no additional cost will replace, modify, or repair test equipment and methods when deficiencies occur. A demonstration will be conducted to determine compliance with this guarantee.

Implementation of these concepts should be an integral part of comprehensive product assurance planning. A key element of planning is the need to relate available product performance agreements or concepts to:

o   A program's design or development objectives.

o   What a product should accomplish once it is deployed.

o   Whether a program's objectives or expectations can be quantified and measured at a reasonable cost.

Once it is determined that the use of product performance agreements is appropriate, it will be necessary to select, develop, or tailor product performance contract provisions to the program involved. Innovative thinking and joint DoD/contractor cooperative development of these provisions should be emphasized throughout the life of the program.

Reference 9, in addition to describing the PPA's in more detail, provides broad guidance for tailoring associated contract provisions to selected programs.

12.2.6.3.2 WARRANTY/GUARANTEE PLANS

Of the PPAs mentioned in the previous subsection, the types most commonly used by DoD to improve reliability and reduce support costs have been warranty-guarantee agreements.

To establish a basis for subsequent discussion, the following definitions are provided:

o   Warranty - a contractual obligation that provides incentives for the contractor to satisfy system field operational objectives of the user. The contractor is given an incentive, through a fixed price commitment, to repair or replace equipment found to be defective during the period of warranty coverage.

o   Guarantee - a commitment embodying contractual incentives, both positive and negative, for the achievement of specified field operational goals.

Table 12.2.6.3.2-1 highlights the principal features of the three basic types of warranty-guarantee plans that have been used in DoD procurements. The following paragraphs briefly describe the plans; more details are provided in the cited references.

Reliability-Improvement Warranty (RIW)

The RIW plan commits the contractor to perform stipulated depot type repair services for a fixed operating time, calendar time, or both, at a fixed price. While the major expenditures of a warranty procurement are for the repair services involved, the primary objectives are to secure reliability improvement and reduce support costs. The question of whether the contractor can provide depot repair services at a cost lower than that of military repair is secondary to the objective of reliability achievement.

Under the RIW, the producer typically agrees, prior to production, that the equipment he delivers will achieve a specific reliability level (MTBF) before expiration of the warranty period. In return, he is paid a fixed warranty price for each warranted item as part of the procurement contract. Typical warranty periods range from two to five years. While the warranty agreement is in effect, the producer will perform all necessary repairs to failed equipment. The agreement may also contain settlement provisions which delineate the producer's liability in the event the reliability goal is not achieved. During the warranty period, the incentive for the producer is to minimize his outlay for repair and potential settlement liability by closely monitoring the actual reliability, and implementing improvements which promote reliability growth.

TABLE 12.2.6.3.2-1: FEATURES OF CURRENT WARRANTY-GUARANTEE PLANS

Features	RIW	RIW/MTBF	LSC
Objective	Secure reliability improvement/reduce support costs	Achieve stated reliability requirements/reduce support costs	Achieve stated logistic-cost goal
Method	Contractor repairs or replaces all applicable items that fail during coverage period; implements no-cost ECPs to improve reliability	Same as RIW; in addition, contractor provides additional spare units to maintain logistic pipeline when MTBF goals are not met	Normal Air Force maintenance; operational test performed to assess LSC: penalty or corrective action required if goals are not achieved
Pricing	Fixed price	Fixed price	Fixed price or limited cost sharing for correction of deficiencies
Incentive	Contractor profits if repair costs are lower than expected because of improved R&M	Similar to RIW, plus possible severe penalty for low MTBF	Award fee if goal is bettered; penalties for poor cost performance

RIWs have been used by all three services for some selected procurements. Some examples are:

o	F-16 Avionics Subsystems	Air Force
o	AN/ARN-118 TACAN	Air Force
o	OMEGA Navigation Set	Air Force
o	Lightweight Doppler Navigation System	Army
o	CN-494A Gyro	Navy
o	ASO-2171 Gyro	Navy

MTBF Guarantee

The MTBF guarantee requires the contractor to guarantee that a stated mean time between failures (MTBF) will be experienced by the equipment in the operating environment. If the guaranteed level is not met, the contractor is typically required to institute corrective action and to provide consignment spares until the MTBF improves.

The MTBF guarantee is normally procured in association with an RIW. An RIW plan provides incentive for MTBF achievement through the contractor maintenance support commitment. The MTBF guarantee provides an even stronger incentive because the contractor is obligated to provide consignment spares to relieve pipeline shortages that may result from low MTBF. The MTBF plan also includes requirements for improving the

MTBF to stated values. The added risk the contractor takes in providing this guarantee will be reflected in his bid price. The procurement organization must then determine if the protection provided is cost effective in relation to the price.

Logistic Support Cost Commitment

The logistic support cost (LSC) commitment is another means of controlling an equipment's operational effectiveness. Under this plan the contractor makes a contractual commitment regarding a specified LSC parameter, which is quantified through an LSC model. A controlled operational field test is subsequently performed to acquire data for the key variables in the LSC model. The measured LSC parameter is then compared with the contractually specified or target value. There is considerable variation among LSC commitment plans regarding the action taken as a result of the operational test. Most plans, in the event of achieving a lower measured LSC, provide for an award fee predicated on the amount by which the goal is underrun. In the event of an overrun, the plans provide for reducing or eliminating the award fee. In addition, some plans have required the contractor to take corrective action to achieve the stated goals or be penalized monetarily. In recognition of the risk inherent in this concept, the contractor bids a fixed price for undertaking a commitment where corrective action may be required. These types of plans are considered to fall under, or are an adjunct to, correction-of-deficiencies (COD) clauses. In the event the cost of correcting deficiencies exceeds the contractor's bid amount, provision may be made for Government and contractor cost sharing the overrun up to some specified ceiling. Costs beyond the ceiling must be borne solely by the contractor.

12.2.6.3.3 WARRANTY APPLICATION CRITERIA

To aid the manager in making a decision as to whether a warranty should be used in his procurement, warranty application criteria have been established (Refs. 7 and 8). They are shown in Table 12.2.6.3.3-1.

The selection criteria have been grouped into three areas; procurement factors, equipment characteristics, and operational factors. The areas are considered equally important with respect to accepting or rejecting the use of warranty.

Some of the criteria are considered more important than others. Three classes of importance have been established:

(1) Major. Failure to meet the stated criterion could be grounds for not using warranty.

(2) Secondary. Failure to meet the stated criterion will generally not be a sufficient basis for rejecting warranty, but a combination of such events could be.

(3) Minor. Failure to meet these criteria is generally not considered serious, but it may require special considerations in structuring the warranty contract or administrative procedures.

It is emphasized that the warranty application criteria are basically qualitative and are intended to indicate the general feasibility of warranty application.

A complete analysis of warranty potential, especially from the economic viewpoint, cannot be made until warranty price and implementation proposals are received from the bidding contractors. The criteria listed in Table 12.2.6.3.3-1 must therefore be viewed as an initial screening device to select those procurements for which the effort in developing a warranty clause is believed to be worthwhile.

12.2.7 TRADEOFFS

Throughout the system acquisition process, system engineers, designers, and acquisition managers are confronted with decision problems concerning the selection of one solution from among many alternatives. The term "tradeoff" as it applies to decision making is defined as the procedure by which several alternatives are evaluated to provide a solid basis for choosing only one. It is essentially, a system optimization problem under a series of constraints. This was discussed in Section 4.

Tradeoff studies are an inherent part of the design process, and are performed in sequence beginning at the highest system level parameters and proceeding downward to equipment design details. For example, as was shown in the previous section, in the early phases of system design, tradeoff studies are performed at the broad system level, e.g., tradeoff of the performance, cost, schedule and risk parameters to arrive at the "best" alternative solution. As design proceeds and requirements become firmer, tradeoff studies are performed involving lower level system parameters, e.g., reliability, maintainability, availability, safety, logistics supportability, and life cycle costs. As these parameters become fixed, tradeoffs are performed within each parameter. For example, in reliability tradeoff studies, one might study the following options to achieve a design of the desired equipment reliability: 1) more reliable parts, 2) design simplification, 3) component derating, 4) reliability growth, or 5) redundancy. Even within each of these parameters further tradeoff studies may be needed; for example 1) active versus standby redundancy, and 2) redundancy at subsystem, equipment, or subassembly level.

Previous sections have described tradeoff procedures for the design engineer. Following is some guidance for the manager on the types of tradeoff studies which should be performed, and when.

12.2.7.1 CONCEPTUAL PHASE TRADEOFF STUDIES

Tradeoff studies should be performed among reliability, maintainability, safety, performance, physical configuration, environmental use conditions, and other system requirements and design constraints to provide the basis for design optimization by the system activities in the conceptual phase. The analyses must be kept current with each design iteration of each alternative consideration during the conceptual phase. Dynamic feedback of analytical results should be provided to system engineering and conceptual design activities for guidance in performing design iterations. These studies should typically include the following:

TABLE 12.2.6.3.3-1: WARRANTY APPLICATION CRITERIA

Criteria	Importance Rating*		
	RIW	RIW/MTBF	LSC
Procurement			
The procurement is to be on a fixed-price basis.	1	1	1
Multi-year funding for warranty services is available.	1	1	N/A
The procurement is competitive.	2	2	2
Potential contractors have proven capability, experience, and cooperative attitude in providing warranty-type services or LSC commitment.	2	2	2
The procurement quantity is large enough to make warranty economically attractive.	2	2	N/A
Analysis of warranty price versus organic repair costs is possible.	2	2	N/A
An escalation clause is included in the contract that is applicable to warranty or LSC costs.	3	3	3
The equipment will be in production over a substantial portion of the warranty period.	3	1	2
Equipment			
Equipment maturity is at an appropriate level.	1	1	2
Control of unauthorized maintenance can be exercised.	1	1	2
Unit is field-testable.	1	1	N/A
Unit can be properly marked or labeled to signify existence of warranty coverage.	1	1	N/A
Unit is amenable to R&M improvement and changes.	1	1	3
Unit is reasonably self-contained.	2	2	3
Unit can be readily transported to the contractor's facilities.	2	2	N/A
Unit has high level of ruggedization.	2	2	N/A
Unit maintenance is highly complex.	3	3	N/A
An elapsed-time indicator can be installed on the equipment.	3	1	1
Operation			
Use environment is known or predictable.	1	1	1
Equipment operational reliability and maintainability are predictable.	1	1	1
Equipment wartime or peacetime mission criticality is not of the highest level.	1	1	N/A
Equipment has a high operational utilization rate.	2	2	3
Warranty administration can be efficiently accomplished.	2	2	N/A
Duplication of an existing or planned government repair facility is not costly.	2	2	N/A
Unit reliability and usage levels are amenable to warranty maintenance.	2	2	N/A
Operating time is known or predictable.	2	2	3
Operational failure and usage information can be supplied to the contractor.	2	1	3
Backup warranty repair facilities are available.	3	3	N/A
Provision has been made for computing the equipment's MTBF.	N/A	1	1

*1 = Major; 2 = Secondary; 3 = Minor.

(1) <u>Performance Analysis</u>. Evaluate reliability as a function of mission performance characteristics. Plot reliability functions for each of several possible alternative definitions of "acceptable" performance.

(2) <u>Maintainability Analysis</u>. Evaluate reliability vs. maintainability under alternative design concepts and life cycle cost objectives for specified levels of availability.

(3) <u>Availability Analysis</u>. Evaluate reliability and maintainability tradeoffs for several "acceptable" levels of availability and for several alternative approaches to availability assurance, e.g., design redundancy, premission system operability testing, preventive maintenance, etc.

(4) <u>Life Cycle Cost Analysis</u>. Evaluate the cost of reliability and maintainability acquisition (for several levels of performance) vs. the cost of maintenance and support in the deployment phase.

(5) <u>Schedule/Risk Analysis</u>. Evaluate the technical risks and schedule requirements associated with the reliability and maintainability acquisition objectives defined in (4).d above.

(6) <u>Operational Suitability</u>. Combine the results of the preceding analyses to produce a family of design configurations which would satisfy the operational requirements with a quantitative assessment of operation suitability, logistics supportability, life cycle costs, and acquisition schedule projected for each configuration. Perform mission simulation analysis for each configuration using computer techniques where necessary, to verify operational suitability estimates and evaluate conformance to the operational requirements.

(7) Select the best all-around configuration from those described in (6) above, and reassess the reliability and maintainability feasibility to verify the reliability and maintainability requirements and potential for the selected design configuration.

An approval decision can be made on results of tradeoff studies if the design concept selected on the basis of the studies satisfies the following criteria:

(1) <u>Conformance</u>. Reliability and maintainability as measures of operational suitability, must satisfy the reliability and maintainability objectives derived from the operational requirement.

(2) <u>Analytical Validity</u>. Reliability and maintainabilty data and mathematical models used in the tradeoff studies must be valid, i.e., must be conservatively realistic with respect to current operational experience.

MIL-HDBK-338-1A

12.2.7.2 VALIDATION PHASE TRADEOFF STUDIES

During this phase, the contractor's system analysis involving reliability and maintainability trade offs against each other, and other design parameters, is reviewed to verify realism, completeness and objectivity in prediction, allocations, and simulation analyses made on each design configuration considered. Contractor reliabilty and maintainability data required for in-process review of this task includes a current updated version of his earlier analysis, to verify that the contractor's proposed allocations are consistent with the mission models for the design, considering relative importance and duty cycle of constituent end items. Procedures (and data) by which requirements are allocated to equipment and lower end item level must be revalidated. Reliability and maintainability requirements must be defined in quantitative terms for integration into the allocated baseline specifications for constituent end items of the system.

The tradeoff and system analysis should typically include the following:

(1) <u>System Description</u>. Verify system description in terms of functional and physical configuration, performance limits associated with primary and alternate modes of operation, maintenance concept applicable to the design, equipment utilization factors, and mission profiles for the defined missions.

(2) <u>Reliability and Maintainability Modeling</u>. Validate block diagrams, taking into consideration redundancy possibilities, alternate modes, and back-up system capabilities.

(3) <u>Data Validity</u>. Validate equipment failure rates and repair rates, etc., used in the simulation study.

(4) <u>Reliability and Maintainability Allocations</u>. Verify consistency of allocated design requirements for each constituent subsystem, equipment, and separately procured end item of the system; and verify that minimum acceptable reliability and maintainability requirements to be demonstrated by test correspond to the allocated design requirements.

(5) <u>Test Requirements</u>. Verify adequacy and applicability of reliability and maintainability demonstration and test requirements, conditions, and acceptance critria for each allocated requirement.

(6) <u>Feasibility Study</u>. Validate feasibility estimates for each of the allocated values, based on current design configuration; evaluate differences between specified, predicted, and allocated reliability and maintainability for each subsystem; evaluate alternative approaches under consideration by system engineering, to achieve the specified requirements.

(7) <u>Problems</u>. Review problems identified within each subsystem/equipment; verify criticality ranking, corrective action

12-25

requirements, and estimated growth potential available through problem correction. Identify areas where further system design and operational analyses are required to determine equipment essentiality, back-up capabilities, etc. Approval of design analyses and reliability and maintainability tradeoff study results at this point are contingent on satisfying the following criteria:

(1) Conformance. Allocated reliability and maintainability requirements, when recombined at the system level, must satisfy system reliability and maintainability requirements defined in the functional baseline specification.

(2) Validity. Analytical procedures and data used in the tradeoff studies must be proven valid by independent assessment.

12.2.7.3 TRADEOFFS DURING FULL SCALE ENGINEERING DEVELOPMENT (FSED), PRODUCTION AND DEPLOYMENT PHASE

During FSED, the contractor is involved in detailed design tradeoff studies concerned with aspects of design philosophy such as level and allocation of redundancy, R&M test methods and procedures, built-in versus external test equipment philosophy, maintenance concepts, etc. This is the phase that transforms the "paper design" of the preceding phases into working hardware for test and evaluation. Hence, during this phase, the role of the acquisition manager and his staff is primarily one of acting as reviewers -- reviewing designs, R&M Program Plans, and Test Plans to insure that they are in consonance with the specification requirements, and that the desired results will be achieved.

This would involve evaluating the results of design analysis and reliability and maintainability engineering tradeoff studies involving considerations of safety, redundancy, failure mode/effects , critical reliability/maintainability factors-degrading interface tolerances, power levels and regulation, physical dimensions, packaging and environment control features and requirements, etc., underlying the configuration selected for production.

Subsequently, within the framework of the previous system studies, contractors and their subcontractors will carry out tradeoff studies at progressively greater levels of detail. These studies will address such factors as testability (test equipment needed and schedules) optimum thermal design, power supply requirements, component choices, and circuit layouts.

The above sequence of tradeoff studies starting with broad issues and converging into equipment details will, in general, be concluded by the end of FSED and Production Phases. However, additional involvement of all parties will be required, even during the Deployment Phase, to assess the desirability of proposed modifications arising from field experience and use.

For example, during the Deployment Phase, it will be necessary to verify that the effect of individual Engineering Charge Proposals (ECPs) on

system R&M (especially when the effect is degrading) is acceptable from the overall mission effectiveness viewpoint, as determined from a tradeoff study with the other system parameter changes for which the change was designed.

12.3 RELIABILITY CONSIDERATIONS

Previous sections of this section discussed life cycle R&M management considerations in general overview terms, guildelines for minimizing life cycle costs, and tradeoff analyses. This section will deal with reliability; methods of specifying, managing, and controlling to achieve the desired result.

12.3.1 RELIABILITY SPECIFICATION REQUIREMENTS

The first and most important task in a reliability program is the selection and specification of realistic requirements. These are derived from systems effectiveness and life cycle cost studies, coupled with projections of what is reasonable to achieve within technology and funding limitations. The exact method of specifying reliability depends upon the equipment/system being developed and its ultimate application.

Figure 12.3.1-1 illustrates four basic ways in which a reliability requirement can be defined.

(1) As a "mean life" or mean-time-between-failure, MTBF (see (1) in Figure 12.3.1-1). This defintion is useful for long life systems in which the form of the reliability distribution is not too critical, or where the planned mission lengths are always short relative to the specified mean life. Although the definition is adequate for specifying life, it gives no positive assurance of a specified level of reliability in early life, except as the assumption of an exponential distribution can be proven to be valid.

(2) As a probability of survival for a specified period of time, t (see (2) in Figure 12.3.1-1). This definition is useful for defining reliability when a high reliability is required during the mission period, but mean-time-to-failure beyond the mission period is of little tactical consequence except as it influences availability.

(3) As a probability of success, independent of time (see (3) in Figure 12.3.1-1). This definition is useful for specifying the reliability of one shot devices. It also specified those which are cyclic, such as the flight reliability of missiles, the launch reliability of launchers, the detonation reliability of warheads, etc.

(4) As a "failure rate" over a specified period of time (see (4) in Figure 12.3.1-1). This definition is useful for specifying the reliability of parts, units, and assemblies whose mean lives are too long to be meaningful, or whose reliability for the time period of interest approaches unity.

Figure 12.3.1-2 summarizes appropriate methods of stating the reliability requirements for various functions, usage, and maintenance conditions.

12-27
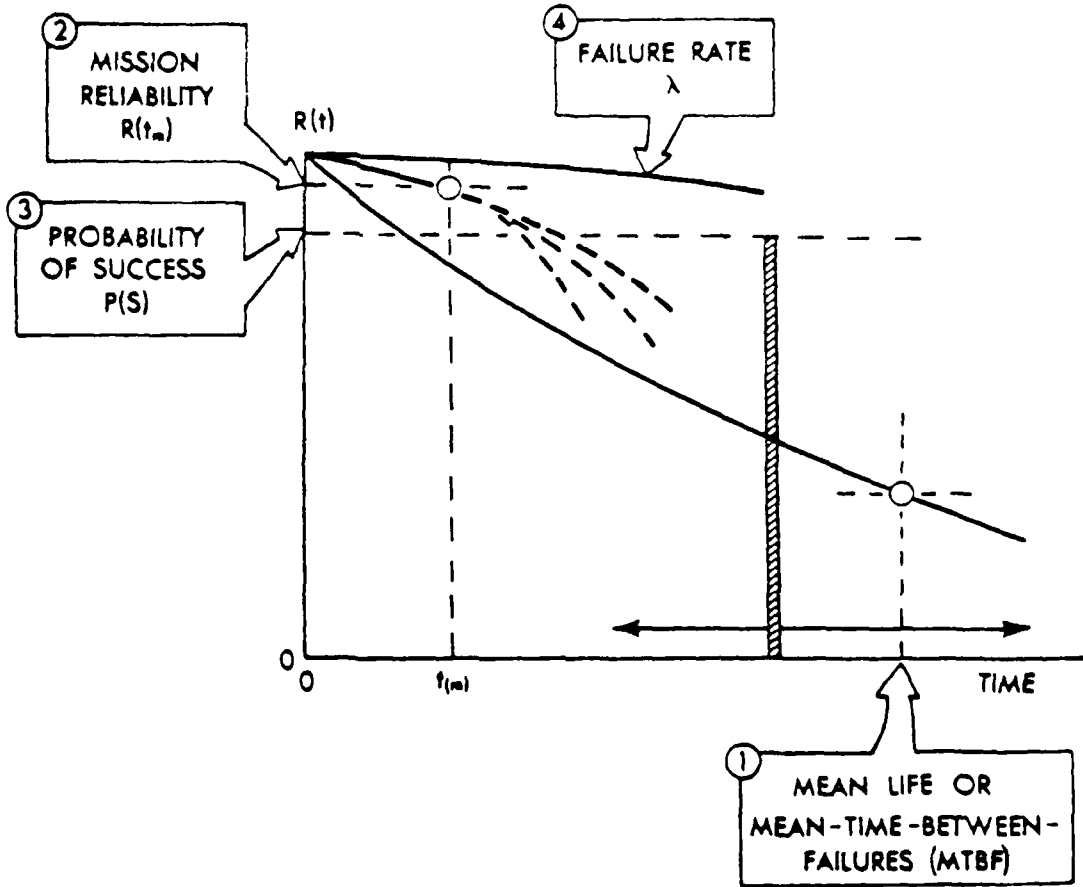
FIGURE 12.3.1-1: <u>FOUR DEFINITIONS OF RELIABILITY</u>

CONDITIONS OF USE / LEVEL OF COMPLEXITY	CONTINUOUS DUTY LONG LIFE (REPAIRABLE)	INTERMITTENT DUTY SHORT MISSIONS (REPAIRABLE)	CONTINUOUS OR INTERMITTENT (NON-REPAIRABLE)	ONE-SHOT (TIME-INDEPENDENT)
COMPLEX SYSTEMS	R(t) OR MTBF	R(t) OR MTBF	R(t) OR MTBF	P(S) OR P(F)
SYSTEMS SUBSYSTEMS SETS GROUPS	R(t) OR MTBF	R(t) OR MTBF	R(t) OR λ	P(S) OR P(F)
UNITS ASSEMBLIES SUBASSEMBLIES PARTS	λ	λ	λ	P(F)

Code:

$R(t)$ = Reliability for specified mission, or period of time, t.
MTBF = Mean-time-between-failures, or mean life.
$P(S)$ = Probability of success.
$P(F)$ = Probability of failure.
λ = Failure rate.

FIGURE 12.3.1-2: METHODS OF SPECIFYING RELIABILITY ACCORDING TO LEVELS OF COMPLEXITY AND CONDITIONS OF USE

The reliability requirement may be specified in either of two ways:

(1) As a NOMINAL value with which the user would be satisfied, on the average (upper test MTBF in MIL-STD-781); it should reflect the current state of the art.

(2) As a MINIMUM value below which the user would find the system totally unacceptable, and could not be tolerated in the operational environment - a value based upon the operational requirement (lower test MTBF in MIL-STD-781).

Whichever value is chosen as the specified requirement, there are two rules that should be applied. These are that when a nominal value is specified as a requirement, always specify a minimum value which the system must exceed; and also that when a minimum value alone is used to specify the requirement, always insure that it is clearly defined as minimum.

Of the two methods, the first is by far the best, since it automatically establishes the design goal at, or above, a known minimum.

