Vol 5

NASA Contract no. NAS#-25809
Task Order 25
SAICNY93-08-31

Probabilistic Risk Assessment (PRA) of the Space Shuttle Phase 1: Space Shuttle Catastrophic Failure Frequency Final Report Revision 1

Submitted to

US National Aeronautics and Space Administration

Lewis Research Center
21000 Brookpark Road
Cleveland, Ohio 44135

Headquarters Office of Safety
and Mission Quality (Code QS)
Washington, DC 20546

by

Science Applications International Corporation
Advanced Technology Division
8 West 40th Street, Suite 1400
New York, NY 10018
(212) 764-2820 FAX (212) 764-3070

16 August 1993

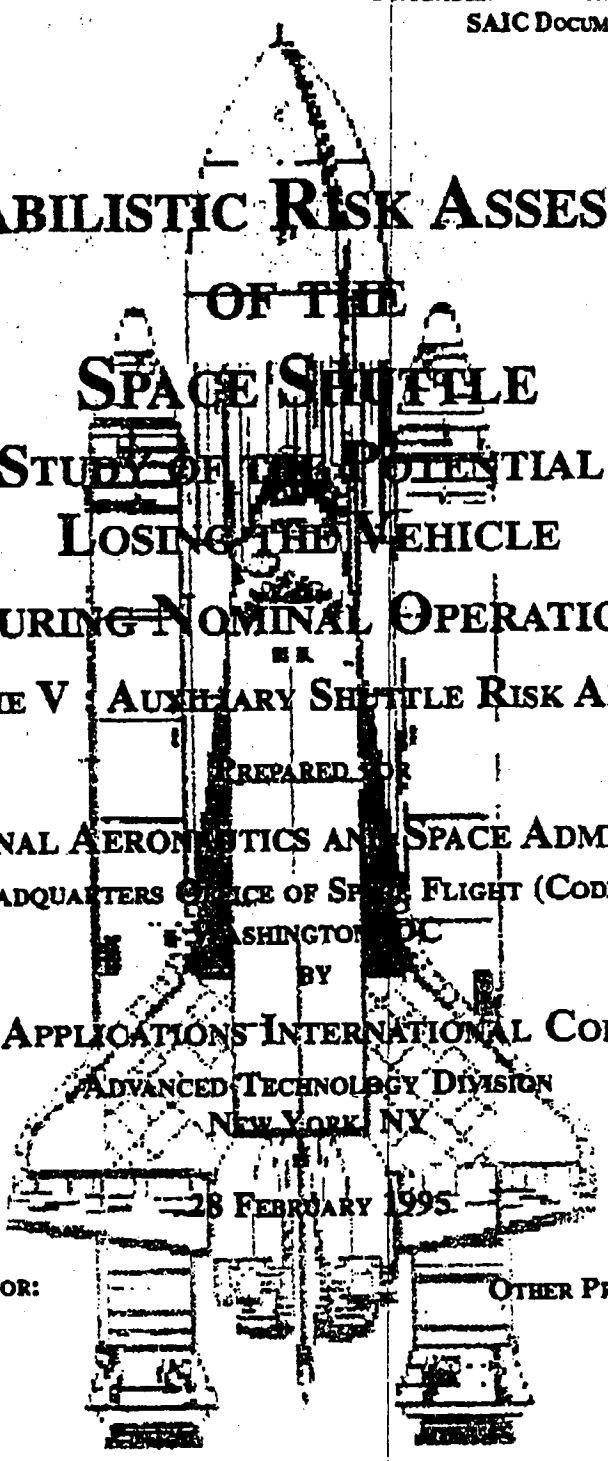
Prepared by
James J. Karns
Senior Staff Scientist

CONTINUATION OF SPACE SHUTTLE
PROBABILISTIC RISK ASSESSMENT, PHASE 3
SAIC DOCUMENT NO. SAICNY95-02-25

PROBABILISTIC RISK ASSESSMENT OF THE SPACE SHUTTLE

A STUDY OF THE POTENTIAL OF LOSING THE VEHICLE DURING NOMINAL OPERATION

VOLUME V : AUXILIARY SHUTTLE RISK ANALYSES



PREPARED FOR

US NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
HEADQUARTERS OFFICE OF SPACE FLIGHT (CODE M)
WASHINGTON DC

BY

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
ADVANCED TECHNOLOGY DIVISION
NEW YORK NY

28 FEBRUARY 1995

PRINCIPAL INVESTIGATOR:
JOSEPH R. FRAGOLA

CHIEF RISK ANALYST:
GASPARE MAGGIO

OTHER PRINCIPAL CONTRIBUTORS:
MICHAEL V. FRANK*
LUIS GEREZ+
RICHARD H. MCFADDEN
ERIN P. COLLINS
JORGE BALLESIO
PETER L. APPIGNANI
JAMES J. KARNS

* SAFETY FACTOR ASSOCIATES, INC.
ENCINITAS, CA
+EMPRESARIOS AGRUPADOS,
MADRID, SPAIN

Science Applications International Corporation
An Employee-Owned Company

Table of Contents:

Executive Summary	1
Introduction	2
Objective	3
Scope	4
Overview of the Analysis	4
Process Overview	4
SRB Sensitivity Cases	6
Results of the Analysis	6
Discussion of the Analysis	12
Solid Rocket Boosters	12
Space Shuttle Main Engines	16
Other Risk Contributors	19
Combining Risk Contributors	19
Mathematical Tools and Methods	21
Conclusion	21

List of Tables:

Table 1:	Risk of Catastrophic Failure for the Space Shuttle, post- STS 56 (April 93)	1
Table 2:	Risk of Catastrophic Failure for the Space Shuttle, STS 34 (October 88) Original *Galileo* Study Results	7
Table 3:	Risk of Catastrophic Failure for the Space Shuttle, STS 34 (October 88) Phase 1 Shuttle PRA -- *Galileo* Era Intermediate Results	8
Table 4:	Risk of Catastrophic Failure for the Space Shuttle, post- STS 56 (April 93) STS PRA Phase 1 Study Results	9
Table 5:	Aggregation of RSRB Surrogates	15
Table 6:	SSME Test Exposure	17

List of Figures:

Figure 1.	Shuttle Failure Frequency Distributions	10
Figure 2.	Risk Element Fractional Contributions to STS Total Risk	11
Figure 3.	Failure Frequency Distributions for the RSRB and Surrogates	16

Appendices:

Appendix A:	Annotated copy of the spreadsheet in which the core calculations are performed
Appendix B:	Bayes Estimators -- Introduction (SAIC Working Notes)
Appendix C:	CARP -- Computerized Aggregation of Reliability Parameters -- User Notes
Appendix D:	Estimating the Exponential Failure Rate from Data with No Failure Events
Appendix E:	A discussion and comparison of Monte Carlo and Latin Hypercube sampling methods
Appendix F:	Text of MSFC Incident Reports for post-*Galileo* Major Incidents
Appendix G:	Example Crystal Ball Simulation Report
Appendix H:	Comments on the differences between the *Galileo* Study Results and *Galileo*-era results in this Study
Appendix I:	Determination of Shuttle Catastrophic Failure Frequency Using No Prior (non-Shuttle) Knowledge of SRB Failure Frequency
Appendix J:	Presentation Viewgraphs

Space Shuttle Catastrophic Failure Frequency

Executive Summary:

This report summarizes the Phase 1 analysis activity of the Space Shuttle Probabilistic Risk Assessment and is submitted in partial fulfillment of the requirements of contract NAS#25809 Task Order 25. The purpose of this analysis is to update the summary results of the 1989 Independent Assesssment of Shuttle Accident Scenario Probabilities for the *Galileo* Mission (the *Galileo* study) [1] to reflect the current (April 1993) test and operational experience base of the Shuttle. It is expected that this analysis will be the first in a series of periodic or event driven updates, to provide a continuously updated benchmark for the catastrophic failure frequency of the Shuttle.

The results of this study are the probability distributions of failure frequency for the Space Shuttle, summmarized in Table 1 below.

Table 1: Risk of Catastrophic Failure for the Space Shuttle, post STS 56 (April 93)

PRA Phase 1 Study results - Based on 484,932 seconds SSME test, 55 flights - 0 SRB failures assumed.						
	5th %	**20th %**	**50th %**	**Mean**	**80th %**	**95th %**
93 RSRB Pair (Base)	1	1	1	1	1	1
(51-L failure not included)	782	388	187	128	90	45
93 SSME Cluster	1	1	1	1	1	1
	1550	741	342	213	153	71
93 ET	1	1	1	1	1	1
	86400	31900	11200	5200	3950	1460
93 Orbiter	1	1	1	1	1	1
	10100	5710	3140	2440	1720	974
93 Prelaunch	1	1	1	1	1	1
	4650	2850	1710	1430	1030	631
93 STS (Base)	**1**	**1**	**1**	**1**	**1**	**1**
(51-L failure not included)	**223**	**146**	**90**	**73**	**54**	**31**
RSRB Sensitivity1 - includes the 51L failure to update the *Galileo* study surrogate prior.						
93 RSRB (Sensitivity1)	1	1	1	1	1	1
(includes 51-L failure)	216	128	74	60	43	25
93 STS (Sensitivity1)	**1**	**1**	**1**	**1**	**1**	**1**
(includes 51-L failure)	**118**	**79**	**52**	**44**	**33**	**21**

This analysis differs from other major analyses of Space Shuttle reliability, notably the on-going analyses of Space Shuttle Main Engines (SSMEs) [2] by F. Safie of Marshall Space Flight Center and Rocketdyne's internal SSME reliability studies [3] in several important respects. First, this is a risk assessment, not a reliability study -- the difference is explored below. Second, the focus is on the Shuttle as a whole, not the SSME. Third, this study is limited to assessing the probability of catastrophic failure of the Shuttle (loss of vehicle, loss of crew). Finally, while this study draws on the test stand experience of the SSME as the best available (non-flight) indicator of SSME in-flight performance, it does not consider test stand experience to be a perfect indicator of in-flight performance, and does not therefore directly combine flight and test experience to determine the probability of SSME failure.

The principal conclusions of this study are: (1) The Space Shuttle is demonstrably one of the most reliable launch vehicles today, and under reasonable assumptions may be considered the most reliable launch vehicle today. (2) The Space Shuttle Main Engine (SSME) test program has had a significant positive impact on the reliability of the Shuttle and has contributed greatly to demonstrating flight reliability and crew safety. (3) The Redesigned Solid Rocket Booster (RSRB) is currently the most significant contributor to the estimated residual risk of catastrophic failure of the Shuttle among the major elements considered in this study (RSRB, SSME, External Tank (ET), Orbiter, and Prelaunch), and will probably continue to dominate the estimated risk in the future since its reliability is demonstrated only through flight successes.

Introduction:

In April 1989 the Safety Division of the Office of the Associate Administrator for Safety, Reliability, Maintainability, and Quality Assurance (Code QS) published the Independent Assessment of Shuttle Accident Scenario Probabilities for the *Galileo* Mission (the *Galileo* study) [1]. The *Galileo* spacecraft carried a radio-isotope thermionic generator (RTG), and the Office of Science and Technology Policy (OSTP) required that an assessment of public risk arising from U.S. space launches involving radioactive materials be performed prior to launch. The *Galileo* study was performed in response to that requirement. One widely distributed result from the *Galileo* study was the set of catastrophic failure frequency distributions for the Space Transportation System (Shuttle).

As part of the Probabilistic Risk Assessment of the Space Shuttle (Shuttle PRA) [5], Office of Safety and Mission Assurance (OSMA), and the Office of Space Flight directed Science Applications International Corporation (SAIC) to update the *Galileo* study results to reflect the current (April 1993) test and operational experience base of the Shuttle. It is expected that this analysis will be the first in a series of periodic or event driven updates, to provide a continuously updated benchmark for the catastrophic failure frequency of the Shuttle.

This study is a risk assessment, meaning primarily that its purpose is to facilitate the making of decisions under risk. In particular this assessment is directed at understanding the risk to the crew and to the payload associated with the use of the Space Shuttle as a launch vehicle. This study does not, in and of itself, make the Shuttle any less "risky" or contribute directly to demonstrating the current level of risk associated with the Shuttle. It does however define, describe, and quantify the risk to the Shuttle and payload while the Shuttle is acting as a launch vehicle. This information is potentially useful in making decisions regarding the future role of the Shuttle, the relative effectiveness of design,

engineering, or operational changes; or to determine what future changes might be required, and whether the current level of risk requires any changes in the risk management strategy.

Decisions are characterized by uncertainty. Uncertainty is generally associated with the subjective elements of a problem: uncertainty in the ability to accurately model a problem, or uncertainty in the applicability of various data to a problem, for example. A basic tenet of risk assessment is that uncertainty in data can be quantified and treated mathematically using the "logic of uncertainty." The quantification of an uncertain decision element (datum) is accomplished by expressing the datum as a probability distribution. Distributions are also used to model variability -- the physically measurable differences between elements in a population of items or events. A "pure" or classical reliability study deals only in variability. Subjective uncertainty is dealt with in a reliability study by establishing ground rules or making assumptions which remove uncertainty from the modeled problem -- the uncertainty is still there, but it is removed from the scope of the analysis. Another approach which can be employed by the reliability analyst to account for uncertainty is the use of conservatism. Adopting a more "conservative" approach reflects that a more negative outcome is postulated than that which might be verified by additional data or modeling. In either case, it is incumbent upon the decision maker to understand and assess the uncertainty implicit in the ground rules and assumptions of a classical reliability analysis before applying the results of that analysis in decision making.

.Probability theory [8] permits the combination of the uncertainty and variability distributions associated with a given parameter. Variability in classical reliability analysis is generally expressed using confidence intervals -- a measure of the likelihood (confidence) that the specified interval will contain the actual mean value of a quantity subject to variability . Another aspect of uncertainty is tolerance -- a measure of the applicability of the parameter to the specific problem (e.g., hardware configuration, application) at hand. Risk analysis uses analogous "uncertainty intervals" to express the distribution, which combines both the tolerance of the estimate and the variability in the quantity. The expression "confidence interval" is reserved to apply only to variability.

This report contains a brief overview of the objective of this study and the analysis methods employed, followed by a summary of the results of the analysis. The analysis process is then defined in depth, including sufficient discussion of the data, assumptions, statistical methods, and tools used to allow audit or replication and extension of this analysis as new data are generated.

Objective:

The objective of this analysis is to produce an up-to-date set of probability distributions for the launch and ascent phase catastrophic failure frequency of the Shuttle. These distributions will be generated by updating the original data used in the 1988 *Galileo* study, and will preserve the assumptions used in the *Galileo* study.

This risk assessment is intended to provide the decision maker with realistic estimates for the current probability of catastrophic failure (failure involving loss of vehicle and loss of crew) of the Space Shuttle. The application of the logic of uncertainty [8] and in particular Bayes' Theorem in this study permits the incorporation of relevant engineering information which could not be included in a classical reliability study. The inclusion of this information produces results that, in our opinion, are a more accurate reflection of the engineering realities of the Space Shuttle than a classical reliability study, which must rely on relatively sparse data. Finally, by explicitly quantifying uncertainty in critical assumptions and ground rules, it provides support for defensible judgments and decisions under uncertainty. (Even if the decision maker disagrees with a particular assumption or ground rule, the

quantification of uncertainty provides some basis for understanding the impact of the assumption on the quantitative results of the study.)

Scope:

This study is intended to provide high-level insight into the current general catastrophic failure probability of the Shuttle. For this reason, the focus of this study is not on particular failure scenarios or mission phases, but on the major functional elements of the Shuttle. Moreover, this study is meant to update results from the earlier *Galileo* study, not to be an independent assessment of the risk. The underlying assumptions of the Galileo study, and the data used in that study, are not re-examined here. It should be noted that the *Galileo* study has several limitations which are not addressed in this analysis: because it was intended to serve only as an input to the assessment of the nuclear safety of the *Galileo* mission, it dealt exclusively with catastrophic failures during pre-launch, launch, and ascent phases of flight. It considered neither mission abort situations nor the on-orbit, reentry, and landing phases of the flight.

Overview of the Analysis:

Process Overview:

> *"I have but one lamp by which my feet are guided, and that is the lamp of experience; I know of no way of judging the future but by the past."*
> Patrick Henry
> Speech in the Virginia Convention; March 23, 1775

A broad introduction to the data and processes used to obtain the failure frequency distributions is provided in this section. This information is presented in greater detail later in this report, and in reference 1, the *Galileo* study final report. The approach used to determine the overall risk of catastrophic failure of the Shuttle in the 1988 *Galileo* study was to analyze the system in terms of its principal risk contributors, determine the distribution of failure frequencies associated with each of the risk contributors, and combine those distributions to determine the overall catastrophic failure frequency distribution associated with the Shuttle.

This assessment is based on historical data. If it were based solely on historical data without any other considerations it would indicate how the Shuttle has performed in the past, but, since the Shuttle has experienced numerous design and operational changes since its first flight, it would not indicate how the Shuttle is expected to perform today and in the future. Moreover, the amount of historical catastrophic failure information directly pertinent to the Shuttle is (thankfully) sparse. To make a realistic estimate of the current catastrophic failure probability, this analysis must therefore deal with two limitations in the available data. It must somehow modify or filter the data to reflect the operational and design changes in the system (incorporate reliability growth); and it must supplement the sparse data with relevant information from other sources. In general, reliability growth can be accommodated in one of two ways. The approach used here is to segregate (filter) the underlying failure data into sets containing those failures which would occur on the current Shuttle and those which would not. An alternative approach is to modify the analysis model to reflect growth (e.g.: to weight the failure occurences based upon their currency).

The principal risk contributors (risk elements) in the Shuttle are the Solid Rocket Booster (SRB) pair, the Space Shuttle Main Engine (SSME) cluster, the External Tank (ET), the Orbiter, and Prelaunch

activities. In this analysis SSME start-up failures are included as part of the SSME cluster risk element, rather than as part of the Prelaunch risk element. The SRB pair and SSME cluster contribute on the order of 90% of the total risk.

To derive failure frequency distributions for each of the risk contributors, a prior distribution of failure frequencies is found based on the performance of surrogate components or systems. Bayes' theorem is then used to update that prior information with the operational flight performance of the element. As applied here, a prior distribution refers to the best available indicator of in-flight reliability performance of the risk contributor, short of the actual in-flight experience. The term surrogate means a system or component sufficiently like the reference system or component in form, function, application, and environment that the failure frequency of the surrogate is a reasonable indicator of the failure frequency for the reference system.

The Bayesian update process used in these studies has the general property of reducing the range of uncertainty associated with a failure frequency distribution, relative to classical statistical methods. This method is employed based on the belief that there are data available -- other than direct flight experience of the Shuttle -- which allows us to determine the catastrophic failure frequency of the Shuttle with greater certainty than flight experience alone would allow. For example, we believe that SSME test stand experience provides useful information regarding the catastrophic failure potential of the SSME. At the same time, we do not think that test stand experience is a perfect indicator of in-flight SSME performance, so it would be inappropriate to pool test performance directly with operational experience. Bayes' theorem allows us to supplement the relatively scant flight experience of the Shuttle by building on the infrastructure of confidence established by test experience. The objective is to find a prior distribution that is ***the best available indicator of in-flight performance***, and combine that prior knowledge with actual flight experience to produce a result in which we are more certain than would have been possible using flight experience alone.

The prior probability distributions for each of the Shuttle risk-contributor elements were selected to be the best available indicators of Shuttle in-flight performance (other than actual Shuttle flight experience). The prior distribution for the SRB was obtained by aggregating the performance of U.S. solid rocket systems. For the SSME, the prior distribution was obtained by examining SSME test stand performance. The prior for the Orbiter was obtained by combining Auxiliary Power Unit (APU) information from the Shuttle Probabilistic Risk Assessment Proof of Concept Study [6] with generic component information for other, non-propulsion, Orbiter systems. For the Prelaunch prior, generic component information was used as surrogate data for the failure modes which would contribute to a pad fire or explosion in Launch Support Equipment (LSE), or inadvertent destruction of the Shuttle by Range Safety Equipment (RSE).

The prior failure frequency distributions are combined with the actual flight experience of the Shuttle using Bayes' theorem to produce "Bayesian Posterior" distributions. Because it combines significant failure-related information about the system (in the prior distributions) with flight experience, the Bayesian posterior generally provides a more useful and accurate indicator of the actual failure frequency performance of the system than a distribution derived from flight experience alone. In the summary charts throughout this report, the distributions reported are Bayesian posterior distributions. A rigorous treatment of Bayes' Theorem is provided in Appendix B and Appendix C.

Note that Bayesian updates were only performed for the SRB and SSME in the 1988 *Galileo* study. The objective of this study was to update the results of the *Galileo* study to reflect current operational

experience, so a Bayesian update using the operational experience (no failures in fifty five flights) was performed for the Orbiter, ET, and Prelaunch risk elements. This constitutes a minor change to the ground rule preserving the method of the original *Galileo* study. Since the failure frequencies for the Orbiter, ET, and Prelaunch risk elements are small, the Bayesian update resulted in little change to the prior distribution, and had essentially no effect on the system level failure frequency.

The Bayesian posterior distributions for two individual SRBs and three individual SSMEs were combined using a Monte-Carlo simulation to determine the failure frequency distribution for the SRB pair and SSME three engine cluster. These distributions were then combined (again using simulation) with the Orbiter, ET, and Prelaunch distributions to produce the STS system level failure frequency distribution. It should be noted for completeness that while the *Galileo* study contractor did use Monte-Carlo sampling in their simulations, the current study used the Latin-Hypercube sampling method, which provides somewhat more accurate results in the tails of distributions. A discussion and comparison of Monte Carlo and Latin Hypercube sampling methods is provided in Appendix E.

This study makes extensive use of the lognormal distribution to express the uncertain quantity "failure frequency." Risk analysts have found the lognormal distribution well suited to conveying uncertainty in failure frequency distributions in a wide spectrum of applications.

SRB Sensitivity Cases

The only in-flight catastrophic failure experienced by the Shuttle was the STS 51-L (*Challenger*) SRB failure. The prevailing belief at the time of the *Galileo* study and today is that the failure mode which caused that accident was removed in the Redesigned Solid Rocket Booster (RSRB). At NASA's direction, the base case therefore did not include the *Challenger* SRB failure in the calculation of SRB failure frequency. To determine how inclusion of that failure would effect the system level outcome, a sensitivity case was added. This case is labeled Sensitivity 1.

At the time of the *Galileo* study there was insufficient SRB test or operational experience to derive a practical and meaningful failure frequency distribution based on SRB experience alone. Based on the experience of one failure in fifty SRB launches, classical statistical methods yield a mean SRB failure frequency of 1/50, and ninety percent certainty bounds of 1/11 and 1/975. The knowledge that we are ninety-percent-confident that the SRB failure frequency is between (essentially) one in ten and one in one thousand may be statistically meaningful, but is of little practical engineering value.

The SRB prior distribution was therefore (necessarily) derived from solid rocket sources not directly related to the SRB. Given the increased experience now available, it is appropriate to question whether such a prior is still *"the best available indicator of in-flight performance."* To determine the extent to which the SRB prior impacts the Shuttle system-level failure frequency distributions, two additional sensitivity cases were analyzed without using the solid rocket prior. The Sensitivity 2 case retains the STS 51-L failure as a valid member of the RSRB reliability data set, and a RSRB failure frequency distribution is calculated based on one failure in 110 SRB / RSRB flights. The Sensitivity 3 case discounts the STS 51-L failure as having been fully corrected, and the RSRB failure frequency distribution is calculated by assuming one-third of a failure in 109 (counted) SRB / RSRB flights. Note: justification for the use of one-third of a failure is discussed more fully in Appendix D.

Results of the Analysis:

Table 2 below shows the distributions derived directly from the published *Galileo* study results. Table 3 shows the *Galileo*-era intermediate results of this study. Table 4 depicts the April 1993 updated

results. The *Galileo*-era results in Table 3 were produced and presented because minor differences in the tools and statistical methods employed in the earlier study relative to this one resulted in slightly different results, particularly in the tails of the distributions. These differences and the reasons for them are discussed in detail in Appendices A and H. The differences between the original *Galileo* study results and the *Galileo*-era results of this study, shown in Tables 2 and 3 are process-oriented. Both studies used the same data and underlying assumptions. The difference between the *Galileo*-era results in Table 3 and the April 93 results in Table 4 are due entirely to the experience acquired since the *Galileo* mission.

Table 2: Risk of Catastrophic Failure for the Space Shuttle, STS 34 (October 88)
Original *Galileo* Study Results

Galileo Study results - Based on 294,230 seconds SSME test, 31 flights - 0 SRB failures assumed.						
	5th %	**20th %**	**50th %**	**Mean**	**80th %**	**95th %**
88 SRB Pair (Base)	7.69E-04	1.60E-03	3.60E-03	5.49E-03	8.06E-03	1.72E-02
(51-L failure not included)	1	1	1	1	1	1
(1 out of ...)	1300	624	278	182	124	58
88 SSME Cluster	8.33E-04	2.18E-03	5.85E-03	1.09E-02	1.56E-02	3.85E-02
	1	1	1	1	1	1
(1 out of ...)	1200	458	171	92	64	26
88 ET	1.25E-05	3.45E-05	1.00E-04	2.00E-04	2.86E-04	7.69E-04
	1	1	1	1	1	1
(1 out of ...)	80000	29000	10000	5000	3500	1300
88 Orbiter	1.09E-04	1.89E-04	3.45E-04	4.17E-04	6.25E-04	1.11E-03
	1	1	1	1	1	1
(1 out of ...)	9200	5300	2900	2400	1600	900
88 Prelaunch	2.94E-04	3.85E-04	5.26E-04	7.14E-04	7.69E-04	1.43E-03
	1	1	1	1	1	1
(1 out of ...)	3400	2600	1900	1400	1300	700
88 STS (Base)	**2.86E-03**	**5.95E-03**	**1.28E-02**	**1.82E-02**	**2.78E-02**	**5.56E-02**
(51-L failure not included)	1	1	1	1	1	1
(1 out of ...)	350	168	78	55	36	18
88 Reliability (Base)	**0.997**	**0.994**	**0.987**	**0.982**	**0.973**	**0.946**
Galileo Study Sensitivity Case 1 - Based on 294,230 seconds SSME test, 31 flights - 1 SRB failure						
88 SRB Pair (Sensitivity1)	1.80E-03	3.98E-03	9.17E-03	1.54E-02	2.08E-02	4.55E-02
(includes 51-L)	1	1	1	1	1	1
(1 out of ...)	555	251	109	65	48	22
88 STS (Sensitivity1))	**4.95E-03**	**9.80E-03**	**2.00E-02**	**2.78E-02**	**4.17E-02**	**7.69E-02**
(includes 51-L)						
(1 out of ...)	1	1	1	1	1	1
	202	102	50	36	24	13
88 Reliability (Sensitivity 1)	**0.995**	**0.990**	**0.980**	**0.973**	**0.959**	**0.926**

Tables 2, 3, and 4 show the failure frequencies associated with each of the risk contributors at the fifth, twentieth, fiftieth (median), eightieth, and ninety-fifth percentiles, as well as the means of the failure frequency distributions. Also shown for each risk contributor are the mean flights between failure (mfbf) associated with the failure frequency. At the system level the reliability associated with the failure frequency is also listed.

As they are used here, the percentile rankings should be interpreted as follows: "We are 95% certain that the actual {failure frequency / reliability} is better than the value shown in the '95th%' column."; or "We are 60% certain that the actual {failure frequency / reliability} falls between the '20th%' and '80th%' values."; and so on. The mean and the median ('50th%') are both widely used indicators of the central tendencies of these distributions. They are not equal because these distributions are skewed -- for the failure frequencies, the distributions are lognormal or nearly lognormal, meaning that the logarithms of the failure frequencies are normally distributed. Historically, the median of the *Galileo* study distributions has been used as the "point estimate of choice" when referring to these results using a single value.

Table 3: Risk of Catastrophic Failure for the Space Shuttle, STS 34 (October 88)
Phase 1 Shuttle PRA -- *Galileo* era Intermediate Results

Galileo era (Intermediate) results - Based on 294,230 seconds SSME test, 31 flights - 0 SRB failures assumed.
(ET, Orbiter, and Prelaunch distributions are the same as Table 1)

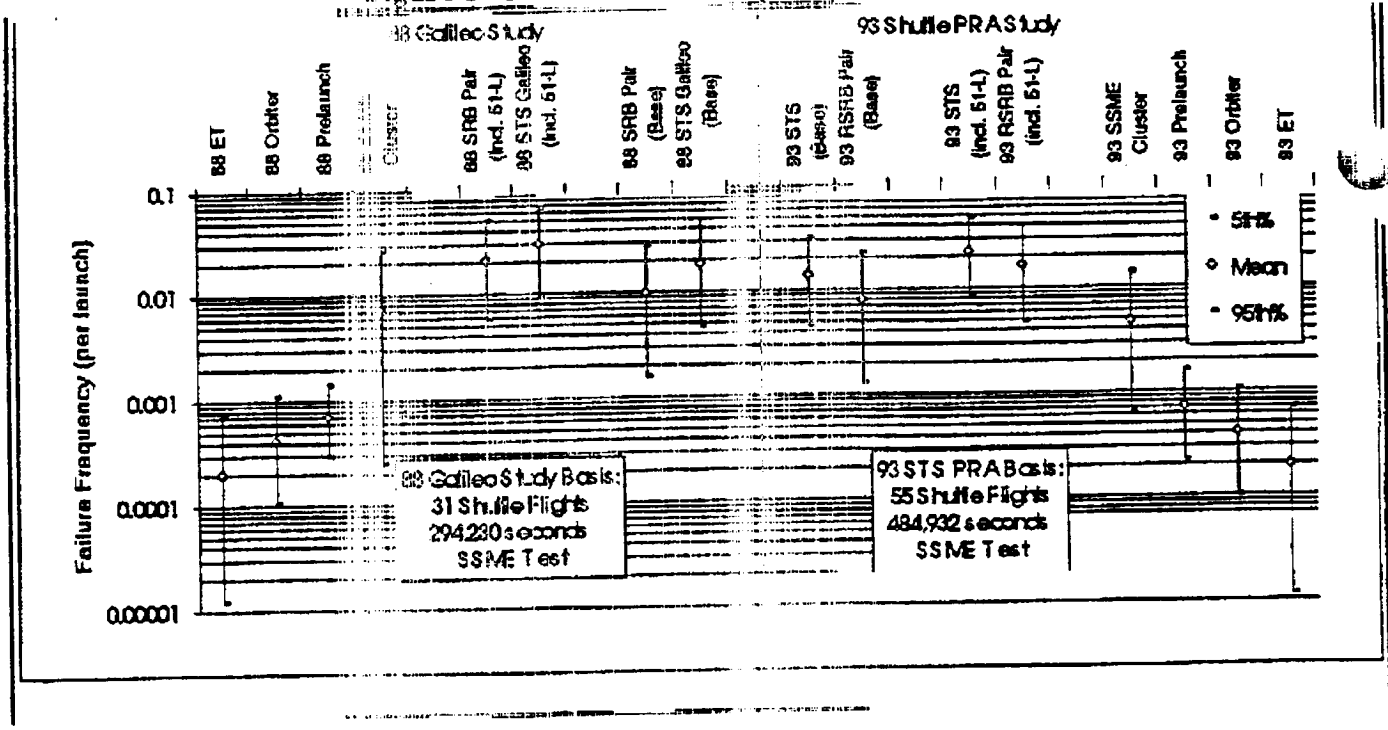
	5th %	20th %	50th %	Mean	80th %	95th %
88 SRB Pair (PRA Base)	1.56E-03	3.28E-03	6.81E-03	9.90E-03	1.41E-02	2.83E-02
(51-L failure not included)	1	1	1	1	1	1
(1 out of ...)	642	305	147	101	71	35
88 SSME Cluster (PRA)	2.49E-04	9.45E-04	2.84E-03	7.38E-03	8.35E-03	2.66E-02
(1 out of ...)	4020	1060	352	136	120	38
88 ET	1.25E-05	3.45E-05	1.00E-04	2.00E-04	2.86E-04	7.69E-04
(1 out of ...)	80000	29000	10000	5000	3500	1300
88 Orbiter	1.09E-04	1.89E-04	3.45E-04	4.17E-04	6.25E-04	1.11E-03
(1 out of ...)	9200	5300	2900	2400	1600	900
88 Prelaunch	2.94E-04	3.85E-04	5.26E-04	7.14E-04	7.69E-04	1.43E-03
(1 out of ...)	3400	2600	1900	1400	1300	700
88 STS (PRA Base)	**4.59E-03**	**7.70E-03**	**1.36E-02**	**1.86E-02**	**2.49E-02**	**4.86E-02**
(51-L failure not included)	1	1	1	1	1	1
(1 out of ...)	**218**	**130**	**74**	**54**	**40**	**21**
88 Reliability (PRA Base)	**0.995**	**0.992**	**0.987**	**0.982**	**0.975**	**0.953**
Sensitivity Case 1 - Based on 294,230 seconds SSME test, 31 flights - 1 SRB failure						
88 SRB Pair (PRA Sensitivity)	5.88E-03	9.92E-03	1.71E-02	2.11E-02	2.96E-02	4.98E-02
(includes 51-L failure)	1	1	1	1	1	1
(1 out of ...)	170	101	58	47	34	21
88 STS (PRA Sensitivity)	**9.70E-03**	**1.51E-02**	**2.43E-02**	**2.98E-02**	**4.01E-02**	**6.68E-02**
(includes 51-L failure)	1	1	1	1	1	1
(1 out of ...)	**103**	**66**	**41**	**34**	**25**	**15**
88 Reliability (PRA Sensitivity)	**0.990**	**0.985**	**0.976**	**0.971**	**0.961**	**0.935**

Table 4: Risk of Catastrophic Failure for the Space Shuttle, post- STS 56 (April 93)
STS PRA Phase 1 Study Results

PRA Phase 1 Study results - Based on 484,932 seconds SSME test, 55 flights - 0 SRB failures assumed						
	5th %	**20th %**	**50th %**	**Mean**	**80th %**	**95th %**
93 RSRB Pair (Base)	1.28E-03	2.58E-03	5.35E-03	7.80E-03	1.11E-02	2.23E-02
(51-L failure not included)	1	1	1	1	1	1
(1 out of ...)	782	388	187	128	90	45
93 SSME Cluster	6.46E-04	1.35E-03	2.92E-03	4.69E-03	6.53E-03	1.41E-02
	1	1	1	1	1	1
(1 out of ...)	1550	741	342	213	153	71
93 ET	1.16E-05	3.14E-05	8.91E-05	1.92E-04	2.53E-04	6.85E-04
	1	1	1	1	1	1
(1 out of ...)	86400	31900	11200	5200	3950	1460
93 Orbiter	9.89E-05	1.75E-04	3.19E-04	4.10E-04	5.80E-04	1.03E-03
	1	1	1	1	1	1
(1 out of ...)	10100	5710	3140	2440	1720	974
93 Prelaunch	2.15E-04	3.50E-04	5.84E-04	7.02E-04	9.73E-04	1.58E-03
	1	1	1	1	1	1
(1 out of ...)	4650	2850	1710	1430	1030	631
93 STS (Base)	**4.48E-03**	**6.83E-03**	**1.11E-02**	**1.38E-02**	**1.86E-02**	**3.20E-02**
(51-L failure not included)	**1**	**1**	**1**	**1**	**1**	**1**
(1 out of ...)	**223**	**146**	**90**	**73**	**54**	**31**
93 Reliability	**0.996**	**0.993**	**0.989**	**0.986**	**0.982**	**0.969**
RSRB Sensitivity1 - includes the 51L failure to update the *Galileo* study surrogate prior.						
93 RSRB Pair (Sensitivity1)	4.63E-03	7.80E-03	1.35E-02	1.66E-02	2.33E-02	3.92E-02
(includes 51-L failure)	1	1	1	1	1	1
(1 out of ...)	216	128	74	60	43	25
93 STS (Sensitivity1)	**8.48E-03**	**1.27E-02**	**1.94E-02**	**2.26E-02**	**3.04E-02**	**4.77E-02**
(includes 51-L failure)	**1**	**1**	**1**	**1**	**1**	**1**
(1 out of ...)	**118**	**79**	**52**	**44**	**33**	**21**
93 Reliability (Sensitivity 1)	**0.992**	**0.987**	**0.981**	**0.978**	**0.970**	**0.953**
RSRB Sensitivity2 - No prior, 1 failure in 110 SRB launches						
93 RSRB Pair (Sensitivity2)	3.14E-04	1.18E-03	4.70E-03	1.82E-02	1.88E-02	7.03E-02
	1	1	1	1	1	1
(1 out of ...)	3180	850	213	55	53	14
93 STS (Sensitivity2)	**3.31E-03**	**5.67E-03**	**1.12E-02**	**2.42E-02**	**2.67E-02**	**7.72E-02**
	1	**1**	**1**	**1**	**1**	**1**
(1 out of ...)	**302**	**176**	**89**	**41**	**37**	**13**
93 Reliability (Sensitivity2)	**0.997**	**0.994**	**0.989**	**0.976**	**0.974**	**0.926**
RSRB Sensitivity3 - No prior, 0 failures in 109 SRB Launches						
93 RSRB Pair (Sensitivity3)	1.06E-04	3.95E-04	1.58E-03	6.11E-03	6.31E-03	2.36E-02
	1	1	1	1	1	1
(1 out of ...)	9480	2530	633	164	159	42
93 STS (Sensitivity3)	**2.54E-03**	**4.11E-03**	**7.44E-03**	**1.21E-02**	**1.48E-02**	**3.38E-02**
(1 out of ...)	**1**	**1**	**1**	**1**	**1**	**1**
	394	**243**	**134**	**83**	**68**	**30**
93 Reliability (Sensitivity3)	**0.997**	**0.996**	**0.993**	**0.988**	**0.985**	**0.967**

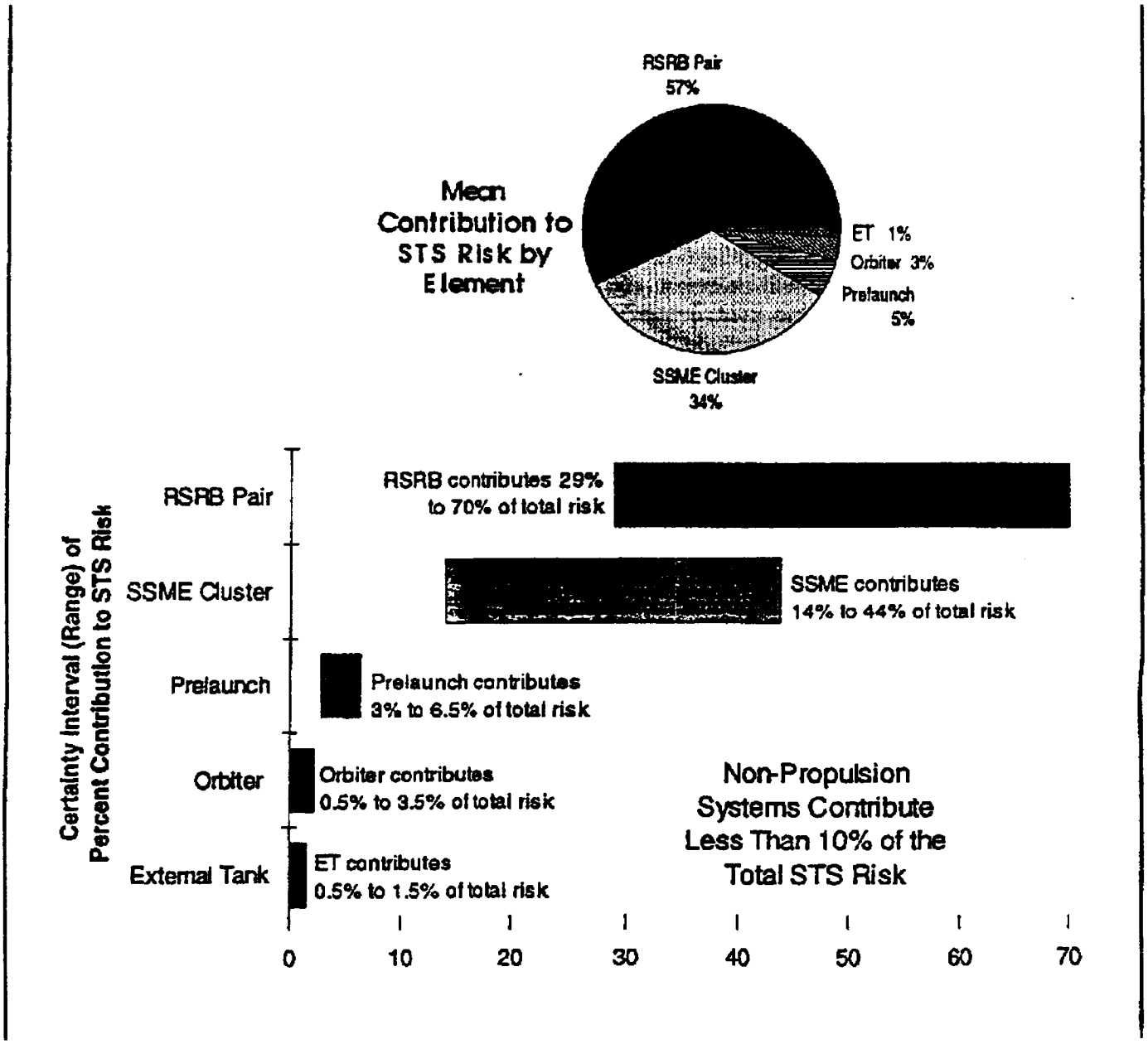
This analysis concludes that, with ninety percent certainty, the current risk of a catastrophic failure leading to loss of a Shuttle during the Prelaunch, Launch, and Ascent phases of a mission is between one-in-thirty-one (1/31) and one-in-two-hundred-twenty-three (1/223), with a mean risk of one-in-seventy-three (1/73), and a median of one-in-ninety (1/90). This is an improvement in estimated mean flights between failure of 30% at the mean and 72% at the worst-case end of the certainty interval (95th percentile) over the computed risk for STS-34, the *Galileo* mission. (In terms of estimated failure frequency, this is an improvement of 23% at the mean, and 41% at the 95th percentile). The principal source of this improvement is increased confidence in the SSME. The SSME data gathered since the *Galileo* study includes: 1 failure in 190,701 seconds of test operation (the equivalent of 122 Shuttle flights); 473 test starts (equivalent to 157 launch starts); and 24 Shuttle flights. This means that the SSME has been accumulating statistically relevant experience at the rate of 4 or 5 equivalent flights per mission. This "experience multiplier" has the effect of improving confidence in the reliability of the SSME much more quickly than if the SSME were exposed to failure only during actual launches. In contrast, the RSRB is only exposed to failure during a Shuttle launch, so the confidence in its reliability performance builds relatively slowly.

Figure 1. Shuttle Failure Frequency Distributions



The Orbiter, ET, and Prelaunch risk contributions remain insignificant compared to the SSME cluster and RSRB pair. Currently, the RSRBs account for between 29% and 70% of the overall risk to the Shuttle (57% at the mean). The SSMEs contribute between 14% and 44% (34% at the mean), Prelaunch contributes about 5%, the Orbiter 3% and the External Tank 1%. The non-propulsion systems contribute less than 10% of the total launch and ascent phase risk to the Shuttle system. The contribution of each risk element to the total Shuttle risk is depicted graphically in Figure 2.

Figure 2. Risk Element Fractional Contributions to STS Total Risk



Discussion of the Analysis

Solid Rocket Boosters

As discussed in the preceding section, a base case and three sensitivity cases were used to calculate the failure frequency for the RSRBs. The baseline case used a prior distribution comprised of the aggregate of U.S. solid rocket experience in launch vehicles, and updated that prior with actual Shuttle flight experience, discounting the STS 51-L SRB failure. The first sensitivity case (Sensitivity1) used the same prior distribution, but included the STS 51-L failure in the update data. The second sensitivity case (Sensitivity2) used no prior distribution and calculated the failure frequency distribution directly from the operational experience of one failure in one-hundred-ten (R)SRB-launches. The third sensitivity case (Sensitivity3) used no prior and calculated the RSRB failure frequency distribution based on no (0) failures in one-hundred-nine (R)SRB-launches. The nomenclature (R)SRB refers to the combination of SRB and RSRB experience.

As of the time of the *Galileo* study, there had been twenty-five STS launches, or fifty SRB exposures. The *Galileo* risk estimate was based on the inclusion of the experience of six successful Shuttle flights prior to the *Galileo* mission. This was appropriate for risk estimation based on the existing launch schedule. If there had been a failure in one of those six missions, the assessment would have been revised to reflect the true experience up to *Galileo* launch time. The total SRB exposures used in the *Galileo* study and *Galileo*-era intermediate analysis of this study is therefore 62 SRB-launches. The current study incorporates operational data through STS-56, fifty-five Shuttle launches. The total exposure is therefore 109 SRB-launches (discounting the STS 51-L failure), or 110 SRB-launches if the failure is counted. It should be noted that the Sensitivity3 case discounts the STS 51-L failure both as a failure and as an exposure. The *Galileo* study retained the 51-L failure as an exposure in calculating the failure frequency distribution, and this apparent oversight was retained in the *Galileo*-era results calculated for this study (Table 3). For the *Galileo* study the magnitude of the difference (at the system level) was approximately 3%, not significant when compared to the overall size of the certainty interval. In the current study the magnitude of the difference is under 2%.

The failure frequencies for the Sensitivity2 and Sensitivity3 cases, and for the surrogate solid rockets used in the prior, were calculated as discussed in the subsequent Treatment of Demand Related Failures section of this report.

(Note: The mathematical expressions presented in the body of this report are intended to allow the interested reader to follow and verify the major calculations. Unwieldy or extensive calculations required to completely replicate this study are presented in the appendices. The mathematical expressions used here and throughout the body of this report use verbose variable names and mathematical operators as they would appear in computer program or spreadsheet. This convention was selected largely as a result of the difficulty experienced reproducing the *Galileo* study results, which was in part due to non-standard (or different standard) mathematical nomenclature. The convention used here sacrifices a little in readability, but ensures that the results can be easily replicated. Mathematical functions and conventions are from Microsoft EXCEL™ v4.0 and are shown in **Boldface**.)

Treatment of Demand Related Failures (SRBs and SSME Start Failures):

1. The means of the failure frequency distributions were set equal to the maximum likelihood estimator (MLE).

MEAN = MLE = Failures / Exposures

1.a. In the RSRB Sensitivity3 case there were no failures. Given the experience base for this study, it was felt that a mean based on the assumption of one-third (1/3) of a failure was justified. Specifically, since the exposure accumulated by the SRB to date (110 SRB-launches) is well within the range of mean trials to failure (mttf) predicted by the surrogate experience, an assumed mean is both justifiable more informative than basing a distribution

Appendix E contains a lengthy justification for this assumption.

2. The fifth-percentile (LOWER) and ninety-fifth-percentile (UPPER) of the distribution for demand related failure frequencies were calculated in terms of the F distribution.

LOWER = (Failures*(FINV(0.95,2*Failures, 2*Exposures-2*Failures+2)) /

Failures*(FINV(0.95,2*Failures, 2*Exposures-2*Failures+2))+(Exposures-Failures+1))

UPPER =((Failures+1)*(FINV(0.05,2*Failures+2, 2*Exposures-2*Failures) /

(Failures+1)*(FINV(0.05,2*Failures+2, 2*Exposures-2*Fails))+(Exposures-Failures)))

(FINV is the inverse F distribution function with arguments "percentile", "numerator degrees of freedom", and "denominator degrees of freedom".)

2.a. For the zero failure case (Sensitivity3), the F distribution LOWER is 0.00, however, when the distribution is converted to a lognormal (Step 6 below), the relationship between the MEAN and the UPPER are used to set a lower boundary on the distribution.

3. The MEDIAN of the distribution was found. (This calculation is tedious, See Appendix C.)

4. The lognormal error factor (EF) is found.

EF = UPPER / MEDIAN

5. The distribution was converted to a lognormal, preserving the MEAN and EF.

See Appendix C.

6. For the surrogate distributions contributing to the prior, the resulting distributions were then aggregated using CARP™ (Computerized Aggregation of Reliability Parameters) or CARP2™.

See Appendix C for a discussion of the aggregation process.

7. The aggregate prior distribution is converted to a lognormal, preserving its mean and median.

8. The converted (lognormal) prior updated with the flight exposure data using Bayes' theorem as follows (see Appendix C for detailed derivation of the mathematics involved):

8.a. The (failure-on-demand) prior is converted to a Beta distribution preserving the mean (M) and the variance (V). The Beta parameters n_0 and x_0 are obtained.

$n_0 = (M * (1 - M)) / V - 1$

$x_0 = M^{\wedge}2 * (1 - M) / V - M$

8.b. The mean (M') and variance (V') of the Bayesian posterior are calculated based on f observed failures in N new demands:

$M' = (x_0 + f) / (n_0 + N)$

$V' = ((x_0 + f) * (n_0 - N - x_0 - f)) / ((n_0 + N)^{\wedge}2 * (n_0 + N + 1))$

9. The Bayesian posterior distribution is lognormal since the Beta and lognormal distributions are complimentary. The lognormal error factor of the Bayesian posterior is determined:

$EF' = EXP(1.6448) * SQRT(LN((V'/M'^{\wedge}2) + 1))$

Note: The quantity 1.6448 is the z value (number of standard deviations) at the 95th percentile.

At several places in this process, a conversion is made from "raw" distributions of failure frequencies to lognormal distributions. These conversions are done to facilitate calculations, and conversion to a lognormal distribution was used both for ease of calculation and because the lognormal has long been accepted as well suited to characterizing failure rate (failure frequency) distributions. In all cases, this study uses the default conversions of the Computerized Aggregation of Reliability Parameters (CARP™) aggregation and Bayesian update algorithms, which have been developed and used extensively in Probabilistic Risk Assessments for a wide variety of applications.

The process used here was designed to preserve the mean and the relationship between the mean and the worst-case (ninety-fifth percentile) value in the original distribution as much as possible. It is believed that the *Galileo* study results differ from the *Galileo*-era interim results of this study largely because a slightly different process, designed to preserve both of the extreme values (fifth and ninety-fifth percentiles) was used in that study. As noted in Appendix H, the disadvantage of that process is that the central tendencies of the original distributions are lost. By preserving the means, "natural" and "expected" relationships based on point value calculations using the mean values of the distributions are preserved. For example, the mean of an aggregate distribution is the average of the means. This result does not hold true if the mean is not preserved in converting distributions.

The exception to the rule of preserving the mean and the relationship between the mean and worst-case values is in aggregation. The raw distribution resulting from aggregation is generally irregular and may be multi-modal. (In contrast, the other "raw" distributions which are converted tend look like the lognormal, right skewed, bound by zero, and long-tailed.) If the mean and 95th percentile are used to convert an aggregate distribution, the information in the other tail of that distribution may be unfairly discounted. Since the purpose of aggregation is to return a readily-used distribution which accurately reflects the experience of the set of aggregated surrogates as a class, and since the raw aggregate may not look as much like a lognormal as the other distributions being converted, it is important that both tails be equally represented in the converted aggregate distribution. For this reason the raw aggregate distributions are converted preserving the mean and median of the distribution, the median being the midpoint between the two extremes.

The Solid Rocket Booster Surrogate Prior:

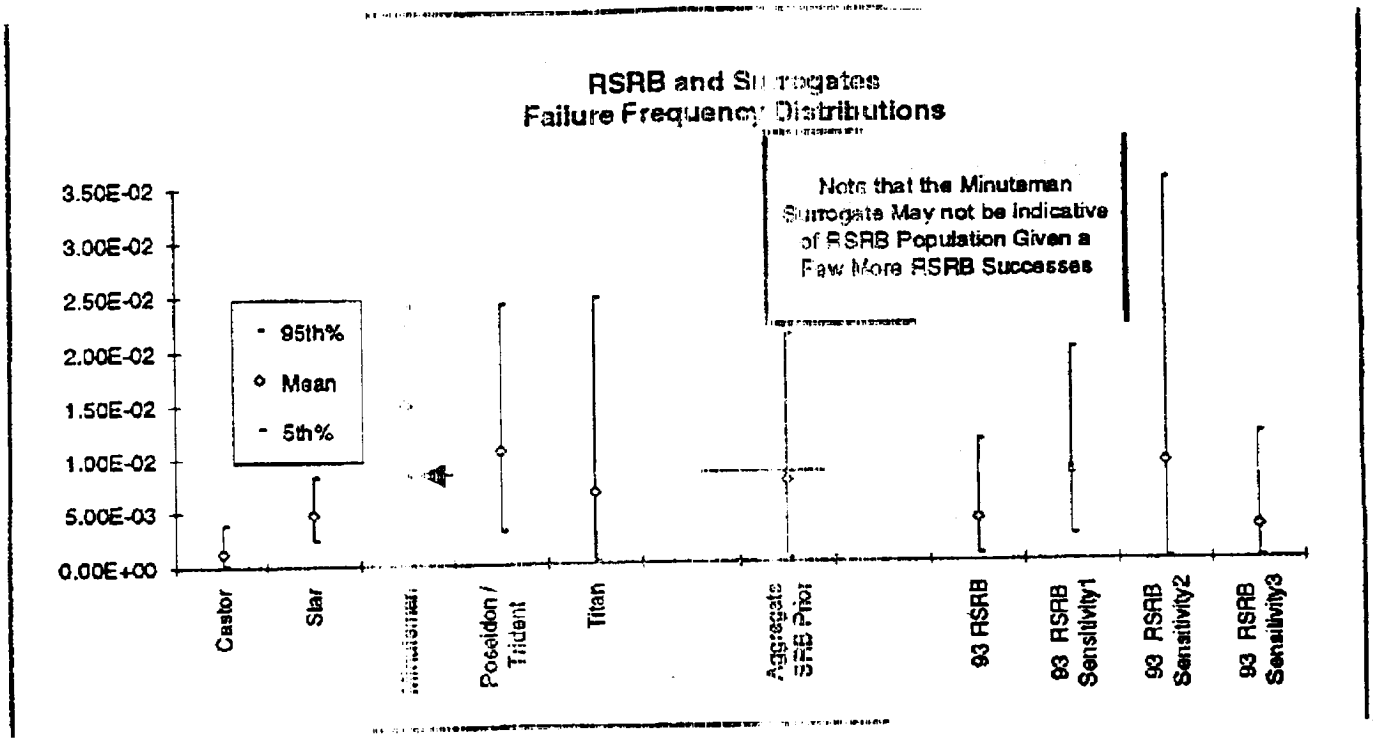
The surrogate data used to generate the prior distribution for the *Galileo* study is shown in Table 5 below. A homogeneity analysis was performed for the *Galileo* study to determine whether a better prior could be arrived at parametrically, based on the reliability of the surrogate systems with respect to diameter, length, and thrust. No statistically meaningful relationship between these parameters was found, so a simple aggregate of the surrogate failure frequency distributions was used to create the prior. A more detailed parametric analysis of solid rocket motors was subsequently performed at Brookhaven National Laboratory ("NASA Reliability Database and SRB Failure Probability Assessment") [7]. This analysis did find weak but statistically significant correlation between length, diameter, average thrust and failure frequency, but did not provide a statistically useful relationship which might have improved on the aggregate prior distribution. Reference 7 also showed that, for the data they had, there was no significant correlation between burn time and failure probability, indicating that a demand-related, rather than time-related approach was appropriate for SRBs.

Table 5: Aggregation of RSRB Surrogates
U.S. Solid Rocket Motor Experience prior to August, 1988

	5th %	20th %	50th %	Mean	80th %	95th %
Castor: 2 failures in 1640 flights (No softgoods in design)						
Castor	1.42E-04	3.18E-04	7.38E-04	1.22E-03	1.72E-03	3.84E-03
Star: 9 failures in 1887 flights (No softgoods in design)						
Star	2.36E-03	3.21E-03	4.43E-03	4.77E-03	6.12E-03	8.33E-03
Minuteman: 12 failures in 806 flights (Softgoods in design)						
Minuteman	8.32E-03	1.08E-02	1.41E-02	1.49E-02	1.86E-02	2.40E-02
Poseidon / Trident: 4 failures in 380 flights (No softgoods in design)						
Poseidon / Trident	3.10E-03	5.11E-03	8.64E-03	1.05E-02	1.46E-02	2.41E-02
Titan: 1 failure in 52 flights (Softgoods in design)						
Titan	2.65E-04	8.01E-04	2.55E-03	6.58E-03	8.13E-03	2.46E-02
Aggregate SRB Prior	3.03E-04		5.08E-03	7.59E-03		2.11E-02

The data in Table 5 are presented graphically in Figure 3 below, along with the 1993 RSRB failure frequency distributions for the baseline and various sensitivity cases. Note that as the mean value and uncertainty of the distribution associated with the RSRB (in particular, Sensitivity3) are reduced due to failure free flights, the probability that the Minuteman missile is in the same statistical population as the RSRB decreases. This fact is significant because the Minuteman distribution drives the aggregate distribution mean down, and increases the uncertainty associated with the aggregate prior distribution. Currently we include the Minuteman experience with the other surrogate solids because there is no compelling engineering or statistical reason to believe that the Minuteman is a less appropriate surrogate than any of the other solid surrogates. If there were a strong statistical justification for removing the Minuteman experience from the set of RSRB surrogates, both the mean and uncertainty associated with the RSRB prior would be significantly reduced. Determining how many failure free flights of the RSRBs are required to ensure that Minuteman missiles are not a valid indicator of RSRB performance, then assessing the effect of that knowledge on our understanding of STS catastrophic failure and the relative contribution of RSRB risk versus SSME risk, is recommended for further analysis.

Figure 3: Failure Frequency Distributions for the RSRB and Surrogates. (For a single SRB)



Space Shuttle Main Engines (SSMEs)

The SSME is a continuously evolving system. To date, there have been four major implementations of the SSME: the current, Phase II engine, used on STS-26 and subsequent flights; the Phase I engine, used on flights 6 through 25; the First Manned Orbital Flight (FMOF) engine, used on flight 1 through 5; and the Pre-FMOF engine, which was never flown. The test exposure of all engine configurations is used, and major failures that have occurred are examined on a case-by-case basis to determine whether that failure would have occurred and resulted in catastrophic damage, in a current flight (operational) system. The Pre-FMOF engine is considered sufficiently different from the later versions of the SSME that no Pre-FMOF failures are used to determine the SSME failure frequency prior distribution.

SSME catastrophic failures are considered in two groups, start-up failures and mainstage failures. Start-up failures are those which appear to be demand-related, and mainstage failures are time-related. The SSME failure history follows the well-known "bathtub curve" of infant mortality, random failure, and wearout, but the existing SSME test program appears to be doing an adequate job of preventing infant mortality or wearout failures in operational engines. Specifically, the "Green Run" program appears to weed out infant mortality failures before operational exposure, and the "Fleet Leader" program identifies wearout failure modes and attempts to ensure that operational components are not exposed in the wearout regime. SSME failures are therefore treated as random events, and the associated failure frequencies (per start for start-up failures, per second of run time for mainstage) are treated as constants.

SSME Exposure:

The test exposure of the engines is listed below in Table 6.

Table 6: SSME Test Exposure

Engine Configuration	Ground Test Seconds	Number of Starts
Pre FMOF	64,359	
FMOF	38,764	
Phase I	98,191	
Phase II (*Galileo* Study)	92,934	
***Galileo* Study Total**	**294,248**	**789**
Phase II (since *Galileo* Study)	190,702	471*
* Excludes tests terminated in less than 4 seconds.		
Total	**484,950**	**1260**

The exclusion of test starts where the test was terminated in less than 4 seconds was to ensure that only those tests which exposed the engine to the full start-up cycle were included in the count of start exposures. In most cases the short terminations were the result of a test-related problem or error. In no case was a catastrophic or potentially catastrophic failure excluded by this filter.

SSME Failures:

There have been no catastrophic failures of an in-flight SSME, although one major incident on the eleventh mission (STS-41C) could have resulted in a catastrophic failure if a programmed normal shutdown of the SSME had not occurred in time to prevent it. All catastrophic SSME failures to date have occurred during testing. To determine the catastrophic failure frequency of the SSME, a prior failure frequency distribution was generated based on the SSME test performance, then updated with the operational experience of the Shuttle. Like the RSRBs, only catastrophic (uncontained) failures, or those failures which could have led to catastrophic failure are included in the count of failures.

At the time of the *Galileo* study there had been 37 test and flight failure events, of which 3 were ultimately considered to be applicable to in-flight failure frequency determination:

> During test 750-160 on 12 February 1982, a blockage of the fuel supply as a result of ice formation occurred during start-up. Both high pressure turbines, the hot gas manifold (HGM), the main injector, the main combustion chamber (MCC), and the nozzle were burned as a result. This failure could recur in flight, but only during startup.
>
> During the eleventh flight (STS-41C) on 3 February 1984, the augmented spark ignitor (ASI) chamber experienced erosion due to a drill chip lodged in an ASI orifice. The engine was cut off by pre-programmed command at the nominal Main Engine Cutoff before the failure could propagate. An ASI fuel filter was subsequently added to the supply line, so the probability of recurrence of the incident, and of its becoming catastrophic, is diminished but still not zero.

During test 902-4[illegible] on 1 July 1987 a crack in the oxidizer pre-burner (OPB) interpropellant plate resulted in the formation and buildup of ice, blocking the fuel supply, which altered the OPB exhaust flow distribution and burned through the liner causing faceplate erosion and high pressure oxidizer turbo-pump (HPOTP) turbine end damage. The failure was caused by cracks in the interpropellant plate-to-element braze joints. The cracks allowed propellant mixing and caused ice contamination to form in the fuel manifold. The failure was determined to be the result of poor braze joints made during manufacture.

Since the *Galileo* study there have been three additional major incidents, of which one is considered to be applicable to in-flight failure frequency determination. The complete text of these incidents is included in Appendix F.

— During test 902-47[illegible] on 2 June 1989 an internal pressure restraint in one of the flex joints in the LPFTP discharge duct failed, releasing a half pound ball into the flow which ruptured the nickel plating of the duct, causing a fire. This failure is counted as an applicable failure event.

During test 904-04[illegible] on 23 June 1989 a HPOTP bearing failed during a 109% rated power level (RPL) extended duration burn. This failure is not counted because it occurred after 1270 seconds of continuous operation and at 109% RPL.

During test 901-60[illegible] on 24 July 1991 a second stage turbine blade in the HPFTP failed (disassembled) at [illegible]32 seconds into the test and less than 100% RPL. This failure is not counted because the root cause (internal microshrinkage porosity allowed hydrogen embrittlement inside the blade) is age related and the HPFTP blades were "fleet leaders" and had accumulated 61 starts and 25,143 seconds of exposure, well beyond the limits allowed for flight components.

To compute the prior failure frequency distributions based on this test data, the start-up incident was treated as a demand related failure and the remaining failures were treated as time-related random failures (Mainstage failures). The two Mainstage failures that were counted in the *Galileo* study were treated parametrically, based on the conditional probability of a catastrophic (loss of the Shuttle) accident given that the failure had occurred. This treatment is described in the *Galileo* study as follows:

"The two Mainstage (Phases 1 and 2) OPB failures identified as major incidents ... were treated as follows. The uncertain conditional probability of the recurrence in flight of each incident resulting in a catastrophic failure was assigned parametric values of 0, 0.5, and 1.0, giving rise to an effective number of catastrophic failures of 0, 1, and 2, respectively .... A Poisson distribution was determined for each case."

"The three cases bounded the expert judgment that the two oxygen preburner failures during tests could have been catastrophic if they had occurred during flight; i.e., they bounded the modeling uncertainty for the Mainstage catastrophic failure probability."

"The three distributions were then aggregated into an average distribution assuming that each case was equally likely to be true." [1]

The test failures (including the potential failure on STS-41C) were combined with the test exposure to generate prior distributions which were then updated using Bayes' Theorem with the actual flight experience. The start-up failure frequency distribution was treated as an on-demand failure, using the process described earlier. The mainstage failures were treated as time-related using the process described in detail below:

Treatment of Time Related Failures (SSME Mainstage Failures):

1. The two Mainstage failures from the *Galileo* study were combined with the new Mainstage failure using the aggregation method from the *Galileo* study. The conditional probability of catastrophic Shuttle failure given the new Mainstage failure (the LPF duct failure) was conservatively set to 1. This resulted in aggregating three distributions based on 1 failure, 2 failures, and 3 failures, vice the 0, 1, and 2 failures of the earlier study. The accumulated test time used was 484,932 seconds.

2. The three distributions (corresponding to 1, 2, and 3 failures in 484,932 seconds) were determined assuming that failures occurred following a Poisson process with a constant failure rate λ.

2a. The mean, fifth-percentile (LOWER), and ninety-fifth-percentile (UPPER) of the distributions for time-related failure frequencies were calculated in terms of the Chi-square distribution.

MEAN = Failures / Exposure

LOWER = CHIINV(0.95, 2*Failures) / (2*Exposure)

UPPER = CHIINV(0.05, 2*Failures + 2) / (2*Exposure)

CHIINV is the inverse Chi-Square distribution, with the parameters "percentile", "degrees of freedom".

The derivation of these equations in provided in Appendices B and C.

3. The resulting distributions were converted to lognormal, preserving the mean and error factor (see Appendix C).

Other risk contributors:

There were no significant new data sources or other indications that the failure frequency distributions calculated for the Orbiter, External Tank, and Prelaunch in the *Galileo* study required recalculation. For the sake of uniformity a Bayesian update of these distributions was performed using the launch experience to date, although this update had little effect on the STS system level failure frequency distributions.

Combining risk contributors:

The failure frequency distributions for the major risk contributors were combined to produce the overall STS failure frequency distribution using a Monte-Carlo type simulation. A commercially available simulation tool, Crystal Ball™ by *Decisioneering*, was used to perform the simulations within the same Excel™ spreadsheet environment that was used for the other calculations in this study. The starting

failure frequency distributions for each of the risk elements (RSRB, SSME, Orbiter, ET, Prelaunch) were converted to lognormal to facilitate sampling from the distribution. The actual sampling technique used was the Latin-Hypercube, as it was found that this technique modeled the tails of the distributions more accurately than Monte Carlo sampling. Appendix B describes the differences between Monte-Carlo and Latin-Hypercube sampling. The simulation model is described below:

Combining Failure Frequencies from the Risk Elements -- The Simulation Model

1. The failure frequency for the RSRB pair was found by converting the RSRB failure frequency to a reliability value squaring it. The resulting RSRB (Pair) reliability was then converted back to a failure frequency. In the simulation these calculations were repeated for each sampled value from the input failure frequency distributions:

R_{SRB} = **EXP**(-SRB Failure Frequency)
(Probability of no SRB failure)

$R_{SRB\text{-}Pair} = R_{SRB} * R_{SRB}$
(Probability that neither SRB will fail)

SRB (Pair) Failure Frequency = -LN($R_{RSRB\text{-}Pair}$)
(Frequency of SRB failure in flight)

2. The failure frequency distribution for the SSME and SSME Cluster were found by running a simulation in which the updated failure-on-demand (start) and (updated) time-related-failure (Mainstage) frequencies were sampled. The sampled frequencies were converted to reliability values. The reliability values were combined (multiplied) as indicated; and the corresponding failure frequency calculated.

R_{Start} = **EXP**(-Start Failure Frequency)
(Probability of no catastrophic SSME failure at startup)

$R_{Mainstage}$ = **EXP**(-Mainstage Failure Frequency * 520 seconds)
(Probability of no catastrophic SSME failure during ascent)

$R_{SSME} = R_{Start} * R_{Mainstage}$
(Probability of no catastrophic SSME failure)

SSME Failure Frequency = -LN(R_{SSME})
(Frequency of catastrophic SSME failures (per SSME - flight)

$R_{SSME\ Cluster} = R_{SSME}^{3}$
SSME Cluster Failure Frequency = -LN($R_{SSME\ Cluster}$)

3. The updated failure frequencies for each of the risk elements were then converted to reliability values and combined (multiplied) to produce the STS catastrophic reliability. STS Reliability was converted back into a failure frequency As above, these calculations were performed for each set of samples from the input failure frequency distributions.

$R_{STS} = R_{SRB\ (Pair)} * R_{SSME\ (Cluster)} * R_{Orbiter} * R_{ET} * R_{Prelaunch}$

STS Failure Frequency = -LN(R_{STS})

4. The resultant (STS failure frequency) distributions were not converted to lognormal since no further calculations with these distributions was anticipated.