Also, when reliability is specified, the definition of satisfactory performance should be included. This can be conveniently tabulated for inclusion in the specification.

Example: A complex radar has both search and track functions. It is also possible to operate the search function in both a low and high power mode. The reliability requirement for this system could be expressed as:

"The reliability of the system shall be at least:

Case 1 - High power search - 28 hours MTBF

Case 2 - Low power search - 40 hours MTBF

Case 3 - Track - 0.98 probability of satisfactory performance for ½ hour."

A portion of the Satisfactory Performance Table for the radar is shown in Figure 12.3.1-3.

System Characteristic	Units	Performance Limits		
		Case 1	Case 2	Case 3
Range	Yards	300,000	120,000	120,000
Resolution - Range	Yards	± 50	± 50	± 10
- Velocity	Ft./Sec.	+100	+100	± 25
Bandwidth	M			

FIGURE 12.3.1-3: SATISFACTORY PERFORMANCE LIMITS

12.3.2 RELIABILITY PROGRAM TASKS

Once reliability has been quantitatively specified, a major problem which confronts all Government and industry organizations is the selection of tasks which can materially aid in attaining program reliability requirements. This task must be judicially selected to reflect funding and schedule constraints, and tailored to the specified program needs.

MIL-STD-785 provides general requirements and specific tasks for reliability programs, and provides guidelines for the preparation and implementation of a Reliability Program Plan. The procedure for implementing or specifying use of MIL-STD-785 is discussed in paragraphs 1.2 and 4.0 of that standard. It is not sufficient to merely list MIL-STD-785 as a reference document, "which forms part of (the system specification) to the extent specified herein" without specific detailed direction as to which paragraphs and sections are applicable. Section 1.2.1 of that standard is quoted here for convenience: "Tasks described in this standard are to be selectively applied to DOD contract-definitized procurements, requests for proposals, statements of work, and Government in-house developments, requiring reliability programs for the development, production, and initial deployment of systems and equipment."

This standard has recently been completely revised and restructured to allow reliability programs to be tailored to meet specific program needs including life cycle cost objectives. The foreword of the revision (MIL-STD-785B) states: "This military standard consists of basic application requirements, specific tailorable reliability program tasks, and an appendix which includes an application matrix and a guidance and rationale for task selection. Effective reliability programs must be tailored to fit program needs and constraints, including lifecycle costs (LCC). This document is intentionally structured to discourage indiscriminate blanket applications. Tailoring is forced by requiring that specific tasks be selected and, for those tasks identified, that certain essential information relative to implementation of the task be provided by the procuring activity.

This revision contains the following fundamental changes from MIL-STD-785A:

(1) Increased emphasis has been placed on reliability engineering tasks and tests. The thrust is toward prevention, detection, and correction of design deficiencies, weak parts, and workmanship defects. Emphasis on reliability accounting has been retained, and expanded to serve the needs of acquisition, operation, and support management; but cost and schedule investment in reliability demonstration tests must be made clearly visible and carefully controlled.

(2) A sharp distinction has been established between basic reliability and mission reliability. Measures of basic reliability such as ... MTBF now include all item life units (not just mission time) and all failures within the item (not just mission critical failures of the item itself)...

(3) Mission reliability is one of four system reliability parameters. The other three are directly related to operational readiness, demand for maintenance, and demand for logistic support. Separate requirements will be established for each reliability parameter that applies to a system, and translated into basic reliability requirements for subsystems, equipments, components and parts.

Table 12.3.2-1 lists the elements of a standard hardware reliability program and shows the importance of each element during the life cycle phases of development and production. This list follows the provision given in MIL-STD-785. However, it must be emphasized that the application of MIL-STD-785 provisions are subject to the discretion of the procuring activity.

The chart given in Table 12.3.2-1 is designed to provide the R&M manager an overview, or feeling, for the average situation. As previously indicated, each development program is different, and the reli ability program must be tailored to its specific needs. This tailoring must be done by reliability specialists working with the program manager to select MIL-STD-785 tasks and requirements that are most suitable to the specific acquisition and to modify these task and requirements where necessary, to assure that each tailored task or requirement involved states only the minimum needs of the program. Appendix A of MIL-STD-785 provides tailoring guidance. Tailoring however, is not a license to specify a zero reliability program.

Full descriptions of each of the program elements listed in Table 12.3.2-1 are given in MIL-STD-785. Section 12.6 discusses output requirements in terms of deliverable documents (or data items). Section 12.3.1 describes the specification preparation process and Section 12.8 provides guidance and criteria for evaluating and monitoring contractor R&M programs.

A brief description follows for each of the program elements included in Table 12.3.2-1.

12.3.2.1 RELIABILITY PROGRAM PLAN

An analysis of the reliability and maintainability requirement set in the Concept phase is the basis of the program plan. The reliability program plan is designed as a basic tool for the procuring activity to:

(1) Assist in managing an effective reliability program

(2) Evaluate the contractor's approach to understanding and execution of his reliability tasks

(3) Evaluate the contractor's planning to insure that his procedures for implementing and controlling reliability tasks are adequate

(4) Evaluate the adequacy of contractor's organization to assure that appropriate attention will be focused on reliability activities/problems.

TABLE 12.3.2-1: MIL-STD-785B APPLICATION MATRIX

Task	Title	Task Type	Program Phase				Task Active at Deployment
			Concept	Valid	FSED	PROD	
101	Reliability Program Plan	MGT	S	S	G	G	
102	Monitor/Control of Subcontractors and Suppliers	MGT	S	S	G	G	
103	Program Reviews	MGT	S	S(2)	G(2)	G(2)	
104	Failure Reporting, Analysis, and Corrective Action System (FRACAS)	ENG	NA	S	G	G	✓
105	Failure Review Board (FRB)	MGT	NA	S(2)	G	G	
201	Reliability Modeling	ENG	S	S(2)	G(2)	GC(2)	
202	Reliability Allocations	ACC	S	G	G	GC	
203	Reliability Prediction	ACC	S	S(2)	G(2)	GC(2)	
204	Failure Modes, Effects, and Criticality Analysis (FMECA)	ENG	S	S(1)(2)	G(1)(2)	GC(1)(2)	
205	Sneak Circuit Analysis (SCA)	ENG	NA	NA	G(1)	GC(1)	
206	Electronic Parts/Circuits Tolerance Analysis	ENG	NA	NA	G	GC	
207	Parts Program	ENG	S	S(2)	G(2)	G(2)	✓
208	Reliability Critical Items	MGT	S(1)	S(1)	G	G	✓
209	Effects of Functional Testing, Storage, Handling, Packaging, Transportation, and Maintenance	ENG	NA	S(1)	G	GC	✓
301	Environmental Stress Screening (ESS)	ENG	NA	S	G	G	
302	Reliability Development/Growth Testing	ENG	NA	S(2)	G(2)	NA	
303	Reliability Qualification Test (RQT) Program	ACC	NA	S(2)	G(2)	G(2)	
304	Production Reliability Acceptance Acceptance Test (PRAT) Program	ACC	NA	NA	S	G(2)	

TASK TYPE:

ACC - Reliability Accounting

ENG - Reliability Engineering

MGT - Management

PROGRAM PHASE:

S - Selectively Applicable
G - Generally Applicable
GC - Generally Applicable to Design Changes Only
NA - Not Applicable
(1) Requires considerable interpretation of intent to be cost effective
(2) MIL-STD-785 is not the primary implementation requirement. Other MIL-STDs or statement of work requirements must be included to define the requirements.

12.3.2.2 MONITOR/CONTROL OF SUBCONTRACTORS AND SUPPLIERS

Continual visibility of subcontractors' activities is essential so that timely and appropriate management action can be taken as the need arises. Accordingly, it is prudent to include contractual provisions which permit the procuring activity to participate, at its discretion, in appropriate formal prime/subcontractor meetings. Information gained at these meetings can provide a basis for follow up actions necessary to maintain adequate visibility of subcontractors progress; technical, cost, and schedule.

12.3.2.3 PROGRAM REVIEWS

An important management and technical tool used by procuring activity's R&M organization is Design Reviews. These reviews should be specified in the statement of work (SOW) to insure adequate staffing and funding. Typical reviews are held to:

(1) Evaluate the progress consisting of technical adequacy, including reliability of a selected design and test approach (Preliminary Design Review).

(2) Determine the acceptability of the detail design approach, including reliability, before commitment to production (Critical Design Review).

(3) Periodically review progress of the reliability program, addressing progress of the reliability tasks specified in the SOW. These reviews should be specified and scheduled in the SOW (Technical Reviews).

12.3.2.4 FAILURE REPORTING, ANALYSES, AND CORRECTIVE ACTION SYSTEMS (FRACAS)

Early elimination of failure causes is a major contributor to reliability growth and attainment of field reliability. The sooner failure causes can be identified, the easier it is to implement effective corrective action. It is, therefore, important to employ a closed loop FRACAS early in the development phase, particularly for complex acquisitions.

The disposition of any failed hardware is critical, and must be properly controlled to preclude premature disposal, and to insure that the actual failure parts are subjected to the required analyses. A disposition team (Failure Review Board), normally consisting of representatives of government, contractor, engineering and quality assurance and manufacturing personnel, is designated to insure that FRACAS is implemented.

12.3.2.5 FAILURE REVIEW BOARD (FRB)

For the acquisition of expensive, complex, or critical equipment on systems, it may be necessary and desirable to formalize FRACAS proceedings to the extent of having them controlled by an FRB. The addition of this task to a reliability program would provide the procuring activity with

additional assurance of a tight control of reporting, analyses, and corrective actions taken on identified failures. However, care should be taken not to duplicate the quality assurance tasks which may have already been called up under MIL-Q-9858 (see Section 11 for a discussion of MIL-Q-9858).

12.3.2.6 RELIABILITY MODELING

A reliability model of the system/subsystem/equipment is required for making numerical apportionments and estimates. Modeling is considered mandatory for evaluating complex equipment arrangements found in modern weapon systems. The model should be developed as soon as program definition permits, even if usable numerical input data are not available, since early modeling can reveal conditions where management action may be required. The model should be continually expanded to the detail level for which planning, mission, and system definition are firm.

Together with duty cycle and mission duration information, the model is used to develop a mathematical expression, or a computer program with which appropriate failure rate and probability of success data can be used to provide apportionments, estimates, and assessments of basic mission reliability.

12.3.2.7 RELIABILITY PREDICTION

The prediction task should be specified by the procuring activity during the early acquisition phases to determine reliability feasibility, and during the development and production phases to determine reliability attainability. Predictions are compared with allocations and interrelated with configuration analyses; iterations are made as necessary. Predictions provide engineers and management with essential information for day-to-day activities, and, in addition, they are important supporting elements for program decision makers.

Predictions should be made as early as possible and updated whenever changes occur. While early predictions based on parts counts are inherently unrefined because of insufficient design detail, they provide useful feedback to designers and managers of the feasibility of meeting the basic reliability requirements. As the system progresses from paper design to hardware stages, predictions mature as actual program test data become available and are integrated into the calculations. The reliability values produced from predictions provide the basis for essential inputs to other related activities, i.e., maintainability, safety, quality engineering, logistics and test planning. They also establish a baseline for comparing progress and performance and can be used to detect overstressed parts and pinpoint critical areas for redesign or application of redundancy.

12.3.2.8 FAILURE MODES, EFFECTS, AND CRITICALITY ANALYSIS (FMECA)

A FMECA is a powerful tool to optimize the reliability/life cycle cost tradeoff between basic and mission reliability at the black

box/component or major subsystem level, where the tradeoffs are most appropriately analyzed and evaluated. Potential design weaknesses are identified through the use of engineering schematics and mission rules to systematically identify the likely modes of failure, the possible effects of each failure, and the criticality of each failure on safety, readiness, mission success, demand for maintenance/logistic support, or some other significant factors.

The initial FMECA can be performed in the CONCEPT phase and, because only limited design definition may be available, only the more obvious failure modes may be identified. As greater missions and design definitions are developed in the VALID and FSED phases, the analyses can be expanded to successively more detailed levels and ultimately, if required, to the part level.

FMECA results may suggest areas where the judicious use of redundancy can significantly improve mission reliability without unacceptable impact on basic reliability, and where other analyses, e.g., electronic parts analyses, should be made, or other provisions such as environmental protection should be considered. Finally, FMECA results should be used to confirm the validity of the model used in computing estimates and subsystems or functional equipment groupings, particularly where some form of redundancy is included.

12.3.2.9 SNEAK CIRCUIT ANALYSES (SCA)

The purpose of SCA is to identify latent paths which cause occurrence of unwanted functions or inhibit desired functions, assuming all components are functioning properly. The analysis should be considered for critical systems and functions where other techniques are not effective. Since SCA is expensive, it is usually performed late in the design cycle after design documentation is complete which makes changes difficult and costly to implement. Therefore, SCA should only be considered for components and circuitry which are critical to mission success and safety.

12.3.2.10 ELECTRONIC PARTS/CIRCUIT TOLERANCE ANALYSIS

This analysis examines, at component interconnection and input and output points, the effects of parts/circuits electrical tolerances and parameters over the range of specified operating temperatures. The analysis considers expected component value variations due to manufacturing tolerance variations, and their drift with time and temperature. Since this analysis is also expensive, its application should be limited to critical circuitry.

12.3.2.11 PARTS SELECTION/APPLICATION CRITERIA

Parts and components are the basic items of higher level assemblies which, in turn, ultimately constitute the system. Significant contributions toward system optimization can be realized by applying attention and resources to parts selection, control, and application, starting early in the VALID phase and continuing throughout the life cycle of the system.

A comprehensive parts program will consist of the following elements:

o   a parts control program (in accordance with MIL-STD-965)
o   parts standardization
o   parts application (derating) guidelines established by the contractor
o   parts testing, screening, or validation
o   GIDEP participation as applicable (MIL-STD-1556)

The basic objective of the procuring activity's parts program is to control the selection and use of standard and nonstandard parts. An effective parts program requires that knowledgeable parts engineers be used by both the procuring activity and the contractor. Government agencies such as the Defense Industrial Supply Center, Defense Electronics Supply Center, and the Rome Air Development Center can provide excellent support in this area.

12.3.2.12 RELIABILITY CRITICAL ITEMS

Reliability critical items are those whose failures can significantly affect system safety, mission success, or total maintenance/logistics support costs. Reliability critical items, once identified, as part of the selected configuration should be retained and included in the RFP for subsequent life cycle phases. These items are the prime candidate for detailed analyses, growth testing, reliability qualification testing, reliability stress analyses, and other techniques to reduce the reliability risk.

12.3.2.13 ENVIRONMENTAL STRESS SCREENING (ESS)

ESS is a test, or a series of tests, specifically designed to disclose weak parts and workmanship defects requiring correction. It may be applied to parts, components, subassemblies, assemblies, or equipment (as appropriate and cost effective) to remove defects which would otherwise cause failure during higher level testing or field service. ESS testing has significant potential return on investment for both the contractor and Government, during both development and production.

12.3.2.14 RELIABILITY DEVELOPMENT/GROWTH TESTING (RDGT)

RDGT is a planned prequalification, test-analyze-and-fix (TAAF), process in which equipments are tested under actual, simulated, or accelerated environments to disclose, design deficiencies and defects. The testing is intended to provide a basis for early incorporation of corrective actions, and verification of their effectiveness, therefore promoting reliability growth.

RDGT must correct failures that reduce operational effectivenss and failures that drive maintenance and logistics support costs. It is imperative that RDGT be conducted using one or two of the first FSED items available. Delay forces corrective action into the formal configuration control cycle, which then adds even greater delays for administrative processing of reliability engineering changes.

```
                                             Life Cycle Phase

                                              Full Scale
                     Conceptual  Validation   Development  Production  Deployment

Requirements Definition  xxxxxxxxxxxxxxxxxxAAAAAA.........

Reliability Model          xxxxxxxxxxxxxxxxxxxxxxxxx......

Reliability Prediction     xxxxxxxxxxxxxxxxxxxxxxxxx......

Reliability Apportionment  oooooooooooooooooooooooooo......

Failure Modes Analysis     oooooooooooooooooooxxxxxx......

Design for Reliability     oooooooxxxxxxxxxxxxxxxxxxxxxxx....  .......

Parts Selection            oooooooxxxxxxxxxxAAAAAA...........  .......

Design Review              oooooooxxxxxxxxxxxxxxxxxx......

Design Specifications    xxxxxxxxxxxxxxxxxxxxxx.........

Acceptance Specifications    xxxxxxxxxxxxAAAAAL.........

Reliability Evaluation Tests  ----xxxxxxxxxxxxxxxxxx

Failure Analysis              ----xxxxxxxxxxxxxxxxxxxxxxxoooooooooooooooooooooooo

Data System                   ----xxxxxxxxxxxxxxxxxxxxxxxoooooooooooooooooooooooo

Quality Control                 ooooooooooxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxoooooooooo

Environmental Tests              xxxxx.......AAAAAAAA........

Reliability Acceptance Tests       xx........AAAAAoooooooooo
```

First contract —— KEY ——

------ Desirable activity (for highest success
       probability)

oooooo Necessary activity (errors seldom disastrous)

xxxxxx Very important activity (errors usually
       disastrous)

...... Low key activity (to update previous results)

AAAAAA Critical Activity

FIGURE 12.3.3-1: RELIABILITY PROGRAM ELEMENTS

12.3.2.15 RELIABILITY QUALIFICATION TEST (RQT)

RQT is intended to provide the Government reasonable assurance that minimum acceptable reliability requirements have been met, before items are committed to production. RQT must be operationally realistic and must provide estimates of demonstrated reliability. It must be clearly understood that RQT is a preproduction test, and that it must be completed in time to provide management information as input for the production decision.

12.3.2.16 PRODUCTION RELIABILITY ACCEPTANCE TEST (PRAT)

PRAT is intended to stimulate in-service evaluation of the delivered item or production lot. It must be operationally realistic, and may be required to provide estimates of demonstrated reliability. PRAT may be required to provide a basis for positive and negative financial feedback to the contractor in lieu of an in-service warranty.

12.3.3 RELATIVE EMPHASIS ON RELIABILITY PROGRAM ELEMENTS (Ref. 10)

Figure 12.3.3-1 lists the elements of a hardware reliability program, and shows the importance of each element during each of the life cycle phases of development. Generally, it tracks with the elements of MIL-STD-785, with some minor variations. The chart is designed to give the acquisition and/or R&M manager an overview or feeling for the average situation. The relative importance rating applies to an "average" development program, and represents the collective wisdom of a number of reliability specialists with many years of experience.

Only the first conceptual study contract milestone is shown. Work to the left of the broken line represents the necessary homework done prior to the preparation of the first statement of work.

12.3.4 QUANTITATIVE EXAMPLE OF THE USE OF WEIGHTING CRITERIA TO DETERMINE RELATIVE PROGRAM EMPHASIS

Following is an example of how weighting criteria can be developed for each of the reliability tasks and used to determine the relative emphasis to be applied to each task for a given procurement. The development and application of such criteria can be a very useful tool to the acquisition/R&M manager in proposal reviews, resource allocation, and contract monitoring.

The quantitative weighting factors for each reliability task are shown in Table 12.3.4-1. The second column represents average cost effectiveness weights assigned (on a scale of 5) to each of the reliability program tasks. The remaining columns also have weights assigned (on a scale of 5) to each of the major evaluation crtieria such as complexity, criticality, quantity produced, operating environment, technology, and storage requirements. Within each criterion, weights are also assigned to each task for each of two significant factors. For example, in the Technology column, weights are assigned depending upon the whether the technology required is somewhat standard or is pushing the state of the art.

TABLE 12.3.4-1: COST EFFECTIVENESS INFLUENCES

TASK DESCRIPTION	AVERAGE C/E*	COMPLEXITY		EQUIPMENT CRIT.		QUANTITY		EQUIP. OPERATING ENVIRONMENT		TECHNOLOGY		STORAGE REQUIREMENT	
		Lo	Hi	Lo	Hi	Lo	Hi	Benign	Hostile	Std	SOA	Short	Long
Rel. Program Plan	2	.5	3	.5	4	1	2	2	2	2	2	2	2
Rel. Management	2	1	3	1	4	1	2	2	2	2	2	2	2
Supplier Control	4	1	4	1	4	1	2	1	3	2	5	2	3
Program Review	3	1	3	1	4	1	2	2	2	2	2	2	2
Design Tech.	4	1	4	1	4	2	2	1	3	2	2	2	4
Rel. Analysis	3	.5	4	1	3	1	1	2	2	2	2	2	2
Parts Rel.	5	1	5	.5	5	1	5	1	5	1	5	2	5
FMEA	3	.1	4	.1	5	2	2	2	2	2	3	2	2
Critical Items	3	.5	3	1	4	1	5	1	3	1	5	2	3
Storage/Handling	4	1	3	1	4	1	4	1	3	1	3	2	5
Design Review	3	1	3	1	4	1	3	2	2	2	2	2	2
Develop Testing	3	1	3	1	4	1	4	1	4	1	5	2	2
Rel. Demo Testing	1	1	3	.1	4	.1	4	1	3	2	2	2	.1
Failure Data	5	.5	5	1	5	.5	5	1	5	1	3	3	2
Production Rel.	2	1	3	1	4	1	5	2	2	2	3	2	3

*5 represents high cost effectiveness

Admittedly, the weights were somewhat arbitrarily developed and are based upon the collective judgment of a group of Government and industry reliability specialists. However, the purpose of this example is to describe a methodology that can be developed as a management decision aid. Each manager may want to develop his own weighting factors, criteria, and the specific numbers for his given application.

In this example, the equipments being evaluated are: 1) an antiaircraft missile fire control system; and 2) the missiles themselves. The equipment characteristics, based upon the criteria in Table 12.3.4-1, are shown in Table 12.3.4-2. The analysis to determine the relative emphasis to be given to each of the reliability tasks is shown in Table 12.3.4-3.

The numbers in the first column of Table 12.3.4-3 (Base) are the average C/E numbers from the second column of Table 12.3.4-1. The weighting factors in each row are derived from Tables 12.3.4-1 and 12.3.4-2, for each equipment. For example, for Equipment #1, in the Reliability Program Plan row, the weights in each column are: complexity (high) = 3, criticality (high) = 4, quantity(low) = 1, environment (moderate) = 2, technology (SOA) = 2, and storage (short) = 2.

The numbers in the Product column represent the product of the numbers in each row. The numbers in the Emphasis column are somewhat arbitrarily derived as follows. For Equipment #1, starting with the highest number in the column (3750), using a scale of 10, assign 10 to that number. One half the highest number (1800) would be assigned the number 5. Thus, 1440 was assigned 4 since it is less than 1800. One-half of 1440 (720) would be assigned 2, etc.

A similar procedure was used for Equipment #2, except that it was based on a scale of 20. The scale used would depend upon the degree of discrimination that the decision maker desires.

From the results of the analysis, it can be readily seen that, for Equipment #1, the major reliability emphasis should be on parts, failure data, and failure mode and effect analysis (FMEA). For Equipment #2, the major emphasis should be on parts and failure data.