Mathematical Tools and Methods:

All of the calculations in this study were performed within the framework of a prototype Space Systems Data Workstation (SSDW™) being developed for NASA by SAIC. The calculation of prior distributions, the aggregation of distributions, and Bayesian updating were performed using CARP2™ a prototype version of SAIC's CARP™ (Computerized Aggregation of Reliability Parameters) which was developed for use within the SSDW™ environment. The core mathematical engine was Microsoft Excel version 4.0 with a variety of enhancements (add-in functions) developed for the SSDW™. *Decisioneering's* Crystal Ball™, a commercial (off-the-shelf) simulation tool for use within Excel™ was also used extensively. @Risk™, an alternative simulation product from *Palisades Software* was used to ensure that no systematic errors were introduced by the use of Crystal Ball™. Appendix A contains an annotated copy of the spreadsheet in which all of the core calculations for this study were performed.

The simulations used throughout this study used 20,000 trials. This number of trials was found to be sufficient to ensure convergence at the tails of the resultant (forecast) distributions. Specifically, it was found that 20,000 trials was sufficient to keep the standard deviation of the 5th and 95th percentiles to less than 5% when performing multiple runs using the same input data and different random number generating "seeds".

Conclusion:

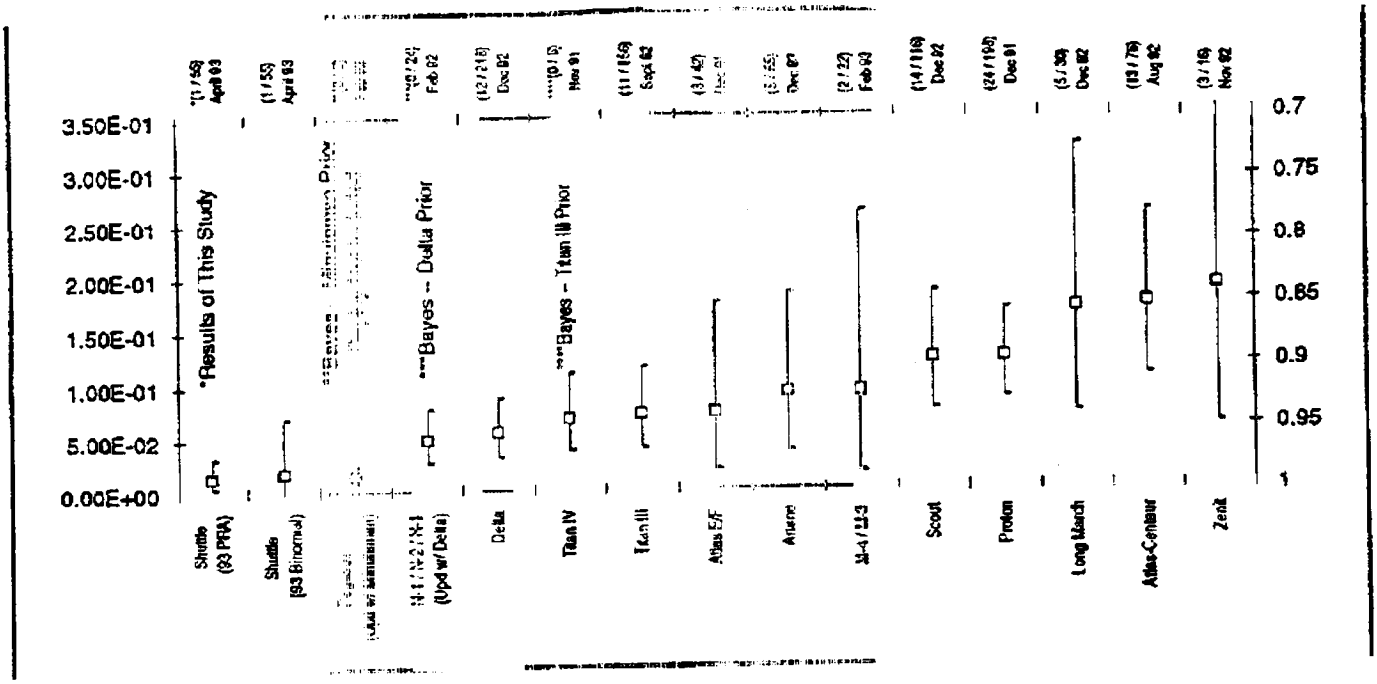
The principal conclusions of this study are: (1) The Space Shuttle today is demonstrably as reliable as any other launch vehicle, and under the reasonable assumptions of this study, more reliable than any other. (2) The Space Shuttle Main Engine (SSME) test program has had a significant positive impact on the reliability and crew safety of the Shuttle. (3) The Redesigned Solid Rocket Booster (RSRB) is the most significant contributor to the estimated residual risk of catastrophic failure to the Shuttle among the major elements considered in this study (RSRB, SSME, External Tank (ET), Orbiter, and Prelaunch), since the only opportunity to demonstrate reliability improvement in the RSRB is through flight experience.

Comparison of STS Catastrophic Reliability with Other Launch Systems:

The scope of this analysis was to determine the catastrophic failure probability of the Shuttle system during prelaunch, launch, and ascent. While this is not the same as mission reliability (the probability of successfully completing the mission), it is essentially equal to the probability of either completing the mission or returning the payload intact for another launch. The unique ability of the Shuttle to return a payload means that, for most purposes, the catastrophic failure probability is the correct value to compare with the mission reliability of expendable launch vehicles (ELVs). This study concludes that, at ninety percent certainty, the current catastrophic reliability of the Shuttle is between 0.969 (1/31) and 0.996 (1/223), with a mean of 0.986 (1/73), and median of 0.989 (1/90). The same quantities, when calculated based on a simple binomial for 1 failure in 55 launches are: 0.917 (1/12) (Lower) to 0.999 (1/1111) (Upper) with a binomial mean of 0.982 (1/55).

The Shuttle results are compared with other launch vehicles in Figure 4, based on data in the letter from P. Rutledge to W. Frazier of Code QS [9]. The failure data was used to derive a binomial which was then fit to a lognormal ELVs with no failures were updated using Bayes' theorem as indicated.

Figure 4: Reliability Comparison of Active Launch Vehicles



In Figure 4 the top axis shows the number of failures / number of exposures, and the "as-of" date for the data. The left-hand axis shows the failure frequency, and the right-hand axis shows the corresponding reliability. The 5th percentile, mean, and 95th percentile are shown for each launch vehicle. The first two entries compare the Shuttle reliability as analyzed in this study and the Shuttle reliability determined using the binomial -> lognormal conversion based on 1 failure in 55 launches. The *Pegasus* launch vehicle distribution reflects a Bayesian update using the Minuteman missile, the core of *Pegasus*. Since the *Pegasus* includes some new hardware and must be successfully deployed from a B-52 prior to engine ignition, the distribution shown probably reflects an optimistic assessment of the actual uncertainty. The launch vehicles are listed in order of increasing mean failure rate. The Shuttle has clearly demonstrated a higher reliability than any other active orbital launch system.

It should be noted that reliability growth was not modelled for the mature launch vehicles in this list, as that was beyond the scope of this study. However, a point check of the Delta launch vehicle using the AMSAA (Army Material Systems Analysis Agency) growth model parameters derived in Space Launch Reliability Growth [10] yields a mean reliability of 0.977 (instantaneous failure probability of 0.023 per launch), based on the 218 launches as of 2/92. This is still well short of the 0.986 reliability computed for Shuttle.

Impact of the SSME Testing Program:

The principal source of demonstrated reliability improvement in this study relative to the *Galileo*-era results is increased confidence in the SSME. Because of the test program, the SSME has been accumulating statistically relevant experience at the rate of 4 or 5 equivalent flights per mission. This "experience multiplier" has the effect of improving confidence in the reliability of the SSME much more quickly than if the SSME were exposed to failure only during actual launches. In contrast, the

engines in an ELV are only exposed during an operational launch, so (like the Shuttle RSRB) the confidence in their reliability performance builds relatively slowly.

Although the test program has served to improve statistical certainty in the SSMEs, this is a relatively minor secondary benefit. The primary benefits of the test program, and its principal objectives, are to "weed out" infant mortality failures in new components, and to determine what components are subject to wearout or life limits, and set operational limits well short of the wear-out region. It is because this is the primary purpose that the SSME test data is not pooled directly with the SSME operational experience for this study -- SSME testing is deliberately more strenuous than the operational environment.

References:

1. Bloomquist, C. et al.; Independent Assessment of Shuttle Accident Scenario Probabilities for the Galileo Mission; PRC, NASA HQ Code QS; April 1989
2. Safie, F. and Heard, B.; Space Shuttle Main Engine Reliability Analysis: NASA MSFC/CTSA; May 1993
3. Biggs, R. et al.; "SSME Reliability Determination" (Viewgraph Presentation); Rockwell International, Rocketdyne Division; December 1990
4. Brodowski, R., Stutzke, M., et. al.; Galileo RTG Risk Assessment Data Analysis Final Report; SAIC, NASA HQ Code QS; May 1992
5. McFadden, R., et. al.; Program Plan: Probabilistic Risk Assessment of the Space Shuttle (Shuttle PRA) Rev 5; SAIC; June 1993
6. Shuttle Probabilistic Risk Assessment Proof of Concept Study
7. Hsu, F. and Azarm, M. A.; NASA Reliability Database and SRB Failure Probability Assessment; Brookhaven National Laboratory; 1992
8. Galvagni, Fragola, Antona; Risk Assessment in Design; Unpublished manuscript, to be presented at the SRA Conference in Rome, Italy, October , 1993
9. Rutledge, P.; Letter to W. Frazier of NASA Code QS;
10. Cotta, R. and Kisko, W.; Space Launch Reliability Growth - Database, Analyses, and Prediction Methodologies; SPARTA, Inc.; March 1992

Appendix A:

Annotated copy of the spreadsheet "RTGUPDT2.XLS"

All calculations used in this report were performed in this spreadsheet.

	p5th	p20th	p50th	mean	p80th	p95th	ef	ef1
Galileo RTG Study Prior - Based on 294,230 seconds SSME test, 31 flights. These numbers from PRC p8 & Bu							95th/50th	50th/5th
Galileo Study PRC results - Based on 294,230 seconds SSME test, 31 flights - 0 SRB failures assumed.								
	5th%	20th%	50th%	Mean	80th%	95th%		
SRB (Pair)	7.69E-04	1.60E-03	3.60E-03	5.49E-03	8.06E-03	1.72E-02	4.79	4.68
mtbf (1 out of ...)	1300	624	278	182	124	58		
SSME (cluster)	8.33E-04	2.16E-03	5.85E-03	1.09E-02	1.56E-02	3.85E-02	6.58	7.02
mtbf (1 out of ...)	1200	458	171	92	64	26		
ET	1.25E-05	3.45E-05	1.00E-04	2.00E-04	2.86E-04	7.69E-04	7.69	8.00
mtbf (1 out of ...)	80000	29000	10000	5000	3500	1300		
Orbiter	1.09E-04	1.89E-04	3.45E-04	4.17E-04	6.25E-04	1.11E-03	3.22	3.17
mtbf (1 out of ...)	9200	5300	2900	2400	1600	900		
Prelaunch	2.94E-04	3.85E-04	5.26E-04	7.14E-04	7.69E-04	1.43E-03	2.71	1.79
mtbf (1 out of ...)	3400	2600	1900	1400	1300	700		
STS System	2.86E-03	5.95E-03	1.28E-02	1.82E-02	2.78E-02	5.56E-02	4.33	4.49
mtbf (1 out of ...)	350	168	78	55	36	18		
Reliability	0.997	0.994	0.987	0.982	0.973	0.946		
Galileo Study Sensitivity Case 1 - Based on 294,230 seconds SSME test, 31 flights - 1 SRB failure								
SRB Sensitivity1 (Pair)	1.80E-03	3.98E-03	9.17E-03	1.54E-02	2.08E-02	4.55E-02	4.96	5.09
mtbf (1 out of ...)	555	251	109	65	48	22		
STS System Sensitivity1	4.95E-03	9.80E-03	2.00E-02	2.78E-02	4.17E-02	7.69E-02	3.85	4.04
mtbf (1 out of ...)	202	102	50	36	24	13		
Reliability	0.995	0.990	0.980	0.973	0.959	0.926		
Step 1.								
Reproduce PRC SSME results for updating								
PRC considered SSME failure rate in two parts, start (demand related) and mainstage (time related).								
PRC data is shown in italics to aid readability.								
Start-up failure rate; 1 failure in 882 engine starts								
PRC found the Chi-square fit to 1 in 882 at the 5th and 95th percentiles then forced a lognormal, preserving the 5th and 95th.								
As a result the mean of the PRC distribution is not the MLE for 1 in 882, and the distribution is more narrow than an								
F distribution fit to the data. The 882 starts apparently includes flights to 31.								
Note: these are per engine start								
Given: PRC p 61	*4.03E-04*		*1.47E-03*	*2.01E-03*		*5.38E-03*	*3.65*	*3.68*
mtbf (1 out of ...)	*2481*		*679.*	*498*		*186*		
CARP (F dist) fit of 1 / 882	1.96E-05	7.34E-05	2.93E-04	1.13E-03	1.17E-03	4.39E-03	14.98	14.96
mtbf (1 out of ...)	51048		3412	882		228		
Note: Because PRC fit this LN distribution to a Chi-square 5th & 95th, their central tendency is not the MLE of 1/882.								

	p5	p20th	p50th	mean	p80th	p95th	ef	ef1
Mainstage failures PRC p 63 (these numbers are per second)								
PRCs use of an aggregate prior seems reasonable, but their input distributions don't appear to match the data.								
Note that the mean values are not even close to MLE values for 0 (1/3 or 1/2), 1, and 2 out of 229861.								
K=0 (0 in 229861s, PRC p 63)	*3.25E-08*		*6.50E-07*	*3.47E-06*		*1.30E-05*	*20.00*	*20.00*
mtbf (1 out of ...)				*288.18*				
K=1 (1 in 229861s, PRC p 63)	*2.20E-07*		*2.10E-06*	*5.57E-06*		*2.10E-05*	*10.00*	*9.55*
mtbf (1 out of ...)				*179.78*				
K=2 (2 in 229861s, PRC p 63)	*1.50E-06*		*6.50E-06*	*9.57E-06*		*2.70E-05*	*4.15*	*4.33*
mtbf (1 out of ...)				*104.51*				
Aggr prior (PRC p 63)	*6.90E-07*		*2.10E-06*	*3.71E-06*		*1.10E-05*	*5.24*	*30.43*
Average of means of aggregated distributions:				*6.13E-06*				
PRC-CARP Aggr prior	3.20E-07	9.00E-07	2.67E-06	6.13E-06	7.90E-06	2.23E-05	8.35	8.34
Note: It is not clear how PRC accomplished their aggregation, but it differs significantly from the CARP aggregation.								
and does not match the average of the means of the aggregated distributions.								
Mainstage failures Using CARP (these numbers are per second)								
K=0 (0 in 229861s)	2.49E-08		3.74E-07	1.45E-06		5.61E-06	15.00	15.02
mtbf (1 out of ...)				689955	=1/3 in 229861			
K=1 (1 in 229861s)	7.48E-08		1.12E-06	4.35E-06		1.68E-05	15.00	14.97
mtbf (1 out of ...)				229955	=1 in 229861 (truncation error)			
K=2 (2 in 229861s)	1.01E-06		6.26E-06	8.70E-06		2.74E-05	5.21	5.21
mtbf (1 out of ...)				114977	=2 in 229861			
CARP Aggr prior	5.09E-07		9.70E-07	4.83E-06		1.85E-05	19.07	19.06
Average of means of aggregated distributions:				4.83E-06				
Update Mainstage to 35 flights:								
Despite PRCs claim that they used "total test and flight time of 229,871 seconds" (p62) for the mainstage prior,								
the 229,871 seconds is the total FMOT Phase I and Phase II ground test exposure -- the appropriate prior exposure.								
The Bayesian Posteriors are found by updating the Priors with 0 failures in 47,000 seconds (30 flights)								
PRC mainstage update given on p63:								
PRC Mainstage Posterior	*5.40E-07*		*1.60E-06*	*3.72E-06*		*1.10E-05*	*6.88*	*29.63*
CARP using PRC K=0, K=1, K=2 distributions and 30 flight (47,000 seconds) update data:								
PRC-CARP Posterior	1.43E-07		1.19E-06	2.77E-06		9.97E-06	8.38	8.32
It is not clear how PRC did their Bayesian update, and it was not possible to replicate their results. The PRC-CARP Posterior								
uses the PRC prior, converts to LN prior using mean and EF, and updates with Gamma distribution for 0 / 47,000 s.								
CARP using CARP K=0, K=1, K=2 and 30 flights (47,000 seconds)								
CARP Posterior	7.94E-08		1.51E-07	7.51E-07		2.89E-06	19.14	19.02
The CARP Posterior is obtained using the CARP Aggr prior above.								

	p5th	p20th	p50th	mean	p80th	p95th	ef	ef1
Determining SSME failure frequency								
These distributions are found using latin-hypercube simulation (20,000 trials) solving for the following for lambda (SSME):								
20,000 trials was found to be sufficient to reduce the standard deviation of the 95th percentile on multiple runs to < 10%								
All input distributions were converted to lognormal preserving mean and error factor.								
SSME (Cluster) = -ln(Rcluster)								
SSME = -ln(Rssme)								
Rcluster = Rssme*Rssme*Rssme								
Rssme = Rstart*Rmainstage								
Rstart = e^(-Start)								
Rmainstage = e^(-Mainstage*t_mainstage)								
First the best approximation of PRC inputs I can determine:								
Means below are calculated directly, median, 5th, 95th are from simulation:								
Start PRC	4.03E-04	7.59E-04	1.47E-03	2.01E-03	2.86E-03	5.38E-03	3.65	3.65
Mainstage PRC	5.40E-08		1.60E-06	3.70E-06		1.10E-05	6.88	29.83
t_mainstage PRC				440				
Note: it was necessary to use 440 seconds vice 520 seconds to meet PRCs final SSME (Cluster) mean using their failure rate								
It was also necessary to use an error factor of 29.6 (median/5th) vice 6.88 (95th/median) to get close to PRC target								
Rstart PRC	= e^(-Start PRC)			0.9980				
Rmainstage PRC	= e^(-Mainstage PRC*t_mainstage PR			0.9984				
Rssme PRC	= Rstart PRC*Rmainstage PRC			0.9964				
Rcluster PRC	= Rssme PRC*Rssme PRC*Rssme PR			0.9891				
SSME PRC	2.74E-04	8.83E-04	2.10E-03	3.64E-03	4.33E-03	9.55E-03	4.55	7.68
SSME (Cluster) PRC	8.21E-04	2.65E-03	6.31E-03	1.09E-02	1.30E-02	2.87E-02	4.55	7.69
mfbf (1 out of ...)	1218	377	158	92	77	35		
PRC "Target" values								
SSME (cluster) PRC Target	8.33E-04	2.18E-03	5.85E-03	1.09E-02	1.56E-02	3.85E-02	6.68	7.02
mfbf (1 out of ...)	1200	458	171	92	64	26		
Start CARP	1.96E-05	7.34E-05	2.93E-04	1.13E-03	1.17E-03	4.39E-03	14.96	14.96
Mainstage CARP1	2.68E-08		5.11E-07	2.55E-06		9.75E-06	19.08	19.07
t_mainstage CARP				520				
Rstart CARP	= e^(-Start CARP)			0.9989				
Rmainstage CARP	= e^(-Mainstage CARP*t_mainstage CA			0.9987				
Rssme CARP	= Rstart CARP*Rmainstage CARP			0.9975				
Rcluster CARP	= Rssme CARP*Rssme CARP*Rssme			0.9926				
SSME CARP	9.04E-05	3.34E-04	9.67E-04	2.46E-03	2.86E-03	8.81E-03	9.11	10.70
SSME (Cluster) CARP	2.49E-04	9.46E-04	2.84E-03	7.38E-03	8.35E-03	2.66E-02	9.37	11.41
mfbf (1 out of ...)	4016	1058	352	136	120	38		
PRC "Target" values								
SSME (cluster) PRC Target	8.33E-04	2.18E-03	5.85E-03	1.09E-02	1.56E-02	3.85E-02	6.58	7.02
mfbf (1 out of ...)	1200	458	171	92	64	26		
SSME derivation summary: There was insufficient information in the PRC report to replicate their findings. In general,								
the central tendencies (mean & median) of the distributions used by PRC were not indicative of the maximum likelihood								
estimators (MLEs) for the observed data.								
The SSME (cluster) CARP distribution above preserves all PRCs input assumptions, but uses statistical methods which								
the mean and error factor of the input distributions.								

	p5th	p20th	p50th	mean	p80th	p95th	ef	eff
Step 2.								
Reproduce PRC SRB results:								
Generate prior from surrogate data (PRC p47):								
Castor	1.42E	3.18E-04	7.38E-04	1.22E-03	72E-03	3.84E-03	5.20	
Star	2.36E	3.21E-03	4.43E-03	4.77E-03	6.12E-03	8.33E-03	1.88	
Minuteman	8.32E	1.08E-02	1.41E-02	1.49E-02	1.86E-02	2.40E-02	1.70	
Poseidon / Trident	3.10E	5.11E-03	8.64E-03	1.05E-02	1.46E-02	2.41E-02	2.79	
Titan	2.65E	8.01E-04	2.55E-03	5.50E-03	8.13E-03	2.46E-02	9.62	
Aggregate SRB Prior	3.03E		5.08E-03	7.59E-03		2.11E-02	4.15	16.77
RSRB update to 31 flights, 62 exposures								
After developing a prior on [p47], PRC			a different prior on [p48], without		indicating justification.			
The CARP / SAIC base case will use t			ginal [p47] prior, ultimately fit to a		normal preserving mean and error factor.			
PRC RSRB (prior p48)	*3.00E*		*7.90E-03*	*9.50E-03*		*2.10E-02*	*2.66*	*26.33*
mfbf (1 out of ...)	*333*		*127*	*105*		*48*		
PRC RSRB (0/62 Upd p48)	*2.00E*		*1.60E-03*	*3.30E-03*		*8.80E-03*	*5.50*	*8.00*
mfbf (1 out of ...)	*500*		*625*	*303*		*114*		
Note: it is not clear how PRC performed			Bayesian update, but it does not seem reasonable that updating 1/105					
with 0/62 would yield 1/303 at the mean			Bayesian update converting p48 p		or to LN preserving mean and error factor			
is shown below.								
Bayes Upd PRC p48 prior, EF	1.51E		1.23E-03	7.52E-03		9.98E-03	8.14	8.14
mfbf (1 out of ...)	664		816	133		100		
The next four lines are attempts to deter			ine how PRC went from the aggrega		prior on p47 to the prior used on p48. (Unresolved)			
RSRB Prior (p47)	3.03E		5.08E-03	7.59E-03		2.11E-02	4.15	16.77
LN fit of RSRB Prior (mn/EF)	1.26E		5.22E-03	7.59E-03		2.17E-02	4.15	4.15
LN fit of RSRB Prior (mn/95th)	1.37E		5.37E-03	7.59E-03		2.11E-02	3.93	3.93
Lognormal fit 5th, 95th of p47	3.03E		2.53E-03	5.81E-03		2.11E-02	8.34	8.34
Bayesian updates of the p47 Aggregate			prior converting prior to LN preserving mean and EF. (Sensitivity1 is 1 SRB failure)					
RSRB (0/62 Bayes Upd of prior	8.16E		3.40E-03	4.95E-03		1.42E-02	4.17	4.17
PRC RSRB Sensitivity1	*8.00E*		*5.00E-03*	*8.60E-03*		*2.40E-02*	*4.80*	*6.25*
RSRB Sensitivity1	2.95E		8.56E-03	1.06E-02		2.49E-02	2.91	2.91
Rrsrb	=e^-RSI	(0/62 Bayes Upd)		9.95E-01				
Rrsrb (pair)	=Rrsrb			9.90E-01				
RSRB (Pair) CARP	1.56E	3.28E-03	6.81E-03	9.90E-03	1.41E-02	2.83E-02	4.16	4.37
mfbf (1 out of ...)	642	305	147	101	71	35		
Rrsrb Sensitivity1	=e^-RSI	Sensitivity1		9.89E-01				
Rrsrb (pair) Sensitivity1	=(Rrsrb	sitivity1)^2		9.79E-01				
RSRB (Pair) Sensitivity1 CARP	5.88E	9.92E-03	1.71E-02	2.11E-02	2.96E-02	4.98E-02	2.91	2.91
mfbf (1 out of ...)	170	101	58	47	34	20		

	p5th	p20th	p50th	mean	p80th	p95th	ef	eff
Reproducing PRCs summary:								
The numbers below are calculated from PRCs final system level distributions, converting to LN preserving mean and EF, and computing STS distributions as products of reliability in simulation.								
Galileo Base Repro								
RSRB (Pair)	7.69E-04	1.60E-03	3.60E-03	5.49E-03	8.06E-03	1.72E-02	4.79	4.88
mtbf (1 out of ...)	1300	624	278	182	124	58		
SSME (cluster) PRC	8.21E-04	2.65E-03	6.31E-03	1.09E-02	1.30E-02	2.87E-02	4.56	7.69
mtbf (1 out of ...)	1218	377	158	92	77	35		
ET	1.25E-05	3.45E-05	1.00E-04	2.00E-04	2.86E-04	7.69E-04	7.69	8.00
mtbf (1 out of ...)	80000	29000	10000	5000	3500	1300		
Orbiter	1.09E-04	1.89E-04	3.45E-04	4.17E-04	6.25E-04	1.11E-03	3.22	3.17
mtbf (1 out of ...)	9200	5300	2900	2400	1600	900		
Prelaunch	2.94E-04	3.85E-04	5.26E-04	7.14E-04	7.69E-04	1.43E-03	2.71	1.79
mtbf (1 out of ...)	3400	2600	1900	1400	1300	700		
Galileo Base Repro PRC	3.48E-03	7.54E-03	1.32E-02	1.77E-02	2.17E-02	3.98E-02	3.02	3.79
mtbf (1 out of ...)	287	133	76	56	46	25		
Galileo Base Original	2.86E-03	5.95E-03	1.28E-02	1.82E-02	2.78E-02	5.56E-02	4.33	4.49
mtbf (1 out of ...)	350	168	78	55	36	18		
Repro Galileo RTG Study Sensitivity1 - Based on 294,230 seconds SSME test, 31 flights - 1 SRB failure								
RSRB Sens. (Pair)	1.80E-03	3.98E-03	9.17E-03	1.54E-02	2.08E-02	4.56E-02	4.96	5.09
mtbf (1 out of ...)	555	251	109	65	48	22		
Galileo Sensitivity1 Repro PR	4.13E-03	9.43E-03	1.56E-02	2.76E-02	2.72E-02	5.09E-02	3.26	3.78
mtbf (1 out of ...)	242	106	64	36	37	20		
Galileo Sensitivity1 Original	4.95E-03	9.80E-03	2.00E-02	2.78E-02	4.17E-02	7.69E-02	3.85	4.04
mtbf (1 out of ...)	202	102	50	36	24	13		
CARP Galileo Baseline								
This case is calculated using PRCs simulations but CARPs algorithms, and preserving mean and EF when fitting distributions.								
This is the case against which subsequent (eg: update to 93) calculations should be compared.								
Orbiter, ET, and Prelaunch distributions are the same as PRCs.								
CARP Galileo Baseline								
RSRB (Pair) CARP	1.56E-03	3.28E-03	6.81E-03	9.90E-03	1.41E-02	2.83E-02	4.16	4.37
mtbf (1 out of ...)	642	305	147	101	71	35		
SSME (cluster) CARP	2.49E-04	9.46E-04	2.84E-03	7.38E-03	8.35E-03	2.66E-02	9.37	11.41
mtbf (1 out of ...)	4016	1058	352	136	120	38		
Galileo Base Repro CARP	4.59E-03	7.70E-03	1.36E-02	1.86E-02	2.49E-02	4.86E-02	3.58	2.98
mtbf (1 out of ...)	218	130	74	54	40	21		
Reliability	0.995	0.992	0.987	0.982	0.976	0.953		
Galileo Base Original	2.86E-03	5.95E-03	1.28E-02	1.82E-02	2.78E-02	5.56E-02	4.33	4.49
mtbf (1 out of ...)	350	168	78	55	36	18		
CARP Galileo RTG Study Sensitivity1 - Based on 294,230 seconds SSME test, 31 flights - 1 SRB failure								
RSRB (Pair) Sensitivity1	5.88E-03	9.92E-03	1.71E-02	2.11E-02	2.96E-02	4.98E-02	2.91	2.91
Galileo Sensitivity1 Repro CA	9.70E-03	1.51E-02	2.43E-02	2.98E-02	4.01E-02	6.68E-02	2.74	2.51
mtbf (1 out of ...)	103	66	41	34	25	15		
Reliability	0.990	0.986	0.976	0.971	0.961	0.935		
Galileo Sensitivity1 Original	4.95E-03	9.80E-03	2.00E-02	2.78E-02	4.17E-02	7.69E-02	3.85	4.04
mtbf (1 out of ...)	202	102	50	36	24	13		
				2.98E-02				

	p[illegible]th	p20th	p50th	[illegible]ean	p80th	p95th	ef	ef1
93 Start Prior – 1 failure on startu[illegible]	**[illegible]73 new test starts (> 5s duration) - Total 1260 Starts**							
Total (882-93)+473=1260 starts, 1 [illegible]ure								
93 Start Prior 1/1260	1.[illegible]E-05		2.05E-04	7.[illegible]E-04		3.07E-03	14.96	14.96
Update to 55 launches (165 Starts)								
93 Start	4.[illegible]E-05		7.17E-05	2.[illegible]E-04		1.08E-03	15.02	15.02
For Comparison – calculate from all [illegible]ata = 882+473+165=1520 (1 failure)					1.52E+03			
Classical 93 Start	1.[illegible]E-05		1.70E-04	6.[illegible]E-04		2.54E-03	14.96	14.96
93 Mainstage Prior - 1 new failure [illegible]284230(p57)+190702 = 484,932 sec[illegible]ratch test								
Sticking with PRCs aggregation met[illegible]using 1 new failure (6/2/89 LPF D[illegible] failure) => Aggregate of 1, 2, 3 failures								
K=1 (1 in 484,932 sec)	3.[illegible]E-06		5.33E-07	2.[illegible]E-06		7.98E-06	14.96	14.96
mfbf (1 out of ...)				[illegible]932				
K=2 (2 in 484,932 sec)	4.[illegible]E-07		2.49E-06	4.[illegible]E-06		1.30E-05	5.21	5.21
mfbf (1 out of ...)				[illegible]193				
K=3 (3 in 484,932 sec)	1.[illegible]E-06		4.68E-06	6.[illegible]E-06		1.60E-05	3.42	3.42
mfbf (1 out of ...)				[illegible]844				
CARP Aggr prior	9.[illegible]E-08		2.42E-06	4.[illegible]E-06		1.35E-05	5.57	25.32
CARP converts Aggr prior to Lognorm[illegible] preserving mean and median								
93 Mainstage Prior	4.44[illegible]E-07		2.42E-06	4.[illegible]E-06		1.32E-05		
Update Mainstage to 55 Launches [illegible] failure in 55*520*3 = 85,800 secon[illegible] flight experience								
93 Mainstage	2.6[illegible]E-07		1.4505E-05	2.[illegible]E-06		7.91E-06	5.45	5.45
t_mainstage				[illegible]520				
For Comparison – calculate from all [illegible]osure – 484,932+85800= 570,732 [illegible] failure equivalents)								
Classical 93 Mainstage	4.0[illegible]E-07		2.12E-06	3.[illegible]E-06		1.10E-05	5.21	5.21
Calculate 93 SSME (Bayesian)								
Rstart				0.9997				
Rmainstage				0.9997				
Rsame				0.9994				
Rcluster				0.9853				
93 SSME	2.1[illegible]E-04		9.76E-04	1.[illegible]E-03		4.71E-03	4.83	4.53
93 SSME (Cluster)	6.4[illegible]E-04	1.35E-03	2.92E-03	4.[illegible]E-03	6.53E-03	1.41E-02	4.83	4.52
mfbf (1 out of ...)	1[illegible]	741	342	[illegible]213	153	71		

	p5th	p20th	p50th	mean	p80th	p95th	ef	eff
Classical 93 SSME -- Combining test & operations exposure directly -- No Bayes								
Using the failure count and type selected for this study. (Reliability growth modeled by screening failures.)								
Rstart				0.9993				
Rmainstage				0.9982				
Rssme				0.9975				
Rcluster				0.9926				
Classical 93 SSME	1.92E-04		1.38E-03	2.48E-03		6.66E-03	4.83	7.19
Classical 93 SSME (Cluster)	9.20E-04	2.06E-03	4.06E-03	7.44E-03	1.05E-02	2.00E-02	4.91	4.42
mtbf (1 out of ...)	1087	485	246	134	95	50		
Comparison with MSFC SSME reliability study (F. Safie)								
MSFC computes SSME reliability using the AMSAA reliability growth model. The Classical computation of reliability above agrees extremely well with Safie, despite very different approaches to reliability growth. In both approaches the test and operational experience are pooled, but in this analysis the "reliability growth" is accounted for by not including test failures which would not cause a catastrophic failure in TODAYS engine. Safie on the other hand counts all failures which would have been catastrophic on the Shuttle at the time of the failure, (6 at or below 104% rated power level), but models reliability growth empirically, using a Weibul distribution.								
93 MSFC (104%)				7.83E-03				
mtbf (1 out of ...)				128				
Bayesian Update with Safie's Failure Assumptions but without growth.								
Prior 6 failures / 121618+46526+26552+1200+18995+33769+35735 = 284,695 sec								
	8.44E-06		1.87E-05	2.11E-06		4.16E-05	2.22	2.22
Bayesian update with 0 failures, 85,800 seconds operations								
	3.67E-06		8.59E-06	9.66E-06		1.91E-05		
				520				
Rsafie				0.9950				
Rcluster				0.9850				
93 SSME				5.02E-03				
Classical 93 SSME (Cluster)				1.51E-02				
mtbf (1 out of ...)				66				
Note that the Bayesian update process is not a substitute for modeling reliability growth in some fashion.								