12.4 MAINTAINABILITY CONSIDERATIONS

Operational requirements for weapons systems and equipment frequently call out an operational readiness or availability requirement as a probability of being operationally ready at any point in time. The requirement may be defined as an "operational" availability requirement, given by:

$$A_o = \frac{MTBF}{MTBF + \overline{MDT}} \tag{12.1}$$

where

$\overline{MDT}$ = mean downtime for maintenance, including active repair time, administrative time, and logistic delay time

TABLE 12.3.4-2: <u>EXAMPLE OF TABLE 12.3.4-1 USAGE</u>

EQUIPMENT 1 MISSILE FIRE CONTROL SYSTEM	
Complexity:	High
Criticality:	High
Quantity:	Low
Environment:	Moderate
Technology:	State of the Art (SOA)
Storage:	Short

EQUIPMENT 2 MISSILE ROUNDS	
Complexity:	Moderate
Criticality:	Moderate to High
Quantity:	High
Environment:	Hostile
Technology:	Standard
Storage:	Long Term

TABLE 12.3.4-3: ANALYSIS OF RELIABILITY TASK EMPHASIS

EQUIPMENT 1 COST EFFECTIVENESS MATRIX								
	Base	Weighting Factors					Product	Emphasis (Note 1)
Program Plan	2	3	4	1	2	2	2	192	1
Management	2	3	4	1	2	2	2	192	1
Supplier	4	4	4	1	2	5	2	1280	3
Program Review	3	3	4	1	2	2	2	288	1
Design Tech.	4	4	4	2	2	2	2	1024	3
Rel. Ana.	3	4	3	1	2	2	2	288	1
Parts	5	5	5	1	3	5	2	3750	10
FMEA	3	4	5	2	2	3	2	1440	4
Critical Items	3	3	4	1	2	5	2	720	2
Storage/Handling	4	3	4	1	2	3	2	576	2
Design Review	3	3	4	1	2	2	2	288	1
Dev. Test	3	3	4	1	3	5	2	1080	3
Demo Test	1	3	4	.1	2	2	2	9.6	0
Failure Data	5	5	5	.5	3	3	3	1687.5	5
Production	2	3	4	1	2	3	2	288	1

EQUIPMENT 2 COST EFFECTIVENESS MATRIX								
Program Plan	2	2	3	2	2	2	2	192	1
Management	2	2	3	2	2	2	2	192	1
Supplier	4	2.5	3	2	3	2	3	1080	3
Program Review	3	2	3	2	2	2	2	288	1
Design Tech.	4	2.5	3	2	3	2	4	1440	4
Rel. Ana.	3	2	2	1	2	2	2	96	0
Parts	5	3	3	5	5	1	5	5625	20
FMEA	3	2	3	2	2	2	2	288	1
Critical Items	3	2	3	5	3	1	3	810	3
Storage/Handling	4	2	3	4	3	1	5	1440	4
Design Review	3	2	3	3	2	2	2	432	1
Dev. Test	3	2	3	4	4	1	2	576	2
Demo Test	1	2	3	4	3	2	.1	14.4	0
Failure Data	5	3	4	5	5	1	2	3000	10
Production	2	2.5	3	5	2	2	3	900	3

NOTES:

1. Numerical values are used as guides to determine approximate emphasis.

$\overline{M}_{ct}$ or $\overline{MDT}$

A$_1$ or A$_0$

MTBF (hours)

$$\text{OPERATIONAL AVAILABILITY } (A_o) = \frac{MTBF}{MTBF + \overline{MDT}}$$

$$\text{INHERENT AVAILABILITY } (A_I) = \frac{MTBF}{MTBF + \overline{M}_{ct}}$$
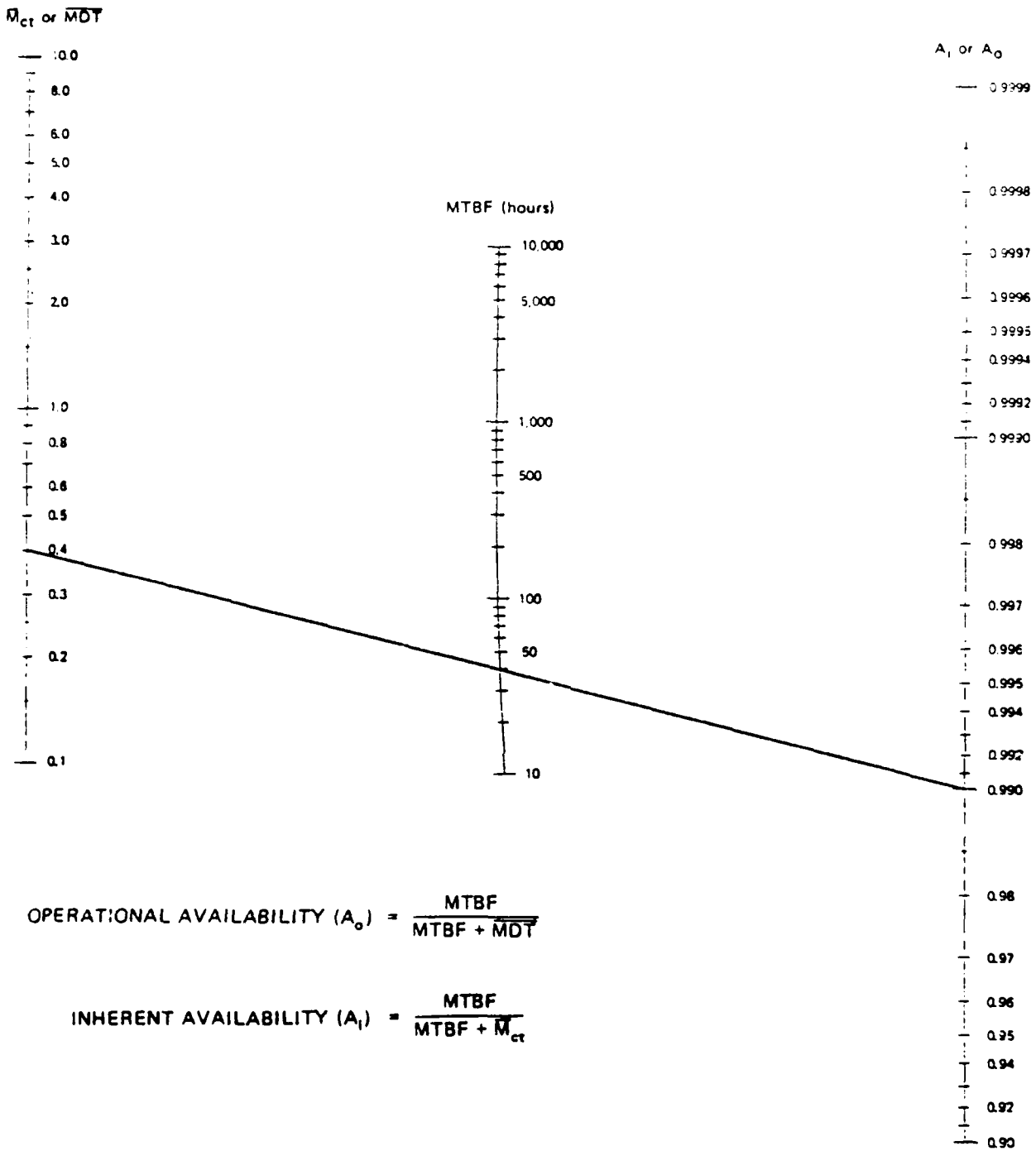
FIGURE 12.4-1: AVAILABILITY NOMOGRAPH

The requirement may also be defined as an "inherent" availability requirement, a characteristic of design without consideration of administrative or logistic time. Inherent availability is given by:

$$A_i = \frac{MTBF}{MTBF + \bar{M}_{ct}}$$ (12.2)

where

$\bar{M}_{ct}$ = mean corrective maintenance time

When the operational requirement for a system defines an inherent availability of, say, 0.99, and the MTBF requirement is 40 hours, the maintainability requirement can be derived directly as follows (as illustrated in the availability nomograph of Figure 12.4-1).

$$MDT \text{ or } M_{ct} = MTBF\left(\frac{1}{A} - 1\right) = 40\left(\frac{1}{0.99} - 1\right)$$ (12.3)

$$= 0.4 \text{ hours, or } 24 \text{ minutes}$$

An important point to be made in this rather simplistic example is the fact that, as shown in previous sections, if two of the parameters are specified, e.g., availability, reliability, the third, e.g., maintainability, is also specified. The nomograph (Figure 12.4-1) can be used as a ready reference to derive the relationship among the availability, reliability, and maintainability parameters.

The other important point to be made is that the quantitative specification of maintainability is an essential ingredient toward the achievement of the desired degree of system availability or operational readiness.

12.4.1 MAINTAINABILITY SPECIFICATION REQUIREMENTS

Figure 12.4.1-1 illustrates a typical cumulative distribution of repair times associated with an equipment. The objective of the maintainability specification is to force control of the distribution by specifying at least one point on the curve to control either the average time $(\bar{M}_{ct})$, the median time $(\tilde{M}_{ct})$, or some designated maximum time $(M_{max_{ct}})$. The preferred method for forcing control of the cumulative distribution is to specify two points, either the median or the mean, and the maximum (e.g., the mean time to repair $\bar{M}_{ct}$, and the maximum time to repair, $M_{max_{ct}}$, for 95% of all repair actions).

Figure 12.4.1-2, from the NAVAIR Maintainability Engineering Handbook (Ref. 11), illustrates an acceptable quantitative specification of maintainability requirements for a hypothetical equipment/subsystem.
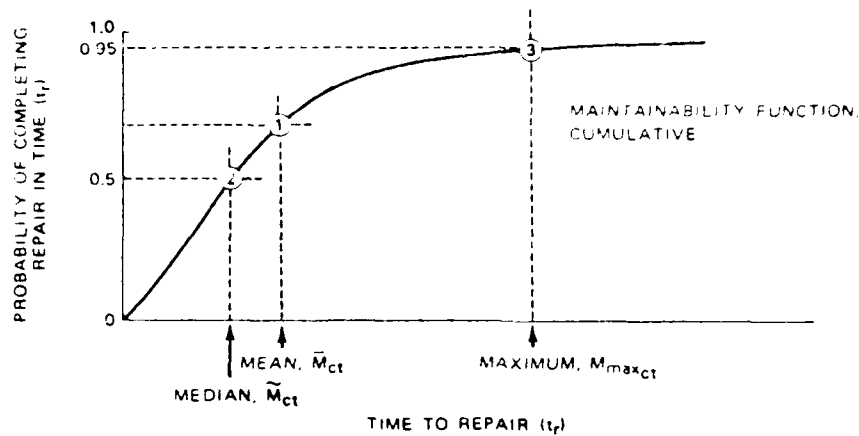
FIGURE 12.4.1-1:   EXAMPLE MAINTAINABILITY FUNCTION DERIVED FROM TIME-TO-REPAIR DISTRIBUTION

3.2   Maintainability requirements

3.2.1   Quantitative requirements.   The MK 1007X shall be designed to meet the following quantitative maintainability requirements for corrective maintenance performed at the organizational level when tested in accordance with provisions of 4.2.1:

Mean time to repair, $\overline{M}_{ct}$ $\leq$ 0.5 Hour

Maximum time to repair, $M_{max_{ct}}$ $\leq$ 1.5 Hour (95th Percentile)

3.2.2   Maintainability allocations.   Requirements defined in 3.2.1 shall be allocated by the contractor to equipment and components within the MK 1007X in accordance with analytical procedures set forth in MIL-HDBK-472.   Contractor shall incorporate these allocations into applicable end item specifications as design requirements and shall prescribe the demonstration test requirements by which conformance to the allocated requirements is to be demonstrated.

FIGURE 12.4.1-2:   EXAMPLE OF MAINTAINABILITY REQUIREMENTS FOR A SUBSYSTEM OR EQUIPMENT SPECIFICATIONS

When both intermediate level and organizational level maintenance are to be performed at the same location, intermediate level maintainability requirements should be specified to insure rapid repair and return of repairables to the organizational level spares inventory. For this case, it is usually only necessary to specify one point (e.g., $\overline{M}_{ct}$) for each of the repairable items. An example is shown in Figure 12.4.1-3 (Ref. 11).

3.2 Maintainability requirements

3.2.3   Intermediate level maintenance.   Replaceable units and modules of the MK 1007X transmitter equipment which are designed for repair at intermediate level shops shall demonstrate the following mean time to repair values when test in accordance with para ( ).

Unit	M_{ct} in Hours
Power Amplifier	2.0
Modulator	3.5
Power Supply	1.5
Cooling System	2.5

FIGURE 12.4.1-3: EXAMPLE OF SPECIFIED INTERMEDIATE LEVEL
MAINTAINABILITY REQUIREMENTS

A quantitative description of preventive maintenance is often neglected in system and equipment specifications. This is not a serious omission, tactically, when the equipment duty cycle is short enough to permit extended periods of downtime for scheduled preventive maintenance at arbitrarily selected intervals (e.g., 1 hour in every 24 calendar hours).   Under certain conditions, however, as during a period of sustained alert status or uninterrupted operation, the freedom in preventive maintenance scheduling cannot be permitted. Under these conditons, appropriate preventive maintenance requirements should be specified.

Figure 12.4.1-4 illustrates the high-utilization-rate, low-duty-cycle case, where scheduled preventive maintenance periods can be permitted conditional on quick return to operational status.   Figure 12.4.1-5 illustrates a requirement for a low-utilization-rate, high-duty-cycle equipment, in which preventive maintenance cannot be permitted during the duty cycle.

3.2.4   Preventive maintenance. Preventive maintenance downtime, including system tests which remove the system from operational status, shall not exceed a total of 1.5 hours in any 24 hour calendar period. The system shall be capable of restoration to full performance within 10 minutes during any period of preventive maintenance, and two minutes during any system test period.

FIGURE 12.4.1-4: EXAMPLE OF A SPECIFICATION FOR A PERMISSIBLE
PREVENTATIVE MAINTENANCE DOWNTIME

3.2.5 <u>Preventive maintenance</u>. The equipment **shall not** require preventive maintenance at intervals of less than 50 operating hours or 5 days, whichever occurs first. Preventive maintenance performed to protect the equipment during extended periods of nonuse shall provide protection against degradation for at least 120 days during which time the equipment will be exercised no more than once each 30-day period, with each exercise period consisting of no more than one hour.

FIGURE 12.4.1-5: EXAMPLE OF A SPECIFICATION FOR UNINTERRUPTED OPERATIONAL
CAPABILITY WITHOUT PREVENTIVE MAINTENANCE

Finally, there is the case where one would like to be able to specify minimum acceptable maintenance manhours per operating hour/flight hour/calendar hour, as appropriate. Figure 12.4.1-6 illustrates this limitation as a specification requirement for a hypothetical ordnance system.

3.2.6 <u>Maintenance support</u>. Maintenance support shall not exceed the following maintenance manhours per operate hour requirements when measured in accordance with para ( ).

		Average Direct Maintenance Manhours Per Operate Hour	
Maintenance Item	Maintenance Level	Corrective	Corrective plus Preventive
System	Organizational	1.5	4.0
System	Intermediate	2.0	4.0
Total for System & Support Equipment	Organizational & Intermediate	4.0	10.0

Based on average utilization rate of 360 hours per month.

FIGURE 12.4.1-6: EXAMPLE OF A SPECIFIED LIMITATION IN
MAINTENANCE MANHOUR REQUIREMENTS

12.4.2 MAINTAINABILITY PROGRAM TASKS

As with reliability, once maintainability has been quantitatively specified, a major problem which confronts all Government and industry organizations is the selection of tasks which can materially aid in attaining program maintainability requirements. These tasks must be judicially selected to reflect funding and schedule constraints, and tailored to the specific program needs.

MIL-STD-470 establishes uniform criteria for a maintainability program, and provides guidelines for the preparation and implementation of a maintainability program plan. Proper implementation of MIL-STD-470 requires that the specific applicable paragraphs of that standard be prescribed. As with MIL-STD-785, it is not sufficient to merely list MIL-STD-470 as a reference document, "which forms part of (the system specification) to the extent specified herein" without specific detailed direction as to which paragraphs and section are applicable. Section 4.1 of MIL-STD-470 states that "The maintainability program shall be integrated with the system/equipment design engineering program to assure effective, timely, and economical accomplishment. The program shall be consistent with the type and complexity of systems/equipment, phase of the procurement, and shall insure attainment of the contractual maintainability requirements. The following listed tasks shall be incorporated into the maintainability program:

    a.   Prepare maintainability program plan
    b.   Perform maintainability analysis
    c.   Prepare inputs to the detailed maintenance concept and detailed maintenance plan
    d.   Establish maintainability design criteria
    e.   Perform design tradeoffs
    f.   Predict maintainability parameter values
    g.   Incorporate and enforce maintainability requirements in subcontractor and vendor contract specifications
    h.   Integrate other items
    i.   Participate in design reviews
    j.   Establish data collection, analysis and corrective action system
    k.   Demonstrate achievement of maintainability requirements
    l.   Prepare maintainability status reports

A brief description follows for each of the program elements mentioned above.

12.4.2.1 MAINTAINABILITY PROGRAM PLAN

The contractor is required to develop a maintainability plan for the acquisition program which will produce the following results when called for by the contract:

    a.   Maintainability Analysis. Perform prediction and failure mode and effects analyses, maintenance and logistics trade studies, GFE investigations, parts and materials evaluation, and maintainability allocation to lower level elements (subsystem, equipment, etc.) to provide the quantitative basis for maintainability specification and control.

    b.   Maintainability Design Support. Provide maintainability design guidance through specific design guidelines, critical area analysis, design verification tests, parts application review, human factors and logistics interface coordination, and maintainability analysis.

c.   <u>Maintainability Control</u>. Integrate maintainability require-
ments and test criteria into system and equipment specifica-
tions, and exercise control of maintainability as part of the
configuration management and change control procedure.
Perform a complete maintainability assessment of the design at
each of the contractually designated formal design review
milestones. Review and exercise control of maintainability
aspects of contractor data.

d.   <u>Maintainability Testing</u>. Prepare, document, and conduct main-
tainability tests as called for by the contract. Develop an
integrated test and evaluation plan in which provisions are
made for acquiring and recording maintainability measurement
data during functional and environmental testing.

e.   <u>Production Maintainability Control</u>. Establish and implement
maintainability controls for items to be procured from subcon-
tractors and vendors, by specific reference to allocated
requirements and control procedures in the subcontract or pur-
chase order. Integrate maintainability assessments of subcon-
tractor and vendor products into the formal design review
schedule.

f.   <u>Logistics Planning</u>. Participate in the development of main-
tenance concepts, repair policies, logistics support, and pro-
visioning plans, as a joint effort. Provide realistic main-
tainability and reliability data to these and other
interfacing activities, the validity of whose final output is
dependent on accurate repair rate and failure rate estimates.

g.   <u>Failure Reporting and Corrective Action</u>. Establish and
conduct a failure reporting, data anlaysis, and corrective
action system to ensure earliest possible detection and
correction of maintainability problems and critical areas of
design. Show how the reporting system will be adaptable to
the standard service maintenance data collection system upon
deployment.

12.4.2.2 MAINTAINABILITY ANALYSIS

Perform requirements and feasibility studies, prediction analysis,
failure mode and effects analysis, tradeoff studies, problem diagnosis,
and allocation analysis to provide design guidance and evaluate design
progress in the achievement of specified maintainability requirements.

12.4.2.3 PREPARE INPUTS TO THE DETAILED MAINTENANCE CONCEPT AND DETAILED MAINTENANCE PLAN

The initial step is to use repetitive maintainability analyses as inputs
to a detailed maintenance concept for supporting the system/equipment in
the planned operational environment. Typical inputs to the maintenance
plan are:

    o   depth and frequency of maintenance requirements at each level
    o   facilities required

o   support equipment and tools required
o   skill levels and number of people required

12.4.2.4   ESTABLISH MAINTAINABILITY DESIGN CRITERIA

This task involves the development and application of design criteria and guidelines with the following goals:

o   providing adequate accessibility, work space, and work clearance
o   reducing the need for and frequency of maintenance activities
o   reducing maintenance downtime
o   reducing maintenance support costs
o   reducing maintenance personnel requirements
o   reducing potential for maintenance error
o   providing built in test capability

12.4.2.5   PERFORM DESIGN TRADEOFFS

Perform tradeoff analyses to determine the relative advantages of one design approach and associated maintenance concept over another. Weigh the advantages and disadvantages of each alternative in terms of the effects on operational effectiveness, logistics and maintenance efficiency, and life cycle costs.

12.4.2.6   PREDICT MAINTAINABILITY PARAMETER VALUES

By the use of MIL-HDBK-472 or other approved methods, perform a prediction, in quantitative terms, of the maintainability system/equipment parameter values for the planned design configuration. Compare the prediction with the specified requirements to judge the adequacy of design, and if corrective design action is required.

12.4.2.7   INCORPORATE AND ENFORCE MAINTAINABILITY REQUIREMENTS IN SUBCONTRACTOR AND VENDOR CONTRACT SPECIFICATIONS

The prime contractor shall include appropriate quantitative maintainability requirements in specifications for subcontractor and vendor items procured for the system/equipments. The requirements shall be verified by maintainability demonstration tests, and adequate surveillance controls shall be imposed to insure that the requirements will be met.

12.4.2.8   INTEGRATE OTHER ITEMS

Insure that procedures and methodology are available and applied for integrating the quantitative maintainability parameters of GFE and subcontractor furnished equipment into the prime contractor's maintainability analysis.

12.4.2.9   PARTICIPATE IN DESIGN REVIEWS

Assess maintainability at each scheduled formal design review milestone, to evaluate maintainability status of the design as a basis for approval

to proceed to the next milestone. Identify maintainability problem areas; define and assign specific action items for the correction of problems; verify conformance to specified maintainability requirements.

12.4.2.10 EXTABLISH DATA COLLECTION, ANALYSIS, AND CORRECTIVE ACTION SYSTEM

Establish a maintainability data collection system for prediction during design, and for evaluation of demonstration results. Analyze the data against qualitative and quantitative maintainability requirements, identify problems, recommend solutions, document corrective actions, and include data collected to prove the effectiveness of corrective actions.

12.4.2.11 DEMONSTRATE ACHIEVEMENT OF MAINTAINABILITY REQUIREMENTS

Demonstrate that the specified maintainability requirements have been met by means of a formal demonstration in accordance with MIL-STD-471.

12.4.2.12 PREPARE MAINTAINABILITY STATUS REPORTS

As required, prepare status reports which provide a current accounting of required, allocated, predicted, and observed values for system/equipment maintainability parameters. Reports should include trends, problems encountered, and action taken or proposed.

12.4.3 MAINTAINABLITY TASKS VS. LIFE CYCLE PHASE

Figure 12.4.3-1 depicts the principal maintainability tasks and subtasks and provides guidance as to when they should be done during the system's life cycle.

12.4.4 RELATIVE EMPHASIS ON MAINTAINABILITY PROGRAM ELEMENTS

As was previously done for reliability, Figure 12.4.4-1 lists the elements of a hardware maintainability program, and shows the importance of each element during each of the life cycle phases of development. The chart is provided to give the acquisition/R&M manager an overview of the average situation. It, too, as was true of Figure 12.3.3-1 with reliability, represents the collective wisdom of a number of Government and industry maintainability practitioners.

12.4.5 R&M MILESTONES VS. SYSTEM LIFE CYCLE PHASE

The figures (12.4.5-1 through 12.4.5-5) and accompany tables (12.4.5-1 through 12.4.5-4) on the following pages are provided as additional guidance for acquisition/R&M managers. They depict (figures) and describe (tables) the R&M milestones and the chronological sequence (number in triangles) in which they should be performed, during each of the life cycle phases of a system/equipment procurement. No table is provided for Figure 12.4.5-5 since the milestones are self-explanatory. For the interested reader, further details are provided in Reference 12.

Maintainability Task Area	Life Cycle Phase					Task Requirements
	Conceptual Phase	Validation Phase	Full-scale Development	Production	Deployment Phase	
Determine maintainability requirements for the system	●	●				● Establish M policies, procedures, and terminology ● Derive M requirements ● Define M concept ● Identify human factor and logistics critical areas ● Optimize M to reliability, availability, and supportability costs ● Evolve M conceptual design criteria and constraints ● Evaluate M design feasibility
Specify maintainability requirements and milestone criteria	●	●	●	●		● Define M requirements and demonstration test criteria in system and equipment specifications ● Define M milestone criteria and task requirements in program documentation ● Define data requirements for M assessment and control ● Specifically call out foregoing requirements in contractual documents
Achieve specified maintainability in design			●	●	●	● Perform M design prediction and failure mode analysis ● Identify and define M problems and critical areas ● Integrate M enhancement features into equipment design ● Integrate ATE into equipment and system design ● Verify design conformance to specified requirements by analysis, verification tests, and formal design review ● Review impact of proposed changes on M design characteristics
Demonstrate specified maintainability in development				●	●	● Prepare detailed plans for maintainability test and evaluation ● Perform M demonstration tests ● Demonstrate adequacy of maintenance manuals, test equipment, and support facilities ● Plan, coordinate and conduct M portion of TECHEVAL
Exercise production maintainability controls				●	●	● Perform parts and materials qualification tests ● Perform interchangeability qualification tests for replaceable items ● Perform M suitability assessment in coordination with OPEVAL of early production items ● Establish M criteria in production inspection, test, and control procedures ● Integrate M related measurements data requirements and criteria into production acceptance tests ● Evaluate impact of proposed changes on maintainability and maintenance
Achieve optimum logistic supportability	●	●	●	●	●	● Develop maintenance plan, repair policies, and maintenance procedures ● Develop and verify adequacy of maintenance manuals ● Determine manning and skill requirements ● Develop M training program ● Prepare M spares provisioning plan ● Prepare contractor M support plan ● Verify conformance to specified logistic support requirements
Evaluate maintainability adequacy in service use					●	● Verify conformance to maintainability requirements under service conditions ● Analyze failure modes, maintenance task times, and problem areas ● Verify adequacy of maintenance support (manuals, test equipment, and facilities) ● Evaluate skill requirements and adequacy of training program ● Identify and evaluate inadequacies in supply support plan ● Investigate problem areas for corrective action

FIGURE 12.4.3-1: **MAINTAINABILITY TASKS IN THE SYSTEM LIFE CYCLE**

Element	Life Cycle Phase				
	Conceptual	Validation	Full Scale Development	Production	Deployment
Requirements Definition	xxxxxxxxxxxxxxxxxxxxxxAAAAAA..........				
Maintenance Concept	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.......				
Maintainability Analysis	xxxxxxxxxxxxxxxxxxxxxxxxxxx.......				
Design for Maintainability	ooooooooxxxxxxxxxxxxxxxxxxxxxxxxx...........				
Maintainability Prediction	oooooooxxxxxxxxxxxxxxxxxxxx.......				
Design Review	oooooooxxxxxxxxxxxxxxxxxxx.......				
Design Specifications	xxxxxxxxxxxxxxxxxxxxxxxxxx...				
Acceptance Specifications	xxxxxxxxxxxxxxAAAAAA..........				
Detailed Maintenance Plan	---oooooooooooooooooooooxxxxxxxxAAAA............				....
Data System	xxxxxxxxxxxxxxxxxxxxxxxxxxxooooooooooooooooooooooooooooo				
Technical Manuals	oooooooooooxxxxxxxxxxAAA............				......
Maintainability Acceptance Test	xx.........AAA.............				

First contract —

KEY
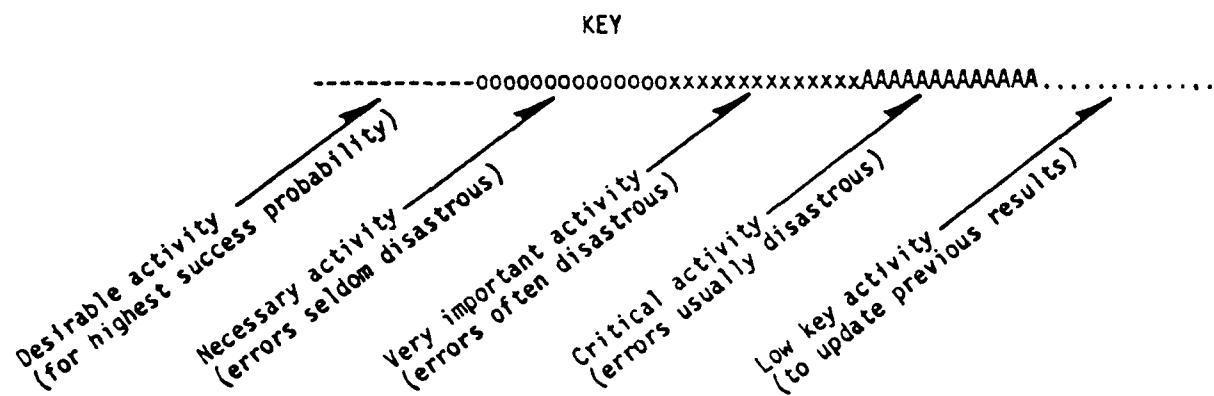
FIGURE 12.4.4-1: MAINTAINABILITY PROGRAM ELEMENTS
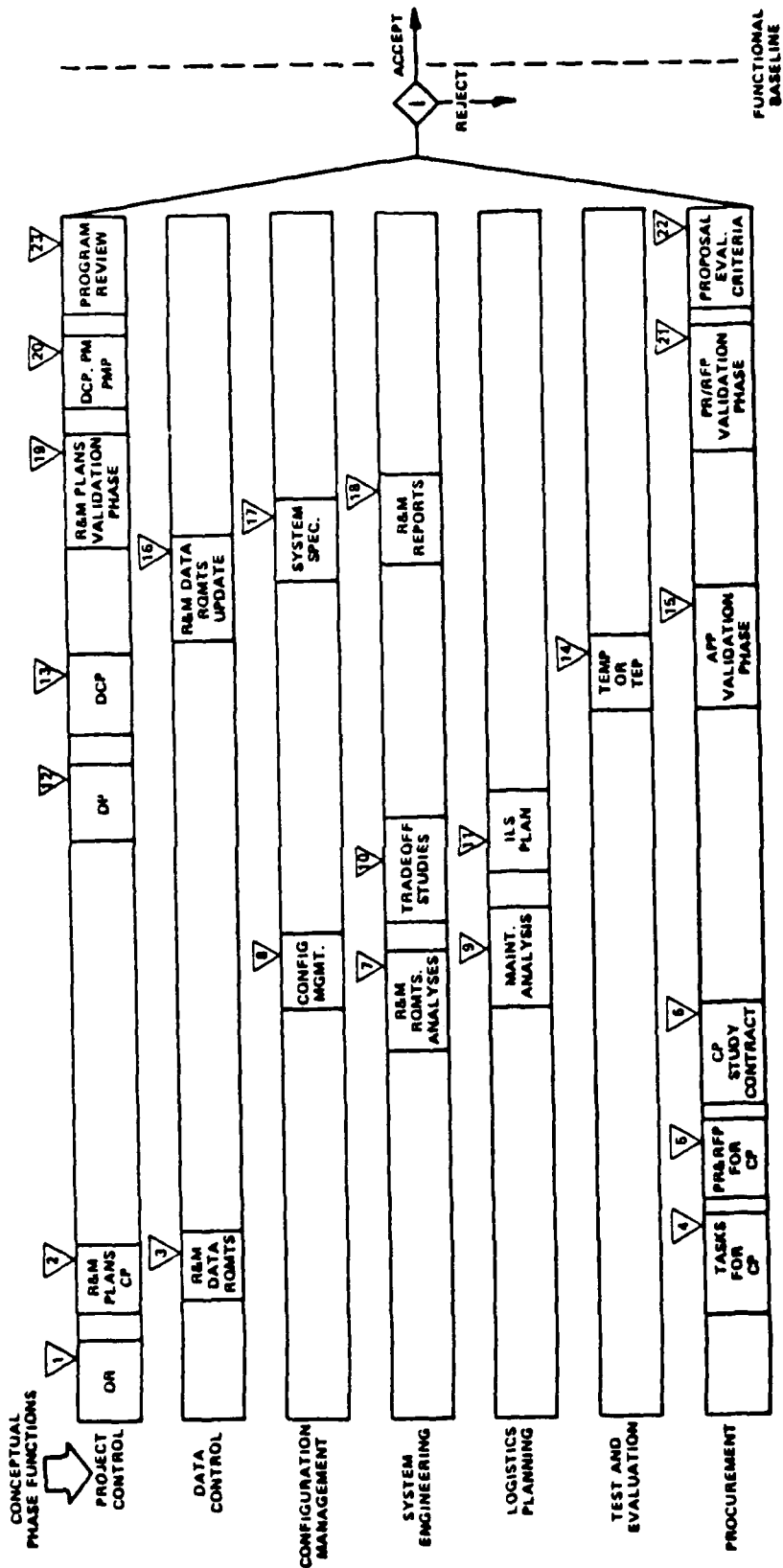
FIGURE 12.4.5-1: CONCEPTUAL PHASE RELIABILITY AND MAINTAINABILITY DECISION POINTS

TABLE 12.4.5-1: SCHEDULE OF CONCEPTUAL PHASE RELIABILITY
AND MAINTAINABILITY TASKS

(1)	Review operational requirement for R&M objectives
(2)	Develop R&M plans for conceptual phase
(3)	Evaluate R&M data requirements
(4)	Prepare R&M inputs for conceptual phase task assignment
(5)	Prepare R&M inputs to PR and RFP for conceptual phase performance
(6)	Review conceptual phase study contract
(7)	Perform system R&M requirements analyses
(8)	Define R&M inputs to configuration management
(9)	Define R&M inputs to maintenance plan
(10)	Perform R&M tradeoff studies with other system effectiveness parameters
(11)	Provide R&M inputs to ILS (Integrated Logistics Support)
(12)	Prepare R&M inputs to development proposal
(13)	Provide R&M inputs for decision coordinating paper
(14)	Prepare R&M inputs for test and evaluation master plan
(15)	Prepare R&M inputs for advance procurement plan
(16)	Update R&M data requirements
(17)	Prepare R&M requirements specifications
(18)	Prepare R&M analysis reports
(19)	Prepare R&M plans for validation phase
(20)	Review R&M inputs to decision coordinating paper
(21)	Prepare R&M inputs to purchase request/request for proposal for validation phase
(22)	Prepare R&M criteria for proposal evaluation
(23)	Perform R&M review of program

TABLE 12.4.5-2: <u>SCHEDULE OF VALIDATION PHASE RELIABILITY</u>
<u>AND MAINTAINABILITY TASKS</u>

(1)	Proposal evaluation
(2)	Contract reliability and maintainability review
(3)	Reliability and maintainability plans for validation
(4)	Preliminary reliability and maintainability design analysis
(5)	Maintenance concept review
(6)	GFE evaluation
(7)	Logistics planning review
(8)	Reliability and maintainability design tradeoff study
(9)	Data review
(10)	Reliability and maintainability design review
(11)	Functional baseline specification
(12)	Design verification tests
(13)	Formal program review
(14)	Parts and materials evaluation
(15)	Approved parts list review
(16)	Reliability and maintainability design support
(17)	Data application review
(18)	Preliminary design review
(19)	Allocated baseline specification
(20)	Engineering change review
(21)	Integrated logistics plan update
(22)	Integrated test plan for full-scale development
(23)	Reliability and maintainability plans for full-scale development
(24)	Data requirements for full-scale development
(25)	Reliability and maintainability preliminary design
(26)	PR/RFP for full-scale development
(27)	Final program review
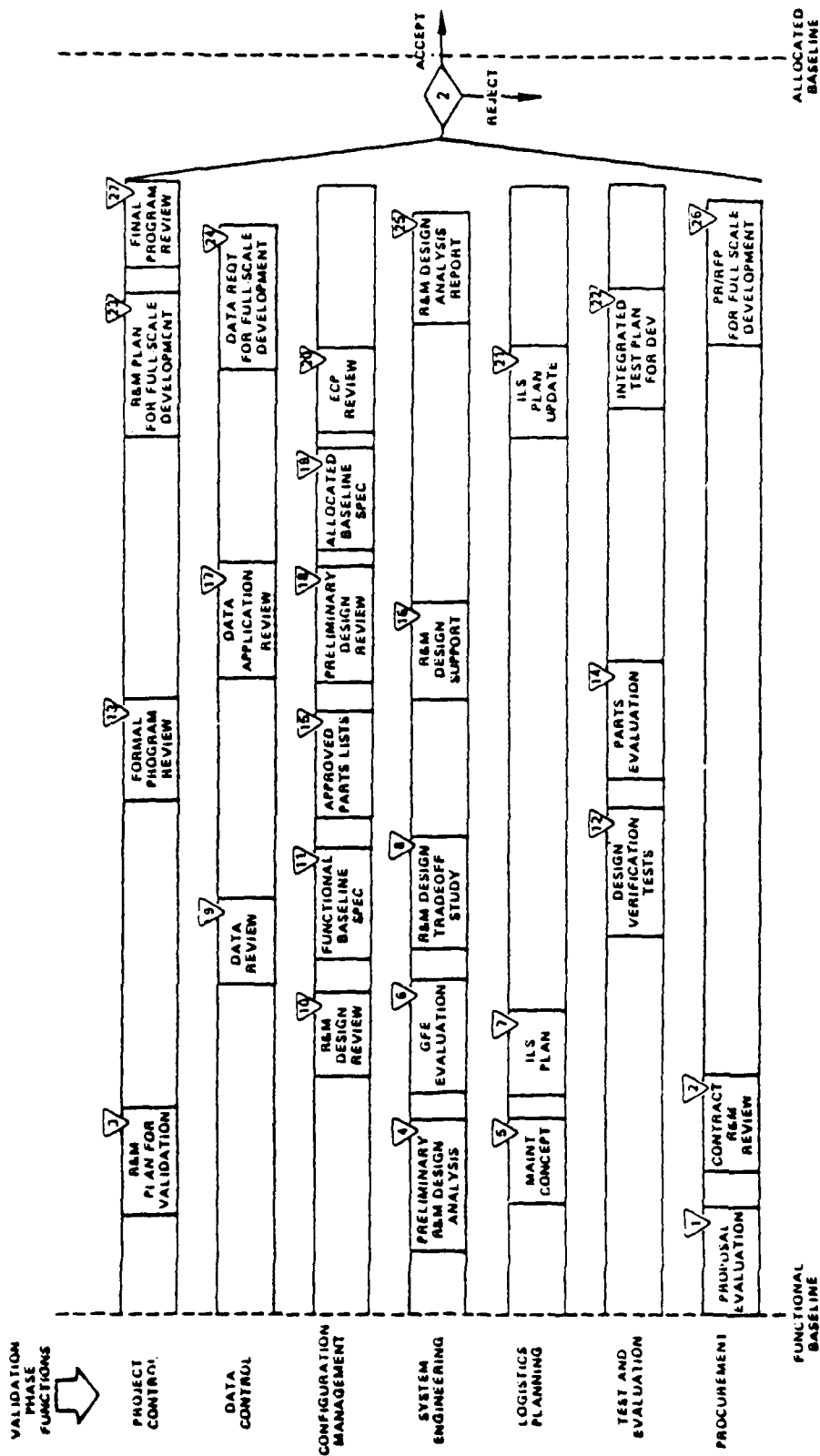
FIGURE 12.4.5-2: VALIDATION PHASE RELIABILITY AND MAINTAINABILITY DECISION POINTS

TABLE 12.4.5-3: <u>SCHEDULE OF FULL-SCALE DEVELOPMENT PHASE TASKS</u>

(1)   Proposal evaluation

(2)   Contract review

(3)   R&M plan review

(4)   Experimental model R&M support

(5)   Integrated test plan

(6)   ECP review

(7)   Maintenance engineering

(8)   Data review

(9)   R&M program review

(10) Design review

(11) Integrated Logistics Support plan

(12) Full-Scale Development RM&QA procedures

(13) Functional tests

(14) Specification review

(15) Engineering model R&M support

(16) Environmental tests

(17) Operation & maintenance manuals

(18) ECP review

(19) Vendor control

(20) R&M program review

(21) Critical Design Review

(22) Specification review

(23) Prototype model R&M support

(24) Subsystem tests

(25) ECP review

TABLE 12.4.5-3: <u>SCHEDULE OF FULL-SCALE DEVELOPMENT PHASE TASKS (Cont'd)</u>

(26)   Preinstallation tests

(27)   System integration R&M support

(28)   Packaging, Handling, Storage, and Transportability

(29)   R&M demonstration tests

(30)   R&M program review

(31)   Preproduction Reliability Design Review

(32)   Technical evaluation

(33)   Operational evaluation

(34)   Parts review

(35)   R&M design report

(36)   Production specification

(37)   Production R&M plan

(38)   Production data requirements

(39)   Production RM&QA procedures

(40)   Production R&M test plan

(41)   PR and RFP for production
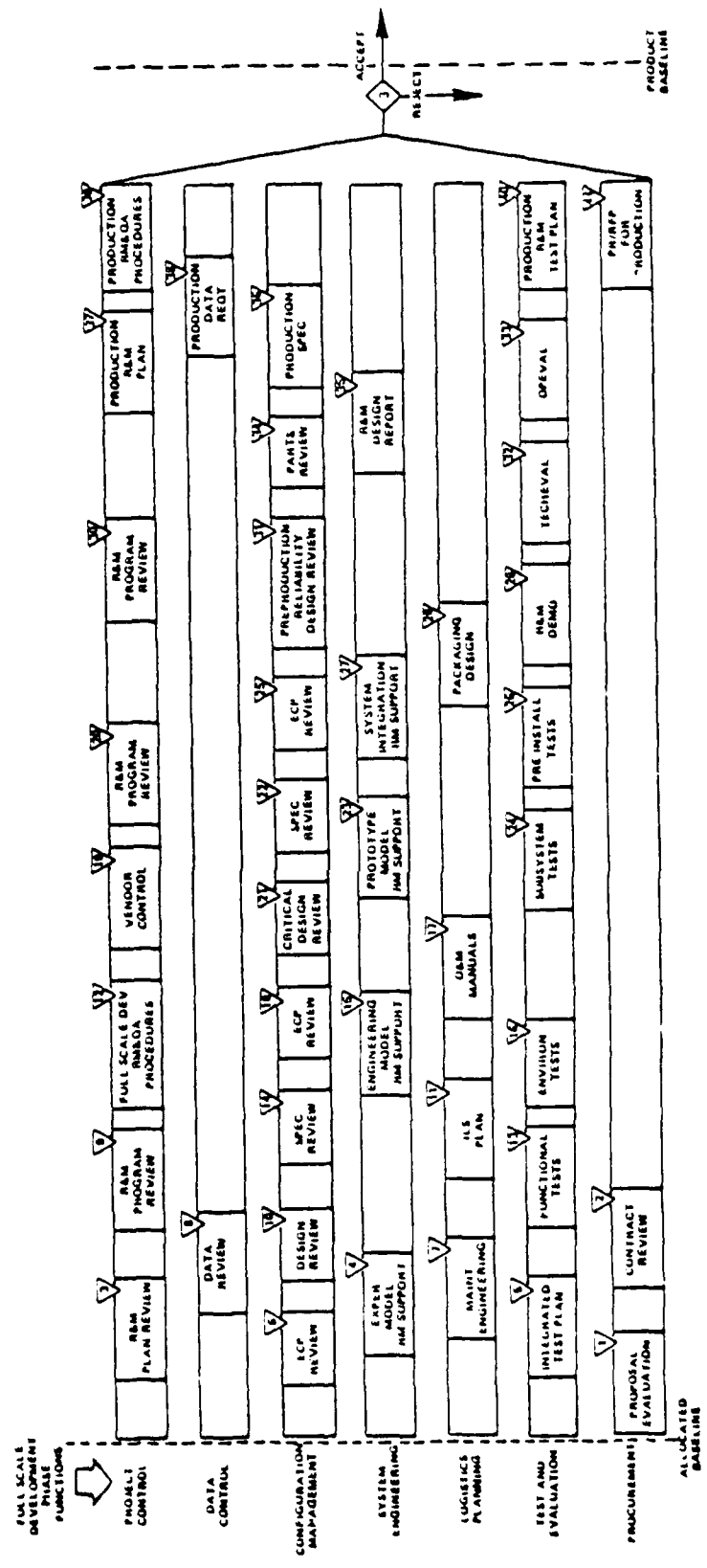
FIGURE 12.4.5-3: FULL-SCALE DEVELOPMENT PHASE RELIABILITY AND MAINTAINABILITY
DECISION POINTS