	p5th	p20th	p50th	mean	p80th	p95th	ef	ef1
RSRB update to 55 flights, 110 expo [illegible] (PRC aggregate prior [p47] updated current [4.15] in prior)								
RSRB Prior	3.03 [illegible]		5.08E-03	7.59 [illegible]-03		2.11E-02	4.15	16.77
93 RSRB	6.41 [illegible]		2.67E-03	3.90 [illegible]-03		1.12E-02	4.17	4.17
Rrsrb				0.9 [illegible]1				
Rrsrb (pair)				0.9 [illegible]2				
RSRB (Pair)	1.28 [illegible]-03	2.58E-03	5.35E-03	7.80 [illegible]-03	1.11E-02	2.23E-02	4.17	4.18
mtbf (1 out of ...)	78 [illegible]	388	187	128	90	45		
RSRB Sensitivity1 case includes th [illegible] failure to update the Galileo pr [illegible] surrogate prior.								
93 RSRB Sensitivity1	2.32 [illegible]		6.74E-03	8.32 [illegible]-03		1.96E-02	2.91	2.91
Rrsrb Sensitivity1				9.9 [illegible]-01				
Rrsrb (pair) Sensitivity1				9.9 [illegible]-01				
RSRB (Pair) Sensitivity1	4.63 [illegible]-03	7.80E-03	1.35E-02	1.66 [illegible]-02	2.33E-02	3.92E-02	2.91	2.91
mtbf (1 out of ...)	21 [illegible]	128	74	60	43	25		
RSRB Sensitivity2 case - No prior, [illegible] rm in 110 SRB launches								
93 RSRB Sensitivity2	1.57 [illegible]		2.35E-03	9.09 [illegible]-03		3.52E-02	14.98	14.98
Rrsrb Sensitivity2				0.9 [illegible]0				
Rrsrb (pair) Sensitivity2				0.9 [illegible]0				
RSRB (Pair) Sensitivity2	3.14 [illegible]-03	1.18E-03	4.70E-03	1.82 [illegible]-02	1.88E-02	7.03E-02	14.96	14.97
mtbf (1 out of ...)	319 [illegible]	850	213	5 [illegible]	53	14		
RSRB Sensitivity3 case - No prior, 0 [illegible] ures in 109 SRB Launches (1/3 f [illegible] assumed for MLE)								
93 RSRB Sensitivity3	5.28 [illegible]		7.90E-04	3.06 [illegible]-03		1.18E-02	14.96	14.98
Rrsrb Sensitivity3				0.9 [illegible]9				
Rrsrb (pair) Sensitivity3				0.9 [illegible]9				
RSRB (Pair) Sensitivity3	1.06 [illegible]-04	3.95E-04	1.58E-03	6.11 [illegible]-03	6.31E-03	2.36E-02	14.96	14.98
mtbf (1 out of ...)	947 [illegible]	2529	633	164	159	42		
RSRB Summary								
Castor	1.42 [illegible]-04	3.18E-04	7.38E-04	1.22 [illegible]-03	1.72E-03	3.84E-03	5.20	
Star	2.36 [illegible]-04	3.21E-03	4.43E-03	4.77 [illegible]-03	6.12E-03	8.33E-03	1.88	
Minuteman	8.32 [illegible]-03	1.08E-02	1.41E-02	1.48 [illegible]-02	1.86E-02	2.40E-02	1.70	
Poseidon / Trident	3.10 [illegible]-03	5.11E-03	8.64E-03	1.05 [illegible]-02	1.48E-02	2.41E-02	2.79	
Titan	2.86 [illegible]-04	8.01E-04	2.55E-03	6.58 [illegible]-03	8.13E-03	2.46E-02	9.62	
Aggregate SRB Prior	3.03 [illegible]-03		5.08E-03	7.59 [illegible]-03		2.11E-02	4.16	16.77
93 RSRB	6.41 [illegible]-03		2.67E-03	3.90 [illegible]-03		1.12E-02	4.17	4.17
93 RSRB Sensitivity1	2.32 [illegible]-03		6.74E-03	8.32 [illegible]-03		1.96E-02	2.91	2.91
93 RSRB Sensitivity2	1.57 [illegible]-03		2.35E-03	9.09 [illegible]-03		3.52E-02	14.98	14.98
93 RSRB Sensitivity3	5.28 [illegible]-04		7.90E-04	3.06 [illegible]-03		1.18E-02	14.96	14.98
ET, Orbiter, Prelaunch update to 56 [illegible]								
ET	1.25 [illegible]-04	3.45E-05	1.00E-04	2.00 [illegible]-04	2.86E-04	7.69E-04	7.69	8.00
93 ET	1.16 [illegible]-04	3.14E-05	8.91E-05	1.92 [illegible]-04	2.53E-04	6.86E-04	7.69	7.69
Orbiter	1.09 [illegible]-03	1.89E-04	3.45E-04	4.17 [illegible]-04	6.25E-04	1.11E-03	3.22	3.17
93 Orbiter	9.89 [illegible]-04	1.75E-04	3.19E-04	4.10 [illegible]-04	5.80E-04	1.03E-03	3.22	3.22
Prelaunch	2.94 [illegible]-04	3.85E-04	5.26E-04	7.14 [illegible]-04	7.69E-04	1.43E-03	2.71	1.79
93 Prelaunch	2.15 [illegible]-04	3.50E-04	5.84E-04	7.02 [illegible]-04	9.73E-04	1.58E-03	2.71	2.71

	p5th	p20th	p50th	mean	p80th	p95th	ef	eff
CURRENT STS ASCENT VEHICLE LOSS PROBABILITY								
Based on 484.932 seconds SSME test, 55 flights								
93 STS	**5th%**	**20th%**	**50th%**	**Mean**	**80th%**	**95th%**		
93 RSRB Pair	1.28E-03	2.58E-03	5.35E-03	7.80E-03	1.11E-02	2.23E-02	4.17	4.18
mfbf (1 out of ...)	782	388	187	128	90	45		
93 SSME Cluster	6.46E-04	1.35E-03	2.92E-03	4.69E-03	6.53E-03	1.41E-02	4.83	4.52
mfbf (1 out of ...)	1548	741	342	213	153	71		
93 ET	1.16E-05	3.14E-05	8.91E-05	1.92E-04	2.53E-04	6.85E-04	7.69	7.69
mfbf (1 out of ...)	86352	31885	11226	5201	3952	1459		
93 Orbiter	9.89E-05	1.75E-04	3.19E-04	4.10E-04	5.80E-04	1.03E-03	3.22	3.22
mfbf (1 out of ...)	10110	5710	3138	2436	1724	974		
93 Prelaunch	2.15E-04	3.50E-04	5.84E-04	7.02E-04	9.73E-04	1.58E-03	2.71	2.71
mfbf (1 out of ...)	4649	2855	1713	1425	1028	631		
93 STS (Base)	**4.48E-03**	**6.83E-03**	**1.11E-02**	**1.38E-02**	**1.86E-02**	**3.20E-02**	**2.88**	**2.48**
mfbf (1 out of ...)	**223**	**146**	**90**	**73**	**54**	**31**		
Reliability	0.996	0.993	0.989	0.986	0.982	0.969		
Reliability w/out RSRB				0.99402733				
RSRB Sensitivity1 - includes the 51L failure to update the Galileo study surrogate prior.								
93 RSRB Sensitivity1	4.63E-03	7.80E-03	1.35E-02	1.66E-02	2.33E-02	3.92E-02	2.91	2.91
mfbf (1 out of ...)	216	128	74	60	43	25		
93 STS (Sensitivity1)	**8.48E-03**	**1.27E-02**	**1.94E-02**	**2.29E-02**	**3.04E-02**	**4.77E-02**	**2.48**	**2.29**
mfbf (1 out of ...)	**118**	**79**	**52**	**44**	**33**	**21**		
Reliability	0.992	0.987	0.981	0.978	0.970	0.953		
RSRB Sensitivity2 - No prior, 1 failure in 110 SRB launches								
93 RSRB Sensitivity2	3.14E-04	1.18E-03	4.70E-03	1.82E-02	1.88E-02	7.03E-02	14.98	14.97
mfbf (1 out of ...)	3184	850	213	55	53	14		
93 STS (Sensitivity2)	**3.31E-03**	**5.67E-03**	**1.12E-02**	**2.42E-02**	**2.67E-02**	**7.72E-02**	**6.89**	**3.38**
mfbf (1 out of ...)	**302**	**176**	**89**	**41**	**37**	**13**		
Reliability	0.997	0.994	0.989	0.976	0.974	0.926		
RSRB Sensitivity3 - No prior, 0 failures in 109 SRB Launches (1/3 failure assumed for MLE)								
93 RSRB Sensitivity3	1.06E-04	3.95E-04	1.58E-03	6.11E-03	6.31E-03	2.36E-02	14.98	14.98
mfbf (1 out of ...)	9479	2529	633	164	159	42		
93 STS (Sensitivity3)	**2.54E-03**	**4.11E-03**	**7.44E-03**	**1.21E-02**	**1.48E-02**	**3.38E-02**	**4.54**	**2.93**
mfbf (1 out of ...)	**394**	**243**	**134**	**83**	**68**	**30**		
Reliability	0.997	0.996	0.993	0.988	0.985	0.967		

Appendix B:

Bayes' Estimators -- Introduction
(SAIC Working Notes)

BAYES ESTIMATORS

Introduction

Classical statistics for point-estimation problems assume that the random variable representing the outcome of the different experiments come from some density $f(\ .\ ;\ \theta)$, where the function f is assumed known. Additionally, it is assumed that the parameter θ, for which an estimation is desired, is a fixed constant, unknown to us.

In many situations, however, there is additional information available about the unknown parameter θ. For example, one may have the evidence (e.g., through considerable experience) that θ itself acts as a random variable for which a realistic density function can be postulated, provided that the past experience is believed to be relevant for the present situation or population. The following sections will address a method to incorporate this additional information in the estimation process.

Baves Posterior Distribution:

If the parameter θ is the value of a random variable Θ, then the density function of a random variable X is $f(x/\theta)$, that is, a conditional density, the density of X given $\Theta = \theta$.

Let us assume that the density function of Θ, $g(\theta)$ is known and completely specified with no unknown parameters and let $X_1, X_2, \ldots, X_N$ be a random sample of size N: $X_1, X_2, \ldots, X_N$. The objective is to find an estimate for θ. For example, θ can represent the failure per demand of a certain component, and the sample $X_1, X_2, \ldots, X_N$, the outcome of each demand trial, that is failure or success. The classical estimate of θ is a single expression that includes the observed sample $x_1, x_2, \ldots, x_N$ and the form of the sample density f. Now a procedure is needed that contains all the information that the classical estimate contains plus the new information of the known density of Θ, $g(\theta)$.

Prior to obtaining the sample, all the information available about θ is that it comes from the distribution $g(\theta)$, therefore called prior distribution. After taking the random sample (e.g., utilizing failure records), a new distribution is needed, which summarizes the prior distribution and the outcome of the actual sample and it is called posterior distribution $f(\theta/x_1, x_2, \ldots, x_N)$, that is, the posterior distribution of Θ given $X_1=x_1, X_2=x_2, \ldots, X_N=x_N$.

For random sampling, this new distribution is given by Bayes' theorem, as follows [Ref. 1, pg.341]:

$$f(\theta|x_1,x_2,\ldots,x_N) = \frac{f(x_1,x_2,\ldots,x_N|\theta)\, g(\theta)}{f(x_1,x_2,\ldots,x_N)} = \frac{\left[\prod_{i=1}^{N} f(x_i|\theta)\right] g(\theta)}{\int \left[\prod_{i=1}^{N} f(x_i|\theta)\right] g(\theta)\, d\theta} \qquad (1)$$

After this posterior distribution is obtained, the corresponding Bayes estimator can be computed as the mean value of θ, that is:

$$\bar{\theta} = \frac{\int \theta \left[\prod_{i=1}^{N} f(x_i|\theta)\right] g(\theta)\, d\theta}{\int \left[\prod_{i=1}^{N} f(x_i|\theta)\right] g(\theta)\, d\theta} \qquad (2)$$

It is stressed that the Bayes procedure lies in the complete specification of the prior distribution. If the past experience is sufficiently extensive, then a reasonable prior probability distribution can be assumed, provided that past experience is relevant to the present case. If past experience is not available, engineering knowledge about the design, fabrication, material, environment, of the components can be used to select the prior. The choice of this prior distribution often involves the additional consideration of mathematical convenience. A flexible distribution family which is easy to handle and which can approximate past experience by choosing the appropriate parameters, is often selected as a prior distribution. The fact that a particular prior is selected, generally does not involve the belief that the parameter is actually distributed that way, but it does mean that such prior fits the data reasonably well and is mathematically convenient.

A common selection for prior distributions are the so called conjugate priors which have the property that the posterior and prior distributions are members of the same family of distributions. Therefore, the posterior function has a closed form analytical representation. Now, one question arises: How is a conjugate prior identified? The answer depends on the problem being solved. A mathematical procedure exists, which finds pairs of distribution (for the prior and random experiment) that produce a posterior distribution of the same family as the prior. For the case being studied in this report, the distribution of the random variable which describes the experiment is known (Bernoulli for failure-on-demand and Poisson for time failure rates) and therefore the appropriate conjugate prior distribution has to be found, keeping in mind that such priors should represent the failure rates fairly well. The following sections discuss two cases of conjugate priors.

Beta Prior Distribution

The most widely used prior distribution for the failure-on-demand probabilities p is the Beta distribution. There are two main reasons for this choice. First, the Beta distribution has the same range as p, that is, the interval (0,1), giving flexibility to represent any failure characteristic within this range. Second, its mathematical tractability, being a conjugate prior, as this section will demonstrate.

Let us restate the problem to solve. An estimate for failure-on-demand probability 'p' is needed for a particular group of components. It is assumed, from past experience or expert opinion, that the components are part of a larger population whose failure-on-demand probabilities are distributed according to the Beta distribution, completely specified by any two parameters (generic data). Additionally, a random sample was obtained from the group of components (data records analyzed) so that the total number of failures is known, as well as the number of demand trials (plant specific data).

The prior distribution $g(p)$ is the only information available before the sample is obtained, and is given by the Beta distribution: [See Appendix, equation (A.1)]:

$$g(p) = \frac{1}{B(x_0, n_0 - x_0)} p^{x_0 - 1} (1-p)^{n_0 - x_0 - 1} \qquad (3)$$

where $0<p<1$, $n_0>x_0>0$ and $B(\ldots)$ is the beta function given by [See Appendix, equation (A.2)]:

$$B(z,w) = \int_0^1 t^{z-1} (1-t)^{w-1} dt$$

The mean M and variance V of this distribution are given by [see Appendix, equations (A.7) and (A.11)]:

$$M = \frac{x_0}{n_0} \qquad (4)$$

$$V = \frac{x_0 (n_0 - x_0)}{n_0^2 (n_0 + 1)} \qquad (5)$$

From equation (4), it is seen that x_0 can be interpreted as failures for the prior distribution and n_0 as demands, therefore called "pseudo failures" and "pseudo demands," respectively.

The prior distribution is usually specified by a mean and variance, rather than the parameters n_0 and x_0. A conversion is necessary to obtain n_0 and x_0 given mean and variance.

From equation (4), $\quad x_0 = M n_0 \qquad (6)$

Inserting equation (6) into (5):

$$V = \frac{M n_0 (n_0 - M n_0)}{n_0^2 (n_0+1)} = \frac{M(1-M)}{n_0+1}$$

Now, solving for n_0:

$$n_0 = \frac{M(1-M)}{V} - 1 \qquad (7)$$

So equations (6) and (7) allow the conversion.

Let us analyze the ~~random~~ random experiment performed to update the prior distribution. Assuming that the failure-on-demand probability p for each component is constant at each demand if X_i is the outcome of the i^{th} demand trial, that is failure or success (numerical values 1 or 0, respectively), then X_i follows the Bernoulli distribution. Therefore, the density function for X_i, given a failure-on-demand probability p is:

$$f(x_i|p) = p^{x_i}(1-p)^{1-x_i}$$

Now, the joint density of an independent random sample of N of such trial demands is given by:

$$f(x_1,x_2,\ldots,x_N|p) = \prod_{i=1}^{N} f(x_i|p) = p^{\sum x_i}(1-p)^{N-\sum x_i} = p^f(1-p)^{N-f} \qquad (8)$$

where $f = \Sigma x_i$ is the total number of failures observed. Note that f, being the sum of Bernoulli variables, is distributed according to the Binomial.

The denominator of equation (1) can be calculated:

$$f(x_1,x_2,\ldots,x_N) = \int_0^1 f(x_1,x_2,\ldots,x_N|p)\, g(p)\, dp = \int_0^1 p^f(1-p)^{N-f} \frac{1}{B(x_0,n_0-x_0)} p^{x_0-1}(1-p)^{n_0-x_0-1}\, dp =$$

$$= \frac{1}{B(x_0,n_0-x_0)} \int_0^1 p^{x_0+f-1}(1-p)^{n_0+N-x_0-f-1}\, dp \qquad (9)$$

This integral can be solved using the definition of the Beta function, with the following substitutions [See Appendix, equation (A.2)]:

$$x_0 + f = z$$
$$n_0 + N - x_0 - f = w$$

Rewriting equation (9):

$$f(x_1, x_2, \ldots, x_N) = \frac{1}{B(x_0, n_0 - x_0)} \int_0^1 p^{z-1}(1-p)^{w-1}\, dp$$

Now, the integral is the Beta function B(z,w). So substituting back $z = x_0+f$ and $w = n_0+N-x_0 - f$:

$$f(x_1,x_2,\ldots,x_N) = \frac{B(x_0 + f,\ n_0 + N - x_0 - f)}{B(x_0,\ n_0 - x_0)} \tag{10}$$

So finally, the posterior distribution is obtained by inserting equations (8), (3) and (10) into equation (1):

$$f(p\,|x_1,x_2,\ldots,x_N) = \frac{p^f (1-p)^{N-f} p^{x_0-1} (1-p)^{n_0-x_0-1}}{B(x_0 + f,\ n_0 + N - x_0 - f)} = \frac{1}{B(x_0 + f,\ n_0 + N - x_0 - f)}\, p^{x_0+f-1} (1-p)^{n_0+N-x_0-f-1} \tag{11}$$

Comparing equation (11) with equation (3), it is noted that the posterior distribution is also from the Beta family, with the parameters modified as follows:

$$x_0 \Rightarrow x_0 + f$$
$$n_0 \Rightarrow n_0 + N$$

Therefore, the posterior mean (Bayes estimate for p) and posterior variance are obtained by making the corresponding replacements in the expressions of the prior mean and variance, equations (4) and (5), that is:

$$M' = \frac{x_0 + f}{n_0 + N} \tag{12}$$

$$V' = \frac{(x_0+f)\,(n_0+N-x_0-f)}{(n_0+N)^2\,(n_0+N+1)} \tag{13}$$

It is noted from equation (12), that the posterior mean, that is, the Bayesian update is the quotient between the pseudo-failures plus observed failures and the pseudo-demands plus the trial demands.

Gamma Prior Distribution

The generally used prior distribution for the time related failures λ is the Gamma distribution. This distribution is adequate to represent failure rates and it is mathematically convenient, being a conjugate prior, as the following derivations will prove.

The problem to solve is analogous to the previous one, but here an estimate for the time related failure is needed, and therefore a Gamma distribution is chosen as prior (generic data). Also, a random sample was obtained from the group of components of interest (analyzing failure records), so that the total number of failures is known, as well as the total exposure corresponding to those failures (plant specific data).

The prior distribution $g(\lambda)$ is here given by the Gamma distribution [See Appendix, equation (B.1)]:

$$g(\lambda) = \frac{\beta^{\alpha}}{\Gamma(\alpha)} \lambda^{\alpha-1} e^{-\beta\lambda} \qquad (14)$$

where $\lambda>0$, α, $\beta>0$ and $\Gamma(\alpha)$ is the gamma function and is given by [See Appendix, equation (B.2)]:

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt$$

The mean and variance of this distribution are given by [See Appendix, equations (B.5) and (B.9)]:

$$M = \frac{\alpha}{\beta} \qquad (15)$$

$$V = \frac{\alpha}{\beta^2} \qquad (16)$$

From equation (15) it is seen that a α can be interpreted as failures for the prior distribution and β as demands, therefore called "pseudo failures" and "pseudo demands," respectively.

The prior distribution is usually specified by a mean and variance, rather than the parameters α and β to mean and variance:

From equation (15): $\alpha = M\beta$ (17)

Inserting Equation (17) into Equation (16):

$$V = \frac{M}{\beta}$$

So now:

$$\beta = \frac{M}{V} \tag{18}$$

$$\alpha = M\beta = \frac{M^2}{V} \tag{19}$$

Equations (18) and (19) allow to obtain α and β given mean M and variance V.

Let us now look into the process of analyzing the failure records (random experiment) to update the prior distribution. If failed items, in the group of components under study, are replaced or repaired "immediately" after failure, and assuming that failures occur independently and at a constant rate in time across different items, then for any given item (and its corresponding replacement, if it fails) a Poisson process is generated with parameter λt, λ being the constant failure rate and t the time length. Defining a random variable X_i representing the number of failures for the i^{th} item, then x_i follows the poisson distribution, that is:

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

Now, the joint density of an independent random sample of n items is given by:

$$f(x_1, x_2, \ldots, x_n|\lambda) = \prod_{i=1}^{n} f(x_i|\lambda) = \frac{e^{-n\lambda t}(\lambda t)^{\sum x_i}}{\prod_{i=1}^{n} x_i!} = \frac{e^{-\lambda t n}(\lambda t)^{f}}{\prod_{i=1}^{n} x_i!} \tag{20}$$

where $f = \Sigma x_i$ is the total number of failures observed. Note that f is also Poisson distribution.

The denominator in Equation (17) can now be calculated:

$$f(x_1, x_2, \ldots, x_n) = \int_0^{\infty} f(x_1, x_2, \ldots, x_n|\lambda)\, g(\lambda)d\lambda =$$

$$= \int_0^{\infty} \frac{e^{-\lambda t n}(\lambda t)^{f}}{\Pi x_i!} \frac{\beta^{\alpha}}{\Gamma(\alpha)} \lambda^{\alpha-1} e^{-\beta\lambda} d\lambda =$$

$$= \frac{t^{f}}{\Pi x_i!} \frac{\beta^{\alpha}}{\Gamma(\alpha)} \int_0^{\infty} \lambda^{\alpha+f-1} e^{-(\beta+tn)\lambda} d\lambda \tag{21}$$

The integral can be solved using the definition of the Gamma function [See Appendix, equation (A.4)], so equation (21) has to be rearranged to an equivalent form as a Gamma function.

Multiplying and dividing by $(\beta + tn)^{\alpha+f-1}$:

$$f(x_1, x_2, \ldots, x_n) = \frac{t^f}{\prod x_i!} \frac{\beta^\alpha}{\Gamma(\alpha)} \int_0^\infty \frac{[(\beta + tn)\lambda]^{\alpha+f-1}}{(\beta + tn)^{\alpha+f-1}} e^{-(\beta+tn)\lambda} \frac{d(\beta+tn)\lambda}{\beta + tn} =$$

$$= \frac{t^f}{\prod x_i!} \frac{\beta^\alpha}{(\beta + tn)^{\alpha+f} \Gamma(\alpha)} \int_0^\infty [(\beta + tn)\lambda]^{\alpha+f-1} e^{-(\beta+tn)\lambda} d(\beta+tn)\lambda$$

Now, substituting inside the integral:

$$\alpha + f = z$$
$$(\beta + tn)\lambda = r$$

it is noted that the integral is the Gamma function $\Gamma(z)$, where $z = \alpha + f$, according to the substitution equations.

Then the integral can be solved.

$$f(x_1, x_2, \ldots, x_n) = \frac{t^f}{\prod x_i!} \frac{\beta^\alpha}{\Gamma(\alpha)} \frac{\Gamma(\alpha+f)}{(\beta + tn)^{\alpha+f}} \quad (22)$$

So finally, the posterior distirbution is obtained by inserting equations (20), (14) and (22) into equation (1):

$$f(\lambda \mid x_1, x_2, \ldots, x_n) = \frac{e^{-\lambda tn} \lambda^{\alpha-1} e^{-\beta\lambda} (\beta+tn)^{\alpha+f}}{\prod x_i! \, \Gamma(\alpha+f)} =$$

$$= \frac{(\beta+tn)^{\alpha+f}}{\Gamma(\alpha+f)} e^{-\lambda(\beta+tn)} \lambda^{\alpha+f-1} \quad (23)$$

Comparing equation (23) with equation (14), it is noted that the posterior distribution is also from the Gamma family (a conjugate prior) with the parameters modified as follows:

$$\alpha \Rightarrow \alpha + f$$
$$\alpha \Rightarrow \beta + tn = \beta + T$$

where $T = nt$ is the the total exposure time.

Therefore, the posterior mean (Bayes estimate for λ) and posterior variance are obtained by making the corresponding replacements in the expressions of the prior mean and variance, equations (15) and (16),that is:

$$M' = \frac{\alpha + f}{\beta + T} \quad (24)$$

$$V' = \frac{\alpha + f}{(\beta + T)^2} \qquad (25)$$

It is noted from equation (24) that the posterior mean is obtained as pseudo failures plus observed failures divided by pseudo exposure plus observed exposure.

A Procedure to Perform a Bayesian Update

This section describes a step by step procedure to obtain a Bayesian Updated estimate of time failure rates and failure-on-demand probabilities, given a lognormally distributed generic rate, specified by its mean value and error factor.

- Step 1: Find variance V for the lognormal.

If the generic data is lognormally distributed, and is given by its mean value M and error factor EF, its variance V is given by [See Appendix, equation (C.12)]:

$$V = e^{2\mu+\sigma^2}\left(e^{\sigma^2} - 1\right) \tag{26}$$

where μ and σ^2 are the mean and variance for the associated normally distributed variable. According to equation (C.7) in the Appendix:

$$M = \exp\left(\mu + \frac{\sigma^2}{2}\right)$$

Inserting log to both sides and multiplying by 2:

$$2\mu + \sigma^2 = 2 \log M \tag{27}$$

The variance σ^2 is related to the error factor [See Appendix, equation (C.15)]:

$$\sigma = \frac{\log (EF)}{1.645}$$

$$\sigma^2 = \left(\frac{\log (EF)}{1.645}\right)^2 \tag{28}$$

The error factor is the ratio of the 95th percentile to the median of the lognormal distribution.

Now, replacing Equations (27) and (28) into equation (26):

$$V = M^2\left[\exp\left(\frac{\log (EF)}{1.645}\right)^2 - 1\right] \tag{29}$$

- Step 2: Conversion to a Beta or Gamma Distribution

a) Failure-on-demand:

Converth the lognormal distribution to a Beta, preserving the mean and variance, and obtain the parameters x_0 and n_0 as given by equations (7) and (6):

$$n_0 = \frac{M(1 - M)}{V} - 1$$

$$x_0 = \frac{M^2(1 - M)}{V} - M$$

b) Time Related Failures

Convert the lognormal error distribution to a Gamma, preserving the mean and variance, and obtain the parameters α and β as given by equations (18) and (19)

$$\alpha = \frac{M^2}{V}$$

$$\beta = \frac{M}{V}$$

- Step 3: Perform Bayesian update:

a) Failure-on-demand

With the observed failures f in N demands, calculate the posterior mean M' and variance V' per equations (12) and (13):

$$M' = \frac{x_0 + f}{n_0 + N}$$

$$V' = \frac{(x_0 + f)(n_0 + N - x_0 - f)}{(n_0 + N)^2 (n_0 + N + 1)}$$

b) Time Related Failures

With the observed failures f and total exposure T, find the posterior mean M' and variance V' per equations (24) and (25):

$$M' = \frac{\alpha + f}{\beta + T}$$

$$V' = \frac{\alpha + f}{(\beta + T)^2}$$

- Step 4: Convert the distribution back into lognormal, calculating the error factor

The transformation is made preserving mean and variance. The posterior error factor EF' can be obtained using equation (26), replacing all variables with the corresponding posteriors, and solving for the error factor EF':

$$EF' = \exp\left[1.645 \sqrt{\log\left(\frac{V'}{M'^2} + 1\right)} \right]$$

The final updated estimate is now given by its mean M' and error factor EF'.

Appendix

A. Beta Distribution

The Beta distribution is given by the following function: [Ref. 2, pg. 658]

$$g(p) = \frac{1}{B(x_0, n_0 - x_0)} p^{x_0 - 1} (1 - p)^{n_0 - x_0 - 1} \tag{A.1}$$

where $0<p<1$, $n_0>x_0>0$, and $B(...)$ is the Beta function, defined as:

$$B(z,w) = \int_0^1 t^{z-1} (1-t)^{w-1} dt \tag{A.2}$$

The Beta function is related to the Gamma function as follows [Ref. 3, pg. 258, Eq. 6.2.2]:

$$B(z,w) = \frac{\Gamma(z)\,\Gamma(w)}{\Gamma(z+w)} \tag{A.3}$$

where $\Gamma(.)$ is the Gamma function, given by [Ref. 3, pg. 255, Eq. 6.1.1]:

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt \tag{A.4}$$

A recurrence formula can be obtained by computing $\Gamma(z+1)$ and integrating by parts:

$$\Gamma(z+1) = \int_0^\infty t^z e^{-t} dt$$

Now defining $u=t^z$ and $dv = e^{-t}\,dt$, and calculating $du = z\,t^{z-1}\,dt$ and $v = -e^{-t}$, the integration by parts can proceed, using the scheme:

$$\int u\,dv = uv - \int v\,du$$

$$\Gamma(z+1) = t^z(-e^{-t})\Big|_0^\infty - \int_0^\infty (-e^{-t})\, z\, t^{z-1}\, dt =$$

Note that $(t^z e^{-t})$ goes to zero in both limits, when t goes to zero and t goes to infinity, therefore the first term in the right hand side vanishes.

$$\Gamma(z+1) = z \int_0^\infty t^{z-1} e^{-t} dt$$

The integral obtained is the Gamma function $\Gamma(z)$ and the recurrence formula is obtained:

$$\Gamma(z+1) = z\,\Gamma(z) \tag{A.5}$$

A-1: Mean for the Beta Distribution

The mean is the expected value of the random variable p ($E[p]=\bar{p}$)and is a measure of central location of the density of p. It is computed as:

$$\bar{p} = E[p] = \int_0^1 p\, g(p)\, dp = \int_0^1 \frac{1}{B(x_0, n_0 - x_0)}\, p^{x_0}(1-p)^{n_0 - x_0 - 1}\, dp =$$

$$= \frac{1}{B(x_0, n_0 - x_0)} \int_0^1 p^{x_0}(1-p)^{n_0 - x_0 - 1}\, dp \qquad \text{(A.6)}$$

Substituting variables inside the integral:

$$x_0 = z - 1 \Rightarrow z = x_0 + 1$$
$$n_0 - x_0 = w$$

Now equation (A.6) can be rewritten as:

$$\bar{p} = \frac{1}{B(x_0, n_0 - x_0)} \int_0^1 p^{z-1}(1-p)^{w-1}\, dp$$

The integral now is the Beta function B(z,w) as defined in equation (A.2) where $z = x_0 + 1$ and $w = n_0 - x_0$ as defined by the change of variables. Therefore:

$$\bar{p} = \frac{B(x_0 + 1, n_0 - x_0)}{B(x_0, n_0 - x_0)}$$

Using the relation with the Gamma function given by equation (A.3):

$$\bar{p} = \frac{\dfrac{\Gamma(x_0 + 1)\,\Gamma(n_0 - x_0)}{\Gamma(n_0 + 1)}}{\dfrac{\Gamma(x_0)\,\Gamma(n_0 - x_0)}{\Gamma(n_0)}} = \frac{\Gamma(n_0)}{\Gamma(n_0 + 1)}\,\frac{\Gamma(x_0 + 1)}{\Gamma(x_0)}$$

Now making use of the recurrence formula (A.5).

$$\bar{p} = \frac{\Gamma(n_0)}{n_0\,\Gamma(n_0)}\,\frac{x_0\,\Gamma(x_0)}{\Gamma(x_0)} = \frac{x_0}{n_0}$$

So the mean value for the Beta distribution is:

$$\bar{p} = \frac{x_0}{n_0} \tag{A.7}$$

A-2: Variance for the Beta Distribution

The variance V of a random variable p is the measure of the spread or dispersion of its density and is expressed as the following expected value

$$V = E\left[(p - \bar{p})^2\right]$$

Expanding the squared term:

$$\begin{aligned} V &= E\left[p^2 - 2p\bar{p} + \bar{p}^2\right] = \\ &= E\left[p^2\right] - 2E[p]\bar{p} + \bar{p}^2 = \\ &= E\left[\bar{p}^2\right] - 2\bar{p}^2 + \bar{p}^2 = \\ &= E\left[p^2\right] - \bar{p}^2 \end{aligned} \tag{A.8}$$

So $E[p^2]$ needs to be calculated:

$$\begin{aligned} E\left[p^2\right] &= \int_0^1 p^2 g(p)\, dp = \\ &= \int_0^1 \frac{1}{B(x_0, n_0 - x_0)} p^{x_0+1} (1-p)^{n_0 - x_0 - 1} dp = \\ &= \frac{1}{B(x_0, n_0 - x_0)} \int_0^1 p^{x_0+1} (1-p)^{n_0 - x_0 - 1} dp \end{aligned} \tag{A.9}$$

Again, changing variables inside the integral:

$$\begin{aligned} x_0 + 1 &= z - 1 \Rightarrow z = x_0 + 2 \\ n_0 - x_0 &= w \end{aligned}$$

Equation (A.9) can be rewritten as

$$E\left[p^2\right] = \frac{1}{B(x_0, n_0 - x_0)} \int_0^1 p^{z-1} (1-p)^{w-1} dp$$

Now the integral is the Beta function B(z,w) as defined in equation (A.2), where $z = x_0 + 2$ and $w = n_0 - x_0$ as defined by the change of variables. Hence:

$$E\left[p^2\right] = \frac{B(x_0 + 2, n_0 - x_0)}{B(x_0, n_0 - x_0)}$$

Using the relation with the Gamma function given by equation (A.3):

$$E\left[p^2\right] = \frac{\dfrac{\Gamma(x_0+2)\,\Gamma(n_0-x_0)}{\Gamma(n_0+2)}}{\dfrac{\Gamma(x_0)\,\Gamma(n_0-x_0)}{\Gamma(n_0)}} = \frac{\Gamma(x_0+2)}{\Gamma(x_0)}\,\frac{\Gamma(n_0)}{\Gamma(n_0+2)}$$

Now using the recurrence formula (A.5):

$$E\left[p^2\right] = \frac{(x_0+1)\,\Gamma(x_0+1)}{\Gamma(x_0)}\,\frac{\Gamma(n_0)}{(n_0+1)\,\Gamma(n_0+1)} =$$

$$= \frac{(x_0+1)\,x_0\,\Gamma(x_0)}{\Gamma(x_0)}\,\frac{\Gamma(n_0)}{(n_0+1)\,n_0\,\Gamma(n_0)} =$$

$$= \frac{x_0\,(x_0+1)}{n_0\,(n_0+1)} \qquad \text{(A.10)}$$

Inserting equation (A.10) into equation (A.8), the variance is obtained:

$$V = E\left[p^2\right] - \bar{p}^{\,2} = \frac{x_0\,(x_0+1)}{n_0\,(n_0+1)} - \frac{x_0^{\,2}}{n_0^{\,2}} =$$

$$= \frac{n_0\,x_0\,(x_0+1) - x_0^{\,2}\,(n_0+1)}{n_0^{\,2}\,(n_0+1)} = \frac{n_0\,x_0^{\,2} + n_0\,x_0 - n_0\,x_0^{\,2} - x_0^{\,2}}{n_0^{\,2}\,(n_0+1)} =$$

$$= \frac{x_0\,(n_0-x_0)}{n_0^{\,2}\,(n_0+1)}$$

Hence, the variance for the Beta distribution is given by:

$$V = \frac{x_0\,(n_0-x_0)}{n_0^{\,2}\,(n_0+1)} \qquad \text{(A.11)}$$

B - Gamma Distribution

The Gamma distribution is given by the following function [Ref. 2, pg. 658]

$$g(\lambda) = \frac{\beta^{\alpha}}{\Gamma^{\alpha}} \lambda^{\alpha-1} e^{-\beta\lambda} \tag{B.1}$$

where $\lambda>0$, $\alpha,\beta>0$ and $\Gamma(\cdot)$ is the Gamma function, defined as

$$\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt \tag{B.2}$$

A recurrence formula for the Gamma function was found in Section A (equation A.5):

$$\Gamma(z+1) = z\,\Gamma(z) \tag{B.3}$$

B.1: Mean for the Gamma Distribution

The mean is the expected value of the random variable λ ($E[\lambda] = \bar{\lambda}$) and is calculated as:

$$\bar{\lambda} = E[\lambda] = \int_0^{\infty} \lambda\, g(\lambda)\, d\lambda = \int_0^{\infty} \frac{\beta^{\alpha}}{\Gamma(\alpha)} \lambda^{\alpha} e^{-\beta\lambda} d\lambda =$$

$$\frac{1}{\Gamma(\alpha)} \int_0^{\infty} (\beta\lambda)^{\alpha} e^{-\beta\lambda} \frac{d(\beta\lambda)}{\beta} \tag{B.4}$$

Changing variables inside the integral:

$$\beta\lambda = t$$
$$\alpha = z-1 \;\Rightarrow\; z = \alpha+1$$

equation (B.4) can be rewritten as:

$$\bar{\lambda} = \frac{1}{\beta\Gamma(\alpha)} \int_0^{\infty} t^{z-1} e^{-t} dt$$

The integral is the Gamma function $\Gamma(z)$ as defined in equation (B.2), where $z = \alpha + 1$, as defined in the above change of variables. Hence:

$$\bar{\lambda} = \frac{\Gamma(\alpha+1)}{\beta\Gamma(\alpha)}$$

Using the recurrence of formula (B.3):

$$\bar{\lambda} = \frac{\alpha\Gamma(\alpha)}{\beta\Gamma(\alpha)} = \frac{\alpha}{\beta}$$

So, the mean value for the Gamma distribution is:

$$\bar{\lambda} = \frac{\alpha}{\beta} \tag{B.5}$$

B.2: Variance for the Gamma Distribution

The variance V can be expressed as:

$$V = E\left[\lambda^2\right] - \bar{\lambda}^2 \tag{B.6}$$

as found in Section A-2, equation (A.8), so $E[\lambda^2]$ has to be computed.

$$E\left[\lambda^2\right] = \int_0^\infty \lambda^2 g(\lambda)\, d\lambda = \int_0^\infty \frac{\beta^\alpha}{\Gamma(\alpha)} \lambda^{\alpha+1} e^{-\beta\lambda}\, d\lambda =$$

$$= \frac{1}{\Gamma(\alpha)} \int_0^\infty \frac{(\beta\lambda)^{\alpha+1}}{\beta} e^{-\beta\lambda} \frac{d(\beta\lambda)}{\beta} \tag{B.7}$$

Now changing variables inside the integral:

$$\beta\lambda = t$$
$$\alpha + 1 = z - 1 \Rightarrow z = \alpha + 2$$

Equation (B.7) can be rewritten as:

$$E\left[\lambda^2\right] = \frac{1}{\beta^2 \Gamma(\alpha)} \int_0^\infty t^{z-1} e^{-t}\, dt$$

Now, the integral is the Gamma function $\Gamma(z)$ as defined in equation (B.2), where $z = \alpha + 2$ as defined by the change of variables. Therefore:

$$E\left[\lambda^2\right] = \frac{\Gamma(\alpha+2)}{\beta^2 \Gamma(\alpha)}$$

Using the recurrence formula (B.3):

$$E\left[\lambda^2\right] = \frac{(\alpha+1)\,\Gamma(\alpha+1)}{\beta^2 \Gamma(\alpha)} = \frac{(\alpha+1)\,\alpha\,\Gamma(\alpha)}{\beta^2 \Gamma(\alpha)} = \frac{\alpha(\alpha+1)}{\beta^2} \tag{B.8}$$

Inserting equation (B.8) into equation (B.6), the variance is obtained:

$$V = E\left[\lambda^2\right] - \bar{\lambda}^2 = \frac{\alpha(\alpha+1)}{\beta^2} - \frac{\alpha^2}{\beta^2} = \frac{\alpha^2 + \alpha - \alpha^2}{\beta^2} = \frac{\alpha}{\beta^2}$$

Hence, the variance for the Gamma distribution is given by:

$$V = \frac{\alpha}{\beta^2} \qquad \textbf{(B.9)}$$

C - Lognormal Distribution

Let us define two random variables X and Y such that $Y = \log X$. If Y is normally distributed, with mean μ and variance σ^2, then the random variable X is said to follow a lognormal distribution.

The probability density function *(pdf)* for the lognormal distribution can be obtained from the normal distribution through a change of variable, as follows:

The cumulative density function for X is:

$$F(X \le x) = F(\log X \le \log x)$$

but $Y = \log X$, then

$$F(X \le x) = F(Y \le \log x) = F\left(\frac{Y - \mu}{\sigma} \le \frac{\log x - \mu}{\sigma}\right)$$

but $\frac{Y - \mu}{\sigma} = Z$ is the standard normal variable, that is, Z is normally distributed with mean 0 and variance 1, therefore:

$$F_x(X \le x) = F_z\left(Z \le \frac{\log x - \mu}{\sigma}\right) \qquad \text{(C.1)}$$

To obtain the pdf, the derivative of equation C.1 is computed:

$$f_x(x) = \frac{d}{dx} F(x) = \frac{dF(z)}{dz}\frac{dz}{dx} =$$
$$= f_z(z)\frac{1}{x\sigma} = f_z\left(\frac{\log x - \mu}{\sigma}\right)\frac{1}{x\sigma} \qquad \text{(C.2)}$$

But z is the standard normal variable, then:

$$f_z\left(z = \frac{\log x - \mu}{\sigma}\right) = \frac{1}{\sqrt{2\pi}} \exp\left\{\frac{z^2}{2}\right\} =$$

$$= \frac{1}{\sqrt{2\pi}} \exp\left\{-\frac{\left(\frac{\log x - \mu}{\sigma}\right)^2}{2}\right\}$$

(C.3)

Substituting equation (C.3) into (C.2):

$$f_x(x) = \frac{1}{x\sqrt{2\pi}\sigma} \exp\left\{-\frac{(\log x - \mu)^2}{2\sigma^2}\right\} \qquad \text{for } x > 0 \qquad \text{(C.4)}$$

Equation C.4 is the pdf for the lognormal distribution.

C.1: Mean of the lognormal Distribution

The mean of the lognormal distribution is computed as the expected value of the random variable x, as follows:

$$\bar{x} = E[x] = \int_0^\infty x f_x(x)\, dx =$$

$$= \int_0^\infty \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{ -\frac{(\log x - \mu)^2}{2\sigma^2} \right\} dx$$

Changing variables:

$$x = e^y$$

$$dx = e^y d_y$$

$$x: 0 \rightarrow \infty \Rightarrow y: \infty \rightarrow \infty$$

Then,

$$\bar{x} = \int_{-\infty}^{\infty} \frac{e^y}{\sqrt{2\pi}\sigma} \exp\left\{ -\frac{(y-\mu)^2}{2\sigma^2} \right\} dy =$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{y^2 - 2\mu y + \mu^2}{2\sigma^2} + y \right\} dy =$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{y^2 - 2\mu y + \mu^2 - 2y\sigma^2}{2\sigma^2} \right\} dy \qquad (C.5)$$

To solve the integral, it is necessary to add and subtract constant terms inside the exponential, so that it can be expressed as $(y-b)^2$.

The term $2\mu\sigma^2 + \sigma^4$ has to be added and subtracted in equation (C.5) for this purpose, so now:

$$\bar{x} = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{y^2 - 2y(\mu+\sigma^2) + (\mu+\sigma^2)^2 - 2\mu\sigma^2 - \sigma^4}{2\sigma^2} \right\} dy =$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{\left[y - (\mu+\sigma^2)\right]^2}{2\sigma^2} + \mu + \frac{\sigma^2}{2} \right\} dy =$$

$$= \frac{e^{\mu+\sigma^2/2}}{\sqrt{2\pi}\sigma}\int_{-\infty}^{\infty} \exp\left\{-\frac{\left[y-(\mu+\sigma^2)\right]^2}{2\sigma^2}\right\} dy \qquad \text{(C.6)}$$

Making another change of variables inside the integral in (C.6)

$$u = \frac{y-(\mu+\sigma^2)}{\sqrt{2}\sigma}$$

$$du = \frac{dy}{\sqrt{2}\sigma} \Rightarrow dy = \sqrt{2}\sigma du$$

Then,

$$\bar{x} = \frac{e^{\mu+\sigma^2/2}}{\sqrt{2}\sigma\sqrt{2}\sigma}\int_{-\infty}^{\infty} e^{-u^2} du$$

Any table of integrals gives the following result:

$$\int_{-\infty}^{\infty} e^{-u^2} du = \sqrt{\pi}$$

So finally:

$$\bar{x} = e^{\mu+\sigma^2/2} \qquad \text{(C.7)}$$

C.2: Variance of the Log-Normal Distribution

The variance can be calculated as shown in Equation (C.8)

$$V = E\left[x^2\right] - \bar{x}^2 \qquad \text{(C.8)}$$

$\bar{x}$ was already calculated, so only $E[x^2]$ is needed.

$$E\left[x^2\right] = \int_0^{\infty} x^2 f_x(x)\,dx = \int_0^{\infty} \frac{x}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{(\log x-\mu)^2}{2\sigma^2}\right\} dx$$

Making the following substitution inside the integral:

$$x = e^y$$

$$dx = e^y dy$$

$$x: 0 \rightarrow \infty \Rightarrow y: -\infty \rightarrow \infty$$

Then:

$$E[x^2] = \int_{-\infty}^{\infty} \frac{e^{2y}}{\sqrt{2\pi}\sigma} \exp\left\{ -\frac{(y-\mu)^2}{2\sigma^2} \right\} dy =$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{y^2 - 2\mu y + \mu^2 + 2y}{2\sigma^2} \right\} dy =$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{y^2 - 2\mu y + \mu^2 - 4\sigma^2 y}{2\sigma^2} \right\} dy =$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{y^2 - 2y(\mu + 2\sigma^2) + \mu^2}{2\sigma^2} \right\} dy \qquad \text{(C.9)}$$

Analogally as before, adding and subtracting $(4\mu\sigma^2 + 4\sigma^4)$ inside the exponential, equation (C.9) can be written as:

$$E[x^2] = \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{y^2 - 2y(\mu + 2\sigma^2) + (\mu + 2\sigma^2)^2 - 4\mu\sigma^2 - 4\sigma^4}{2\sigma^2} \right\} dy =$$

$$= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{[y - (\mu + 2\sigma^2)]^2}{2\sigma^2} + 2\mu + 2\sigma^2 \right\} dy =$$

$$= \frac{e^{2(\mu+\sigma^2)}}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\infty} \exp\left\{ -\frac{[y - (\mu + 2\sigma^2)]^2}{2\sigma^2} \right\} dy \qquad \text{(C.10)}$$

Now, changing variables inside the integral in (C.10):

$$u = \frac{y - (\mu + 2\sigma^2)}{\sqrt{2}\sigma}$$

$$du = \frac{dy}{\sqrt{2}\sigma} \Rightarrow dy = \sqrt{2}\,\sigma\, du$$

Therefore:

$$E\left[x^2\right] = \frac{e^{2(\mu+\sigma^2)}}{\sqrt{2\pi}\sigma}\sqrt{2}\sigma\int_{-\infty}^{\infty} e^{-u^2}du$$

The integral is the same as in the previous section:

$$\int_{-\infty}^{\infty} e^{-u^2}du = \sqrt{\pi}$$

So now:

$$E\left[x^2\right] = e^{2(\mu+\sigma^2)} \tag{C.11}$$

Inserting equations (C.11) and (C.7) into equation (C.8):

$$V = E\left[x^2\right] - \bar{x} = e^{2(\mu+\sigma^2)} - \left[e^{\mu+\sigma^2/2}\right]^2 =$$
$$e^{2\mu+2\sigma^2} - e^{2\mu+\sigma^2} = e^{2\mu+\sigma^2}\left(e^{\sigma^2}-1\right)$$

So finally:

$$V = e^{2\mu+\sigma^2}\left(e^{\sigma^2}-1\right) \tag{C.12}$$

C.3: Error Factor for the Lognormal Distribution

The Error Factor (EF) is defined as the ratio between the 95th percentile and the median or 50th percentile.

$$EF = \frac{x_{.95}}{x_{.50}} \qquad (C.13)$$

The error factor is a measure of variation about a central tendency and is used more often that the variance.

A relation can be established between the error factor EF and the variance σ of the associated normal variable as follows:

Taking log in both sides of equation (C.13):

$$\log EF = \log \left[\frac{x_{.95}}{x_{.50}} \right] = \log x_{.95} - \log x_{.50}$$

but $\log x = y$, then:

$$\log EF = y_{.95} - y_{.50} \qquad (C.14)$$

But recalling that $y = \log x$ is normally distributed, a change of variables can be made to the standard normal variable:

$$z = \frac{y - \mu}{\sigma} \Rightarrow y = \mu + \sigma z$$

Replacing into equation (C.14):

$$\log EF = \mu + \sigma z_{.95} - (\mu + \sigma z_{.50}) =$$
$$= \sigma (z_{.95} - z_{.50})$$

But the 95:h percentile of the standard normal distribution is approximately 1.645 and the 50th percentile is zero. Then:

$$\log EF = \sigma \, 1.645$$

So finally:

$$\sigma = \frac{\log EF}{1.645} \qquad (C.15)$$

References:

[1] A. Mood, F. Graybill, D. Boes, *Introduction to the Theory of Statistics*, 3rd ed., 1974, ~~page 241~~

[2] H. Martz, R. Waller, *Bayesian Reliability Analysis*, ~~pages 95~~ and 558-560

[3] M. Abramowitz, I. Stegun, *Handbook of Mathematical Functions*.

SAIC, New Yo

A.1: DEMAND RELATED FAILURES

When a certain population of components is selected to perform a plant or vehicle-specific data analysis for demand related failures, a generally used method is to count the number of failures, within the selected population, that occurred as a result of a number N of total demand trials. Assuming that the failure-on-demand probability p for each component is constant at each demand, and defining a random variable X_i representing the outcome of the i^{th} demand trial, that is failure or success (numerical values 1 or 0 respectively), then X_i follows the Bernouili distribution, that is:

$$P(X_i=x) = p^x (1-p)^{1-x}$$

After N demand trials, a random sample $X_1, X_2, \ldots, X_N$ is obtained. The objective is to estimate the failure-on-demand probability with a single value (point estimate) using the information provided by the random sample.

Several techniques can be used to accomplish this desired result. The method of maximum likelihood is here chosen among the other methods because it gives estimators with desirable properties and are fairly easy to obtain. The procedure of this method follows [1]:

Let $X_1, X_2, \ldots, X_n$ be the random sample obtained from n demand trial observations. Each of these n random variables has a density function (probability distribution) $f(X_i; \theta)$, where θ is the unknown parameter to estimate. Then the joint density function for the random sample is:

$$f(X_1, X_2, \ldots, Xn; \theta) = f(X_1; \theta)\, f(X_2; \theta) \ldots f(X_n; \theta)$$

since $X_1, X_2, \ldots, X_n$ are mutually independent.

After the sample is obtained, f is a function of θ only. This function is called the likelihood function and is indicated by $L(\theta)$. The method of maximum likelihood consists of finding the value $\hat{\theta}$ of θ which maximizes the likelihood function. Such $\hat{\theta}$ is called the maximum likelihood estimator of θ.

Returning to the original random sample $X_1, X_2, \ldots, X_N$, each variable being Bernouili distributed, the likelihood function is:

$$L(p) = \prod_{i=1}^{N} p^{x_i} (1-p)^{1-x_i} = p^{\Sigma x_i} (1-p)^{N-\Sigma x_i}$$

where $\sum x_i$ represents the sum of X_i from $i=1$ to $i=N$ and is therefore the total number of failures observed.

Maximizing L is equivalent to maximizing its logarithm, i.e. $Log(L)$, then:

$$\text{Log}(L) = \sum x_i * \text{Log}(p) + (N-\sum x_i) * \text{Log}(1-p)$$

A byproduct of this is that the mathematics is simplified.
To obtain the maximum of $Log(L)$, the derivative with respect to p is equated to zero:

$$\frac{\delta \text{Log}(L)}{\delta p} = \frac{\sum x_i}{p} - \frac{N-\sum x_i}{1-p} = 0$$

And solving for p, the maximum likelihood estimator is obtained:

$$\hat{p} = \frac{\sum x_i}{N} = \frac{f}{N}$$

That is, the point estimator for p is obtained dividing the total number of failures observed, by the total number of demand trials N.

It is noted that if N is fixed, then $\hat{p}$ is a random variable, and being the sum of Bernoulli variables, it is distributed according to the Binomial with parameters p and N.

Now a numerical interval is desired to bound the unknown parameter p with a certain degree of confidence. The idea is to find two functions, $L(.)$ and $U(.)$, of the random sample $X_1, X_2, \ldots, X_n$ so that, prior to observing the sample, there is a certain known probability that the parameter of interest p is contained in the interval $L(.),U(.)$. That is:

$$P[L(.) \le p \le U(.)] = 1 - \gamma \qquad 0<\gamma<1$$

After the sample is observed, the functions $L(.)$ and $U(.)$ yield two numbers l and u that constitute the confidence interval of level $(1-\gamma)$.

Some confusion arises regarding the interpretation of this confidence interval. Its interpretation is as follows: Prior to obtaining the sample, it can be stated that the probability that the data obtained will yield an interval (l,u) containing the unknown parameter p is $(1-\gamma)$. Note that after the sample is obtained, the values l and u are fixed and the interval (l,u) either contains the point p or not (i.e. probability 1 or 0). Another way of looking at this would be to obtain several random samples $X_1, X_2, \ldots X_n$ and generate one confidence interval of level $(1-\gamma)$ for each sample. Then, it is expected, on the average and in the long run of sampling, that $100(1-\gamma)\%$ of the obtained intervals will contain the actual value of p.

Several methods are available to establish confidence limits . The so called "statistical method" [1] is used for this case in which the probability distribution of the estimator is known. The method consists of finding two functions L(.) and U(.), functions of the random sample. L and U are found by solving for θ the following equations:

$$\int_{-}^{T} f_T(t;\theta)\,dt = p_l \quad \rightarrow \text{Solution } \theta = U(.)$$

$$\int_{T}^{-} f_T(t;\theta)\,dt = p_u \quad \rightarrow \text{Solution } \theta = L(.)$$

where T is the estimator, function of the random sample. If the variable is discrete (i.e. it can only take discrete values), the integrals in the above equations would need to be replaced by summations.

P_l and P_u can be arbitrarily chosen, though they are usually chosen to get certain desirable properties, for example they may be selected so that the resulting interval (l, u) has minimum length. For the present situation they will be selected so that $P_l = P_u = \gamma/2$ for a $(1-\gamma)100\%$ confidence interval, that is "equal tails".

Going back to the point estimator

$$\hat{p} = \frac{\Sigma x_i}{N} = \frac{f}{N}$$

an upper bound for p (p_u) can be obtained solving the following equation for p_u:

$$\sum_{s=0}^{f} \binom{N}{s} p_u^s (1-p_u)^{N-s} = \gamma/2$$

A Binomial table could be used to find p_u given N and f, but it is more convenient to make a transformation into a continuous variable F-distributed using the following relations:

a) The Binomial is related to the Incomplete Beta Function as follows:

$$\sum_{s=a}^{n} \binom{n}{s} p^s (1-p)^{n-s} = I_p(a, n-a+1)$$

[Ref. 2, p. 945, 26.5.24]

b) The Incomplete Beta Function relates to the F-distribution as follows:

$$Q(F / \nu_1, \nu_2) = \text{Prob}[\mathcal{F} \geq F] = I_x\left(\frac{\nu_2}{2}, \frac{\nu_1}{2}\right)$$

$$\text{with } x = \frac{\nu_1}{\nu_2 + \nu_1 F} \qquad \text{[Ref. 2, p. 945, 26.5.28]}$$

where $\mathcal{F}$ is a random variable F-distributed with ν_1 and ν_2 degrees of freedom, and $Q=1-P$, P being the cumulative probability.

Merging the above relations into one:

$$\sum_{s=a}^{n} \binom{n}{s} p^s (1-p)^{n-s} = Q\left(\frac{1-p}{p} \frac{a}{N-a+1} / \nu_1, \nu_2\right) = 1 - P\left(\frac{1-p}{p} \frac{a}{N-a+1} / \nu_1, \nu_2\right)$$

with $\nu_1 = 2(N-a+1)$ and $\nu_2 = 2a$

Rearranging and using this relationship, the equation becomes:

$$\sum_{s=0}^{f} \binom{N}{s} p_u^s (1-p_u)^{N-s} = 1 - \sum_{s=f+1}^{N} \binom{N}{s} p_u^s (1-p_u)^{N-s} = \gamma/2$$

$$\sum_{s=f+1}^{N} \binom{N}{s} p_u^s (1-p_u)^{N-s} = Q(Y / \nu_1, \nu_2) = 1 - \gamma/2$$

$$P(Y / \nu_1, \nu_2) = \gamma/2$$

where $Y = \frac{1-p_u}{p_u} \frac{f+1}{N-f}$; $\nu_1 = 2N-2f$ and $\nu_2 = 2f+2$

All that is needed is a value Y from the F-distribution (ν_1 and ν_2 degrees of freedom) whose cumulative probability is $\gamma/2$, that is:

$$Y = \mathcal{F}_{\gamma/2}(2N-2f; 2f+2) = \frac{1-p_u}{p_u} \frac{f+1}{N-f}$$

Now, solving the equation for p_u:

$$p_u = \frac{(1+f)}{(1+f) + (N-f)\,\mathcal{F}_{\gamma/2}(2N-2f\,;\,2f+2)}$$

Making use of the known reciprocal relation for the F-distribution:

$$\mathcal{F}_{\gamma/2}(\nu_1;\nu_2) = \frac{1}{\mathcal{F}_{1-\gamma/2}(\nu_2;\nu_1)}$$

So the final value for p_u is:

$$p_u = \frac{(1+f)\,\mathcal{F}_{1-\gamma/2}(2f+2\,;\,2N-2f)}{(N-f) + (1+f)\,\mathcal{F}_{1-\gamma/2}(2f+2\,;\,2N-2f)}$$

Now an analogous procedure is followed for the lower bound of p (p_l). In this case the following equation has to be solved:

$$\sum_{s=f}^{N} \binom{N}{s} p_l^s\,(1-p_l)^{N-s} = \gamma/2$$

Again, using the transformation relations, the following equation is obtained:

$$Q(Y/\nu_1,\nu_2) = 1 - P(Y/\nu_1,\nu_2) = \gamma/2$$

where $Y = \frac{1-p_l}{p_l}\,\frac{f}{N-f+1}$: $\nu_1 = 2N-2f+2$ and $\nu_2 = 2f$

Solving for p_l:

$$p_l = \frac{f}{f + (N-f+1)\,\mathcal{F}_{1-\gamma/2}(2N-2f+2\,;\,2f)}$$

Or equivalently, using the reciprocal relation for the F-distribution:

$$p_l = \frac{f\,\mathcal{F}_{\gamma/2}(2f\,;\,2N-2f+2)}{(N-f+1) + f\,\mathcal{F}_{\gamma/2}(2f\,;\,2N-2f+2)}$$

Let's summarize the results obtained for the demand related failures:

$$\hat{p} = \frac{f}{N}$$

$$p_l = \frac{f \; \mathcal{F}_{\gamma_2}(2f : 2N-2f+2)}{(N-f+1) + f \; \mathcal{F}_{\gamma_2}(2f : 2N-2f+2)}$$

$$p_u = \frac{(1+f) \; \mathcal{F}_{1-\gamma_2}(2f+2 : 2N-2f)}{(N-f) + (1+f) \; \mathcal{F}_{1-\gamma_2}(2f+2 : 2N-2f)}$$

where:

$\hat{p}$	= failure-on-demand probability point estimate
f	= number of demand related failures
N	= number of demands over which the f failures occurred
p_l	= failure-on-demand probability lower confidence bound
p_u	= failure-on-demand probability upper confidence bound
$\mathcal{F}_p(\nu_1, \nu_2)$	= p^{th} percentile of an F distribution with ν_1 and ν_2 degrees of freedom

A.2: TIME RELATED FAILURES

For the case of time related failures, a common practice to perform a plant or vehicle-specific data analysis is to count the number of failures, for a certain population of size n, that occurred during a certain fixed period of time. If failed items are replaced or repaired "immediately" after failure, and assuming that failures occur independently and at a constant rate in time across different items, then for any given item (and its corresponding replacements if it fails) a Poisson process is generated with parameter λt, λ being the constant failure rate and t the time length.

Defining a random variable X_i representing the number of failures for the ith item, X_i follows the poisson distribution, that is,

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

With the number of failures for each of then items, a random sample $X_1, X_2, \ldots, X_n$ is obtained. To estimate the failure rate: λ from the information provided by the sample, the method of maximum likelihood is used. The likelihood function is:

$$L(\lambda) = \prod_{i=1}^{n} f(x_i;\lambda) = \prod_{i=1}^{n} \frac{(\lambda t)^{x_i}}{x_i!} e^{-\lambda t} = \frac{e^{-n\lambda t} (\lambda t)^{\Sigma x_i}}{\prod x_i!}$$

Now finding the maximum for *LOG(L)*:

$$\text{Log}(L) = -n\lambda t + \sum_{i=1}^{n} x_i \log(\lambda t) - \sum_{i=1}^{n} \log(x_i!)$$

$$\frac{\delta \text{Log}(L)}{\delta \lambda} = -n t + \frac{\Sigma x_i}{\lambda} = 0$$

$$\hat{\lambda} = \frac{\Sigma x_i}{n t} = \frac{\Sigma x_i}{T} = \frac{f}{T}$$

So the point estimator for λ is obtained dividing the total number of failures by the total time exposure, i.e. $n t = T$.

It is noted that $\hat{\lambda}$ is also a random variable, and being the sum of independent poisson processes and assuming n and T fixed and known, $\hat{\lambda}$ is Poisson distributed also.

The corresponding confidence interval can be found in a similar fashion as for p, the failure-on-demand probability.

For the upper bound λ_u, the following equation has to be solved:

$$\sum_{s=0}^{f} \frac{(\lambda_u T)^s e^{-\lambda_u T}}{s!} = \gamma/2$$

Using the following relation between the Poisson and the Chi-Squared distribution with n degrees of freedom:

$$Q(\chi^2/\nu) = \text{Prob}\left(\chi^2 \geq \chi^2_\nu\right) = \sum_{j=0}^{c-1} \frac{e^{-m} m^j}{j!}$$

[Ref. 2, p.941, 26.4.21]

with $c = \frac{\nu}{2}$, ν even, $m = \frac{\chi^2}{2}$

Incorporating this relation to the original equation:

$$Q(2\lambda_u T / \nu = 2f+2) = 1 - P(2\lambda_u T / \nu = 2f+2) = \gamma/2$$

$$P(2\lambda_u T / \nu = 2f+2) = 1 - \gamma/2$$

Now solving for λ_u:

$$\lambda_u = \frac{\chi^2_{1-\gamma/2}(2f+2)}{2T}$$

For the lower bound λ_l, the equation to solve is:

$$\sum_{s=f}^{\infty} \frac{(\lambda_l T)^s e^{-\lambda_l T}}{s!} = 1 - \sum_{s=0}^{f-1} \frac{(\lambda_l T)^s e^{-\lambda_l T}}{s!} = \gamma/2$$

Using the relation to the Chi-squared:

$$Q(2\lambda_l T / \nu = 2f) = 1 - P(2\lambda_l T / \nu = 2f) = 1 - \gamma/2$$

$$P(2\lambda_l T / \nu = 2f) = \gamma/2$$

Solving for λ_l:

$$\lambda_l = \frac{\chi^2_{\gamma/2}(2f)}{2T}$$

Let's summarize the results obtained for the time related failures:

$$\hat{\lambda} = \frac{f}{T}$$

$$\lambda_u = \frac{\chi^2_{1-\gamma/2}(2f+2)}{2T}$$

$$\lambda_l = \frac{\chi^2_{\gamma/2}(2f)}{2T}$$

where:

$\hat{\lambda}$ = failure rate point estimate
f = number of time related failures
T = time interval over which the f failures occurred (multiplied by number of items)
λ_l = failure rate lower confidence bound
λ_u = failure rate upper confidence bound
χ^2_p = p^{th} percentile of an Chi-squared distribution

A.3: CARP - A Computer Tool

CARP (Computerized Analysis of Reliability Parameters) is a computer code for manipulating failure data. It was designed by SAIC and has evolved over several years in support of reliability data analysis projects. The main features of CARP include:

1. Tolerance aggregation of data
2. Determination of plant-specific failure rates (point estimates for maximum likelihood estimators)
3. Calculation of confidence intervals for time and demand related failures
4. Bayesian updating using conjugates
5. Automatic access to a generic database

Features 2 and 3 are performed following the methodology explained in detail in the previous sections. The only thing that is worth mentioning is that whenever the number of failures observed is zero, CARP uses number of failures f=0.33 to obtain the point estimates.

Feanures 4 and 5 were not used for this particular study, and will not be discussed here.

Feanure 1 was extensively used in this report and deserves special attention.

TOLERANCE AGGREGATION

An aggregation method is needed to combine multiple data sources into a single estimate. CARP is able to perform this aggregation into a composite estimate using a technique which preserves the tolerance of the individual data sources. This aggregation technique consists of three steps as follows:

STEP 1: Fit Individual Data Sources

Each individual data source for a given component type and failure mode is fitted to a log-normal distribution described by its median and logarithmic standard deviation. The log-normal distribution is used because it is easy to deal with computationally and is well suited to expressing uncertainty bounds (via error or range factors).

Individual data sources provide statistical information in a variety of styles which form two broad classes:

(1) sources that provide distributional information
(2) sources which provide failure counts and exposures

The methods used to form the log-normal uncertainty distribution depend upon the type of information provided.

Distributional Information: Here, distributional information is specified (e.g., mean value, point estimate, upper and lower percentiles, etc.). Such information may be difficult to assess since sometimes generic data sources do not provide adequate information to interpret the supplied

values. (For example, do the supplied values consider both data confidence and tolerance? Is the point value a distribution mean, median or mode? What distributional type is used?)

Failure Count and Exposure: This style provides the total number of failures that have occurred over a specified time period or number of demands (or, alternatively, cycles or trials). There are three issues of concern in using this style of information:

a. It is not possible to ascertain whether or not the information is consistent with an assumption of constant failure rates and constant failure-on-demand probabilities as the time (or demands) between failures is given.

b. Generic data sources typically do not state if the data has been statistically censored. If the last failure occurred exactly at the end of the exposure period, then the data is uncensored. If failures were counted until a preset total failure count was reached, then the data is Type I censored. If failures were counted for a preset time period, then the data is Type II censored. Knowledge of the censoring scheme used to collect the data is necessary to provide meaningful uncertainty estimates.

c. Only failure and exposure totals may be given even though the accompanying explanatory text of a generic data source may state that the population is heterogeneous. In such cases, the information appears to have a high information content (due to the large number of failures); however, there is no way to separate the data confidence from the data tolerance.

Step 2: Form Aggregate Distribution

The data sources can be combined into a single estimate by forming the weighted sum of each input generic data source's distribution function:

$$P[X \le x] = \sum_{i=1}^{N} \omega_i P[X_i \le x]$$

where:

N = number of generic data sources

$P[X \le x]$ = distribution function of the aggregate reliability parameter

ω_i = weight of the i^{th} generic data source

$P[X_i \le x]$ = distribution function of the i^{th} generic data source

This aggregation method, developed by SAIC for EPRI during the Component Reliability Parameter Studies and based on the work of Stone [3] and Winkler [4], ensures that data tolerance is preserved. By "smearing" the uncertainty of all input generic data sources, an aggregate uncertainty bound is created which properly encompasses the entire range of uncertainty. Each input generic data is assumed to be log-normally distributed.

It can be shown that, regardless of the input data source distributional type(s), the mean of the aggregate distribution is the weighted sum of the input means. Determination of the aggregate distribution percentiles typically requires a numerical solution. Using the previous assumptions (i.e., log-normally distributed input data sources and equal weights), the following equation applies:

$$p = \sum_{i=1}^{N} \frac{1}{N} \Phi\left[\frac{\ln\left(\frac{x_p}{\tilde{x}_i}\right)}{\sigma_i}\right] = \sum_{i=1}^{N} \frac{1}{N} \int_0^{x_p} \frac{1}{\sqrt{2\pi}\,\sigma_i t} \exp\left\{-\frac{\left[\ln\left(\frac{t}{\tilde{x}_i}\right)\right]^2}{2\,\sigma_i^2}\right\} dt$$

where:

$\tilde{x}_i$ = median of the i^{th} input data source
σ_i = logarithmic standard deviation of the i^{th} input data source

This latter equation is solved (i.e., the value of x_p determined for a given value of p) for the 5th percentile (p=0.05), the median (p=0.50), and the 95th percentile (p=0.95). These bounds are subsequently converted into a log-normal distribution.