TABLE 12.4.5-4: <u>SCHEDULE OF PRODUCTION PHASE TASKS</u>

```
(1)    Contract review

(2)    Production RM&QA program plan

(3)    Production specification

(4)    Production test plan

(5)    Parts and materials test program

(6)    R&M data review

(7)    ECP review

(8)    Preproduction R&M support

(9)    Contractor performance evaluation

(10)   Production R&M evaluation tests

(11)   ILS validation

(12)   Configuration audit

(13)   Production reliability acceptance tests

(14)   R&M engineering

(15)   Production specification

(16)   RM&QA program evaluation

(17)   R&M demonstration tests

(18)   ECP review

(19)   Production R&M support

(20)   Configuration audit

(21)   Failure data collection system

(22)   Production reliability acceptance tests

(23)   Production specification

(24)   Contractor performance evaluation

(25)   ILS update

(26)   R&M demonstration tests

(27)   Follow-on operational test and evaluation

(28)   Production R&M monitoring
```
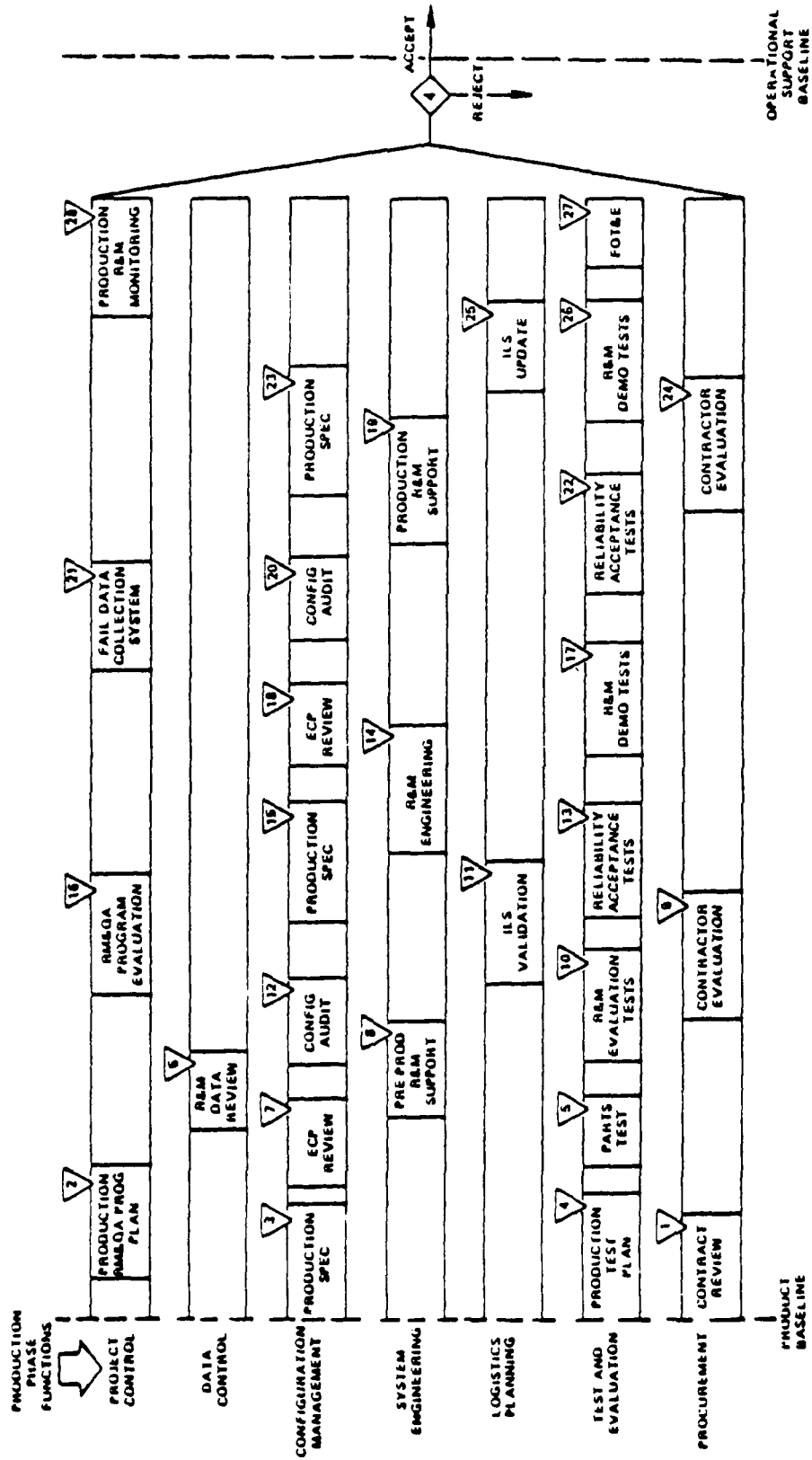
FIGURE 12.4.5-4:   PRODUCTION PHASE RELIABILITY AND MAINTAINABILITY DECISION POINTS
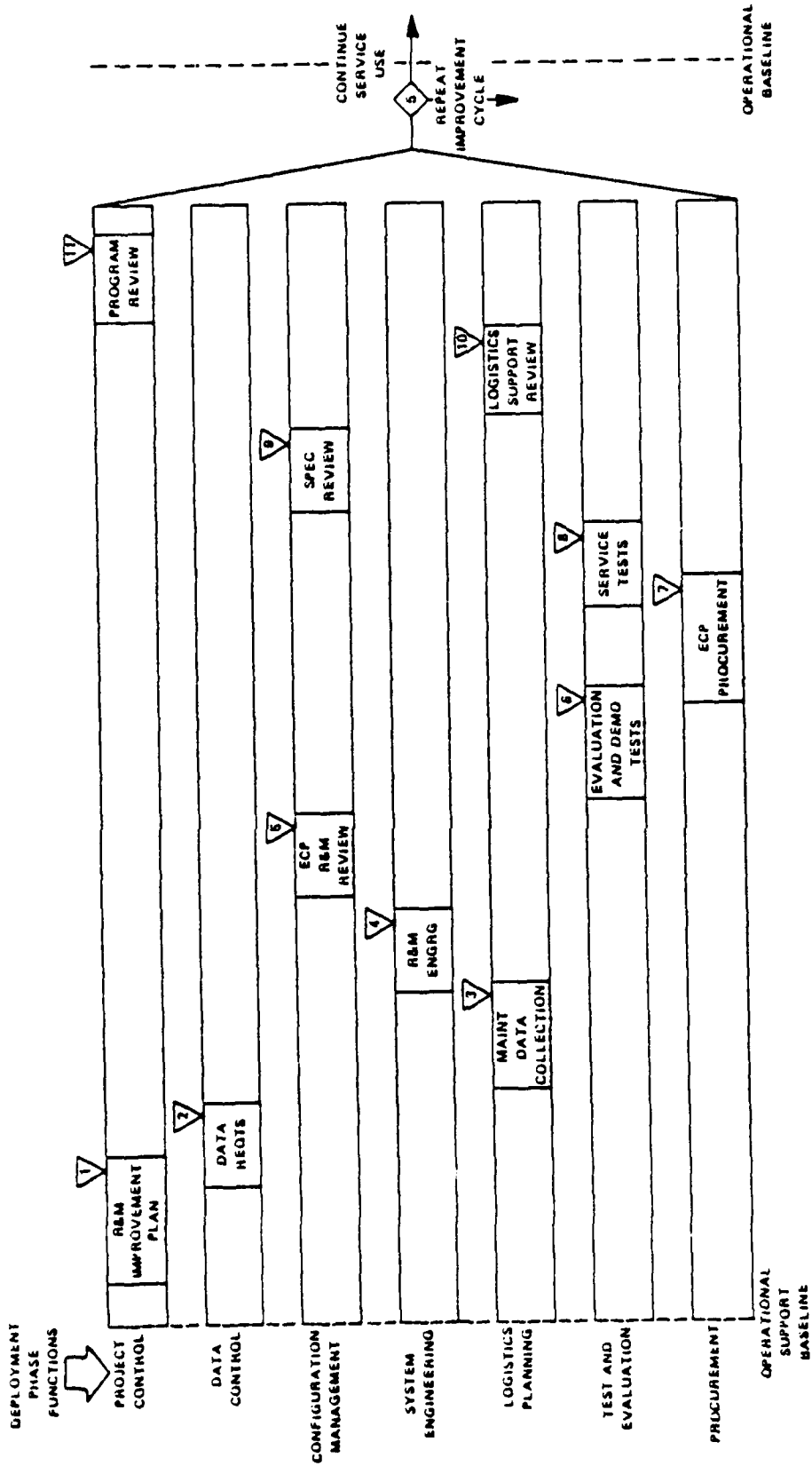
FIGURE 12.4.5-5: DEPLOYMENT PHASE RELIABILITY AND MAINTAINABILITY DECISION POINTS

12.5 COMPUTER SOFTWARE R&M CONSIDERATIONS

12.5.1 INTRODUCTION

Previous sections of this section dealt with hardware R&M considerations; this section deals with the software aspects, from a management point of view. The technical aspects were treated, in significant detail, in Section 9.

Despite the fact that software R&M has not reached the sophisticated stage of evalution of that of hardware, there are some procedures available which a manager can use to help achieve the desired software, quality, reliability, and maintainability. Admittedly, these procedures are not geared solely to R&M achievement; however, their proper and timely application has been shown to enhance the R&M of the developed software.

First let us look at the hardware/software relationships during a "systems" life cycle phases. These are shown in Figure 12.5.1-1. Each of the phase depicted in Figure 12.5.1-1, pertaining to software development, is briefly described as follows:

o   The requirement phase involves performing preliminary hardware/software tradeoffs to produce a statement of system requirements. The statement will provide specific system functional specifications/requirements as well as the constraints (design, cost, etc.) that the system must meet.

o   In the preliminary design phase, the requirements are translated into well defined functional specifications. Detailed hardware/software tradeoffs are performed, and a design approach is selected among the various alternatives. The computer program design specification is prepared during this phase, and a preliminary design review is normally held at the end of this phase to assess the adequacy of the selected approach.

o   During the detailed design phase, the software component definition, interface, and data definition are developed and verified against the requirements. Functional flow charts and detailed flow charts are prepared. Detailed flow charts are used to define the information processing in terms of logical flow and operations to be performed by the computer program. The relationship between the computer program and the interfaces between the software, the computer(s), and other peripheral devices are also defined at this time. A preliminary computer program product specification is prepared at the completion of this phase. At the end of the design phase, and prior to the coding and testing phase, a design review is usually held to establish the integrity of the flow charts and the preliminary computer program specification.

o   During the coding and debug phase the detailed design is translated into actual program code, and the initial testing of the code is performed. This initial testing normally is designed to check for correct outputs using predefined inputs.
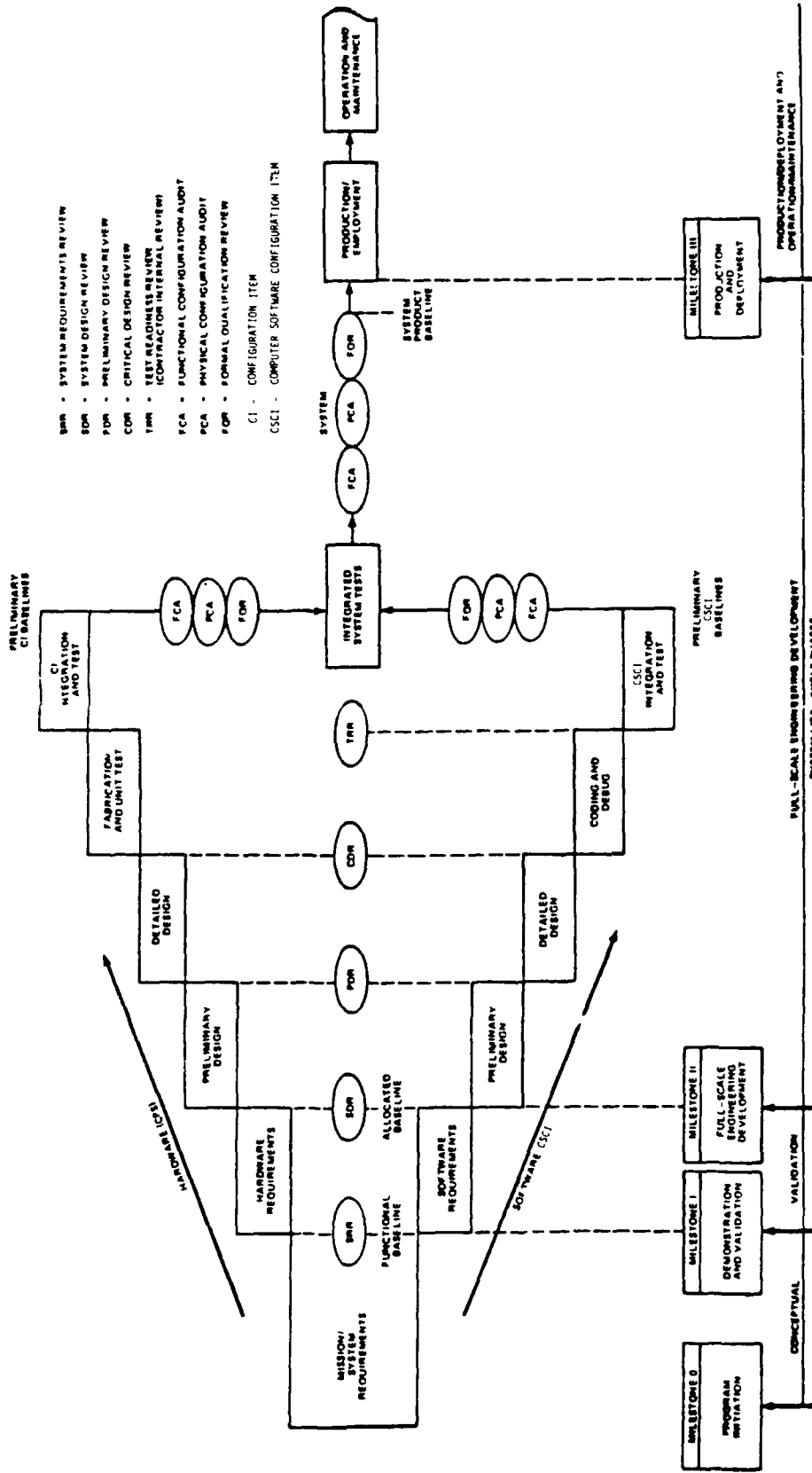
FIGURE 12.5.1-1: HARDWARE/SOFTWARE SYSTEM
LIFE CYCLE RELATIONSHIPS

o   In the integration and test phase, the computer programs are tested against the requirements as stated in the preliminary program specifications, and, once tested, the software package is prepared and integrated with the system hardware components. The computer program product specification is finalized during this phase.

o   During the integrated system tests, the computer programs are loaded and run to ensure that the system performance meets requirements. The system is completely documented during this phase, and all changes resulting from the previous phases are incorporated into the supporting documentation, including the flow charts and final product specification.

Thus, a complex set of relationship exists between hardware/software development areas. The interplay of analysis, system test and other functions must be evident throughout the development cycle in order to assure reliability. Each task must not only contribute to the total program, but also provide timely inputs to other tasks in relation to system and software milestones. Overall management must begin with the development of system requirements and continue through preparation of specifications during system analysis, interact with design and development efforts and extend through control of changes. Reliability analyis must be performed as part of early system analyses (tradeoffs) to establish the optimum levels of R&M to be achieved in both hardware and software design. These analyses must extend through design and development to further define R&M requirements to establish the basis for meaningful integration tests, and finally, through assessments performed during system test, to determine achieved levels of R&M. The test program must include package/system testing during development to force out design errors and system integration and acceptance testing prior to delivery, to assure, with confidence, that the requirements are met.

Thus, to assure system R&M, proper consideration must be given during the early requirements definitions phase, and must be rigorously applied with proper emphasis in subsequent development phases. Considerations should include:

(1) Supporting the early requirement definition phase with appropriate technical and system analysis to describe the purpose and expected use of the system. The system analysis should identify control functions and parameters and associated criticality of failure, safety related issues, special conditions of use (and possible misuse), environmental and human factors which have the potential for introducing error and malfunction, and the mechanics of the man/machine interface.

(2) Establishing reliability requirements for the software by preparing a system requirement statement - the statement should contain a description of the goals and objectives to be achieved by the software routines and how they will be integrated with the hardware requirements.

(3) Selecting the optimum hardware/software "mix" through detail consideration and tradeoffs of component availability, cost, flexibility, application requirements, vendor support, and R&M.

(4) Performing system engineering (prediction, FMEA, etc.) during hardware/software design and development to assure R&M, and that critical hardware failure modes and software errors cannot contribute to unsafe operation of the system.

(5) Establishing R&M requirements for the computer(s) the peripherals, and the software, from review of manufacturers' data and specifications, from actual test and experience data, and other sources such as MIL-HDBK-217, the Reliability Analysis Center (RAC), and the Data and Analysis Center for Software (DACS).*

(6) Preparing an integrated test plan that provides a full description of the tests to be performed to demonstrate the acceptability of the hardware and software designs.

(7) Implementing a well documented configuration management system that provides traceability of the system configuration as well as all changes to the hardware and associated software after final acceptance.

12.5.2 SOFTWARE RELIABILITY TOOLS AND TECHNIQUES

Software reliability has begun to develop into an organized body of data, knowledge and techniques, within the past several years. Although there are few industrial or military standards (MIL-S-52779, DoD-STD-2167, and Refs. 13-15) that address this subject, most experts agree that the most critical elements in the development of software systems to achieve adequate reliability are:

(1) the centralization of a well planned and carefully controlled software organization that emphasizes program management, thorough documentation and configuration control.

(2) the performance of reliability analysis and tradeoff studies,

(3) the use of software development techniques that restrict the growth of complex unmanageable and unreliable programs, and

(4) the application of thorough test procedures.

Table 12.5.2-1 presents a list of some of the provisions, techniques and tools utilized with respect to these areas.

As was done for hardware R&M, Figure 12.5.2-1 (Ref. 10) lists the principal elements of a software development program, and shows the importance of each element during each of the system's life cycle phases. Also shown is the percentage distribution (column 2) of contractor manhour effort for the various elements for an "average" program. Each of the elements of Figure 12.5.2-1 is addressed in the following paragraphs.

*Data and Analysis Center for Software (DACS) sponsored by the Rome Air Development Center (RADC), operated by the IIT Research Institute.

TABLE 12.5.2-1: <u>SOFTWARE RELIABILITY PROVISIONS, TECHNIQUES AND TOOLS</u>

```
O    Software Reliability Organization
     -    Policy
     -    Cost & resource estimation and budgeting
     -    Staffing
     -    Management tools and guidelines
     -    Training

O    System Acquisition Specification
     -    Software Performance Requirements
     -    Software/Hardware interface requirements
     -    R&M requirements

O    System Control During Development
     -    R management plan
     -    R analysis (prediction, FMEA, etc.)
     -    Maintenance
     -    Design review
     -    Error Analysis
     -    Configuration Management

O    Standards & Specifications
     -    System specification requirements
     -    Software performance specification
     -    Interface standards
     -    Design specification requirements
     -    Program specification requirements
     -    Coding standards
     -    Language standards
     -    Reliability analysis methods
     -    System Control Requirements

O    Software Development Tools and Techniques
     -    Structured Programming
     -    Higher order language
     -    Top down modular design
     -    Specified coding structure
     -    Program testing
     -    Integrated testing
     -    Acceptance Testing

O    Reliability Analysis Methods
     -    Software/hardware tradeoffs
     -    Prediction and error assessment
     -    Failure Modes & Effect Analysis
     -    Software Sneak Analysis

O    Error Data Collection, Analysis & Feedback

O    Software Reliability Improvement
```

Element	%Effort	Life Cycle Phase				
		Conceptual	Validation	Full Scale Development	Production	Deployment
Requirements Definition	5	xxxxxxxxxΛΛVΛΛ............	....			
System Analysis	10	xxxxxΛΛΛΛxxxxxxxxxxxxxxAAA......				
Package Design	10	---ooooxxxxxxxx....		....	....	
Unit Design, Code & Debug	15		---oooooooooxxxx......	....	....	
Package Integration & Test			---oooxxxxxAAA....	....		
System Integration & Test	30			xxAAAAxx..........		
Acceptance Test				xxxAAA..........		
Program Plan		---oooooooxxxxxxxxxxxxxxxxxxx......				
Specifications		xxxxxxxxxxxxxxxxxxxxxxxxxxxxAAAAA...........				
Data System	30	oooooooooooooooooooooooooxxxxxxx...........				
Program Review		oooooooxxxxxxxxxxxxxxxxxxxAAAAA...........				
Test Plan			----ooooxxxxxxxxAΛΛA....			
Technical Manuals				oooooooxxxxxxxxAA.......	......	

First contract

KEY

------------oooooooooooooxxxxxxxxxxxxxxxxxAAAAAAAAAAAAA............

Desirable activity (for highest success probability)

Necessary activity (errors seldom disastrous)

Very important activity (errors often disastrous)

Critical activity (errors usually disastrous)

Low key activity (to update previous results)
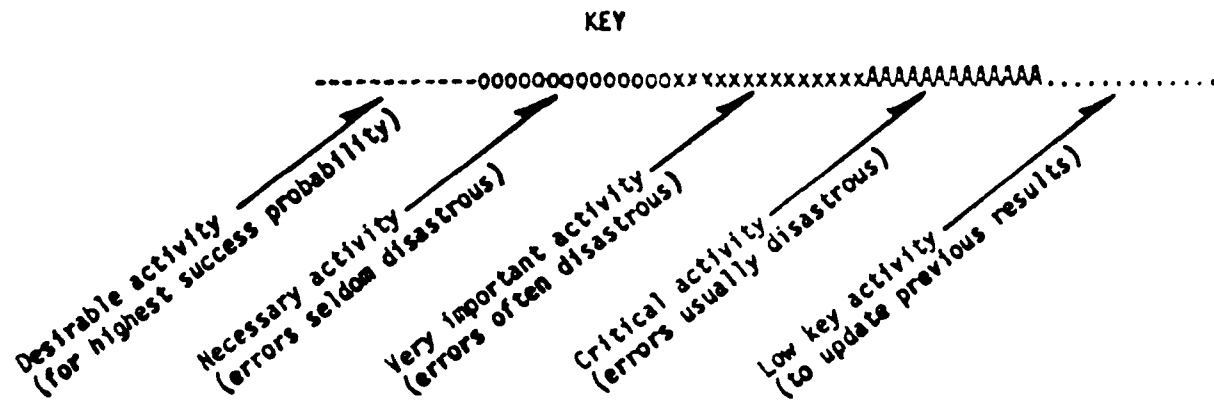
FIGURE 12.5.2-1: ELEMENTS OF A SOFTWARE DEVELOPMENT PROGRAM

12.5.2.1 REQUIREMENTS DEFINITION

Software requirements define the overall mission problem to be solved by the software, the operational constraints, and any fixed interfaces with system hardware and people. Requirements must cover the following kinds of information:

o   mission problems to be solved by the software system

o   software-related system hardware design decisions not subject to tradeoff studies

o   software design contraints imposed on the system

o   input data sources, rates and formats (if established)

o   output data destinations, rates, and formats (if established)

o   adaptability required for system modifications in operational use

o   software-dependent maintenance concepts and plans

o   security needs

o   operational hazards and environment

o   reliability and maintainability needs

Requirements are determined, so far as possible, by the System Program Office as an in-house task. The work is done before the first contract, depending heavily upon user and logistics requirements. After the first contract, the contractor will further refine and define the requirements through systems analysis and discussions with the System Program Office. Requirements must be "pinned down" by the early part of the validation phase, and are documented in the program plan, system specifications, and interface specifications.

12.5.2.2 SYSTEM ANALYSIS

System analysis proceeds in parallel with requirements definition, and evaluates the system design tradeoffs between hardware and software. It considers computer hardware options, maintenance options, and in general, all of the software-related hardware alternatives. The objective is to design the hardware/software system so as to maximize the chances of success at the lowest life cycle cost. These chosen design options are documented in system and interface specifications used by the software designers. The first set of A's on Fig. 12.5.2-1 refers to delivery of these hardware parameters to the specification writers.

Another important area of system analysis which continues through the middle of full scale engineering development, is the development of schemes for system testing and acceptance. The thoroughness of these schemes directly affects the verification of software R&M. Test schemes

are documented in the system test plans and acceptance specifications. The second set of A's on Figure 12.5.2-1 refers to delivery of this test planning information to the test plan writers.

12.5.2.3 PACKAGE DESIGN

Package design refers to the development of the complete software system functional organization. That is, the programming hierarchy of tasks of the software system are defined in terms of a categories and subcategories, all the way down to the unit level. (The process is analogous to organizing a large group of people with diverse skills to carry out a project). To enhance R&M of a large software system, this software functional organization must be thorough, well documented, and all interface rules between functional elements must be precisely defined and their application carefully controlled.

A "chief programmer" or a senior software system engineer is usually assigned to oversee and manage this whole process. Subordinate program- mers responsible for the separate programs in the functional categories are assigned to him. In other words, there will be a hierarchical organization of people (programmers) with supervisors and subordinates that pretty much parallels the functional organization of the software system. The chief programmer must not only be an engineer experienced in development of large software systems, but must also be skilled in applying the traditional management tools to plan, organize, staff, direct, and control his people and project.

In turn, the subordinate manager of each program, or subprogram, will plan, organize, direct and control the detailed coding, testing, and documentation of programming within his domain using the ground rules laid down by the chief programmer. At the same time, each subordinate manager will devise schemes for testing to insure quality. The results of this work are documented in the test plan, data system and specifications discussed below.

In addition to organizing the whole operation, the chief programmer must identify the source program languages to be used (from system analyses documented in the system and interface specifications) and the general rules for program structure and progress documentation throughout his organization. The programming rules should be documented in one of the computer program design specifications.

To enhance the readability and testability of the computer programs, "structured programming" techniques should be employed. In part, this means that the programmer is restricted to a small set of standard language constructs which prevent him from skipping to some remote segment of the computational sequence. This approach reduces the possibility of logical traps or "dead ends". Software specialists will know what structured programming means.

12.5.2.4 UNIT DESIGN, CODE AND DEBUG

Another attribute of "structured programming" is the size restriction on program units or models. The unit is typically defined to be about 50 lines of program code which will fit on one listing page. Furthermore,

unit will have only one link from the preceding unit and one link to the following unit. These rules enhance readability, comprehension, and independent testability of each unit. Each "Chief" will supervise the design, code, debug, and test of his group's output. He may, of course, be responsible for a number of units in the overall software program. He will document his work in the data system, and the appropriate computer subprogram design document noted below in the discussion of specifications.

12.5.2.5 PACKAGE INTEGRATION AND TEST

Package integration and test means that units, subprograms, subroutines, etc., and programs are assembled and tested in groups of increasing size until the entire software package is put together. This assembly and testing is usually done with tne aid of general purpose computers, since the operational hardware computer may not be available until late in full scale development. The Test Plan is used throughout this process, and results are documented in the data system. The thoroughness of this element of the software development process is critical to software reliability.

12.5.2.6 SYSTEM INTEGRATION AND TEST

System integration and test means that the software package is inserted into the operational hardware, and complete system tests are run to insure that ha dware and software are compatible and that operational requirements can be fulfilled. This element is also critical to verification of operational suitability. It occurs in the final phases of full scale development, and hopefully, only minor changes will be necessary then. The Test Plan is used to conduct these tests.

12.5.2.7 ACCEPTANCE TEST

The software acceptance test is defined in the Test Plan, and possibly in an overall system acceptance specification. This test is the final test which formally establishes acceptability of software products for delivery under the development or production contract.

Preparation of numerical acceptance criteria is hampered by the lack of any widely accepted measures of software R&M. Nevertheless, the Program Office must be sure that acceptance criteria are developed during the conceptual and validation phases. This is partly an in-house task using help from Government software engineers, but is also a task for the contractors under system analysis and package and unit design. Criteria are documented in the Test Plan and acceptance specifications.