STEP 3: Fit Aggregate Distribution

To facilitate use of the aggregated distributions in traditional PRA uncertainty calculations, each is converted to a log-normal distribution.

A.4: REFERENCES

[1] A. Mood, F. Graybill, D. Boes, *Introduction to the Theory of Statistics*, 3rd ed., 1974.

[2] M. Abramowitz, I. Stegun, *Handbook of Mathematical Functions*.

[3] M. Stone, *The Opinion Pool*, Annals of Mathematical Statistics, Vol. 32, pp. 1339-1342, 1961.

[4] R. Winkler, *The Consensus of Subjective Probability Distributions*, Management Science, Vol. 15, pp. 861-875, 1968.

Appendix C:

CARP™
Computerized Aggregation of Reliability Parameters
User Notes

CARP

COMPUTERIZED AGGREGATION OF RELIABILITY PARAMETERS

USER NOTES

GARY M. DEMOSS

JUNE 1990

FOREWORD

CARP is an computer code for manipulating failure data. It was designed and has evolved over several years in support of our reliability data analysis projects. SAIC will not be responsible for any problems resulting from the use of CARP nor will it ensure that CARP users are supported. All reasonable requests for help will be honored in the interest of further refining CARP, it's algorithms, or data analysis in general.

INTRODUCTION

CARP was developed by SAIC for the analysis of failure data during PRAs and other reliability studies. In the current version, CARP can aggregate up to 20 generic data sources, assuming that all input sources are log-normal or Poisson data sets and that the desired output is log-normal. Additional features include:

1. Determination of plant-specific failure rates, given Poisson data sets ("numerator-denominator" information), including uncertainty estimates using χ^2 or F-distribution bounds;

2. Bayesian updating using conjugates.

3. Automatically access a generic data base.

CARP is written in the dBASE III Plus programming language, and was compiled using Clipper (Summer '87 Version).

CARP REQUIREMENTS

1. IBM PC, XT, or AT (or 100% compatible)

2. PC-DOS or MS-DOS, version 2.0 or higher.

3. Must have 384K of RAM available use the DOS command (CHKDSK to find out if you have enough.

4. The CONFIG.SYS file should have the following (as a minimum) statements:

```
FILES =    20
buffers =   8
```

5. CARP must be able to find COMMAND.COM. Use SET COMSPEC if necessary to identify the correct path and drive.

6. HP Laserjet printer; CARP will probably not work as well on other printers since as it sends ESC sequences to select fonts. However, CARP will provide plain text file output that can be sent to any printer.

7. If the generic data base is to be used with CARP, a hard disk is required.

INSTALLATION

Six files comprise the CARP software:

1. CARP.EXE, the machine executable image;
2. CARP1.DBF and CARP2.DBF templates to create data files for CARP.
3. SAIC.DBF, the generic data base.
4. COMMPREF.NTX, CODES.NTX and CITU.NTX, indexes for SAIC.DBF to improve speed.

CARP OPERATION

CARP is menu-driven and intended to be easy to use. Of course, software is never really user-friendly; here are some guides through CARP. CARP uses 3 basic interfaces to allow your control from the keyboard. All depend heavily on the cursor. The position of the cursor is identifiable on each screen by a change in color and or intensity. Table 1 list the various keys that can be used to move the cursor.

The first and most friendly type of interface is the scrollable menu. You will be presented with several choices and sometimes amplifying information. There are many ways to make a choice, the simplest being to strike the first letter of desired selection. In menu with no repeated first letters, this completes the process. In menus with repeated first letters, you must follow with an <Enter> keystroke. You can also scroll through these menus using the arrows or a variety of other keys described in Table 1.

The second common interface is used to answer simple questions throughout the code. If the answer to the question is yes, simply strike the 'Y' key or if the answer is no, the 'N' key.

The third interface requires the input of data. The area in which to type the data is indicated by a change in background color. CARP has numerous checks and balances to ensure that the data is entered correctly, (e.g., characters are not accepted in numeric fields) but it cannot prevent all mistakes.

Screen 1

From DOS, type CARP to start execution of CARP. It takes some time to load CARP into memory, so be patient. Strike any key to leave the welcome screen, once it is displayed.

CARP also has a quick entry mode. Type CARP <filename> and if the file exists you will be in the main menu (Screen 3). If CARP does not find the file, you will be asked if you want to create this file (Screen 2b).

Screen 2

After the welcome screen, you will be asked to choose one of the following:

a. Return to DOS:

b. Enter a project name: You will be provided with space to enter or edit a drive/path spec and a file spec for either a new project or an existing project. Note that these specs are in DOS format, e.g.

drive/path	d:\PRA\DATA\	
File	PRA_CR3	Extension is not necessary; CARP will add .DBF

Note: This could be a problem if there are other dBase files in the drive/path you entered.

If the drive/path/file spec you entered already exists, CARP will load it. Otherwise, you will be asked to verify that you want to create a new file with the spec you entered.

c. *Continue work on an existing project:* Upon selecting this option, you will be provided with a scrollable menu of CARP projects. Move the cursor to the desired project and select using the enter key.

Screen 3

You are now in CARP's main menu, which is shown in Figure 1. From the menu, you access all the features of CARP.

a. The first two choices, *append and edit*, allow you to add a record and edit an existing record respectively. The edit option will provide a scrollable list of components that have already been extended into the database. The append option will require that you enter component type and failure mode codes.

Note: Records in CARP are keyed to the component type code; that is, only one record may be entered for each type code.

Either option will send you to Screen 4.

b. The *delete* option gives you the capability to delete selected component type/failure mode combinations from the analysis. Information deleted in this step is not recoverable.

c. The *generate report* option sends you to CARPs report writer (Screen 6)

d. The *load generic data* option sends you to the generic data base - Screen 7.

e. The *return to project selection menu* returns you to Screen 2, from which you can

start a new project or return to DOS. All analysis is saved (or deleted) at this point.

Screen 4

CARP's data analysis is controlled from this screen, referred to as the 'General' screen. The screen shows and allows editing of the component name and failure mode, accepts plant specific data and allows the user to control some of the statistical analyses. To shift CARP into the editing mode, select Edit from the green menu at the bottom of the screen. Default choices have been placed in the Bayesian Updating and Final Selection of the screen. The Bayesian Updating section requires a simply Y or N (Yes or No) for whether a Bayesian Update 5 calculation should be performed. The choices for the final basis, or the recommended final statistic are:

P - Plant Specific
G - Generic
B - Bayesian

The preferred scheme for fitting values to a lognormal distribution (MN-EF) preserves the central tendency of the distribution. The optional scheme (EF-EF) preserves the spread of the distribution. These schemes are described in Appendix A. Striking the key F2 provides some help.

The green bar at the bottom of the screen provides the necessary program control options. Initially, CARP is in the display mode and the options include General, five numbered screens, Edit and Save. Selection of one of the five moves you to the screen containing those generic data sources, which are described under Screen 5. Selecting Edit shifts CARP to the editing mode, and selection of a numbered screen or the General screen allows editing of that screen. The Save option saves the data to disk and returns you to the main menu, Screen 3.

Once in the edit mode, the screen-to-screen movement is as described above. Editing the general screen is described below. Two new options now appear: AG CNTL and CALC. AG CNTL controls the aggregation methods from the three available choices:

T - Tolerance
A - Arithmetic
G - Geometric

and the weighting methods with choices:

Equal weights
User supplied weights (CARP will normalize these.)
Variance-related weights (Inversely proportional).

The CALC option begins the aggregation, Bayesian updating and other necessary calculations. Upon completion of the calculation, you will be returned to the General screen in the display mode.

Screen 5

There are 5 screens, labeled 1 to 4, 5 to 8, 9 to 12, 13 to 16, and 17 to 20. These show each generic data source, and can be assessed by first locating a desired screen with → or ← keys then ⊥. These screens operate identically.

Each generic source looks like:

	D	MEAN	LOWER	MEDIAN	UPPER	EF	WEIGHT
1							
LER	1	5.65-07	4.04-07		7.35-07		1.000
		5.65-07	4.22-07	5.57-07	7.35-07	1.3	

Note: NUREG/CR-1740; DATA FOR ALL REACTOR TYPES

Note: Failure rates and parameters MUST BE entered in the format

e.g. $5.876 \times 10^{-3} \rightarrow 5.87 - 03$

In order to edit the 'Note' field, you must move the cursor to the area and strike F5. This will allow you to type notes documenting your analysis. Strike <CTRL> W to exist and save from the note field.

Screen 6

The report writer control screen provides a series of scrollable menus to control the report options. The options selected are continuously displayed. The initial menu allows you to select one of the following:

- Options
- Printer
- Go
- Return

Options: Selecting options will lead you to a series of choices on how to configure your report. The first choice is between the summary and detailed reports (shown in Figure TBD.) The summary report always covers all type codes, but you will be required to choose a scope (final statistics only or all statistics) for your report. The detailed report will allow you to report on all type codes or a single, selected type code. Then it will provide a choice of the scope of the report. The final choice is whether you want text (Figure TBD) and/or interval bars (Figure TBD).

Printer: The printer options allow you to direct output to a Hewlett Packard (HP) Laserjet+, HP Laser Jet, other printer or a file. The Laserjet+ option requires that you write a batch file to download soft fonts. The HP Laserjet+ and HP Laserjet support both text and interval bars (graphics). Other printers generally can be configured to print out the text, but will not support

the interval bars. Postscript printers are not supported. The output can also be directed to a file. You can use your own word processor or spreadsheet software and printer to produce attractive output.

Go: Starts the printing or writing to a file. Caution, interval bars take a while.

Return: Takes you to the main menu

Screen 7

Screens 7, 8 and 9 are designed to assist you in efficiently finding generic data in the large data base that comes with CARP. Note that dBase III or IV can also be used to access the data base. (SAIC.dbf) The initial generic data search screen sets the strategy for accessing the data. Search strategy 1 asks you to input a type code and a failure mode code. The appropriate fields are filled in the data base but are not regularly updated. These fields are based on an analysts preferred coding scheme and are your responsibility to maintain. Unless a rigorous coding scheme is established and maintained, this search strategy is not recommended. Search strategy 2, the default strategy is recommended. Selecting this strategy brings up a scrollable list of component types. Choose a component type and you will be asked to choose from available failure modes. You will then either be given the option of refining the identification by choosing from a selection of component subtypes or, in some cases, you will be directly placed into Screen 8 for choosing subtypes.

Screen 8

Screen 8 allows further identification of the component using the component type attributes. The available choices appear in the scrollable menu in the box on the left side of the screen. The <enter> key is used to move selections into and out of the box on the right side of the screen. When the box on the right contains the proper entries, strike the F10 key to move to the next screen, screen 9, which displays the generic data sources.

Screen 9

Screen 9 is designed to display the generic data sources that meet the criteria specified in screens 7 and 8. This is the final screen before loading the generic data into the calculation portions of CARP (Screen 5). Note that using the right arrow key you can view additional information and data from the sources. In this screen, the delete key will toggle sources into and out of the analysis. Deleted or removed sources are marked with an asterisk. Once you have selected the desired sources, strike 'L' to load the data into the calculational portions of CARP. Additionally, the 'R' key is available to return to Screen 6 and search the data base.

DRAFT -- May 16, 1990

APPENDIX A: CARP

Aggregation

An aggregation method is needed to combine multiple data sources into a single estimate. When dealing with surrogate or generic data, aggregation of several acceptable sources is almost always better than searching for one source that could be considered optimal. A credible method of aggregation must consider each of the following:

- Data tolerance
- Data confidence
- Data relevance

Data tolerance deals with the difference in location (i.e., one source gives a higher number than another) between the available sources. The tolerance is generally not explainable, but often comes from slightly different engineering or statistical assumptions and rules used by in compiling different generic data sources. Since a generic data source that exactly matches the component in question, including component construction, design, operating policy and environment, maintaining this tolerance through aggregation ensures that the central estimate and bounding values consider the potential differences. Increasing the sample size will not reduce the measured tolerance, and ideally could only increase it.

The data confidence deals with the measurement error associated with how well the experimentally measure parameter represents the actual parameter. As the sample size increases, the confidence will decrease since it deals only with statistical errors and not with engineering non-homogeneities.

The data relevance deals with the appropriateness of data. Numerically, sources can be weighted based on their perceived relevance.

CARP uses the percentiles from the input cumulative distribution functions (CDFs) to arrive at the percentiles of the aggregate distribution. Before aggregation, the input distributions have been fit to lognormal forms. The method would work for any CDF with a closed form solution or numeric approximation, but since lognormal is the most common format for published generic data, CARP has only been programmed to handle the lognormal distribution. CARP will iteratively determine a percentile of the aggregate distribution using a recursive scheme with each input CDF. A Newton-Raephen type iteration is used to solve the following equation for the unknown λ as follows:

$$Pr\{\Lambda \le \lambda\} = \sum_{i=1}^{n} \alpha_i Pr\{\Lambda_i \le \lambda\}$$

where:

$Pr\{\Lambda \le \lambda\}$	The percentile of interest in the aggregate distribution. CARP will calculate the 5th, 50th, and 95th percentiles.
n	The number of input distributions
Λ_i	The random variables of the input distributions.
λ	The failure rate occurring at the percentile of interest in the aggregate distribution.
α_i	The weight of a distribution. We usually use equal weights making this quantity equal to 1/n.

The resultant aggregate is then fit to a lognormal distribution.

Bayesian Updates

The Bayesian update methodology of CARP is the commonly used method of conjugate priors. The gamma (Γ) distribution is used to perform the Bayesian calculations when the failure rate (per hour) is used. The α and β parameters that characterize the Γ distribution are related to the mean and variance of the lognormal as follows:

$$\alpha = \frac{\lambda}{\sigma^2}$$

$$\beta = \frac{\lambda^2}{\sigma^2}$$

The posterior mean and variance are calculated by:

$$\lambda' = \frac{K+\beta}{\tau+\alpha}$$

$$\sigma^2 = \frac{K+\beta}{(\tau+\alpha)^2}$$

where:

K = The number of failures.

τ The exposure time

The posterior distribution is then fit to a lognormal distribution.

Transformation and Fitting of Distributions

In several different portions of the code, CARP needs to transform a CDF into another functional form (lognormal) which preserves some general properties of the original CDF.

Gamma to Lognormal

Following a Bayesian update, a gamma distribution ($\Gamma(\alpha,\beta)$) is transformed into a lognormal ($\mathcal{L}$,ef) as follows:

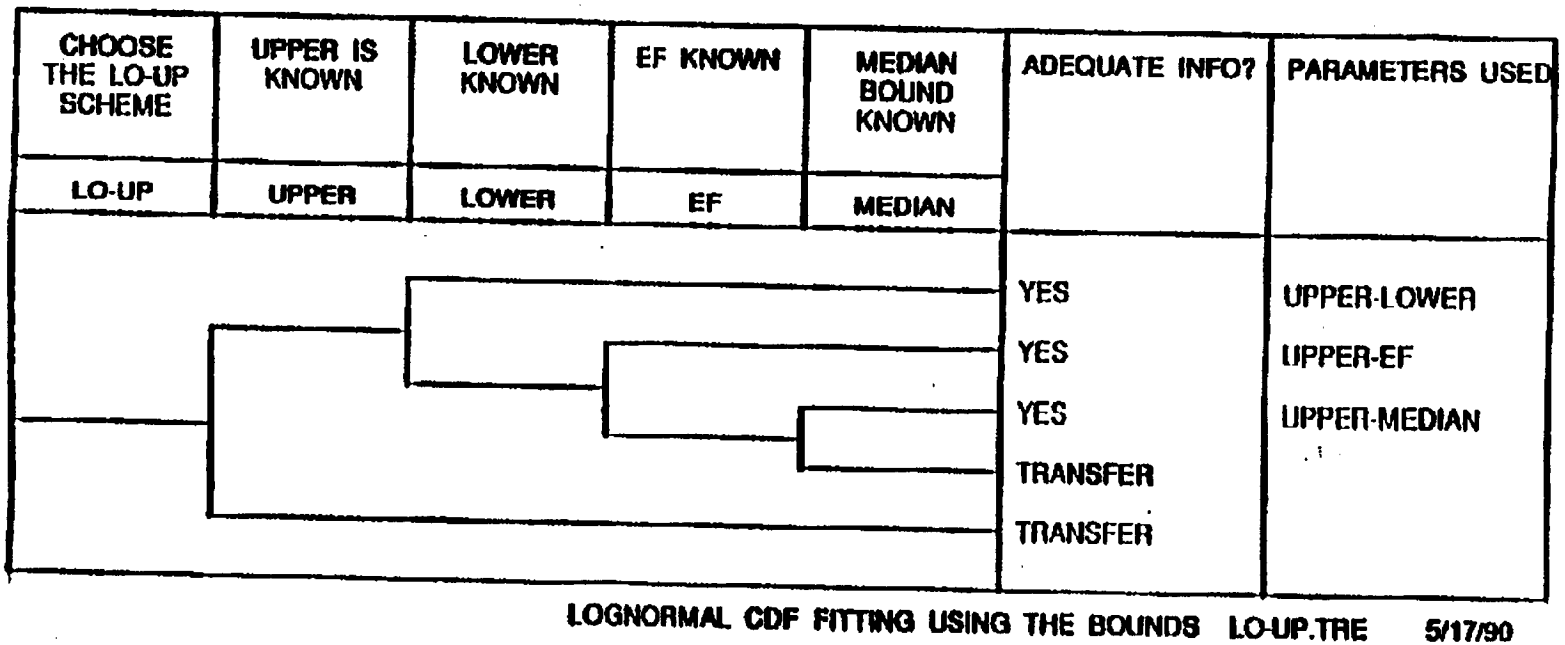
$$\sigma = \sqrt{\ln(1/\alpha^2 + 1)}$$

$$x = \frac{\alpha}{\beta} e^{-\sigma^2/2}$$

$$ef = e^{1.645\sigma}$$

General or Unspecified to Lognormal

Two parameters (any 2 of the mean, median, ef, variance, or percentiles) are required to define a lognormal distribution. The CARP code uses this characteristic and allows a choice between two schemes for distribution fitting. The first, and the default method, called Mean-EF, focuses on the knowledge of the data's central tendencies and as shown in the event tree of Figure 2, places a priority toward using the mean or median. The second, called Lower-Upper, focuses on the bounding values and allows the central estimates to shift. As shown in Figure 3, this method places a priority toward using the bounding values or the error factor. Note that if the bounds are not available, this method then shifts to the logic encompassed shown in Figure 2.



LOGNORMAL CDF FITTING USING THE BOUNDS LO-UP.TRE 5/17/90

Figure 27

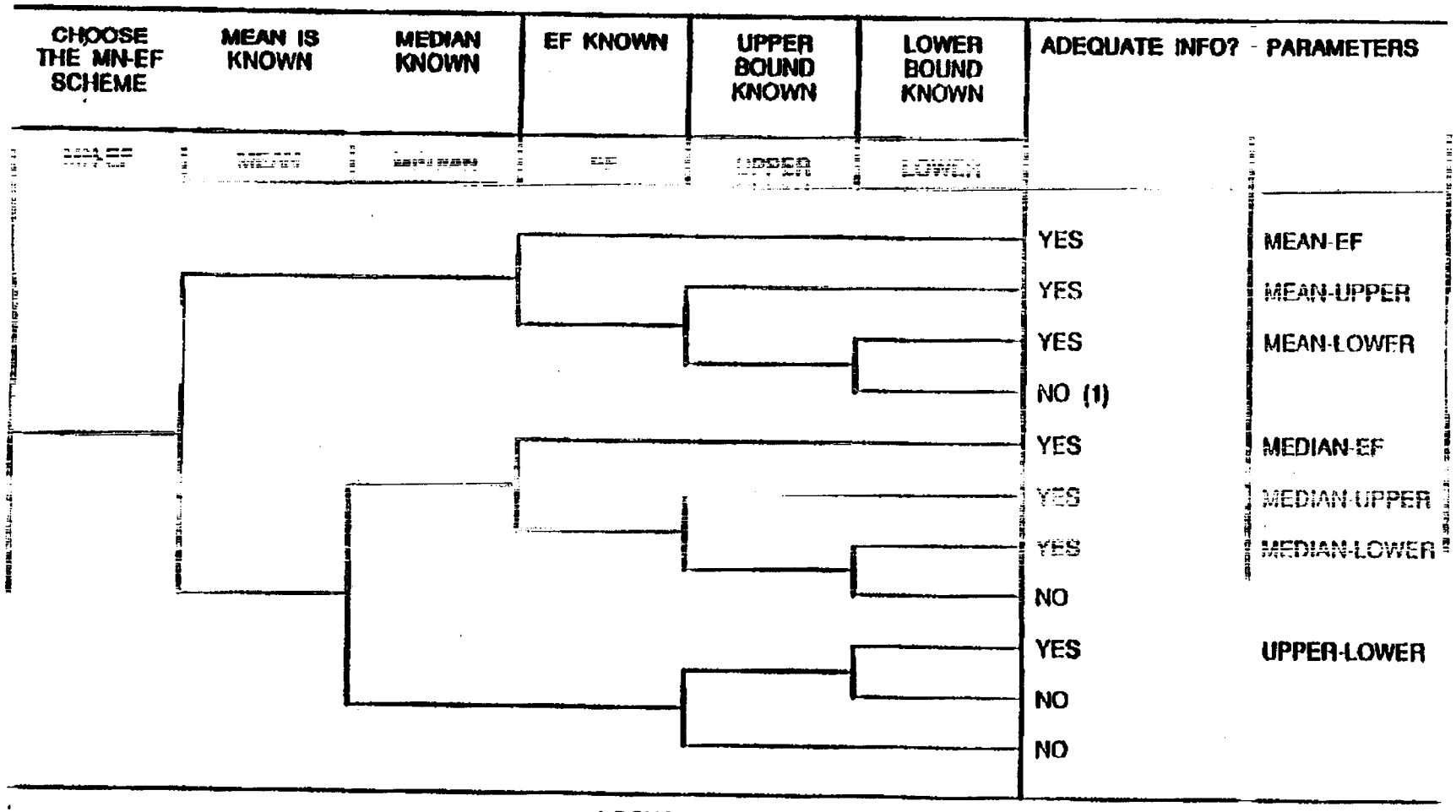

CHOOSE THE MN-EF SCHEME
MEAN IS KNOWN
MEDIAN KNOWN
EF KNOWN
UPPER BOUND KNOWN
LOWER BOUND KNOWN
ADEQUATE INFO?
PARAMETERS
YES
YES
YES
NO (1)
YES
YES
YES
NO
YES
NO
NO
MEAN-EF
MEAN-UPPER
MEAN-LOWER
MEDIAN-EF
MEDIAN-UPPER
MEDIAN-LOWER
UPPER-LOWER
LOGNORMAL CDF FITTING USING MEAN AND EF MN-EF.TRE 5/16/90

Figure 2R

CARP

(COMPUTERIZED AGGREGATION OF RELIABILITY PARAMETERS)

What is CARP?

CARP is an analysis tool [illegible] to perform the effort required to quantify component failure rates. It includes a C[illegible] Data Base, and [illegible] to interactively extract data from the Generic Data Base, aggregate the data [illegible] plant specific data, perform Bayesian [illegible] store, and print the results. These processes are integrated and controlled by a user-friendly menu system, providing a useful [illegible]-based system.

The Generic Data Base contains an [illegible] collection of component failure data from published sources and [illegible] from the nuclear, military, a[illegible] and other industries. The breadth of this data base exceeds that necessary to quantify a nuclear power plant PRA and the data base is several sources deep for most [illegible] failure modes [illegible].

The aggregation method used by CARP ensures that the information from more than one generic data source can be correctly used in an analysis. SAIC has performed the research and development necessary to find and apply an aggregation method that combines sources in a manner such that the inter- and intra-source variabilities are retained and fully propagated in the final statistics. (Most generic data analysis methods either discard all but one source or combine sources in a manner that shrinks the final variability excessively.)

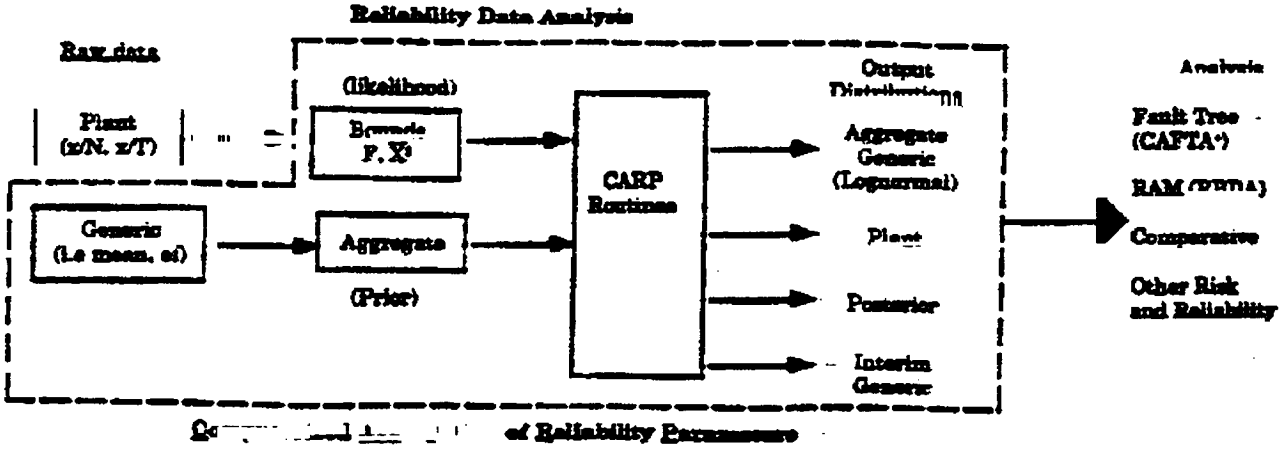
The aggregation, Bayesian updating, and data handling routines give engineers the powerful statistical tools, and present the tools and the output statistics in an easily interpretable manner. This significantly enhances the speed and accuracy of reliability data analysis.

Why CARP?

A detailed risk or reliability analysis will invariably proceed to a point at which quantitative failure rate information is needed. The ideal source for estimating a component failure rate is to have complete, detailed records of the [illegible] in question's performance. However, few components in nuclear power plants and other technological applications fail more often than once per year, and many fail much less frequently. Therefore, field data is rarely adequate to quantify, with reasonable statistical accuracy, component failure rates. In these cases, analogous or generic data must be used. SAIC has developed an extensive collection of generic data from published sources in the nuclear industry, SAIC-performed plant specific data analyses, and published non-nuclear (chemical, aerospace, off-shore oil, military, etc.) sources. CARP provides the benefit of SAIC's reliability data collection and analysis experience in an easy to use PC software package.

What has CARP been used for?

- For research and development in creating a Generic Data Base.
- To compile and quantify the generic data base for several nuclear power plant PRAs.
- Assorted reliability analyses in the nuclear power, non-nuclear power and aerospace industries.



Computation of Reliability Parameters

For Further Information Contact: *Gary DeMoss, McLean, VA (703) 448-6485*
Joseph R. Fragola, New York, NY (212) 661-5780

Appendix D:

Estimating the Exponential Failure Rate from Data with No Failure Events

August 24, 1990

MEMORANDUM

TO: Gary DeMoss, Ernie Lofgren
FROM: Dr. Martin Shooman, Pete Appion.....

SUBJECT: Zero Failures

Introduction
We recently used CARP to analyze some interval failure rate data where zero failures had occurred. The purpose of this memo is to explore the mathematics behind how CARP apparently treats such a situation.

Confidence Limits
The basic mathematical work on confidence limits for test data from an exponential distribution (constant hazard) was done by Epstein and Sobel [1], they showed that if the variable 2r

$$2r = 2n\hat{T}\lambda \qquad (1)$$

where,

r = number of failures,
n = number on test,
T = test hours,
λ = failure rate

had an χ^2 distribution with 2r degrees of freedom at the lower confidence bound and (2r+2) degrees of freedom at the upper confidence bound.

Also, it is well known that the maximum likelihood estimate $(\hat{\lambda})$ is given by $\frac{r}{n\hat{T}}$.

Problem With Zero Failures

The problem with zero failures is that the maximum likelihood estimate $(\hat{\lambda})$ goes to zero and the lower confidence bound is no longer defined since the number of degrees of freedom of the χ^2 distribution is zero. The upper confidence bound is still clearly defined, and the upper 95% bound on the variable $2nT\lambda$ for a χ^2 distribution with 2 degrees of freedom is 5.991. Using this value, the upper bound on (λ) is given by,

$$\lambda < \frac{5.991}{2nT} = \frac{2.995}{nT} = \frac{3}{nT} \qquad (2)$$

Since we are unable to define a lognormal distribution with a single data point, there is a difficulty in using CARP. Some analysts say to assume one failure and calculate a point estimate of the failure rate using $\frac{1}{nT}$. Welker, and Lipow [2] have investigated this in depth and based on a number of different statistical estimation principles they suggest that one use as the point estimate.

$$\left(\frac{1}{3} \times \frac{1}{nT}\right) \qquad (3)$$

Using the values given by Equations (2) and (3) as the upper confidence limit and the mean, we can define a distribution.

Calculation Using CARP

Experiments with CARP for a specific example lead to the conclusion that CARP also uses the value $\left(\frac{1}{3} \times \frac{1}{nT}\right)$ for the mean and $\frac{3}{nT}$ for the upper 95% confidence limit.

The following example was entered into the CARP program:

The input data for the first run was;
Number of failures = 0
Exposure time = 67832 hours.

The results are shown in Table 1 and hand calculations verify that the upper confidence limit is computed from $\frac{3}{nT}$ and the mean is from $\left(\frac{1}{3} \times \frac{1}{nT}\right)$.

One can also verify by taking the ratio of the 95% point to the 50% point or the ratio of the 50% point to the 5% point, that the error factor for a lognormally distributed distribution determined by these two points is approximately 15.

This was also repeated by using as input the upper 95% confidence limit and the mean calculated from $\frac{3}{nT}$ and $\left(\frac{1}{3} \times \frac{1}{nT}\right)$, and CARP computed the same results which are shown in Table 2 which are identical with Table 1. Therefore, we conclude that in the zero failure case CARP uses Equations (2) and (3).

References:

(1) Epstein, B. and M. Sobel, "Life Testing", J. Am. Statist. Assoc., vol. 48, no. 263, pp. 486-502, September, 1953.

(2) Welker, Everett and Myron Lipow, "Estimating the Exponential Failure Rate from Data with No Failure Events", Proceedings 1974 Annual Reliability and Maintainability Symposium, pp. 420-427.

CARP -- DATA ANALYSIS DETAILED REPORT

Component Type Code: A Component Name: ZERO FAILURES TRY
Failure Mode Type Code: 2 Failure Mode: CALCULATE λ USING ZERO FAILURES

	D	MEAN	LOWER	MEDIAN	UPPER	EF
Plant-specific	L	4.91-06			4.42-05	
Interim aggregated					4.42-05	
Aggregated generic	L	1.14-05	1.96-07	2.95-06	4.42-05	15.0
Bayesian updating						
Final	L	4.91-06	8.45-08	1.27-06	1.90-05	15.0

PLANT-SPECIFIC DATA

Units (N for demands, H for hours, etc.): H
Number of failures: (ZERO FAILURES ASSUMES 1/3 FAILURE)
Exposure (time or number of demands): 67832

BAYESIAN UPDATING

Bayesian updating performed: N

FINAL

Final basis (P,G,B): P
Lognormal fitting method used: LO-UP

AGGREGATION DETAILS

Aggregation method (T,A,G): T Weighting method (E,I,P,U,S): E

	MEAN	LOWER	MEDIAN	UPPER	EF	FAILURES	EXPOSURE	WEIGHT
1 ---								
95TH AND ERROR FACTOR				4.42-5	15.0			1.000
	1.14-05	1.96-07	2.95-06	4.42-05	15.0			

TABLE 1

Results of using CARP to fit a lognormal distribution for the case of zero failures in 67632 hours

CARP -- DATA ANALYSIS DETAILED REPORT

Component Type Code: A Component Name: ZERO FAILURES TRY
Failure Mode Type Code: 2 Failure Mode: Using Mean and Upper

	D	MEAN	LOWER	MEDIAN	UPPER	EF
Plant-specific	L					
Interim aggregated		4.91-06			4.42-05	
Aggregated generic	L	4.91-06	8.44-08	1.27-06	1.90-05	15.0
Bayesian updated						
Final	L	4.91-06	8.44-08	1.27-06	1.90-05	15.0

PLANT-SPECIFIC DATA
Units (N for demands, H for hours, etc.): H
Number of failures:
Exposure (time or number of demands):

BAYESIAN UPDATING
Bayesian updating performed: N

FINAL
Final basis (P,G,B): G
Lognormal fitting method used: MM-EF

AGGREGATION DETAILS

Aggregation method (T,A,G): T Weighting method (E,I,P,U,S): E

	MEAN	LOWER	MEDIAN	UPPER	EF	FAILURES	EXPOSURE	WEIGHT
1								
MEAN UPPER	4.91-6			4.42-5				1.000
	4.91-06	8.44-08	1.27-06	1.90-05	15.0			

NOTE: Mean and Upper were calculated by using [mean = ((1/3)/T) and Upper = (3/T)]

TABLE 2

Results of using CARP to fit a lognormal distribution for the case of mean = 4.91E-6 and an Upper bound = 4.42E-5

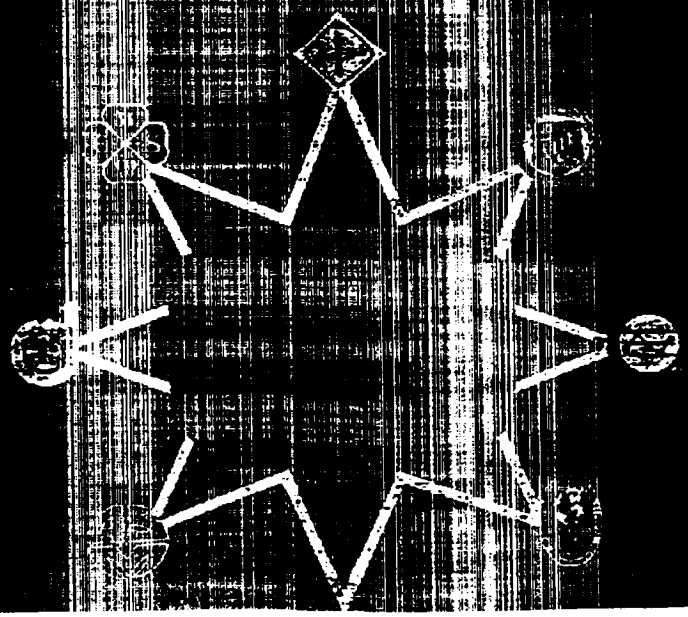
PROCEEDINGS

1974 ANNUAL

RELIABILITY AND MAINTAINABILITY

SYMPOSIUM

LOS ANGELES, CALIFORNIA, JAN. 29-30, 31-1974



1194

ESTIMATING THE EXPONENTIAL FAILURE RATE FROM DATA WITH NO FAILURE EVENTS

Everett L. Welker
TRW Systems Group
Redondo Beach, California

Myron Lipow
TRW Systems Group
Redondo Beach, California

Descriptors: 411, 422, 410
(ASQC Literature Classification System—see page xiii)

Introduction

Assume an exponential failure pattern with unknown constant failure rate λ. Suppose that there are n failures in T operating part hours. The maximum likelihood and unbiased estimate of λ is $\hat{\lambda}$, given by the formula [1]

$$\hat{\lambda} = n/T, \; n = 0, 1, 2, \ldots \; .$$

This estimate is routinely used except for the zero failure case. If no failures occur in the test, the estimate

$$\hat{\lambda} = 0/T = 0$$

is usually considered to be unsatisfactory in spite of the fact that it is an unbiased value derived by the maximum likelihood method. This point of view reflects the judgement that a non-zero failure rate really does apply but that the test time, T, has by chance been too short to exhibit a failure event. There is no generally accepted method for handling this zero failure problem. In this paper, we will describe some alternative approaches, with emphasis on methods which modify the maximum likelihood formula when $n = 0$ but leave it unchanged when $n \geq 1$.

The Basic Mathematical Relationships Involved In Estimating the Constant Failure Rate

Consider first an approach in which the maximum likelihood estimate is modified for $n = 0$ but is unchanged for $n \geq 1$. The estimation formula can be written as

$$\hat{\lambda} = f(T)/T \qquad \text{for } n = 0$$

and

$$\hat{\lambda} = n/T \qquad \text{for } n = 1, 2, \ldots \; .$$

where n is the number of failures observed in test time T. Thus the modification in the formula is expressed as a change from zero in the numerator to f(T). We will discuss a number of modifications in which f(T) is assigned a constant value independent of test time. It is obvious that we should restrict f(T) by the inequality

$$0 < f(T) \leq 1.$$

The lower bound assures that the estimate is positive. The upper bound assures that our failure rate estimate for zero failures is not greater than the estimate when a failure event occurs.

With respect to the population, the following formulas are pertinent. The time to failure density function is

$$u(t) = \lambda e^{-\lambda t} \qquad 0 \leq t < \infty$$

$$= 0 \qquad -\infty < t < 0.$$

The probability of n failures in T operating part hours is

$$f(n,T) = \frac{(\lambda T)^n e^{-\lambda T}}{n!}, \; n = 0, 1, 2, \ldots$$

Return to a consideration of the alternative approach in which the maximum likelihood estimate is used for all cases except the one in which no failures occur in a test time of T part hours. The estimator for zero failures is given by $\hat{\lambda} = k/T$ where k is the value of f(T), either a constant for all T or the value obtained by substituting the specific value of T in the function f(T).

The probabilities for the different values of $\hat{\lambda}$ are as follows.

Number of Failures	$\hat{\lambda}$	Probability
0	k/T	$e^{-\lambda T}$
$n = 1, 2, \ldots$	n/T	$(\lambda T)^n e^{-\lambda T}/n!$

The average or expected value of the estimator is

$$E[\hat{\lambda}] = \frac{k}{T} e^{-\lambda T} + \lambda.$$

The variance of $\hat{\lambda}$ is

$$\sigma^2_{\hat{\lambda}} = \frac{1}{T^2}\left[\lambda T - 2k\lambda T e^{-\lambda T} + k^2 e^{-\lambda T} - k^2 e^{-2\lambda T}\right].$$

The mean and variance of the maximum likelihood estimator, $\hat{\lambda}$, are obtained by letting $k = 0$ in the above expressions. This gives

$$E[\hat{\lambda}] = \lambda \quad \text{and} \quad \sigma^2_{\hat{\lambda}} = \frac{\lambda}{T}.$$

The bias in the modified estimator is

$$\frac{k}{T} e^{-\lambda T}.$$

Two Commonly Used Constant Replacements For Zero in Estimating Failure Rates

The literature contains numerous instances in which the zero failure problem has been handled by using a somewhat arbitrarily selected number of failures in lieu of the observed number, zero. The most frequently encountered selections are unity and one half. These two values are suggested on the basis of very similar logic. In a sense, each of them yields a reasonable upper bound on the failure rate estimate in the zero failure case. We have already observed that it would be illogical to replace zero failures by more than one failure, so unity is indeed

an upper bound from the common sense viewpoint. The use of one half is a direct application of the Yates correction in community. Observed data yield only integral numbers of failures, so one interprets the occurrence of n failures as covering a range from n - 0.5 to n + 0.5. Thus, we would say that n = 0 covers the range from 0 up to n = 0.5 and therefore n = 0.5 is a logical upper bound to use in estimating the failure rate in the zero failure case.

Evaluations of these two estimates will be presented later in this paper. However, we would like to comment here about one basic weakness in the use of a constant replacement for zero, independent of the time duration of the test. Suppose two separate tests have been performed with n_i failures in T_i hours, i = 1 and 2. These tests generate failure rate estimates $\hat{\lambda}_i = n_i/T_i$. Now consider the estimate generated by combining the experience from the two tests.

$$\hat{\lambda} = \frac{n_1 + n_2}{T_1 + T_2}.$$

Suppose $\hat{\lambda}_1 < \hat{\lambda}_2$. It is easy to show that $\hat{\lambda}_1 < \hat{\lambda} < \hat{\lambda}_2$. That is to say, combining test data from two tests gives an estimate intermediate between the estimates for the separate tests. Now consider the case in which $n_1 = n_2 = 0$ and we use a constant k which satisfies $0 < k < 1$ instead of zero. We then have

$$\hat{\lambda}_1 = k/T_1,\ \hat{\lambda}_2 = k/T_2 \text{ and } \hat{\lambda} = k/(T_1 + T_2).$$

In this case, $\hat{\lambda}$ is not between $\hat{\lambda}_1$ and $\hat{\lambda}_2$ - rather it is smaller than either. This is not a serious problem, but it does constitute a slight inconsistency.

Before we leave the subject of the use of a constant replacement for zero in the failure rate estimation formula, we would like to reference one other approach which is similar to the use of 0.5 as discussed above. Suppose we agree to record failure rates to six decimal places. Proper rounding procedures would yield interpretations as follows. If

$$\hat{\lambda} = .000002,$$

we would interpret this to mean

$$.0000015 < \hat{\lambda} < .0000025$$

We would say, therefore that in the zero failure case,

$$\hat{\lambda} = .000000$$

really means

$$.000000 < \hat{\lambda} < .0000005$$

and the seven decimal upper bound would be an eminently appropriate estimate.

The Use of an Upper Confidence Limit in Lieu of a Point Estimate in the Zero Failure Case

Perhaps the most common approach in the zero failure case is to replace the $\hat{\lambda} = 0$ point estimate by an upper confidence limit. For n = f failures in T hours, an upper confidence limit at confidence level α is ([2], p. vii),[3].

$$\chi^2_{\alpha,\ 2f\ +\ 2}/2T.$$

Therefore, for zero failures, the use of the upper confidence limit for the point estimate is expressed by the formula

$$\lambda = \chi^2_{\alpha,\ 2}/2T,$$

In effect, this replaces f = 0 by

$$f = \chi^2_{\alpha,\ 2}/2.$$

There is no agreement on a preferred confidence level, α, but the values 50 percent and 60 percent seem to predominate. Table 1 shows the replacement values of f for these two confidence levels and for three other levels which will be needed in the discussion to follow.

100 α Percent	$\chi^2_{\alpha,\ 2}/2$
39.3	.5
40	.511
50	.693
60	.916
63.2	1.000

TABLE 1.

The values of α included in Table 1 cover a range from one half to one in the number of failures which are used in place of zero in the failure rate estimation formula. Since $\chi^2_{\alpha,\ 2}/2$ increases with α, it would be illogical to consider any α larger than 63.2 percent. At the low end, we rather arbitrarily stopped at α = 39.3 percent, the level which generated the failure replacement value of 0.5. The 40 percent level is shown because it is the closest level to 39.2 which is readily available in published tables of the χ^2 distribution. Indeed it has been suggested that the 60 percent level is often used because it is available in published tables and it is close to the level α = 63.2 percent which yields a replacement of zero by unity.

Is It Logical to Use a Confidence Limit As a Point Estimate?

There is a fundamental difference between a point estimate and a confidence limit. Therefore, it is appropriate to consider the implications of this difference on the use of a confidence limit as an estimate of the failure rate in the zero failure case. We recognize that any estimation method is acceptable if it generates good answers regardless of the purposes for which it was developed. However, analyses of the original purpose and of the properties of the estimation method itself may shed some light on the logic of the novel application under consideration. For purposes of brevity and emphasis we will oversimplify this discussion.

A point estimate is an answer to the following question. Based on a specific set of sample observations, what is the best guess I can make as to the single value of a particular population parameter? In our case the parameter is the constant failure rate. On the other hand, a confidence limit answers an entirely different question. For each possible population parameter value, we ask the following question. If this were the true population parameter, would a sample at least as good as the observed one be likely or unlikely? The answers for all possible parameter values are summarized by dividing them into two groups, one containing all values for which the observed sample is likely and the other containing the values for which it is unlikely. A boundary between these two groups is a confidence limit. A useful approximate summary is as follows. A point estimate is an answer to the question, given a sample, what can I say about the population? A confidence limit, on the other hand, is derived by considering the probabilities of obtaining certain samples from different populations. We should note that the term "best

guess" must be defined for obtaining a point estimate and quantitative levels for likely and unlikely must be specified in obtaining a confidence limit.

The concepts of point estimate and confidence limit are illustrated in Figure 1. A test for T hours yielded two failures giving a point estimate of $\hat{\lambda} = 2/T$. The 60 percent upper confidence limit is 3.11/T. A sample at least as good in this case is one with zero, one or two failures. The probability of such a sample is at least 1-0.60 = .40 if $\lambda \leq 3.11/T$ and it is no more than 0.40 if $\lambda > 3.11/T$. Thus, all values of λ in the range zero to 3.11/T are classified as being likely and those above 3.11/T are classified as unlikely at the 60 percent confidence level. Of course the point estimate appears as a single point, the best guess of the value of λ based on the observed sample.

It is apparent that the upper confidence limit is really quite different from a point estimate. Indeed, it much more logical to compare or match the point estimate to the entire interval, $0 \leq \lambda \leq 3.11/T$, rather than to focus attention on the upper limit of this interval. We might well consider some point within the interval as a more appropriate analogue of the point estimate, as, for example, the midpoint, 1.555/T. We wish to emphasize, however, that in spite of the fundamental difference between the concepts of a point estimate and an upper confidence limit, it is entirely appropriate to use the confidence limit to derive a point estimate for the zero failure case if the estimate has the required desirable properties.

It has been suggested in some reports that the 50 percent upper confidence limit is appropriate in lieu of a point estimate because the 50 percent limit is just as likely to be above the true value as below it. This reasoning appears to be a somewhat incorrect interpretation of the basic confidence interval concept. Consider the following description for the constant failure rate estimation. For a population with failure rate λ, the probability of n failures in T hours is

$$(\lambda T)^n e^{-\lambda T}/n!,$$

the maximum likelihood estimate is

$$\hat{\lambda} = n/T,$$

and the upper confidence limit on $\hat{\lambda}$, denoted by $\hat{\lambda}_u$, at level α is

$$\lambda_u = \chi^2_{\alpha,\ 2n\ +\ 2}/2T,\quad n = 0, 1, 2 \ldots .$$

We can then say that the probability of obtaining an upper confidence limit of

$$\hat{\lambda}_u = \chi^2_{\alpha,\ 2n\ +\ 2}/2T$$

is

$$(\lambda T)^n e^{-\lambda T}/n!,\quad n = 0, 1, 2, \ldots .$$

It can be shown that α is the probability that $\hat{\lambda}_u > \lambda$.

Now consider the 50 percent level. It is true that, considering all numbers of failures, $n = 0, 1, 2, \ldots$, 50 percent of the upper confidence limits would be expected to exceed the true population rate, and 50 percent would not. When there are no failures, the 50 percent upper confidence limit is .693/T, and this is the suggested point estimate when using the upper confidence limit in lieu of $\lambda = 0$.

Consider two categories of possible values of the true population failure rate.

1. If $\lambda < .693/T$, the probability of zero failures in time T is greater than 0.5 so $\hat{\lambda}_u = 6.93/T$ exceeds λ more than half of the time.

2. If $\lambda > .693/T$, the probability of zero failures in time T is less than 0.5 so $\hat{\lambda}_u = .693/T$ exceeds λ less than half of the time.

In order to get the even split of confidence limits — one-half above and one-half below — we would have to include confidence limits for the cases with failure events along with the zero failure value. Therefore, regardless of the true λ, if we use the 50 percent upper confidence limit as a point estimate only for the zero failure case, we do not have an estimator which is as likely to be too high as too low.

A Solution For the Zero Failure Case Using a Modification of the Upper Confidence Limit

Let us now consider some of the relationships between the maximum likelihood point estimate and the upper confidence limit for the constant failure rate case:

$$\left.\begin{array}{ll} \text{Point Estimate} & \hat{\lambda} = n/T \\ \text{Upper Confidence Limit:} & \hat{\lambda}_u = \chi^2_{\alpha,\ 2n\ +\ 2}/2T \end{array}\right\} n = 0, 1, 2, \ldots .$$

Certain significant facts about $\hat{\lambda}$ and $\hat{\lambda}_u$ are revealed in the following tabulation

Number of Failures n	$\hat{\lambda}T$	$\hat{\lambda}_u T$		
		$\alpha = .40$	$\alpha = .50$	$\alpha = .60$
0	0	.51	.69	.92
1	1	1.38	1.68	2.02
2	2	2.29	2.67	3.11
3	3	3.21	3.67	4.18

TABLE 2

For convenience, we have tabulated $\hat{\lambda}T$ and $\hat{\lambda}_u T$ rather than $\hat{\lambda}$ and $\hat{\lambda}_u$. The upper confidence limit $\hat{\lambda}_u$ increases with the confidence level α for each n and it also increases with n for each α. We also observe that, for any particular α, the net difference and the percentage difference between $\hat{\lambda}$ and $\hat{\lambda}_u$ approach zero as the number of failures increases. This observation lead us to consider the following approach to the zero failure case.

Consider the ratio between the point estimate, $\hat{\lambda}$, and the upper confidence limit, $\hat{\lambda}_u$, for a selected value of α and for various numbers of failures, n. We first selected $\alpha = .60$ and we computed $\hat{\lambda}_u/\hat{\lambda}$ and $\hat{\lambda}/\hat{\lambda}_u$ for $n = 0, 1, 2, \ldots, 10$. The results are listed in Table 3.

An examination of the ratios in Table 3 led us to consider the possibility of modifying the zero failure estimate by some type of extrapolation of the ratios for the cases with failures. The method is illustrated in Figure 2. Consider first the upper curve which shows the ratio $\hat{\lambda}_u/\hat{\lambda}$ for $n = 1, 2, \ldots, 10$ with a smooth curve connecting the points from $n = 2$ to $n = 10$. For $n = 0$, the curve would approach the vertical axis as an asymptote for the maximum likelihood zero failure estimate. In lieu of this, we decided to make an extrapolation of the $\hat{\lambda}_u/\hat{\lambda}$ curve back to the vertical axis, find the intercept, and compute a modified estimate for the failure rate for $n = 0$. The curve shows a straight line extrapolation, using the line through the points for $n = 1$

n	$\hat{\lambda}_u/\hat{\lambda}$	$\hat{\lambda}/\hat{\lambda}_u$
0	∞	0
1	2.022	.494
2	1.653	.644
3	1.392	.719
4	1.309	.764
5	1.258	.795
6	1.224	.817
7	1.199	.834
8	1.179	.848
9	1.164	.859
10	1.152	.868

Ratios Between Point Estimates and Upper Confidence Limits, α = .60

TABLE 3

and n = 2. This line intersects the axis in the point (0, 2.5). The 60 percent upper confidence limit for n = 0 is .916/T. Therefore, a modified $\hat{\lambda}$ for n = 0 is obtained by solving the equation .916/T$\hat{\lambda}$ = 2.5 giving $\hat{\lambda}$ = .366/T. Using parabolic interpolation through the points for n = 1, 2, and 3, the estimate is $\hat{\lambda}$ = .327/T. As we increase the degree of the curve, we would approach the maximum likelihood estimate $\hat{\lambda}$ = 0 as a limit. We chose to consider only the linear extrapolation for simplicity. The lower curve in Figure 3 shows the reciprocal ratio, $\hat{\lambda}/\hat{\lambda}_u$ and the linear extrapolation of this curve gives a zero failure estimate of $\hat{\lambda}$ = .316/T.

If this modification method is to be worthy of serious consideration as a possible solution for the zero failure problem, we must establish that it does have reasonably suitable properties. One immediate question related to the sensitivity of the answer to the confidence level. To check on this, we computed modified estimates for various values of α by both ratios as shown in Table 4.

Confidence Level, α	$\hat{\lambda}$ Estimate Based On	
	$\hat{\lambda}_u/\hat{\lambda}$	$\hat{\lambda}/\hat{\lambda}_u$
.40	.32	.30
.50	.34	.31
.60	.37	.32
.63	.38	.32

TABLE 4

These estimates do cover the relatively small range from $\hat{\lambda}$ = .30 to $\hat{\lambda}$ = .38, so sensitivity to the selection of α does not seem to be a problem. We will discuss other properties of the estimate later.

The Use of Bayesian Statistics to Solve the Zero Failure Problem

Since Bayesian statistical methods provide for the combination of prior information or hypotheses with current test data, they offer a plausible approach for solving the zero failure problem of interest here. Therefore, we have considered Bayesian methods to obtain failure rate estimates based on a number of prior distributions of the population failure rate, λ. We will briefly review the basic equations of Bayesian estimation and then we will summarize the results which were obtained.

The basic formula of the Bayesian method adapted to the failure rate estimation problem is

$$w(\lambda|n = f) = \frac{P(n = f|\lambda)\, w(\lambda)}{P(n = f)}$$

where the symbols are defined as follows.

- n — is a general symbol for the number of observed failures in T part hours
- f — is the number of failures observed in a particular test of T part hours
- λ — is the unknown constant part failure rate
- $w(\lambda)$ — is the prior distribution or the assumed density of λ
- $P(n = f|\lambda)$ — is the conditional probability of observing f failures, given the value of λ.
- $P(n = f)$ — is the unconditional probability of observing f failures based on the assumed prior.
- $w(\lambda|n = f)$ — is the posterior distribution of λ, conditional on the observation of f failures, assuming the prior, $w(\lambda)$.

The function $P(n = f)$ is determined by forming the joint density of n and λ, setting n = f, and integrating on λ.

For present purposes, we need these functions for the exponential population with failure rate λ. They are

$$P(n = f|\lambda) = \frac{(\lambda T)^f}{f!} e^{-\lambda T}$$

The joint density of n, λ is

$$P(n = f|\lambda)w(\lambda) = \frac{(\lambda T)^f}{f!} e^{-\lambda T} w(\lambda)$$

Therefore

$$P(n = f) = \int_{\lambda_1}^{\lambda_2} \frac{(\lambda T)^f}{f!} e^{-\lambda T} w(\lambda) d\lambda$$

where λ_1 and λ_2 are the endpoints of the range for which $w(\lambda) > 0$. Then

$$w(\lambda|n = f) = \frac{\frac{(\lambda T)^f}{f!} e^{-\lambda T} w(\lambda)}{\int_{\lambda_1}^{\lambda_2} \frac{(\lambda T)^f}{f!} e^{-\lambda T} w(\lambda) d\lambda}$$

To use this relationship, it is necessary to select a specific function for $w(\lambda)$. We are interested in examining the properties of the posterior function, $w(\lambda|n = f)$, corresponding to various selections for $w(\lambda)$.

A natural first choice is

$$w(\lambda) = a, \quad 0 < \lambda < 1/a$$
$$= 0 \quad \text{for all other } \lambda.$$

This prior generates the posterior

$$w(\lambda \mid n = f) = \frac{(\lambda T)^f}{f!} e^{-\lambda T} \Big/ \int_0^{1/a} \frac{(\lambda T)^f}{f!} e^{-\lambda T}\, d\lambda.$$

The integral in the denominator can be written in terms of the incomplete gamma function denoted by I(u,p) and defined by the integral [2, p. v]

$$I(u,p) = \frac{1}{p!} \int_0^u v^{p+1} v^p e^{-v} dv.$$

By appropriately expressing the denominator in the form of the incomplete gamma function and simplifying the resulting expression, we obtain

$$w(\lambda \mid n = f) = \frac{(\lambda T)^f e^{-\lambda T}}{f! \sqrt{f+2}\, I(T/a \sqrt{f+1}, f)}.$$

It is customary to use the mean of the posterior distribution of λ as an estimate, $\hat{\lambda}$. In this case, then,

$$\hat{\lambda} = \int_0^{1/a} \lambda\, w(\lambda \mid n = f)\, d\lambda$$

which, upon integration becomes

$$\hat{\lambda} = \frac{(f+1)\sqrt{f+1}\; I(T/a \sqrt{f+2}, f+1)}{T \sqrt{f+2}\; I(T/a \sqrt{f+1}, f)}.$$

We decided to use two values of the constant a in this study. It was natural to let a = T since this restricts λ to the range from zero to 1/T as discussed above. As a matter of academic interest, we did want to consider the limiting case as a approaches zero. We then obtain the following estimation formulas.
For a = T,

$$\hat{\lambda} = \frac{(f+1)\sqrt{f+1}\; I(1/\sqrt{f+2}, f+1)}{I(1/\sqrt{f+1}, f)}.$$

For $a \to 0$

$$\hat{\lambda} = \frac{f+1}{T}.$$

For small numbers of failures, f, the following estimates are obtained for these cases.

f	$\hat{\lambda}$ a = T	$\hat{\lambda}$ $a \to 0$
0	.412/T	1/T
1	.506/T	2/T
2	.610/T	3/T
3	.744/T	4/T

It was decided to look also at the gamma prior density

$$w(\lambda) = k^{a+1} \lambda^a e^{-k\lambda},\ k > 0,\ a > -1,\ 0 \leq \lambda < \infty.$$

Using the same mathematical relationships as before, we obtain

$$w(\lambda \mid n = f) = \frac{(T+k)^{a+f+1} \lambda^{a+f} e^{-(T+k)\lambda}}{(a+f)!}$$

and the failure rate estimate

$$\hat{\lambda} = \frac{a+f+1}{T+k}.$$

Since this paper is concerned with the zero failure case, we were naturally led to consider priors with a maximum at or near $\lambda = 0$. The simplest prior of this type is represented by a straight line joining the point $\lambda = 0$, $w(0) = 2T$ to the point $\lambda = \frac{1}{T}$, $w(\frac{1}{T}) = 0$, the equation being

$$w(\lambda) = 2T - 2T^2\lambda.$$

Using the formulas given above and supposing a test with no failures in T part hours, the resulting posterior density is

$$w(\lambda \mid n = 0) = e^{-\lambda T + 1} (T - \lambda T^2).$$

The corresponding failure rate estimate is

$$\hat{\lambda} = E[\lambda] = \int_0^{1/T} \lambda e^{-\lambda T + 1} (T - \lambda T^2) d\lambda$$

$$= (3 - e)/T$$

$$\approx .28/T.$$

As a natural next step, we considered the use of the above posterior as a prior. If we let

$$w(\lambda) = e^{-\lambda T + 1} (T - \lambda T^2),$$

and if we suppose T test hours with no failures, we obtain the posterior density

$$w(\lambda \mid n = 0) = e^{-2\lambda T + 1} (T - \lambda T^2) / .25 (e + e^{-1}).$$

As above, the corresponding failure rate estimate is

$$\lambda = 2/T (e^2 + 1) \approx .2384/T.$$

We can repeat this process, using the last derived posterior as a prior, generating a new posterior and a new $\hat{\lambda}$, and continuing to derive

additional estimates. Use the notation $w_0(\lambda)$ for the initial straight line prior, $w_1(\lambda)$ the posterior derived from $w_0(\lambda)$, $w_2(\lambda)$ the posterior derived by using $w_1(\lambda)$ as a prior, and so on. The following results are obtained.

Prior – Posterior Density $0 \leq \lambda \leq 1/T$	Failure Rate Estimate $\hat{\lambda} = E[\lambda]$
$w_0(\lambda) = 2T - 2T^2\lambda$	$\frac{1}{3T} = \frac{.333}{T}$
$w_1(\lambda) = e^{-\lambda T + 1}(T - \lambda T^2)$	$\frac{3-e}{T} = \frac{.282}{T}$
$w_2(\lambda) = \frac{4e^{-2\lambda T}(T - \lambda T^2)}{1 + e^{-2}}$	$\frac{2}{T(1 + e^2)} = \frac{.238}{T}$
$w_3(\lambda) = \frac{9e^{-3\lambda T}(T - \lambda T^2)}{2 + e^{-3}}$	$\frac{5 + e^3}{3T(1 + 2e^3)} = \frac{.203}{T}$
$w_4(\lambda) = \frac{16e^{-4\lambda T}(T - \lambda T^2)}{3 + e^{-4}}$	$\frac{6 + 2e^4}{4T(1 + 3e^4)} = \frac{.175}{T}$
•	•
•	•
•	•
•	•
$w_k(\lambda) = \frac{k^2 e^{-k\lambda T}(T - \lambda T^2)}{k - 1 + e^{-k}}$	$k + 2 + (k - 1)e^k$ / $Tk[1 + (k - 1)e^k]$

TABLE 5

Discussion

This paper has considered alternatives to the method of maximum likelihood for estimating an unknown constant failure rate from data consisting of the number of failures, n, observed in T cumulative hours of operation. Of course, the maximum likelihood estimate $\hat{\lambda} = n/T$, is entirely acceptable for $n \geq 1$. However, for the zero failure case, the estimate $\lambda = 0$ is presumed to be too low. We will evaluate the alternatives which have been described previously and select a preferred procedure. Modifications in the estimating formulas will be expressed as replacements of n = 0 failures in the likelihood formula, $\hat{\lambda} = n/T$, by non-zero values of n generated by the various alternatives. These modifications are presented in Table 6.

For an initial comparison of the alternatives, let us consider the logic underlying each of the approaches. The first method involves the replacement of n = 0 by a constraint which is an upper bound in some sense. The selection of such a constant does introduce an element of arbitrariness but it will be observed that this is really true for the other methods as well. It is somewhat illogical to use an upper bound in place of a point estimate. By its very nature, a point estimate is an average or measure of central tendency and we therefore usually prefer a "best estimate" rather than an upper or lower bound.

The upper confidence limit was used as the basis for three different methods. The first one used the upper confidence limit directly as a point estimate, a procedure frequently encountered in the literature. The second one used the midpoint of the accept interval as the point estimate. The third method involved an extrapolation using a ratio relationship between the upper confidence limits and the point estimates for the non-zero failure cases. There are two basic objections to the use of the upper confidence limit itself as a point estimate. The confidence limit is an upper bound and not a "best estimate" and it is very sensitive to the choice of confidence level. Both of these objections are to a large extent removed by the use of the midpoint of the "accept" confidence interval which ranges from zero to the upper confidence limit

$$\hat{\lambda}_u = \chi^2_{\alpha,2}/2T$$

The extrapolation of the ratios between $\hat{\lambda}_u$ and $\hat{\lambda}$ for $n \geq 1$ back to the $n = 0$ axis seems to have an intuitively natural appeal. Such an extrapolation appears to establish a consistency between the estimates based on tests with failure points and the modification for the zero failure case.

Bayesian estimation methods are of course attractive since the basic concepts of Bayesian statistics are expressed in terms of combining test information with previously conceived ideas about the parameters being estimated. The most serious weakness in the Bayesian approach for the present application is the extreme sensitivity to the choice of the prior — almost any answer can be generated by selecting a suitable prior.

In selecting confidence levels and priors to be used in developing numerical substitutions for zero failures, we attempted to cover a reasonably complete and logical range of alternatives as discussed previously in the paper. We can examine the entire collection of these numerical results to gain some insight into the sensitivity of the answers to the estimation methods and to the selections of confidence levels and priors. The non-zero failure replacements shown in Table 6 are ordered in Table 7 without reference to method of derivation. The "zero plus 5 in an extra decimal place" is necessarily omitted.

SUMMARY OF MODIFICATIONS OF
ZERO FAILURE ESTIMATES
(REPLACEMENT FOR ZERO AS NUMBER OF FAILURES)

Constant Replacements				
Unity				
One Half				
Zero plus 5 in an extra decimal place				
Replacements Based on Confidence Limits				
Level	Upper Limit	Interval Midpoint	Extrapolated $\hat{\lambda}_u/\hat{\lambda}$	Value $\hat{\lambda}/\hat{\lambda}_u$
.40	.51	.26	.32	.30
.50	.69	.35	.34	.31
.60	.92	.46	.37	.32
.63	1.00	.50	.38	.32

Bayesian Estimates	
Posterior	Estimate
Uniform, 0 to $1/T$	.41
Uniform, 0 to ∞	1.00
$2T - 2T^2\lambda$ (Used only as a prior in the text)	.33
$e^{-\lambda T + 1}(T - \lambda T^2)$	.28
$4e^{-2\lambda T}(T - \lambda T^2)/(1 + e^{-2})$	.24

TABLE 6

Ordered Non-Zero Failure Replacements

.24	.33	.50
.26	.34	.51
.28	.35	.69
.30	.37	.92
.31	.38	1.00
.32	.41	1.00
.32	.46	1.00
.32	.50	

TABLE 7

There is a rather smooth progression from .24 to .51, followed by wide intervals from there to the upper value, 1.00. The five highest values come from the upper confidence limit used as a point estimate, unity as an arbitrary choice, and an unrealistic Bayesian prior.

Recall that our objective is to discard the maximum likelihood estimate of λ for at least the one case in which no failures have occurred and replace it by some substitute which is judged to be reasonable. For an estimate to be reasonable it must have a likely value and of course a logical derivation would increase its credibility. Previously presented arguments have essentially established that the five highest values are derived by the least logical methods. Since these five are all markedly above the next lower value, it is concluded that we are justified in discarding them from further consideration and that we focus our attention on the remaining 18 which spread quite evenly from a low of .24 to a high of .51. Seventeen of these estimates are derived as midpoints of confidence intervals, or as extrapolations of ratios involving confidence limits and point estimates or by Bayesian estimation methods. Previously presented arguments suggest that each of these approaches is basically logical.

Consider now the numerical values of these 18 replacements for zero failures. We have explained why we wish to use a replacement greater than zero and not greater than unity. The 18 values all fall in a portion of this range which we believe to be entirely reasonable. Since we are dealing with the zero failure case, it is realistic to select a value in the lower half. It is conservative to select a value in the upper portion of this lower half. This logic suggests a zero replacement k satisfying the inequality:

$$.24 < k < .51,$$

the range between the extremes of our 18 values. The choice of a single value to replace the observed $n = 0$ failures is necessarily arbitrary. Our preference is to assume the value one third, giving the zero failure estimator

$$\hat{\lambda} = 1/3T$$

This zero replacement value, 1/3, is near the median of the 18 values listed in Table 7; it is close to midpoint of the logical range covered by the values, and it is certainly easy to remember.

Conclusions

It is our conclusion that an upper confidence limit is an unsatisfactory substitute for a point estimate of a constant failure rate, especially because of its sensitivity to the confidence level. However, a more reasonable point estimate can be developed as the midpoint of a confidence interval or as an extrapolation of ratios between upper confidence limits and point estimates for cases with failure events. Bayesian statistical methods are appropriate, but sensitivity to the choice of the prior is a serious handicap. We did not find any reasonable substitute for the maximum likelihood estimator in cases where failures did occur. For the zero failure case, we recommend the assumption of one third of a failure, giving the failure rate estimator

$$\hat{\lambda} = 1/3T$$

The arguments which we have presented indicate that this estimator is numerically reasonable and that it is generated by rather logical methods. It is recognized that there is no single correct solution to this problem. We are merely trying to replace a maximum likelihood estimate which we believe to be grossly unrealistic by a replacement which is numerically more acceptable and we believe that the suggested estimator is appropriate.

REFERENCES

1. W. Grant Ireson, Ed., Reliability Handbook, McGraw Hill, Inc., New York, 1966, p. 1-44.

2. H. Leon Harter, New Tables of the Incomplete Gamma-Function Ratio and of Percentage Points of the Chi-Square and Beta Distributions, Aerospace Research Laboratories, Office of Aerospace Research, USAF, 1964. (Obtainable from the Superintendent of Documents, Washington, D.C.)

3. ARINC Research Corporation, Reliability Engineering, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1964, p. 12-1.