12.5.2.8 PROGRAM PLAN

The Program Plan outlines and explains all elements of the software development effort. It shows requirements, interfaces, organization, task breakdown, responsibilities, schedules, and the approach to solving all the software development problems so as to fulfill the requirements on schedule and within projected cost. This plan is developed mostly by the contractors during conceptual and early validation phases, but must be continuously updated.

12.5.2.9 SPECIFICATIONS

Specifications formally and precisely document all requirements and design decisions. They may be grouped into several categories:

o   System Specification

   Defines the system requirements and the overall hardware/software system design in top level detail.

o   Software Performance Specification

   Defines the software requirements, software design ground rules, selected software-dependent hardware parameters, interface identification, and overall structure of the software system. This specification goes into a second level of detail below the System Specification.

o   Interface Specifications

   Defines the interface design details between software and hardware elements and between software subdivisions. It goes into a second level of detail below the preceding Software Performance Specification.

o   Software Design Specification

   Defines and describes the computer programs that will meet the Software Performance Specifications in functional flow diagram detail. It also defines the programming scheme and rules which will be used by programmers to implement the functional elements in computer code.

o   Subprogram Design Document

   Gives a detailed technical description of each subprogram including input, output, functional flow, narrative description, limitations, interfaces, and mathematical equations solved or operations performed. It also describes the tests used to check it out.

o   Common Data Base Design Document

   Gives a detailed technical description of all data items used by the software system. This includes constants, variables, and tables. Details include data name, table index, purpose, dimensions, units, initial values, range of values, exact format, etc.

o   Acceptance Specification

   Defines the criteria to be used in judging formal acceptability of software products under contract.

12.5.2.10 DATA SYSTEM

The data system, also called the program support library, is designed to provide management control information and documentation discipline. It will consist of some kind of periodic reporting procedure where every programmer will be required to submit at least a weekly report on his effort. The reports might include estimates of coding completion of assigned units, numbers and classifications of errors found in debugging and testing, information shortages which hamper coding progress, specification errors discovered, manhours spent on separate units, documentation contributions, etc. Listings of each run are also collected and stored in this system. The chief programmer will have an administrative staff to compile the reports into composite summary charts, graphs and narratives for use in management reviews. The data system must also cover status of the documentation, and some very disciplined scheme must be devised to insure that documentation keeps up with changes in requirements, system design and software design.

Notice in Figure 12.5.2-1 that the data system continues through production and deployment. This means that the Air Force must adopt a data system for use throughout the software life cycle. In contrast to hardware, software is relatively easy to change in the field and documentation changes must be thoroughly disciplined.

12.5.2.11 PROGRAM REVIEW

The contractor will have frequent in-house program reviews, and the Government less frequent reviews. In the Government program reviews, overall program progress is reviewed and compared with the Computer Program Development Plan. Also, a technical review of the software is performed by the Program Office backed up by software specialists from Government laboratories or specialists from some other advisory organization. These reviews are formally documented with action items assigned to the Government or contractor for resolution by specified dates.

The Air Force, for example, requires at least four formal reviews; the systems requirements review (SRR), the system design review (SDR), the preliminary design review (PDR), and the critical design review (CDR). The PDR and CDR were described earlier. The SRR is conducted after a significant portion of the system functional requirements have been established, and is used to evaluate contractor responsiveness to the statement of work and the contractor's interpretation of the system requirements. The SDR is conducted prior to the beginning of preliminary design by the contractor, and is used to review system documentation and assess the degree of accomplishment of the engineering management activities.

12.5.2.12 TEST PLAN

Several test plans are prepared during the software development cycle to define procedures for package integration and test and system integration and test. These plans explain who does what and when. They may also specify test requirements down to the unit level. The

principal test plans prepared are for development tests & evaluation (DT&E), initial operational test and evaluation (IOT&E) and follow-on operational test and evaluation (FOT&E). These test plans are developed from data provided by requirements, system analysis, package design, and unit design. They are prepared to support the Test and Evaluation Master Plan (TEMP) which is the overall master test plan prepared in conjunction with the PMD. These test plans are used to define the test problems to be solved by the software along with acceptable solutions. R&M test criteria are, of course, included.

The use of the DT&E tests plan is formally evaluated via preliminary qualification testing (PQT) and formal qualification testing (FQT). PQT is conducted on the "critical" functions of the software package during the time period between completion of CDR and the start of FQT. FQT is a complete and comprehensive test of the software package performed after completion of the design, and which culminates in a functional configuration audit (FCA).

12.5.2.12 TECHNICAL MANUALS

While the various specifications and design documents described above document the exact structure of the software, those documents are not necessarily suitable for field use in training and operations. The technical manuals are written using those specifications and documents, but are written by people who know how to convey that information to field personnel in the most effective way. The manuals normally include the following types:

o   User's Manual

o   Computer Operator's Manual

o   Sofware Maintenance Manual

o   System Maintenance Manual

All types may not be needed for a particular system. As mentioned before, the contractor's and individual Service data systems must include administrative procedures to insure that these manuals reflect all changes in specifications and design documents throughout the software life cycle.

12.6 R&M DATA ITEMS

The outputs of each of the R&M program tasks, as was discussed, are normally defined in terms of a deliverable document or data item. This documentation is necessary to provide a basis for completely specifying and planning development/production programs, and to demonstrate that the R&M tasks are adequately implemented. The purpose of the documentation is to disseminate information, record data, document design/production decisions (and the underlying logic), and to report program status.

Data Item Descriptions (DIDs) define the data requirements to be prepared and delivered by DOD Contractors, the tasks, such as tests, design, analysis, reviews, and controls, and the source of information required to prepare the data product are described in specifications/standards. Reference 16, "Department of Defense Acquisition Management Systems and Data Requirements Control List (AMSDL)," contains a comprehensive list of DIDs for use by acquisition Managers on DOD procurements. The purpose of the AMSDL is to provide Managers with a list of standard data items that can be directly called out in contracts, thus negating the need for individual preparation of data items, and minimizing the proliferation and duplication of data requirements currently being placed on contracts. Those DIDs which are unique to R&M and software have been extracted from the AMSDL and are listed in Tables 12.6-1 through 12.6-4.

Also, included in the following pages (EXAMPLES 1, 2, and 3) are detailed descriptions of specific DIDs. Note that they are usually referenced to a specification, standard, or handbook. The current goal of DOD is to associate each DID with a specification, standard, or handbook, so that they will not be included in contracts as end items in themselves.

An important point to be made, is the fact that the DIDs should be tailored to the task requirements of the SOW.

Specific DIDs may be obtained from:

> Naval Publications and Forms Center
> 5801 Tabor Avenue
> Philadelphia, PA   19120

TABLE 12.6-1: R&M DIDS

DI-R-1724	Quality Inspection Test, Demonstration, and Evaluation Report
DI-R-3547	Reliability and Maintainability Report on Commercial Equipment
DI-R-5420	System Effectiveness Program Plan (SEPP)
UDI-R-21131	Report, Reliability and Maintainability Program
UDI-R-21133	Report, Reliability and Maintainability Allocation
UDI-R-21135	Report, Reliability and Maintainability Test Plan
UDI-R-21136	Report, Reliability and Maintainability Test Results
UDI-R-21137	Report, Reliability and Maintainability Status

TABLE 12.6-2: RELIABILITY DIDS

DI-R-1701, with Addendum 2 (ER)	Burn-In Procedures
DI-R-1710, with Addendum 1 (ER)	Reliability Test, Demonstration, and Evaluation Procedures
DI-R-2114	Report, Reliability Allocation
DI-R-3541	Computer-Programmed Mathematical Model for Reliability
DI-R-3548B	Suspect Material Deficiency Notice (ALERT) and Response
DI-R-5299C	Failure Analysis and Corrective Action Report
DI-R-5468A	Quality Status/Reliability Summary Report
DI-R-7040	Report, Burn-In Test
DI-R-7079	Reliability Program Plan
DI-R-7080	Reliability Status Report
DI-R-7081	Reliability Mathematical Model(s)

TABLE 12.6-2: <u>RELIABILITY DIDS (CONT'D)</u>

DI-R-7082	Reliability Predictions Report
DI-R-7083	Sneak Circuit Analysis Report
DI-R-7084	Electronic Parts/Circuits Tolerance Analysis Report
DI-R-7085A	Failure Mode, Effects, and Criticality Analysis Report
DI-R-7086	Failure Mode, Effects, and Criticality Analysis Plan
DI-R-7094	Reliability Block Diagrams and Mathematical Models Report
DI-R-7095	Reliability Prediction and Documentation of Supporting Data
DI-R-7100	Reliability Report for Exploratory Advanced Development Model
DI-R-30507	Failure Modes and Effects Analysis (FMEA) Report
DI-R-30508	Critical Items List
DI-R-30509A	Reliability Allocations, Assessments, and Analysis Report
DI-R-30511	Critical Item Control Plan
UDI-R-21138	Report, Environment
DI-R-21599	Development and Production Failure Summary
DI-RELI-80247	Thermal Survey Report
DI-RELI-80248	Vibration Survey Report
DI-RELI-80249	Environmental Stress Screening (ESS) Report
DI-RELI-80250	Reliability Test Plan
DI-RELI-80251	Reliability Test Procedures
DI-RELI-80252	Reliability Test Reports
DI-RELI-80253	Failed Item Analysis Report
DI-RELI-80254	Corrective Action Plan
DI-RELI-80255	Failure Summary and Analysis Report

TABLE 12.6-3: <u>MAINTAINABILITY DIDS</u>

DI-R-1742	Maintainability Mathematical Model(s)
DI-R-2129	Plan, Maintainability Demonstration
DI-R-3549A	Repair Level Analysis Reports (RLA)
DI-T-4901	First Article Inspection Procedure
DI-T-4902	First Article Inspection Report
DI-T-4903	Production/Acceptance Inspection Procedures
DI-T-4904	Production Inspection Reports
DI-R-5189	Maintainability Prediction Data
DI-R-5192A	Maintainability Demonstration Report
DI-R-5318	Maintainability Demonstration Plan
DI-S-6170	Verification, Demonstration and Evaluation Plan
DI-R-7103	Maintainability Program Plan
DI-R-7104	Maintainability Status Report
DI-R-7105	Data Collection, Analysis and Corrective Action System, Reports
DI-R-7106	Maintainability Modelling Report
DI-R-7107	Maintainability Allocations Report
DI-R-7108	Maintainability Predictions Report
DI-R-7109	Maintainability Analysis Report
DI-R-7110	Maintainability Design Criteria Plan
DI-R-7111	Inputs to the Detailed Maintenance Plan and Logistics Support Analysis
DI-R-7112	Maintainability Demonstration Test Plan
DI-R-7113	Report, Maintainability Demonstration
UDI-R-23711	Report, Maintainability Test Procedures

TABLE 12.6-4: <u>SOFTWARE QUALITY ASSURANCE DIDS</u>

DI-R-30510	(USAF) Quality Program Plan
UDI-R-21374A	(Navy-AS) Plan, Quality Assurance Program
DI-R-2174	Software Quality Assurance Plan
DI-MCCR-80010	Software Quality Evaluation Plan
DI-MCCR-8XXXX	Software Quality Program Plan

DID EXAMPLE No. 1

DATA ITEM DESCRIPTION	2	IDENTIFICATION NO(S).	
		AGENCY	NUMBER

1. TITLE

RELIABILITY PREDICTION AND DOCUMENTATION OF SUPPORTING DATA | DoD | DI-R-7095

3. DESCRIPTION/PURPOSE

3.1 This report documents contractor quantitative predictions of end item Reliability. The Reliability Prediction Report is intended as support for feasibility evaluation, comparison of alternative configurations, identification of potential problems, logistics support planning, logistics cost studies, determination of data deficiencies, tradeoff decisions, allocation (apportionment) or requirements, and criteria for reliability growth and demonstration testing.

4. APPROVAL DATE

81 NOV 18

5. OFFICE OF PRIMARY RESPONSIBILITY

AIR-5185

6. DDC REQUIRED

6. APPROVAL LIMITATION

7. APPLICATION/INTERRELATIONSHIP

7.1 The data contained in this Data Item Description (DID) satisfies paragraph 4.9 and Task Section 200 of MIL-STD-756B.

7.2 The data content of this report is consistent with the requirements of MIL-STD-785 for reliability programs.

7.3 This DID is not applicable to the production phase unless its use is warranted under the circumstances, such as design changes or improvement programs.

7.4 DI-R-7094 is normally required as a prerequisite for this DID.

7.5 This DID supersedes DI-R-2117, DI-R-5130, DI-R-5188, DI-R-21134 and DI-R-3535.

8. REFERENCES (Mandatory as cited in block 10)

*MIL-STD-756B
MIL-STD-847
MIL-STD-12

MCSL NUMBER(S)
OMB EXEMPT
*AMSC No. N3125

10. PREPARATION INSTRUCTIONS

10.1 Unless otherwise stated in the solicitation, the effective date of the documents cited in this block shall be that listed in the issue of the DoD Index of Specifications and Standards (DoDISS) and the supplements thereto specified in the solicitation and will form a part of this Data Item Description to the extent defined within.

10.2 General requirements.

10.2.1 Format. The report shall comply with the general requirements of MIL-STD-847. Covers shall be provided for each report having five (5) or more pages and shall be cut to page size. Each report shall include the contract number for which the report is rendered, including task designations, project number, etc. This should be included in a statement "Prepared under Contract No. #####-##-#-#### for the (Name of the Procuring Activity)".

10.2.2 Body of report.

10.2.2.1 Text. The text shall be written in clear and simple language, free of vague terms or those subject to misinterpretation. Unfamiliar words, words having more than one meaning, and unusual technical and trade expressions shall be avoided. Sentences shall be as short and concise as possible. Punctuation should aid in reading and prevent misreading. Well-planned word order requires a minimum of punctuation. All sentences shall be complete in accordance with the rules of grammar.

DD FORM 1664   S/N 0102-LF-019-4000   • GPO 1974-603-610/3274 2-1   PAGE ___1___ OF ___4___ PAGES
0-1617

DI-R-7095

10. PREPARATION INSTRUCTIONS (Continued)

10.2.2.2 Worksheets. Legible, handwritten worksheets may be used in all reports.

10.2.2.3 Abbreviations. Abbreviations shall be in accordance with MIL-STD-12, where applicable. Other abbreviations employed shall be those in common usage and not subject to misinterpretation. The first time an abbreviation is used in text, it shall be spelled out in full followed by the abbreviated form in parenthesis. This rule does not apply to abbreviations used for the first time in forms, tables, or equations.

10.2.2.4 Acronyms. Acronyms used in reports shall be in accordance with Federal and military standards where applicable. Other acronyms used shall be those in common usage and not subject to misinterpretation. The first time an acronym is used in text, it shall be spelled out in full followed by the abbreviated form in parenthesis. This rule does not apply to acronyms used for the first time in forms or tables.

10.2.2.5 Symbols. The only symbols to be used in text are degree ($^{\circ}$) and the "+", "-", and "$\pm$" to express ranges or tolerances. Other symbols may be used in equations and tables. Graphic symbols, when used in figures, shall be in accordance with military standards. (Any symbol formed by a single character should be avoided if practicable, since an error destroys the intended meaning.)

10.2.3 Decimals. Decimals shall be used in text instead of fractions wherever possible.

10.2.4 Reference material. A table of references shall be included in each report that references other material.

10.2.4.1 References. References shall be restricted to documents that are specifically and clearly applicable to the report, and are current and available. Specifications, reports and other documents necessary for proper report interpretation and substantiation, which are not normally availaable to persons outside the report originating location, shall be included with the report either as an appendix or an exhibit and shall be listed as "attached". When only small portions of related documents are applicable for reference purposes, those portions may be exerpted and included as an appendix. Each appendix shall be properly identified on each page and in the table of contents.

10.2.4.2 Abbreviations, acronyms and symbols. A table of abbreviations, acronyms, and symbols shall be included in each report using them. This table shall provide a definition for each abbreviation, acronym, or symbol used in the report.

10.2.5 Production.

10.2.5.1 Page size. The finished page size for all text material shall be 8 1/2 x 11 inches. Sketches, drawings and diagrams included with the text material may exceed the 8 1/2 inch dimension to form foldouts. Worksheets should normally not exceed 11 x 25 1/2 inches.

PAGE 2 OF 4 PAGES

DI-R-7095

10. PREPARATION INSTRUCTIONS (Continued)

10.2.5.2 Volume size. No single volume shall exceed two (2) inches in thickness including additions, revisions, appendices, exhibits and corrections.

10.2.5.3 Binding. Each report may be bound in two volumes. The 8 1/2 x 11 inch text material shall be bound along the left hand margin by means suitable for holding the volume together and for easy removal and insertion of revision pages without special tools. The worksheets shall be bound along the top margin by means suitable for holding the volume together and for easy removal and insertion of revision pages without special tools. Staples, spiral-wire, or multi-loop plastic bindings or similar devices are not acceptable for binding reports.

10.2.5.4 Alternate format. Documentation may be provided in contractor's format if stated in the contract by the acquiring activity.

10.2.6 Revisions. Changes to an item made subsequent to the latest submitted report shall require submittal of new data and reports, or revisions to previously delivered data and reports.

10.2.6.1 Front cover and title page. The front cover and title page shall bear notation "Revision" directly under the originator's report number. The latest revision letter shall be used to identify the issue of the entire report. A revision letter shall not be used on the initial issue.

10.2.6.2 Page revisions. Minor changes in a report normally shall be made by reissuing completely revised pages on which the changes are to be shown. Revised pages shall bear the same page numbers as those pages which are to be replaced, plus the word "Revised" and the date of the revision. Additional pages shall be identified by the previous page number followed by a lower case letter unless the additional pages follow the last page of the report. Pen and ink changes are permissible for minor changes.

10.2.6.3 Complete revisions. Complete revisions shall be prepared when changes to the report are of considerable length in relation to the original content, or when necessary to change the security classification. Revision shall conform to the details outlined herein for reports of original issue, except that the document identifier shall be followed by the revision symbol (see 10.2.6.1 of this DID).

10.3 Detail requirements.

10.3.1 Content. The report shall contain the documented results of the reliability prediction. Applicable failure rates, failure distributions, failure rate adjustment factors, and reliability variables used in the calculation of each subdivision of the end item shall be shown. The report shall identify the source(s) and evaluate the validity of data used in the reliability prediction..

10.3.1.1 Item description. Each item of the block diagram shall have a description of the purpose and function provided.

PAGE 3 OF 4 PAGES

DI-R-7095

10. PREPARATION INSTRUCTIONS (Continued)

10.3.2 Reliability prediction. The reliability prediction of each subdivision of the hardware breakdown structure for each mission, mode of operation, and periods of non-operation and storage from an item's final factory acceptance through its terminal expenditure or removal from inventory shall be included in the report.

10.3.2.1 The type and method of reliability prediction shall be identified in accordance with paragraph 5.1 of MIL-STD-756B.

10.3.2.2 Operating and environmental stress factors and ratios used in determining part failure rates shall be cited in the report and individually identified as Estimated (E), Calculated (C), or Measured (M).

10.3.2.3 Procuring activity approval for failure rate data sources used in the reliability prediction shall be identified.

10.3.4 Data identification. Reliability prediction reports shall document or adequately cross-reference the following data used in performing predictions:

     a. Parts description
     b. Failure rate data and sources
     c. Failure distributions
     d. Assumptions
     e. Constraints
     f. Item Definition
     g. Service use profile
     h. Reliability block diagram
     i. Reliability mathematical model
     j. Environmental data
     k. Stress data

10.3.5 Conclusions and recommendations. Reliability prediction reports shall include contractor conclusions and recommendations based upon the prediction effort. They shall be consistent with the phase of item development and the revision status of the report. The contractor shall provide interpretation and comments relative to the prediction and courses of action to resolve deficiencies or discrepancies identified from the prediction effort. Consideration shall be given to Contractor Furnished Equipment (CFE) and Government Furnished Equipment (GFE) integration problems, tradeoff, risks associated with the prediction, reliability interactions which affect planning, qualitative or quantitative aspects which affect the item development, actions taken or proposed related to the prediction, or other factors related to the prediction process and item reliability.

PAGE 4 OF 4 PAGES

DID EXAMPLE No. 2

DATA ITEM DESCRIPTION	2. IDENTIFICATION NO(S).	
	AGENCY	NUMBER

1. TITLE

Maintainability Program Plan

3. DESCRIPTION/PURPOSE

3.1 This plan describes the contractors maintainability program, how it will be conducted and the controls and monitoring provisions levied on subcontractors and vendors. It describes in detail the specific techniques and tasks to be performed and their integration and development in conjunction with other specified related plans. The principle uses are to provide the contracting activity a basis for review and evaluation of the contractors maintainability program (and its proposed components) and for determining contractual compliance.

7. APPLICATION/INTERRELATIONSHIP

7.1 This DID satisfies the data requirements of Para 101.2 in Task 101 of MIL-STD-470A. This DID is applicable whenever Task 101 "Maintainability Program Plan" of MIL-STD-470A is called out as part of an acquisition program. This DID may be used to satisfy the updating or revision of a previously generated plan.

7.2 This DID supersedes the following DIDs: DI-R-1740; DI-R-2127; DI-R-3533; DI-R-5190; UDI-R-21416A; UDI-R-23558; and UDI-L-25571.

AGENCY	DOD
NUMBER	DI-R-7103

4. APPROVAL DATE

1983 January 3

5. OFFICE OF PRIMARY RESPONSIBILITY

AFSC

6. DDC REQUIRED

8. APPROVAL LIMITATION

9. REFERENCES (Mandatory as cited in block 10)

*MIL-STD-470A

MIL-STD-847

MCSL NUMBER(S)

OMB Exempt

*AMSC No. F3216

10. PREPARATION INSTRUCTIONS

10.1 Unless otherwise stated in the solicitation, the effective date of the document(s) cited in this block shall be that listed in the issue of the DoD Index of Specifications and Standards (DoDISS) and the supplements thereto specified in the solicitation and will form a part of this Data Item Description to the extent defined within.

10.2 The contractor shall prepare a plan of the proposed Maintainability Program. The Maintainability Program Plan shall identify, describe and tie together those Maintainability Program components described in paragraph 101.2 of Task 101 "Maintainability Program Plan" of MIL-STD-470A as tailored to the particular needs of the acquisition program.

10.3 <u>Format.</u> The plan shall be prepared in accordance with MIL-STD-847.

DID EXAMPLE No. 3

DATA ITEM DESCRIPTION	2. IDENTIFICATION NO(S).	
	AGENCY	NUMBER

1. TITLE		
Maintainability Demonstration Test Plan	DOD	DI-R-7112

3. DESCRIPTION/PURPOSE

3.1 To provide the details and procedures for determining end item compliance with respect to specified maintainability requirements.

4. APPROVAL DATE

1983 January 3

5. OFFICE OF PRIMARY RESPONSIBILITY

AFSC

6. DDC REQUIRED

8. APPROVAL LIMITATION

7. APPLICATION/INTERRELATIONSHIP

7.1 This DID in conjunction with DI-R-7113 satisfies the data requirements of para 301.2 in Task 301 of MIL-STD-470A. This report shall be used by the Contracting Activity for determining the adequacy of the Maintainability Demonstration Test Program. It is applicable to the performance of Task 301 of MIL-STD-470A.

7.2 This Data Item Description is used in conjunction with DI-R-7113 (Report, Maintainability Demonstration).

7.3 If the demonstration test is prepared in accordance with the requirements of MIL-STD-471A, DI-R-2129 shall be used in lieu of this report.

7.4 This DID supersedes DI-R-3538; and UDI-R-23564.

9. REFERENCES (Mandatory as cited in block 10)

* MIL-STD-470A

MIL-STD-847

MCSL NUMBER(S)

OMB Exempt
*AMSC F3216

10. PREPARATION INSTRUCTIONS

10.1 Unless otherwise stated in the solicitation, the effective date of the document(s) cited in this block shall be that listed in the issue of the DoD Index of Specifications and Standards (DoDISS) and the supplements thereto specified in the solicitation and will form a part of this Data Item Description to the extent defined within.

10.2 The Maintainability Demonstration Test Plan shall contain all the information necessary to evaluate the demonstration test; procedures to be followed; test selection rationale; test duration; test start date; scenario; and ground rules; as defined in MIL-STD-470A, paragraph 301.2 of Task 301 as tailored for the particular acquisition.

10.3 Format. This plan shall be in accordance with MIL-STD-847.

DD FORM 1664

PAGE ___1___ OF ___1___ PAGES

12.7 R&M PROGRAM REQUIREMENTS BASED UPON THE TYPE OF PROCUREMENT

This section of the handbook discusses basic program requirements within the framework of MIL-STD-785 and MIL-STD-470, which would form R&M programs considered applicable to the procurement of military systems. There are three major categories of procurements that exist to meet a specified need:

o   existing commercial
o   modified commercial
o   military requirements

Commercial procurements provide for the purchase of existing hardware systems in order to obtain a low cost, quick response capability for certain requirements. Advantages of this type of procurement include use of a proven design, reduced leadtimes and minimal development expense. Possible disadvantages associated with commercial procurements include inability to meet R&M requirements, limited performance, parts availability, reduced control of model changes, and increased logistic support requirements.

Commercial procurements seldom require analysis to specify R&M levels. Criticality in terms of mission requirements is normally low and the cost of acquisition may be optimal if the equipment is an off-the-shelf or commercial type item and no new development is required. Procurement of commercial equipment requires effort to select items with "as is" suitability and demonstrated acceptability to meet project needs. Specification efforts should be restricted to describing only those requirements in functional terms necessary to assure hardware acceptability. Design requirements are to be specified only to the extent necessary and essential to satisfy procurement requirements. The description and specification of additional reliability and quality controls should be avoided. Validated commercial tests should not be repeated. Procurement emphasis is in selection, not specification. Among the factors to be considered when selecting commercial products are:

o   identification of one or more established products that appear suitable.
o   analysis of all available data,
o   consideration of industrial standards,
o   reliability, maintainability, service life and spare parts availability.
o   an estimate of the extent to which reliance can be placed on warranties.

Many times a reliability/maintainability report on commercial equipment is provided, and used by the procuring agency to determine minimum R&M levels and to compare information furnished by contractors to aid in the selection of future equipment. The report should provide service and life-test reliability and maintainability data on designated equipment. The information should include such items as the conditions under which the data were generated; the mean/time/cycles between failures; the manhour rate for each corrective maintenance, preventive maintenance, and servicing task or other reliability and maintainability parameters; and the expected service life of the equipment.

Modified commercial procurement provides for use of the basic commercial configuration with modifications to meet certain specifications. Possible advantages to this form of procurement are quicker availability and lower development cost than a new military design item. Possible disadvantages include the loss of integrity of the commercial product, the addition of unproven components, and the compromise of mission capability.

The procurement of systems to meet military requirements present the greatest challenge. Included are two subcategories:

(1) Existing development (production or build-to-print contracts); ECP's which do not significantly impact schedule, require extensive requalification, or involve substantial redesign; a smooth transition to production which involves existing production facilities. In this subcategory, the establishment of R&M levels is aided by the existence of previous demonstration and/or field data, prior R&M estimates, and judgement factors arising from the consideration of these data.

(2) New development which involves a completely new design or changes to major components and major redesign of existing system. New system development is characterized by the establishment of a program office.

The possible advantages of procuring a newly designed item are that the item can fully meet military requirements, that the design and configuration can be government controlled, and that the logistic support can be assured. Possible advantages of procurement of an existing design are the shorter lead times involved, the use of less costly changes to reach required performance objectives and the utilization of existing technology.

In developing the procurement approach the application of a reliability improvement warranty (RIW) should be given consideration as a means for committing the contractor to a specified actual reliability and reducing life cycle costs. The thrust of a warranty is to achieve acceptable reliability through a warranty improvement profit incentive. Warranties are covered in more detail in Section 12.2.6.3, as part of Product Performance Agreement.

New (or modified) military procurements involve many interrelated variables that must be balanced to produce a cost effective system. It is here that the designer must make selective tradeoffs between the R&M levels and projected life cycle cost of the system. R&M and cost tradeoffs are essential in cases where the system is complex and where high availability and long service life are expected.

It should be emphasized that the program requirements for each new procurement must be structured and tailored to coincide with its specific procurement category and meet its specified R&M objectives. Specifying appropriate R&M program tasks involves a number of decisions. The R&M tasks for each procurement must be structured to coincide with the contract type and to meet is specified level of R&M. The R&M tasks

as discussed in Sections 12.3.2 and 12.4.2 generally include: (1) definition and implementation of an effective management and control program; (2) continuous application of systematic and highly disciplined engineering tasks (R&M allocation, prediction, and assessment); (3) performance of demonstration tests; (4) implementation of a production reliability assurance program; (5) establishment of subcontractor R&M control; (6) application of design reviews; and (7) implementation of a closed loop failure reporting analysis, and corrective action program. The scope, extent, and depth of the tasks are governed by the criticality of the equipment, the equipment design configuration, the technical state-of-the-art, the maintenance concept, and the cost limitation. The relationship of the specific MTBF and MTTR to the state-of-the-art and the required R&M improvement attributes provide a basis to determine the scope and rigor of the R&M program tasks and provisions.

The determination of appropriate R&M specification levels as well as program task activities involves reviewing the type of contract in view of the R&M design requirements. The nature of the procurement (for example, commercial, military, etc.) will, to a large extent, dictate the R&M requirements. If the hardware to be procured is an off-the-shelf, commercial product, no reliability prediction or reliability growth and demonstration testing would be included. However, depending upon the design reliability level, acceptance and screening tests may be required. The relationship of the specified R&M levels to the state-of-the-art will also dictate the extent of the R&M program activities. If the specified reliability, for example, is close to the maximum that can be achieved within the state-of-the-art (i.e., if there is little room for reliability improvement) then, possibly, a very vigorous and intensive R&M program would be structured and implemented. The program in that case would then include R&M predictions, FMECA, reliability growth tests, demonstration tests, screening tests, and production acceptance tests to assure compliance to specified requirements with high confidence. However, if the specified value is not stringent and there is ample room for reliability improvement, then the program would not have to be extensive.

Sections 12.3.2, 12.4.2, and 12.5.2, as well as MIL-STD-785 provide guidance and rationale to aid in selecting and scoping R&M tasks and requirements. The results of the Army and FAA programs described in the following paragraphs with accompanying Figures and Tables are also provided as further general guidance, in terms of tailoring R&M requirements to the type of procurement involved.

The Army Aviation Research and Development Command (AVRADCOM) has developed a matrix for aviation systems and components based on MIL-STD-785 and MIL-STD-470 (Reference 17), and, as such, provides further guidance in structuring R&M program requirements. This matrix, given in Figures 12.7-1 through 12.7-4, defines provisions, specifications and controls for programs where the highest possible reliability is essential and strict requirements are imposed on system reliability mission accomplishment and flight safety.

R & M Techniques	Option 1 — Existing Commercial	Option 2 — Modified Commercial	Option 3 — Existing Military	Option 3 — New Development Military
Organization	1) R/M coverage during production	1) R/M coverage during design, development and production.	1) Detailed emphasis on production aspects of R/M – Failure Analysis – Production R Assurance – Data Collection – Reduction & Analysis – Procurement Control	1) Well stated organization covering all aspects of R/M including detailed coverage of – R/M Management – Design Analysis – R/M Analysis – Component Engineering – R/M Test & Demo – Failure Analysis – Production R Assurance – Data Collection, – Reduction & Analysis
Control Tasks	1) Emphasis on internal control elements focusing on flight safety provisions.		1) Full and detailed R/M plan that defines all control elements, key personnel and their responsibilities and interrelationships. 2) Complete list of control tasks including reference procedures for implementation, manhours for each task and person responsible for implementation. 3) Definition of R/M milestones included in schedule. 4) Established methods for providing R/M data and information to design, production, i.e., proven methods for forcing R/M program activities to impact design and production. 5) R/M training program.	
Subcontractor & Supplier P/M Programs	1) Qualify vendor via survey & audit to manufacturers requirements. 2) Approved supplier list maintained & defined on procurement documents. 3) Major component suppliers require certification. 4) Purchase orders for major subcontractor items should require: – R/M planning provisions		1) Qualify vendor via survey & audit to MIL-STD-785. 2) Approved supplier list maintained & defined on procurement documents. 3) Surveillance & source inspection at parts suppliers or major subcontractors (full time residence by Quality part time by Reliability) 4) Purchase orders for major subcontractor items need: – Reliability Program Plan – Closed-Loop Failure Reporting System – Failure Analysis – Reliability Demonstration Test per MIL-STD-781 – Engineering tests as required.	5) Reliability prediction 6) Failure mode & effects analysis.
Program Review	Not performed.	Same as Option 3B governed by internal contractor operating procedures.	Not performed.	1) Formal reliability program reviews for major subcontractor items at end item & item unit levels. Update as needed. 2) As required by procuring activity in program schedule.

MANAGEMENT

FIGURE 12.7-1: PROGRAM MATRIX--MANAGEMENT

R & M Techniques	Option 1 Existing Commercial	Option 2 Modified Commercial	Option 3 A Existing Military	Option 3 B New Development Military
Design Analysis	Not performed.	Not performed.	Not performed.	1) Probabilistic Design-SSI 2) Fatigue Analysis-PSW 3) Mechanical systems analysis using Bayesian failure distributors-CAD 4) Electrical ckt. analysis 5) Design analysis on ckt. 6) Transient & thermal analysis. 7) Monte Carlo analysis
R/M Apportionment & Predict.	Not performed.	1) Math model on functional basis for equip. or replacement unit	Not performed.	1) Preliminary MIL-HDBK-217 2) Update to include design changes as necessary.
Component Reliability	1) Max use of existing specs, test & qual data manufacturing methods & in-process controls. 2) Components of nominal R. Criteria set to reduce probability of devices outside limits.	1) Compile & issue Preferred Parts List. Keep current, minimal test for reduced risk. 2) Components of nominal R. Criteria set to reduce probability of devices outside limits.	1) Preferred Parts List 2) Max use of existing specs, test & qual, etc 3) Review non-standard data. 4) Compile & issue Approved Materials & Process Lists.	1) Parts Control Board - develop part/component list 2) Extensive spec requirements for regulated product 3) Submit non-standard data 4) Compile & issue Approved Materials & Process Lists.
Failure Mode And Effect Analysis	Not performed.	1) FMEA on major parts for catastrophic failure modes.	Not performed.	1) FMEA at end item equip. component, & part levels for significant fail. modes
Reliability Critical Items	Same as Option 3A	Same as Option 3B	1) Review existing list of critical items; revise as necessary.	1) Maintain a reliability critical item list; update monthly.
Effects of Storage, Shelf-Life, Packaging, Transportation Handling & Maintainence	Same as Option 3A	Same as Option 3B	1) Review effects of storage, transportation & handling on all critical parts, units, etc. 2) Establish procedures for reducing reliability degradation for selected critical items.	1) Evaluate environments for storage, transportation & handling of all critical parts, units & end items. 2) Establish formal procedures & instructions for reducing R degradation for selected critical items.
Design Review Data	Not performed.	Not performed.	Not performed.	1) Supply R information for formal review at system, equip. item & component levels. Update per CDRL.

DESIGN EVALUATION

FIGURE 12.7-2: PROGRAM MATRIX--DESIGN EVALUATION

R & M Techniques	Option 1	Option 2	Option 3	
	Existing Commercial	Modified Commercial	A — Existing Military	B — New Development Military
Transition Prod. Development		Defines production reliability test & control plan, verifies performing inspection, in-process testing, & receiving, burn-in & final testing.	Test, critical parameters as defined per engineering procurement documents part activities & critical	1) Same as Options 1 & 2 2) Plan requires government approval
Receiving Inspection			Validates adequate inspection instructions, criteria, test equipment, personnel, etc. to assure high efficiency. Inspection of safety or reliability critical parameters.	
In-Process Testing			Tests critical parameters or dimensions at appropriate points in the assembly process based on derived from engineering documents. Validates adequate procedures, equipment, inspection criteria & personnel to assure high efficiency. Inspection of safety or reliability critical parameters.	
Screening & Burn-in		Not performed.	1) Review existing methods & procedures. Revise or incorporate screens.	1) Tests designed to uncover defects at the major assembly, component system level 2) Operational stress tests to find design weakness, weak parts or workmanship errors. 3) Useful in uncovering time-dependent defects
Final (Acceptance) Testing		Conducted on all systems leaving production. Tests performed to assure proper functioning of elements. Performed per written test procedure.	Same as Options 1 & 2	
Final Cost Product		Provides specific documented coverage of acceptance criteria. Contains detailed check lists for visual, mechanical & electrical tests & inspections. Identifies critical parameters of inspections. Plan requires government approval. Provides detailed methods, defines required test equipment, fixtures & step by step instructions.		
Analysis & Actions		Establish specific mechanisms for collecting & reducing data from factory & test operations. Includes data items of interest, plan usage of data collected. FRACAS, FAMMS for feedback requirements. Includes data formats & other documents for factory data collections.	Same as Options 1 & 2	

FIGURE 12.7-3: PROGRAM MATRIX--PRODUCTION RELIABILITY & DATA COLLECTION

Reliability Techniques	Option 1 Existing Commercial	Option 2 Modified Commercial	Option 3 A Existing Military	Option 3 B New Development Military
Development Testing	Not performed.	1) Environmental tests performed as applicable.	Not performed.	1) Environmental tests per MIL-STD-810, 781, etc. 2) Reliability growth per MIL-STD-781 performed on development units as needed to reach desired level of reliability. 3) Assure spares are available to sustain testing. All spares to be to the same conditioning tests as prime. 4) Special reliability tests on critical equip
Reliability Test Plan	Not performed.	1) Prepare integrated test plan covering "forced defect" testing during fabrication of test units R growth test & reliability demo. 2) Test plan must define failure & success criteria.	Not performed.	1) Same as Option 2 2) Plan must be based on MIL-STD-781, etc. & needs govt. approval
Reliability Demonstration	Not performed.	Not performed.	1) Test per MIL-STD-781 & Applicable Test Level. Assure the spares are available to sustain testing	
Test Records & Reporting	Not performed.	Not performed.	1) Adequate test records including operating item, failure data, test logs & reporting per CDRL.	
Failure Reporting	For all failures which occur during: - Acceptance tests	For all failures which occur during: - Demonstration, production & final acceptance tests.	For all failures which occur during: Demonstration, production & final acceptance tests.	- Demonstration, production & final acceptance tests. - Development tests. - R growth
Analysis	- Analyze and close out all reported failures.			
Corrective Action	- Initiate corrective action and follow-up on all reported failures.			
Failure Summary	- Submit failure report summaries to all cognizant activities.			

FIGURE 12.7-4: PROGRAM MATRIX—TEST/DEMONSTRATION & FAILURE REPORTING

The Federal Aviation Administration (FAA) has developed a similar R&M program matrix applicable to the acquisition of National Airway Systems (NAS) and equipment (Reference 18). The matrix, given in Table 12.7-1, is also based on MIL-STD-785 and MIL-STD-470, and, as such, provides further guidance in structuring R&M programs. It identifies essential R&M program and test requirements relative to basic procurement types for high R&M requirements as well as normal R&M requirements. The high R&M requirements relate to R&M efforts and controls applicable to systems where the highest possible reliability is essential. It applies to procurements where:

o   High reliability is a requirement for minimum unscheduled maintenance downtime, total performance, and safety.

o   System performance is critical, the system has long life requirements, and is the most costly to maintain.

o   Performance of unscheduled maintenance action is difficult, expensive, and "downtime" is highly critical.

o   Specified MTBF and MTTR approximate the state-of-the-art.

For these procurements, full MIL-STD-785 and 470 requirements are specified, including production tests and controls are consistent with a well defined, tightly regulated system.

The normal R&M requirements relate to R&M efforts and controls applicable to systems where performance is not critical, maintenance and replacement can be readily accomplished and downtime is not critical, and specified MTBF and MTTR are well within the R&M state-of-the-art. For these procurements, partial program requirements and controls per MIL-STD-785 and 470 are specified. Manufacturers must apply adequate material and process controls during critical production stages.

Once the R&M program has been structured for a given system, the requirements are incorporated into different sections of the procurement specification. One section is the Requirements Section of the specification where quantitative requirements must be incorporated which reflect minimum acceptable operational demands, definitions of satisfactory performance, and criteria for success or failure by mode, function and degree. Also included are time frames of interest, environmental, and special field conditions, program requirements specifications including reporting requirements, submission dates for special reports required by applicable specifications or referenced documents called out, and date of submission of detailed acceptance test plans for approval.

Another section contains the Quality Assurance Requirements where the test requirements are incorporated, including general test or inspection conditions (or duty cycles), description of item(s) to be accepted under tests if different from the total system, the number and sampling plan for selection of times to be tested, together with the estimated test duration. Also included are success and failure criteria related to

TABLE 12.7-1: R&M PROGRAM AND TEST MATRIX

R&M Program Element/ Contract Type	Development High R&M	Development Normal R&M	Production High R&M	Production Normal R&M	Commercial
(1) Program Plan	o	o	o	o	
(2) Organization	o	o	o	o	
(3) Subcontractor and Supplier Control	o	o	o		
(4) Program Review	o	o	o		
(5) R&M Status Reports	o	o	o	o	
(6) Thermal Design Analysis	o				o
(7) Allocation	o	o			
(8) R Prediction-average Stress	o	o			o
(9) R Prediction-detailed Stress	o				
(10) M Concept	o	o			
(11) M Design Concept	o	o			
(12) Design Trade-offs	o	o			
(13) M Prediction	o	o			
(14) Parts Control	o	o			
(15) Component Derating	o	o	o	o	
(16) Failure Mode Effects & Criticality Anal.	o				
(17) Sneak Circuit Anal.	o		o		
(18) Critical Item Control	o		o		
(19) Production Degradation Analysis & Control	o		o		
(20) Environmental Stress Screening			o	o	
(21) Effects of Storage, Shelf Life, etc.	o		o		o
(22) Design Review (PDR, CDR)	o	o			o
(23) Test Plan	o	o	o	o	o
(24) R Growth	o				
(25) R Demonstration	o	o			
(26) M Demonstration	o				
(27) Production Scrn'g.			o		
(28) Acceptance - Lot				o	o
- 100%			o		
(29) FRACA	o	o	o	o	o
(30) FRACA Summary	o		o		
(31) Assessment			o	o	o

test conditions, the accept/reject criteria of the test plan, and possibly a statement of customer's risk (a measure of the adequacy of the test plan in discriminating between acceptable and unacceptable products).

To expedite the process and to help assure the preparation of complete well disciplined cost effective specifications, procurement activities many times prepare requirements corresponding to various procurement combinations depicted in Figures 12.7-1 through 12.7-4 and Table 12.7-1. These requirements provide an initial basis for formulating the R&M specifications to be incorporated into the sections of the procurement specification. It must be emphasized, however, that preestablished requirements should not be used like a "cookbook". Specific tasks must be selected and specified by incorporating appropriate requirements that are structured to meet the specific needs and constraints of the individual procurement.

The FAA is studying the feasibility of automating the specification development process. The intent is to develop an automatic system specification tool consisting of a printer, CRT, Keyboard and an interface processor. An engineer using the specification tool will then be able to input the generic type of equipment/system he wishes to specify e.g., Navigation, Radar etc. For each generic type of equipment, "key elements" that are peculiar to that specification would be displayed for the engineer's consideration. If the "key element" is deemed important, the CRT display would perhaps show an annotated bibliography of all applicable Military, Industrial and FAA Standards. Next, criteria for determining engineering requirements, such as R&M features and attributes, as well as required analyses and test, based on risk, functional criticality and life cycle cost, would be displayed. Once an engineering decision has been made to incorporate a requirement, the contractual verbage could then be formulated at different levels of hierarchy, commensurate with system needs as determined by the engineer.

12.8 R&M PROGRAM EVALUATION AND SURVEILLANCE

The procuring activity, in addition to preparing R&M requirements that are integrated into system specifications, the statement of work, and other contractual documentation, also evaluates proposals, reviews data items (i.e., R&M program plans, predictions, analyses, etc.) participates in design reviews, prepares R&M responses and, in general, continually evaluates and monitors R&M program outputs throughout development and production. Specifically the contractor's R&M programs are evaluated and monitored to:

o   Determine the effectiveness of specific programs,
o   Rate and compare different programs,
o   Track the implementation of R&M programs by surveying contractor's facilities, participating in design reviews and evaluating test plans, procedures and results.

Essential to effective contractor monitoring is the evaluation of the R&M program plans. The R&M program plans may vary in emphasis and scope, yet when properly weighted and implemented, have the same effect in producing the final R&M levels. The contractor's R&M programs should be dynamic and flexible enough to accomodate change if these actions are indicated.

12-97

The contractor's program plans are first evaluated during source selection by performing a detailed review of the preliminary plans submitted as part of the proposal. This initial evaluation provides a basis for contractor selection. Evaluation continues, after selection, throughout the development and production phases by surveying contractor facilities and monitoring contractor program implementation and modifications thereto.

The evaluation process involves first developing criteria from a review of the contractual requirements, including the specification, the statement of work, the documentation requirements, and other supplemental information to form a detailed program evaluation basis. The evaluation criteria is then applied to determine the adequacy of contractors planned R&M efforts.

The R&M program considerations that are stressed when formulating R&M specifications (as was discussed in Section 12.7) are also used to formulate criteria for evaluating the programs. Such considerations as the establishment of a formally organized program with central management, a documented program plan, clear definition of the relationship of the R&M program to other project functions, and separate accountability for program resources are stressed when formulating specific evaluation criteria. Furthermore, the R&M program should be negotiated together with the overall project contract (rather than after contract execution). The intent is to establish a realistic program that fully delineates the scope and cost of all R&M efforts. The program should also include periodic reviews which provide for revisions of the program plan, if necessary, depending on the results of the reviews. These reviews can be jointly conducted by the procuring activity and the contractor, and serve as a means of implementing the recommendations of the R&M program evaluation effort.

The criteria must stress that the prime contractor maintains control of his own R&M effort as well as that of subcontractor and supplier R&M programs, and determine their effect on reliability of the overall system. Also, that project data is accessible and visible to the procuring activity and its representatives, including independent R&M assessment contractors. In order to provide for the most convenient accessibility, a central file or data center for documentation could be established. Also, one integrated test program (covering development, reliability growth, demonstration and acceptance testing) should be planned instead of separately managed testing programs. This will prevent both duplications and omissions in testing and, also, provide a single test baseline in parallel with a closely interrelated program of reliability assessment. Integrated testing emphasizes the intimate tie-in of the reliability assessment effort with the requirements of the project, and underscores its role as an input to the various project decision points.

An example of some specific criteria that can be used to evaluate bidders during proposal evaluation is presented in Table 12.8-1. Effective proposal evaluation will not only select the most qualified contractor with respect to R&M, but will also establish the course for subsequent R&M management activities during development and production.

TABLE 12.8-1: PROGRAM EVALUATION CRITERIA (CONTRACTOR SELECTION)

Compliance with Requirements

o   R&M parameter values defined in the RFP documents must be met.

o   The intent of applicable specifications and data requirements must be complied with.

o   Demonstration of R&M values must be possible without minimizing performance capability or incurring excessive cost.

Understanding of the Problem

o   Contractor's understanding of the scope or range of tasks that make up the R&M effort must be demonstrated.

o   Understanding of R&M technologies such as: mathematical, statistical modeling, hardware engineering (stress factors), physics of failure, etc., must be demonstrated.

o   Knowledge of advanced, yet proven methods for R&M programs must be shown.

o   Understanding of the interaction between various R&M elements and the system design and development process, including the interface aspects of R&M with development milestones must be shown.

Soundness of Approach

o   Manpower, facilities, and other resources must be adequate to implement the described approach.

o   R&M approach must show sufficient flexiblity to accomodate design changes, program delays, or extension of R&M elements.

o   Contractor must show ability to meet the objectives of the R&M program within the scheduled time period.

o   Suggested extensions or executions proving beneficial should be included in the approach.

Technical Expertise

o   Background or prior experience in R&M and related areas must be shown to convince the procuring activity of capability.

Management

o   Must show how the contractor's R&M management structure for the proposed program functions within the overall corporate and program management. This includes personnel assigned, their technical expertise, management techniques, and lines of communication.

This proposal evaluation can be aided by utilizing the guidelines given in Table 12.8-2 and their associated criteria. These criteria are representative of a well rounded R&M program applicable to a high reliability, full-military-development type of program. The information provided by contractors' proposals relative to these guidelines provides the data base for evaluation. Quantitative evaluation can be performed by assigning weight factors to criteria derived from the guidelines. Contractor proposals for other development options and levels can be evaluated relative to reduced or restricted criteria derived from the guidelines given in Section 12.7.

Several military organizations have developed checklists for evaluating and monitoring R&M programs. Examples of these are provided in Appendices to Section 7. These checklists can be directly applied or at least provide a basis to formulate or tailor more specific criteria to evaluate and monitor R&M development and production programs in general. They should be used in conjunction with Section 12.4.5 which lists the R&M tasks to be performed during each life cycle phase. Included in these checklists are evaluation considerations and monitoring criteria with respect to individual R&M tasks and control elements. It should be noted that in addition to the technical criteria associated with each task, certain aspects associated with management and control are covered. The intent is that each activity is evaluated and monitored with respect to management including their interaction with other activities within the framework of the overall R&M plan, as well as how each task impacts design activities. The guidelines covering overall R&M organization and control stress factors within the areas of organization, methods of control, planning, and reporting activities.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES

---

(1) Reliability (R)Allocation Criteria

o Overall allocation methodology shall be based on criticality, complexity of design and function, operational use environment, previous experience with similar equipment and relation to the state-of-the-art.

o Specific allocations shall be based on conceptual goals and predictions and shall possibly include a further improvement factor which challenges designers; e.g., improvement factor could be 125% of predicted value.

o Allocations shall be made to the component level and provide design goals for components and higher level assembly.

o Allocations shall be completed shortly after the state of the detail design phase; submittal should be well in advance of PDR.

(2) Reliability Prediction Criteria

o Effort shall consist of analytical estimates of system reliability and/or MTBF based on mathematical models, failure rates and stress/environmental factors and underlying statistical distribution of failures.

o Predictions shall include factors for mission profile, duty cycle, operating and nonoperating failure rates and known applicable failure modes and mechanisms.

o Predictions shall establish inherent reliability to aid in design based tradeoff decisions, provide criteria for the starting point of reliability growth testing, and foster elimination of design flaws.

o Predictions shall be performed during design to show the feasibility that the system meets the inherent reliability MTBF resulting from conceptual design tradeoff studies.

o Predictions shall be made using the methods and data base of MIL-HDBK-217 and the nonelectronic notebook (other sources required the approval of the procuring activity).

o Prediction is an iterated process-initially based on gross part counts and subsequently based on detailed stress analyses.

o Scheduling should show predictions as a continuous effort during detail design with predictions updated periodically; submittals correspond to PDR and CDR.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

(3) Failure Mode Analysis Criteria

o   Shall be a part-by-part (and possibly a failure-mode-by-
     failure-mode) analysis to determine the consequences of
     failure on system reliability, mission success, and safety
     which relates parts, components and functions to their failure
     effects.

o   Analysis shall be based on data and nformation from design
     configurations, components engineering and part failure rates
     resulting from prediction studies, relevant historical
     information and earlier analyses.

o   Analysis shall quantitatively determine the probability of
     failure for each mode identified and which allows ranking by
     numerical probability.

o   Results of analysis shall be used to accomplish the following:

     o   provide input to reliability predictions and aid in
          defining corrective action priorities.

     o   identify critical parts, assemblies, parameters, and
          characteristics that can be used as basic criteria for
          production inspection.

     o   establish corrective action criteria in advance of equip-
          ment fabrication without early large scale testing and
          aid in the generation of test plans and procedures.

     o   provide failure-rate-by-mode distributions.

     o   provide basic data for safety analysis and ranking of
          safety critical parts, assemblies and their failure modes
          for design or other corrective action.

o   Analysis shall be updated periodically, based on data from
     failure analysis and other data collection activities.

o   Effort is performed continuously during design iterations;
     submittals correspond to PDR and CDR.

(4) Maintenance Concept Criteria

o   Contractor's plans shall provide definition as to what consti-
     tutes a repair action and the scope of maintenance activities
     planned for execution by organizational, intermediate and
     depot repair personnel. Contractor's approach to periodic or
     scheduled maintenance activities should be included.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

o   Contractor's maintenance concept shall state the scope and
     character of fault isolation and post-repair checkout
     activities including the following:

    o   requirements for AGE needed to support the system at each
        level of repair.

    o   Amount of ground operating time needed to perform
        preflight and post-repair checkouts.

    o   personnel skill level requirements.

o   Plans shall describe the methods and criteria established by
     which the maintenance concept is translated into hardware
     design features.

o   Scheduling shall show the finalization of the maintenance con-
     cept during the early stages of the detail design effort.

o   Definitions of the maintenance concept are submitted and
     finalized at the PDR.

(5) Maintainability (M) Allocation Criteria

o   Contractors' plans shall show how they quantitatively assign
     repair times (or MTTR) to systems, components, and levels of
     assembly corresponding to the repair activities performed at
     the organization, intermediate and depot levels of maintenance
     and which provide goals for designers.

o   Each repair time assigned shall include an improvement factor
     over and above a strict subdivision of system MTTR
     requirements, which forces emphasis and provides goals during
     detail design activites. (Improvement factors could possibly
     be based on a 25% reduction in MTTR).

o   The results of the allocation shall be used to generate $\underline{M}$
     demonstration and test plans, provide design goals and
     indicate marginal areas requiring concentrated effort tc
     improve maintainability.

o   Specific allocations of MTTR shall account for anticipated
     repair frequency based on system and component failure rates.

o   Allocations for maintainability are a one time study which is
     completed shortly after the start of detail design activities;
     submittal should be well in advance of PDR.

(6) Maintainability Prediction Criteria

o   Predictions should provide a quantitative evaluation of the
     design in terms of MTTR, repair rates and other statistical $\underline{M}$
     parameters for each level of repair.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

o   Predictions shall indicate the feasibility of meeting system MTTR objectives and shall provide an assessment of the probability of correct fault indication.

o   Predictions shall be supported by maintenance level diagrams, work factors and other data determined via maintenance analysis.

o   Analysis shall identify areas requiring periodic cleaning, adjustment or replacement.

o   Predictions shall be used to define preventive maintenance intervals, identify time replaceable items and aid in logistics/supply provisioning.

o   Results of predictions shall be submitted corresponding with major review points -- PDR and CDR.

(7) Component Control & Standardization Criteria

o   Contractor component control and standardization effort shall be directed to select, specify and control all critical electrical, mechanical and electromechanical parts; a continuous effort should be applied to minimize numbers and types of parts and components used.

o   The selection process shall include design evaluation, reliability history review, construction analysis, failure mode and effects analysis and cost effectiveness studies as necessary.

o   The control effort should include the development of meaningful procurement specifications which, when completed, reflect a balance between design requirements, QA and reliability needs consistent with apportionment studies and vendor capabilities and which cover:

    o   lot acceptance testing,

    o   QA provisions (including incoming inspection),

    o   qualification testing, if required.

o   Contractor component qualification approach should include detailed and formal submittal of data to support approval requests (data to be either statistical test data or analytical data for components where similarity exists or a combination of these two types). Note: Those components that require formal statistical test data for qualification should be entered under critical item control.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

o   Contractors components control should indicate the maximum allowable (design application) stress levels for each component type.

o   Contractor shall establish vendor control program, audits of vendor processes, associated documentation and needs for source inspection.

o   A continuous component improvement effort should be provided which emphasizes state-of-the-art physics of failure techniques combined with controlled testing programs.

(8) Critical Item Control Criteria

o   Contractor plans shall list initial critical items and include parts, equipment, components, and other items considered critical from any of the following standpoints:

   o   perform critical functions relative to mission success and safety,

   o   are reliability sensitive (from early R studies, apportionments, etc.),

   o   have limited life,

   o   are high cost items,

   o   have long procurement lead time,

   o   require formal statistical qualification testing.

o   Plans shall provide for critical item identification, control, special handling and shall identify critical item characteristics to be inspected or measured during incoming inspection. Methods include MRB (Material Review Board) procedures, traceability of material and periodic audits.

o   Plans shall cover rules for early procurement of critical parts as well as early build-up and reliability growth testing of critical components as deemed necessary. Specific supplier controls or test methods, which indicated how defects are forced out and R growth is achieved, shall be identified.

o   Contractors shall document their efforts for all items identified as critical, and shall code those items considered safety critical. Contractors' efforts shall describe procedures, test, test results, growth status and efforts to reduce the degree of criticality of each item.

o   Documentation for critical items shall be submitted initially prior to PDR and updated quarterly.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

(9) Subcontractor R&M Control Criteria

o   Contractors' plans shall show approaches and methods to control subcontracted material including the imposition of requirements on subcontractors in accordance with MIL-STD-785 and 470.

o   Subcontractor programs shall include:

    o   analytical tasks such as apportionment, prediction, FMECA, FRACA and performed with the same degree of rigor as contractor efforts,

    o   a component control and standardization effort which interrelates with contractor's control program (especially in the areas of commonality of critical component approval, maximum stress criteria and qualification rationale),

    o   growth tests, demonstration tests and qualification tests on selected subcontracted items.

o   Subcontractor's documentation shall include an R&M program plan, a schedule for accomplishing R&M tasks and a list of deliverable documentation.

o   Submittals of subcontractor data and reports shall be timed to fit logically into contractor's development schedule.

(10) Design Review Criteria

o   Reviews shall be performed against a comprehensive checklist and criteria for R&M and provide the means for formal assessment of contractor design effort.

o   Review procedures shall provide for formal reviews (i.e. PDR, CDR, with PA (Procuring Activity) participation) as well as informal reviews conducted internally.

o   Specific checklists shall be prepared for each review and shall cover the items shown below:

Preliminary Design Review (PDR)

    o   Identification of critical components
    o   Program plans
    o   Preliminary test plans
    o   Design progress
    o   R&M allocations and predictions
    o   Maintenance concept
    o   Special studies (e.g., detailed tradeoffs, etc.).
    o   Component derating and thermal guidelines

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

Critical Design Review (CDR)

- o Subsystem and component specifications
- o Test plans and procedures
- o Critical component evaluations
- o Final design configuration
- o Safety features
- o R&M allocations & predictions
- o FMECA
- o Failure data
- o Growth Test Data
- o Production R Assurance
- o Test results

o Review procedures shall contain methods for deficiency follow-up control.

o A detailed checklist and agenda shall be submitted prior to formal review--prior to PDR and CDR.

(11) Reliability Growth Tests Criteria

o Contractor's development test plan for reliability growth testing shall show a vigorous test, fix, retest program which emphasizes comprehensive and detailed failure analysis activity, show relationships between various time factors, growth rates and starting/end points.

o Specific growth test plans shall be formulated as part of the integrated test program and shall show:

- o predicted MTBF,
- o demonstrated MTBF,
- o starting point,
- o growth rate.

o Growth plans shall include the cumulative test time required to grow to the specified MTBF, the number of test units subjected to growth tests and the anticipated test time per unit. In addition:

- o Contractor's growth plans shall indicate realistic time factors which recognize that, in order to grow under a constant level of corrective action, sufficient downtime must be allowed for adequate implementation of corrective action before restarting the growth tests.

- o plans shall include:

  calendar time/month available,
  test time/calendar time,
  description of test cycle (environment on/off time).

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

o   Growth test plan shall be submitted as parts of overall inte-
     grated test plan at CDR.

o   Progress of growth testing shall be tracked, and logs and data
     forms maintained that record number of units on test, test
     time accumulated, failures, corrective actions and level of
     reliability of MTBF achieved during time period.

o   Final Growth test report shall be submitted within 30 days
     after completion of test.

(12) Reliability Demonstration Test Criteria

o   Contractor test plan shall indicate test to be conducted per
     MIL-STD-781.

o   Plan shall indicate reliability level (i.e., MTBF) to be
     demonstrated and the associated confidence level, and shall
     show the relationship between demonstrated MTBF, confidence,
     test time, etc.

o   Plans shall show number of units for test, expected test time,
     calendar time factors, and scheduling of effort.

o   Contractor's plan shall indicate the kinds of data to be
     gathered during the test and relationship to M tests.

o   Contractor shall submit the R demonstration plan 90 days prior
     to testing.

o   Program of demonstration testing shall be tracked and
     logs/data forms maintained that record number of units on
     test, test time accumulated, failures corrective action,
     statistical decision factors and accept/reject critieria.

o   Interim reliability test results should be reported in the R&M
     Status Report.

(13) Maintainability Demonstration Test Criteria

o   Contractor test plans shall indicate test to be conducted per
     MIL-STD-471. Plan should include:

     o   parameters to be demonstrated,

     o   confidence associated with demonstration (i.e., relation-
          ship of the number of failure events (trials) to the
          total potential failure modes from FMEA studies),

     o   number of units (or systems) involved,

     o   repair levels.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

o PA (Procuring Activity) R&M task force representatives shall be involved in the selection of simulated maintenance trails (failures) to be induced into the system.

o M demonstration plan shall specify scheduling of M demonstration effort and duration of effort, and shall indicate data to be recorded during test.

o Plan shall be submitted in time for CDR.

o Progress of demonstration testing shall be tracked and logs/data forms maintained which record number of trials, nature of repair, repair time, statistical decision factors and criteria for success.

o A final report shall be prepared within 30 days after completion of test.

(14) Failure Reporting, Analysis and Corrective Action Criteria

o Contractor's plans shall describe methods for reporting, analysis and corrective action of all failures regardless of their apparent magnitude through a formal "closed loop" failure analysis function.

o Plan shall indicate that activities are to be controlled by a formal written procedure which describes methods, personnel responsiblities, forms, documentation submittals and scheduling of effort. Plans shall indicate specific failure recurrence control procedures and include the following:

   o basic failure analysis approach,
   o failure analysis procedures,
   o depth of analysis,
   o forms and reporting formats,
   o corrective action follow-up procedures.

o Contractor's plans shall indicate the applicability of FRACA activities with regard to all development, qualification, pre-qualification, acceptance, growth, demonstration, critical item and other test activities, and their extension through design, development and production of the system. Plans shall contain sufficient detail to describe the sequence of events which occur upon detection of a failure including methods for failure verification and classification.

o Failure analysis methods shall be described which indicate the physical analysis techniques and controlled testing efforts currently used to determine the causes of failure.

o Plans shall describe corrective measures based on physics of failure techniques to eliminate (or minimize) the failure mechanism. These measures involve (as applicable):

12-109

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

o   resource requirements,

o   logistics requirements,

o   training requirements,

o   overhaul programs,

o   system improvement,

and provide the basis for accurate field assessments of R&M.

o   Plans shall provide specific mechanisms for collecting operational, maintenance and installation data at field sites, depots, disposal areas and during factory test for feedback.

o   Data collection shall consist of detailed procedures, document forms and delineate responsibilities for implementation and shall utilize, where practicable, existing procedures, forms and methods of collection.

(16) Production Reliability Assurance Criteria

o   Contractor's plans shall indicate methods by which he assures that the inherent reliability designed into equipment is not degraded during production. Plans shall describe methods for incoming inspection, inprocess and final (acceptance) testing. Plans shall show effort in the areas of test, fabrication and inspection procedures and methods of handling/storing components, subassemblies and other production items.

o   A statistically derived quality control plan shall be implemented and designed to achieve maximum control at minimum cost, and which includes increased and more comprehensive inspection at all levels of assembly.

o   Plans shall show methods by which stress/screening tests are applied at lower levels of assembly.

o   Reliability shall be continually assessed during production through detailed analysis of production process flow, actual reject rate statistics and estimates of inspection efficiency factors.

o   Scheduling shall show production reliability procedures to be prepared during design with initial submittal at· CDR and updated as required prior to full scale production. Summary reports indicating current production reliability shall be submitted continually during full scale production.

TABLE 12.8-2: R&M PROGRAM EVALUATION GUIDELINES (Cont'd)

(17) R&M Assessment Criteria

o Contractor's plans shall show method to assess achieved relia- bility based on system test or data from actual field use.

o Assessments shall indicate the relationship between predicted R&M values and achieved R&M values.

o Assessments shall be performed during validation, development, production, deployment and disposal phases. Bayesian statistics could be used to combine the results of theoretical considerations, engineering analysis and test results to yield R&M assessments which utilize the widest possible range of available data and information.

o Plan shall show sources of data, data reduction effort and the feedback of these results to the PA via an assessment report.

o Assessments should include all pertinent data, such as analytical results (e.g., predictions), development test data (e.g., R growth), demonstrations, production and field test data.

(18) R&M Organization & Control Criteria

o The organization for R&M shall consist of an identifiable group, separate from design, QC, etc., whose manager has direct access to program management and who reports at the same level as design.

o The R&M organization shall be defined with respect to its own critical R&M functions as well as with respect to allied func- tions (e.g., QC, manufacturing, etc.).

o The names of key people shall be listed.

o The R&M organization shall consist of a team of specialists which include expertise covering all R&M areas (e.g., statis- tics, physics of failure, component engineering, etc.).

o The R&M manager shall possess sign-off authority of design efforts with respect to R&M.

o The overall guiding philosophy of the R&M program shall be defined and the impact on the design effort established (e.g., define fully the tie in with early design results and describe the interaction of all R&M tasks).

o A schedule shall be provided showing all tasks as well as the interaction of each task with other R&M tasks and task time- liness relative to design and other efforts. Programs and hardware milestones shall identify applicable R&M constraints.

TABLE 12.8-2: <u>R&M PROGRAM EVALUATION GUIDELINES (Cont'd)</u>

o   A list of deliverable items and delivery dates shall be provided.

o   Contractor's program plans shall state his intended methods of control (e.g., meetings, PERT, reviews, audits, etc.), and include discussions of policy formulation and information dissemination and status reporting.

o   Plans shall indicate R&D status reporting including format, scheduling and delivery.

REFERENCES

1. Arsenault, J.E., and J.A., Roberts, Reliability and Maintainability of Electronic Systems, Computer Science Press, Potomac, MD, 1980.

2. Tookey, Edward F., and Alberto B. Calvo, "Cost Analyses for Avionics Acquisition," Proc. 1980 Annual Reliability and Maintainability Symposium (San Francisco), 1980.

3. Department of Defense Directive 5000.28, "Design to cost," May 23, 1975.

4. Joint Design-to-Cost Guide, Department of the Army, the Navy, and the Air Force; DARCOM P700-6, NAVMAT P5242, AFLC/AFSCP 800-19; June 1976.

5. Use of Warranties for Defense Avionic Procurements, RADC-TR-73-249 (AD-769399).

6. "Interim Guidelines, Reliability Improvement Warranty (RIW)," Hq USAF DCS/Systems and Logistics (AF/LGP), July 74.

7. Guidelines for Application of Warranties to Air Force Electronics Systems, RADC-TR-76-32, (AD-A023956).

8. Warranty Guarantee Application Guidelines for Air Force Ground Electronic Equipment, RADC-TR-79-287, (AD-A082318).

9. Product Performance Agreement Guide, Joint AFSC/AFLC Publication, Aug. 1980.

10. Coppola, A., and Sukert, A., Reliability and Maintainability Management Manual, RADC-TR-79-200, AD-A073299, July 1979.

11. NAVAIR 01-1A-33, Maintainability Engineering Handbook, Naval Air System Command, July, 1977.

12. NAVAIR 01-1A-31, Reliability and Maintainability Management Handbook, July 1977.

13. ESD-TR-77-225, Software Acquisition Management Guidebook: Software Quality Assurance, Aug. 1977.

14. ASD-TR-78-8, Airborne System Software Acquisition Engineering Guidebook for Quality Assurance, Aug. 1977.

15. AFSCR 74-1, Quality Assurance Program, Nov. 1978.

16. Department of Defense Acquisition Management Systems and Data Requirements Control List (AMSDL), DoD 5000.19-L Vol. II, July 1981.

17. Reliability and Maintainability Planning Guide for Army Avaiation Systems and Components, US Army Aviation Research and Development Command, St Louis MO, 1974.

18. Reliability and Maintainability Planning Notebook, Federal Aviation Administration, Washington DC, 1980.

Concluding Material

1. Subject term (key word) listing

Derating	Quality Assurance
Design tradeoffs	Reliability
Environmental analysis	Repairability
Failure modeling	Serviceability
Failure modes and effects analysis	Sneak circuits
Human engineering	Software reliability
Life cycle cost	Statistical distributions
Maintainability	System engineering

2. Changes from previous issue. Marginal notations are not used in this revision to identify changes with respect to the previous issue due to the extensiveness of the changes.

Custodians: Preparing Activity:

Army - CR   Air Force - 17

Navy - EC   Project RELI-0052

Air Force - 17

Review Activities:

Army - MI, AV

Navy - SH, AS, OS

Air Force - 11, 13, 18, 19, 99

User Activities:

Army - AT, ME, GL

Navy - CG, MC, YD, TD

INSTRUCTIONS: In a continuing effort to make our standardization documents better, the DoD provides this form for use in submitting comments and suggestions for improvements. All users of military standardization documents are invited to provide suggestions. This form may be detached, folded along the lines indicated, taped along the loose edge *(DO NOT STAPLE)*, and mailed. In block 5, be as specific as possible about particular problem areas such as wording which required interpretation, was too rigid, restrictive, loose, ambiguous, or was incompatible, and give proposed wording changes which would alleviate the problems. Enter in block 6 any remarks not related to a specific paragraph of the document. If block 7 is filled out, an acknowledgement will be mailed to you within 30 days to let you know that your comments were received and are being considered.

NOTE: This form may not be used to request copies of documents, nor to request waivers, deviations, or clarification of specification requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

(Fold along this line)

(Fold along this line)

DEPARTMENT OF THE AIR FORCE

RADC/RBE-2
Griffiss AFB NY 13441-5700

NO POSTAGE
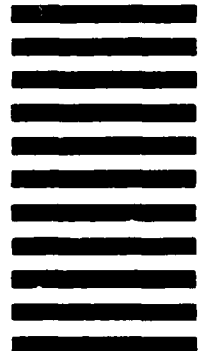NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST CLASS   PERMIT NO. 73236   WASHINGTON D. C.

POSTAGE WILL BE PAID BY THE DEPARTMENT OF THE AIR FORCE

Rome Air Development Center
ATTN: RBE-2
Griffiss AFB NY 13441 -5700

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL
(See Instructions – Reverse Side)

1. DOCUMENT NUMBER	2. DOCUMENT TITLE
MIL-HDBK-338-1A Vol I	Electronic Reliability Design Handbook

3a. NAME OF SUBMITTING ORGANIZATION

4. TYPE OF ORGANIZATION *(Mark one)*

☐ VENDOR

☐ USER

☐ MANUFACTURER

☐ OTHER *(Specify)*: _____

b. ADDRESS *(Street, City, State, ZIP Code)*

5. PROBLEM AREAS

a. Paragraph Number and Wording:

b. Recommended Wording:

c. Reason/Rationale for Recommendation:

6. REMARKS

7a. NAME OF SUBMITTER *(Last, First, MI)* – Optional	b. WORK TELEPHONE NUMBER *(Include Area Code)* – Optional
c. MAILING ADDRESS *(Street, City, State, ZIP Code)* – Optional	8. DATE OF SUBMISSION *(YYMMDD)*

DD FORM 1426 82 MAR ⸱ PREVIOUS EDITION IS OBSOLETE.

(TO DETACH THIS FORM, CUT ALONG THIS LINE.)

END