FIGURE 1
TWO FAILURES IN T HOURS
CONFIDENCE LEVEL 80%

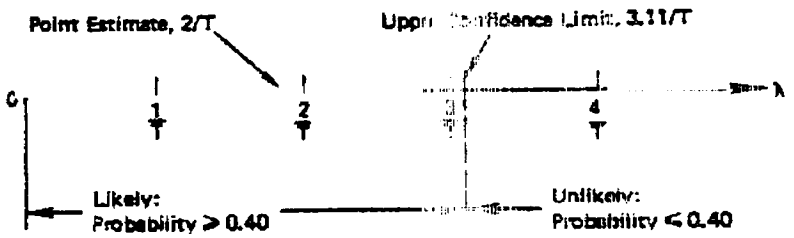
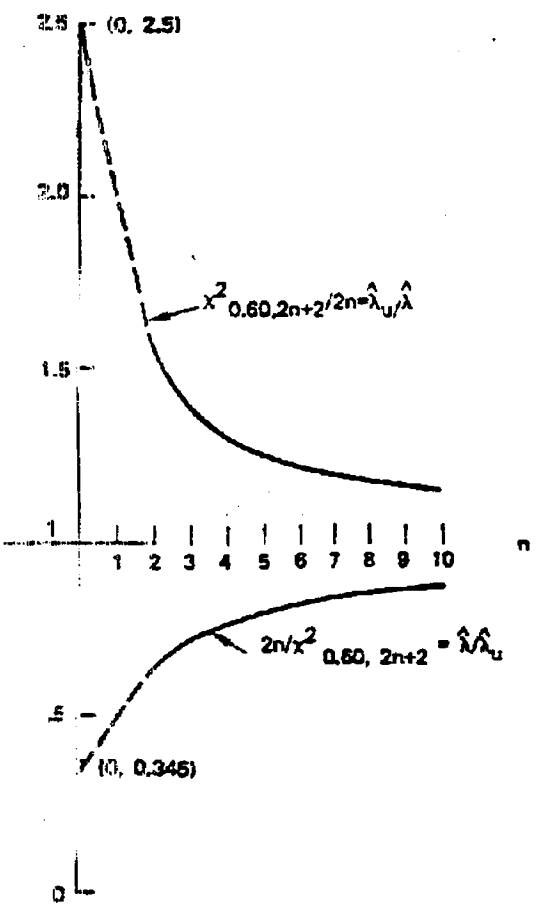


FIGURE 2



Appendix E:

Discussion and Comparison of Monte Carlo and Latin Hypercube Sampling Algorithms

(reproduced from the

@Risk™ User's Guide, Copyright 1990, Palisade Corporation
with the permission of
Palisade Corporation
31 Decker Rd.
Newfield, NY 14867)

@RISK

Risk Analysis and Simulation Add-In for Microsoft Excel

Windows or Apple Macintosh Version

Release 1.1 User's Guide

February 6, 1992

PALISADE
Corporation

31 Decker Rd.
Newfield, NY USA 14867
(607) 277-8000

Appendix F:
Sampling Methods

- **Introduction** F-3
  - What is Sampling? F-3
- **Cumulative Distribution** F-4
- **Monte Carlo Sampling** F-6
- **Latin Hypercube Sampling** F-8
  - Latin Hypercube Sampling and Low Probability Outcomes F-9
  - Testing the Techniques F-9
- **More About Sampling Techniques** F-10

Introduction

Sampling is used in an @RISK simulation to generate possible values from probability distribution functions. These sets of possible values are then used to evaluate your Excel worksheet. Because of this, sampling is the basis for the hundreds or thousands of "what-if" scenarios @RISK calculates for your worksheet. Each set of samples represents a possible combination of input values which could occur. Choosing a sampling method affects both the quality of your results and the length of time necessary to simulate your worksheet.

What is Sampling?

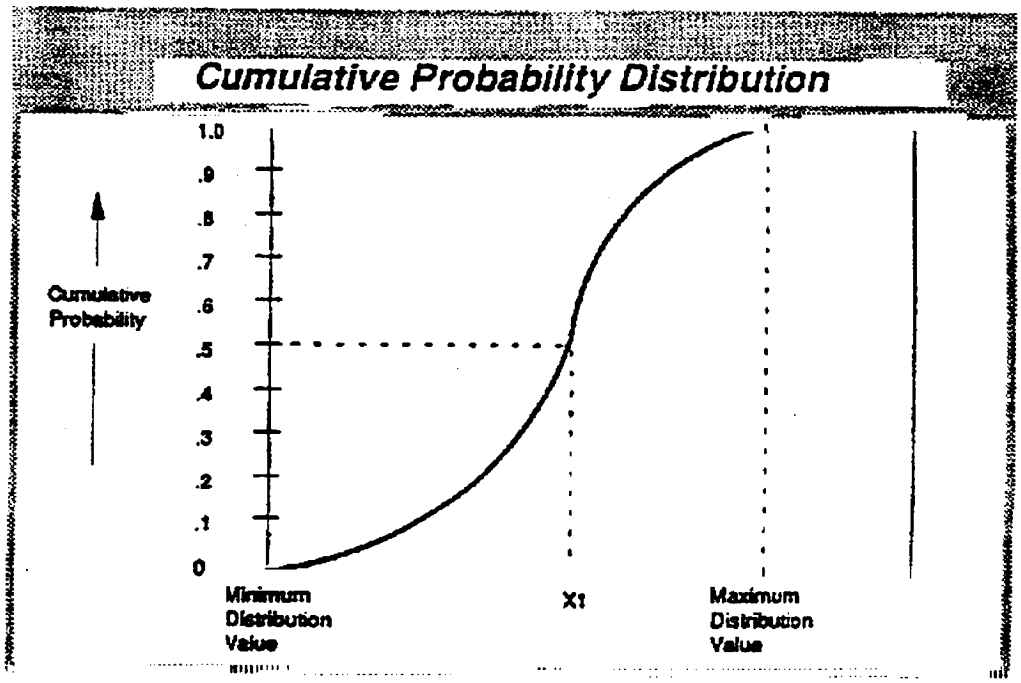
Sampling is the process by which values are randomly drawn from input probability distributions. Probability distributions are represented in @RISK by probability distribution functions and sampling is performed by the @RISK program. Sampling in a simulation is done repetitively — with one sample drawn every iteration from each input probability distribution. With enough iterations, the sampled values for a probability distribution will become distributed in a manner which approximates the known input probability distribution. The statistics of the sampled distribution — mean, standard deviation and higher moments — will approximate the true statistics that were input for the distribution. The graph of the sampled distribution will even look like a graph of the true input distribution.

Statisticians and practioners have developed several techniques for drawing random samples. The important factor to examine when evaluating sampling techniques is the number of iterations required to accurately recreate an input distribution through sampling. Accurate results for output distributions depend on a complete sampling of input distributions. If one sampling method requires more iterations and longer simulation runtimes than another to approximate input distributions, it is the less "efficient" method.

The two methods of sampling used in @RISK — Monte Carlo sampling and Latin Hypercube sampling — differ in the number of iterations required until sampled values approximate input distributions. Monte Carlo sampling often requires a large number of samples to approximate an input distribution, especially if the input distribution is highly skewed or has some outcomes of low probability. Latin Hypercube sampling, a new sampling technique used in @RISK, forces the samples drawn to correspond more closely with the input distribution and thus converges faster on the true statistics of the input distribution.

Cumulative Distribution

It is often helpful, when reviewing different sampling methods, to first understand the concept of a cumulative distribution. Any probability distribution may be expressed in cumulative form. A cumulative curve is typically scaled from 0 to 1 on the Y-axis, with Y-axis values representing the cumulative probability up to the corresponding X-axis value.



In the cumulative curve above, the .5 cumulative value is the point of 50% cumulative probability (.5 = 50%). Fifty percent of the values in the distribution fall below this median value and 50% are above. The 0 cumulative value is the minimum value (0% of the values will fall below this point) and the 1.0 cumulative value is the maximum value (100% of the values will fall below this point).

Why is this cumulative curve so important to understanding sampling? The 0 to 1.0 scale of the cumulative curve is the range of the possible random numbers generated during sampling. In a typical Monte Carlo sampling sequence, the computer will generate a random number between 0 and 1 — with any number in the range equally likely to occur. This random number is then used to select a value from the cumulative curve. For the example above, if a random number of .5 was generated during sampling, the value sampled for the distribution shown would be X1. As the shape of the cumulative curve is based on the shape of the input probability distribution, more likely outcomes will be more likely to be sampled. The more likely outcomes are in the range where the cumulative curve is the "steepest".

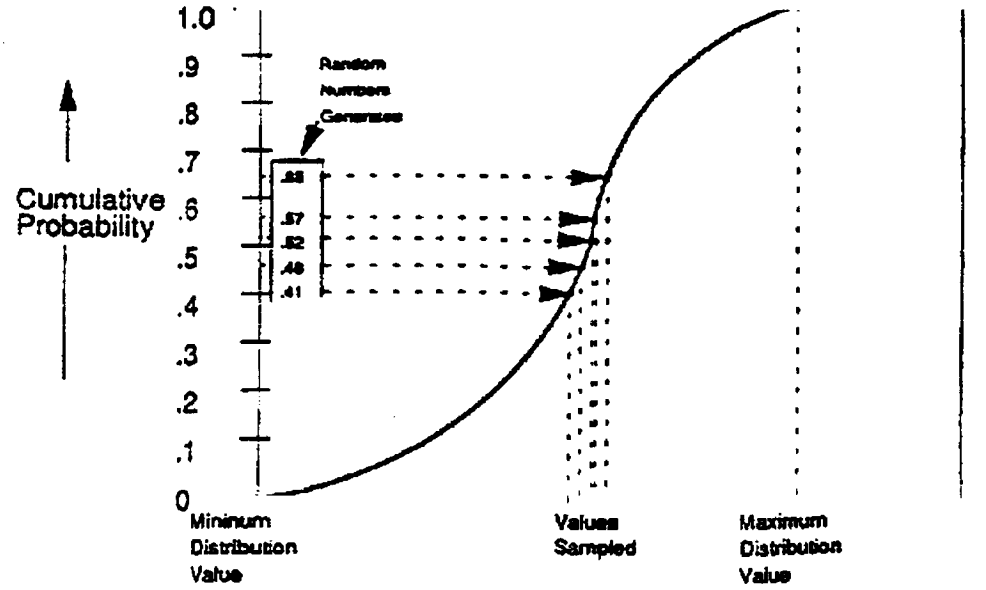
TECHNIQUES ATTENDANT SAMPLE

Monte Carlo Sampling

Monte Carlo sampling refers to the traditional technique for using random or pseudo-random numbers to sample from a probability distribution. The term "Monte Carlo" was introduced during World War II as a code name for simulation of problems associated with development of the atomic bomb. Today, Monte Carlo techniques are applied to a wide variety of complex problems involving random behavior. A wide variety of algorithms are available for generating random Monte Carlo samples from different types of input probability distributions.

Monte Carlo sampling techniques are entirely random — that is, any given sample may fall anywhere within the range of the input distribution. Samples, of course, are more likely to be drawn in areas of the distribution which have higher probabilities of occurrence. In the cumulative distribution shown earlier, each Monte Carlo sample will use a new random number between 0 and 1. With enough iterations, Monte Carlo sampling will "recreate" the input distributions through sampling. A problem of clustering, however, arises when a small number of iterations are performed.

Five Iterations of Monte Carlo Sampling With Clustering



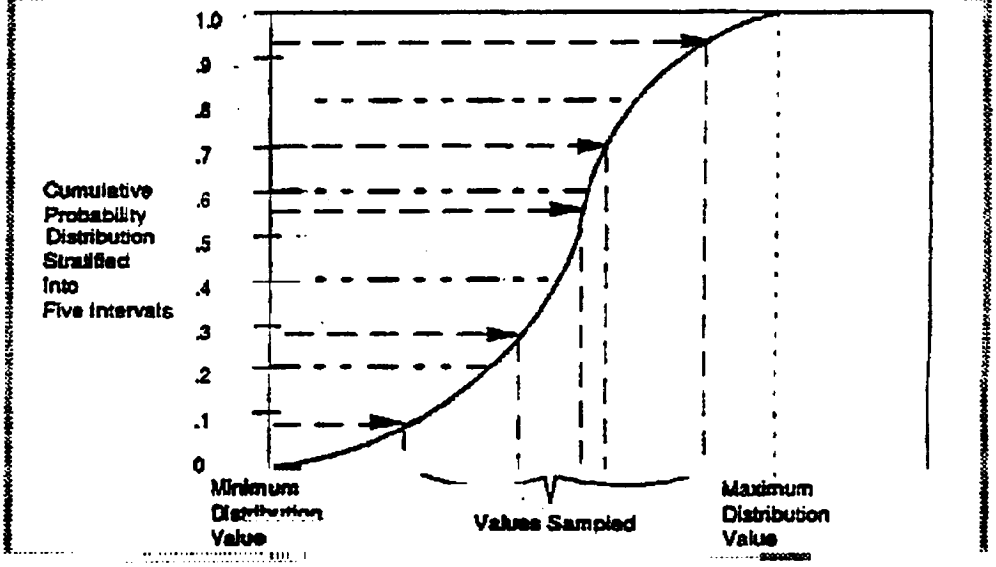
In the illustration shown here, each of the 5 samples drawn falls in the middle of the distribution. The values in the outer ranges of the distribution are not represented in the samples and thus their impact on your results is not included in your simulation output.

Clustering becomes especially pronounced when a distribution includes low probability outcomes which could have a major impact on your results. It is important to include the effects of these low probability outcomes and, to do this, these outcomes must be sampled. But if their probability is low enough, a small number of Monte Carlo iterations may not sample sufficient quantities of these outcomes to accurately represent their probability. This problem has led to the development of stratified sampling techniques such as the Latin Hypercube sampling used in @RISK.

Latin Hypercube Sampling

Latin Hypercube sampling is a recent development in sampling technology designed to accurately recreate the input distribution through sampling in fewer iterations when compared with the Monte Carlo method. The key to Latin Hypercube sampling is stratification of the input probability distributions. Stratification divides the cumulative curve into equal intervals on the cumulative probability scale (0 to 1.0). A sample is then randomly taken from each interval or "stratification" of the input distribution. Sampling is forced to represent values in each interval, and thus, is forced to recreate the input probability distribution.

Five Iterations of Latin Hypercube Sampling



In the illustration above, the cumulative curve has been divided into 5 intervals. During sampling, a sample is drawn from each interval. Compare this to the 5 clustered samples drawn using the Monte Carlo method. With Latin Hypercube, the samples more accurately reflect the distribution of values in the input probability distribution.

The technique being used during Latin Hypercube sampling is "sampling without replacement". The number of stratifications of the cumulative distribution is equal to the number of iterations performed. In the example above there were 5 iterations and thus 5 stratifications were made to the cumulative distribution. A sample is taken from each stratification. However, once a sample is taken from a stratification, this stratification is not sampled from again -- its value is already represented in the sampled set.

How does sampling within a given stratification occur? In effect, @RISK chooses a stratification for sampling then randomly chooses value from within the selected stratification.

When using the Latin Hypercube technique to sample from multiple variables, it is important to maintain independence between variables. The values sampled for one variable need to be independent of those sampled for another (unless, of course, you explicitly want them correlated). This independence is maintained by randomly selecting — for each variable — which interval to draw a sample from. In a given iteration, Variable #1 may be sampled from stratification #4, Variable #2 may be sampled from stratification #22, and so on. This preserves randomness and independence and avoids unwanted correlation between variables.

Latin Hypercube and Low Probability Outcomes

As a more efficient sampling method, Latin Hypercube offers great benefits in terms of increased sampling efficiency and faster runtimes. These gains are especially noticeable in a PC based simulation environment such as @RISK. Latin Hypercube, however, also helps the analysis of situations where low probability outcomes are represented in input probability distributions. By forcing the sampling of the simulation to include these outlying events, Latin Hypercube sampling assures they are accurately represented in your simulation outputs.

When low probability outcomes are very important it often helps to run an analysis which just simulates the contribution to the output distribution from the low probability events. In this case the model simulates only the occurrence of low probability outcomes — they are set to 100% probability. Through this you will isolate those outcomes and directly study the results they generate.

Testing the Techniques

The concept of convergence is used to test a sampling method. At the point of convergence, the output distributions are stable — that is, additional iterations will not markedly change the shape or statistics of the sampled distribution. The sample mean versus the true mean is typically a measure of convergence, however, skewness, percentile probabilities and other statistics are often used in measuring convergence.

@RISK provides a good environment for testing the speed at which the two available sampling techniques converge on an input distribution. Run an equal number of iterations with each of the sampling techniques while selecting an input distribution @function as a simulation output. Look at the closeness of the sample statistics to the true statistics which were specified in the distribution @function. It should be evident that Latin Hypercube sampling converges faster on the true distributions when compared with Monte Carlo sampling.

More About Sampling Techniques

The academic and technical literature has addressed both Monte Carlo and Latin Hypercube sampling. Any of the references to simulation in the *Recommended Readings Appendix* at the end of this chapter will give the reader an introduction to Monte Carlo sampling. References which specifically address Latin Hypercube sampling are included in a separate section of these references.

Appendix F:

Text of MSFC Incident Reports for post-*Galileo* Major Incidents

MSFC RPT # : A12281 | SYSTEM : PLUMBING | FMEA # : K100
STATUS : CLOSED | FUNCT CRIT : 1 | HRDWR CRIT : 1
FAIL MODE : MS | LOCATION : SSC A2 | CAUSE : MAP
R/C CODE 1 : 2 | TEST OPER. : Q | DEFECT : DC
NCA NOMEN : LPFTP DISC DUCT | NCA PART # : RS007018-511 | NCA SERLOT : 4917969
FAIL DATE : 06/02/89 | MSFC CLOS : 12/12/89
PROB TITLE : 5" X 2" SPLIT IN THE LPFTP NICKEL INSULATION
PROB DESCR :

REFERENCE IDCR 820
1) VISUAL INVESTIGATION OF LPF DUCT REVEALED A SPLIT IN THE NICKEL INSULATED COVER 5" LONG BY 2" WIDE LOCATED 18" FROM F3, WITH A 3/4" HOLE IN CENTER OF DAMAGED AREA 2) BELLOWS #3 IS STRETCHED OUT OF CONFIGURATION TO APPROXIMATELY 6 1/4" LONG 3) WITH PURGE ON LPF DUCT THE OVERMOLD ON THE F3 SIDE OF BELLOWS #3 HAS LEAKAGE.
NOTE: THE ABOVE DAMAGE RESULTED IN ENGINE TEST TERMINATION 14.7 SECS. INTO THE 300 SEC TEST. REF IDCR 819
DISCOVERED 890602

INVESTIGATION/RESOLUTION :

7/26/78 - STS-28 - FAR DEFERRAL RATIONALE
DEFERRAL FAR: THE PROBLEM CLOSURE IS DEFERRED FOR FLIGHT STS-34.
PROBLEM DESCRIPTION: DURING A PLANNED 300 SECOND DURATION TEST ON ENGINE 2206, THE INTERNAL PRESSURE RESTRAINTS IN ONE OF THE FLEX JOINTS IN A LPFP DISCHARGE DUCT FAILED. THE THREE LEGS ATTACHED TO THE BALL SIDE OF THE INTERNAL BALL AND SOCKET MECHANISM DETACHED FROM ITS SUPPORT TRIPOD, ALLOWING THE ONE-HALF POUND BALL (AND THREE LEG "STUBS") TO BE CARRIED BY THE FLOW DOWNSTREAM. AT THE FIRST DUCT ELBOW, IT PUNCTURED THE DUCT WALL, CAUSING A HYDROGEN LEAK UNDER THE INSULATION, WHICH RUPTURED THE NICKEL PLATING OF THE DUCT. THIS RESULTED IN AN ENGINE FIRE, WHICH WAS EXTINGUISHED BEFORE ANY SIGNIFICANT ENGINE OR FACILITY DAMAGE OCCURRED. THE POSITION "C" FLEX JOINT (THIRD DOWN STREAM FROM THE INLET FLANGE) EXTENDED ROUGHLY 100% AS A RESULT OF THE LOSS OF RESTRAINT ON THE AXIAL PRESSURIZATION FORCES ACTING ON THE BELLOWS. THE PLASTICALLY STRETCHED BELLOWS DID NOT FAIL OR LEAK.
DEFERRAL RATIONALE: THE DEFERRAL RATIONALE IS AS FOLLOWS:
PRESENT STATUS: THE FAILED DUCT HAS BEEN SECTIONED AND EXAMINED, AND THE FRACTURE SURFACES IN THE "C" POSITION FLEX JOINT HAVE BEEN ANALYZED.
PRESENT STATUS: THE FAILED DUCT HAS BEEN SECTIONED AND EXAMINED, AND

THE FRACTURE SURFACES IN THE "C" POSITION FLEX JOINT HAVE BEEN ANALYZED. HIGH CYCLE (NON-PLASTIC) FATIGUE WAS THE PRIMARY FAILURE MECHANISM IN ONE LEG, AND A COMBINATION OF PLASTIC FATIGUE AND DUCTILE OVERLOAD IN

THE OTHER TWO LEGS.
OTHER ARTICULATING DUCT UNITS OF THE SAME AND DIFFERING PART NUMBERS HAVE BEEN SECTIONED AND EXAMINED FOR SIMILAR FAILURE, AND NON-DESTRUCTIVE INSPECTIONS ON EXTERNALLY TIED FLEX JOINTS HAVE BEEN PERFORMED. NO CRACKING HAS BEEN FOUND. IN ADDITION, THE TRIPOD LEGS AND HUBS WITHIN THE SECTIONED LPFP DISCHARGE DUCT JOINTS WERE DIMENSIONALLY EXAMINED. A LIST OF EXAMINED DUCTS IS AS FOLLOWS:

PART NO:	SERIAL NO:	TIME/STARTS:
RS007018	4881753	35564/82
RS007018	4887572	25286/64
RS007015	4881352	17100/60
RS007043	4879399	33744/75
RS007034	4881228	31730/69
RS007016	4882257	28947/60
RS007035	4886508	42300/90
RS007037	4881319	22039/37

VENDOR RECORDS HAVE BEEN REVIEWED FOR BOTH FUEL AND LOX INTERNALLY-TIED, TRIPOD-TYPE FLEX JOINTS. TWO GENERIC PROBLEMS WITH RS008981 AND RS008961 FLEX JOINTS HAVE BEEN UNCOVERED. FIRST, TWO LOTS OF TRIPOD LEGS WERE FOUND TO HAVE DISCREPANT CROSS-SECTIONS (OVER RADIUSED LEADING EDGE AND LONG TRAILING EDGE CHAMFER). SECONDLY, THE CRITICAL TRIPOD LEG/TRIPOD HUB TRANSITION "DOGLEG" RADIUS IS NOT INSPECTED AFTER FINAL HAND-BLENDING, AND HAS BEEN FOUND TO BE AS SMALL AS .020" ON AN "A" TYPE FLEX JOINT (BLUEPRINT MINIMUM IS .060"). THIS RADIUS WAS THE CRACK INITIATION SITE ON THE FAILED UNIT. THE "PRIMARY FAILURE" LEG EXHIBITED BOTH DISCREPANT CROSS-SECTION AND UNDERSIZE DOGLEG RADIUS (.029').
THE INFORMATION COLLECTED INDICATED A HIGH CYCLE FATIGUE TYPE FAILURE IN ONE LEG, LEADING TO BREAKAGE IN THE OTHER TWO LEGS AFTER SOME OPERATIONAL TIME. THE FAILURE WAS DUE TO A COMBINATION OF EXCESSIVE STRESS CONCENTRATION AT THE UNDERSIZE RADIUS, INCREASED STRESS LEVEL AS A RESULT OF THE DECREASED LEG CROSS-SECTION, AND HIGH HOT-FIRE TIME.
RATIONALE FOR DEFERRAL: THE FAILED UNIT HAD 90 STARTS AND 31,853 SECONDS OF HOT FIRE OPERATION AND WAS THE SECOND HIGHEST FLEET LEADER UNIT IN TIME AND NORMALIZED DAMAGE. EXAMINATION OF THE OTHER LEGS IN THE FAILED UNIT AS WELL AS TRIPOD LEGS FROM TWO OTHER FLEET LEADER UNITS SHOWED THE FAILED TRIPOD LEG TO HAVE THE WORST OBSERVED COMBINATION OF HOT FIRE TIME, DOGLEG RADIUS, AND SECTION MODULUS, AND WAS LOCATED IN THE HIGHEST STRESS FLEX JOINT, "C".
ANALYZING THE STRESSES AND LIFE USING THE POTENTIAL CASE OF A 0.020 RADIUS ON A "C" FLEX JOINT YIELDED A LIFE OF 3,600 EFPL SECONDS. THIS LIFE CORRELATED TO THE ENGINE 2206 FAILURE AND TO THE LIFE OF THE 0.020 TRIPOD AN "A" FLEX JOINT ASSUMING FAILURE WOULD HAVE OCCURRED ON THE

NEXT TEST IN CONJUNCTION WITH A CORRECTION FOR THE LOWER STRESSES IN AN "A" FLEX JOINT.
ALTHOUGH THE PROBABILITY IS EXTREMELY SMALL FOR HAVING A COMBINED SET OF CONDITIONS MORE SEVER THAN THE ENGINE 2206 FAILURE, AN INTERIM LIMIT OF 3600/2= 1800 EFPL IS ESTABLISHED AS A LIMIT (REFERENCE DAR 2296). A TABLE OF COLUMBIA ENGINE LPFP DISCHARGE DUCT TIMES IN RELATION TO THE FAILED UNIT IS AS FOLLOWS:

COLUMBIA ENGINE	DAMAGE FRACTIONS FOR STS-28 PRE	POST (NOM)	POST (ABORT)
2019	.33	.41	.53
2022	.33	.41	.53
2028	.19	.28	.59

ALL OTHER TYPE OF ARTICULATING DUCTS ON COLUMBIA ARE ACCEPTABLE FOR FLIGHT BASED ON THEIR MORE FAVORABLE GEOMETRY WITH RESPECT TO FATIGUE, AND ON THE COMPARATIVELY LOW HOT-FIRE TIME. ALL NEXT FLIGHT LPOP DISCHARGE DUCTS, FUEL BLEED DUCTS, LPFP TURBINE DRIVE DUCTS, AND OXIDIZER TANK PRESSURANT DUCTS ARE LESS THAN 25% OF THE FLEET LEADER, AND OF FULLY PENETRANT INSPECTED HIGH TIME UNITS.
EFFECT ON ENGINE: CRITICALITY 1 FAILURE
RATIONALE: THE WORST CASE SCENARIO FOR FAILURE OF THE INTERNAL RESTRAINT MECHANISM IN THE LOW PRESSURE FUEL DUCT IS RUPTURE OF THE FLEX JOINT BELLOWS, LEADING TO UNCONTROLLED FIRE AND LOSS OF VEHICLE.
7/28/89 - PROBLEM DEFERRED FOR STS-28 PER RATIONALE E. THE PROBLEM IS TIME/AGE/CYCLE RELATED AND THE FLIGHT UNITS WILL HAVE ACCUMULATED LESS THAN 50 PERCENT OF THE CRITICAL PARAMETERS AT THE END OF THE NEXT FLIGHT.
9/26/89 - STS-34 DEFERRAL RATIONALE
DEFERRAL FAR: D. DAVIS: D/529: 890912
THE PROBLEM CLOSURE IS DEFERRED FOR FLIGHT STS-34.
PROBLEM DESCRIPTION: DURING A PLANNED 300 SECOND DURATION TEST ON ENGINE 2206, THE INTERNAL PRESSURE RESTRAINTS IN ONE OF THE FLEX JOINTS IN A LPFP DISCHARGE DUCT FAILED. THE THREE LEGS ATTACHED TO THE BALL SIDE OF THE INTERNAL BALL AND SOCKET MECHANISM DETACHED FROM ITS SUPPORT TRIPOD, ALLOWING THE ONE-HALF POUND BALL (AND THREE LEG "STUBS") TO BE CARRIED BY THE FLOW DOWNSTREAM. AT THE FIRST DUCT ELBOW, IT PUNCTURED THE DUCT WALL, CAUSING A HYDROGEN LEAK UNDER THE INSULATION, WHICH RUPTURED THE NICKEL PLATING OF THE DUCT. THIS RESULTED IN AN ENGINE FIRE, WHICH WAS EXTINGUISHED BEFORE ANY SIGNIFICANT ENGINE OR FACILITY DAMAGE OCCURRED. THE POSITION "C" FLEX JOINT (THIRD DOWN STREAM FROM THE INLET FLANGE) EXTENDED ROUGHLY 100% AS A RESULT OF THE LOSS OF RESTRAINT ON THE AXIAL PRESSURIZATION FORCES ACTING ON THE BELLOWS. THE PLASTICALLY STRETCHED BELLOWS DID NOT FAIL OR LEAK.

(CONTINUATION)

MSFC #: A12281 IFA #: CONTRACTOR #: A008935

164 AA.

DEFERRAL RATIONALE: THE DEFERRAL RATIONALE IS AS FOLLOWS:
PRESENT STATUS: THE FAILED DUCT HAS BEEN SECTIONED AND EXAMINED, AND THE FRACTURE SURFACES IN THE "C" POSITION FLEX JOINT HAVE BEEN ANALYZED.
PRESENT STATUS: THE FAILED DUCT HAS BEEN SECTIONED AND EXAMINED, AND THE FRACTURE SURFACES IN THE "C" POSITION FLEX JOINT HAVE BEEN ANALYZED.
HIGH CYCLE (NON-PLASTIC) FATIGUE WAS THE PRIMARY FAILURE MECHANISM IN ONE LEG, AND A COMBINATION OF PLASTIC FATIGUE AND DUCTILE OVERLOAD (50%) IN THE OTHER TWO LEGS.
OTHER ARTICULATING DUCT UNITS OF THE SAME AND DIFFERING PART NUMBERS HAVE BEEN SECTIONED AND EXAMINED FOR SIMILAR FAILURE, AND NON-DESTRUCTIVE INSPECTIONS ON EXTERNALLY TIED FLEX JOINTS HAVE BEEN PERFORMED. NO CRACKING HAS BEEN FOUND. IN ADDITION, THE TRIPOD LEGS AND HUBS WITHIN THE SECTIONED LPFP DISCHARGE DUCT JOINTS WERE DIMENSIONALLY EXAMINED. A LIST OF EXAMINED DUCTS IS AS FOLLOWS:

PART NO:	SERIAL NO:	TIME/STARTS:
RS007018	4861753	35564/82
RS007018	4867572	25286/64
RS007015	4881352	17100/60
RS007043	4879299	32744/75
RS007034	4881228	31730/69
RS007016	4882257	28947/60
RS007035	4866508	42300/90
RS007037	4881319	22039/37

VENDOR RECORDS HAVE BEEN REVIEWED FOR BOTH FUEL AND LOX INTERNALLY-TIED, TRIPOD-TYPE FLEX JOINTS. TWO GENERIC PROBLEMS WITH RS008981 AND RS008961 FLEX JOINTS HAVE BEEN UNCOVERED. FIRST, A NUMBER OF TRIPOD LEGS WERE FOUND TO HAVE DISCREPANT CROSS-SECTIONS (OVER-RADIUSED LEADING EDGE AND LONG TRAILING EDGE CHAMFER). SECONDLY, THE CRITICAL TRIPOD LEG/TRIPOD HUB TRANSITION "DOGLEG" RADIUS IS NOT INSPECTED AFTER FINAL HAND-BLENDING, AND HAS BEEN FOUND TO BE AS SMALL AS .020" ON AN "A" TYPE FLEX JOINT (ENGINEERING MINIMUM IS .060"). THIS RADIUS WAS THE CRACK INITIATION SITE ON THE FAILED UNIT. THE "PRIMARY FAILURE" LEG EXHIBITED BOTH DISCREPANT CROSS-SECTION AND UNDERSIZE DOGLEG RADIUS (.029").
THE INFORMATION COLLECTED INDICATED A HIGH CYCLE FATIGUE TYPE FAILURE IN ONE LEG, LEADING TO BREAKAGE IN THE OTHER TWO LEGS AFTER SOME OPERATIONAL TIME. THE FAILURE WAS DUE TO A COMBINATION OF EXCESSIVE STRESS CONCENTRATION AT THE UNDERSIZE RADIUS, INCREASED STRESS LEVEL AS A RESULT OF THE DECREASED LEG CROSS-SECTION, AND HIGH HOT-FIRE TIME.
RATIONALE FOR DEFERRAL: THE FAILED UNIT HAD 90 STARTS AND 31,853 SECONDS OF HOT FIRE OPERATION AND WAS THE SECOND HIGHEST FLEET LEADER UNIT IN TIME AND NORMALIZED DAMAGE. EXAMINATION OF THE OTHER LEGS IN THE FAILED UNIT AS WELL AS TRIPOD LEGS FROM TWO OTHER FLEET LEADER UNITS SHOWED THE FAILED TRIPOD LEG TO HAVE THE WORST OBSERVED COMBINATION OF HOT FIRE TIME, DOGLEG RADIUS, AND SECTION MODULUS, AND WAS LOCATED IN

MSFC PROBLEM REPORTING AND CORRECTIVE ACTION (PRACA) SYSTEM

(C O N T I N U A T I O N)

MSFC #: A12281 IFA #: CONTRACTOR #: A008935

THE HIGHEST STRESS FLEX JOINT, "C".
ANALYZING THE STRESSES AND LIFE USING THE POTENTIAL CASE OF A 0.020 RADIUS ON A "C" FLEX JOINT YIELDED A LIFE OF 3,600 EFPL SECONDS. THIS LIFE CORRELATED TO THE ENGINE 2206 FAILURE AND TO THE LIFE OF THE 0.020 TRIPOD ON AN "A" FLEX JOINT ASSUMING FAILURE WOULD HAVE OCCURRED ON THE NEXT TEST IN CONJUNCTION WITH A CORRECTION FOR THE LOWER STRESSES IN AN "A" FLEX JOINT. ALTHOUGH THE PROBABILITY IS EXTREMELY SMALL FOR HAVING A COMBINED SET OF CONDITIONS MORE SEVERE THAN THE ENGINE 2206 FAILURE, AN INTERIM LIMIT OF 3600/2 = 1800 EFPL IS ESTABLISHED AS A LIMIT FOR DUCTS WITH UNKNOWN TRIPOD LEG DOGLEG RADII AND CROSS SECTION IN THE POSITION "C" FLEX JOINT (REFERENCE DAR 2296-R1).
THE TIME REMAINING FOR THE ATLANTIS ENGINES ON THE PROPOSED DAR COVERS ANY PLANNED MISSION/ABORT. A TABLE OF ATLANTIS ENGINE LPFP DICHARGE DUCT REMAINING TIMES IN RELATION TO THE FAILED UNIT IS AS FOLLOWS:

ATLANTIS ENGINE	DUCT PRE-FLT REMAINING TIME (SEC) @104%P.L.	@109%P.L.	
2027	905	680	*
2030	6450	3900	**
2029	890	660	*

* INSPECTION NOT REQUIRED. 0.020 RADIUS ASSUMED.
** 0.030 RADIUS (MINIMUM) VERIFIED BY BORESCOPE INSPECTION.
ALL OTHER TYPES OF ARTICULATING DUCTS ON ATLANTIS ARE ACCEPTABLE FOR FLIGHT BASED ON THEIR MORE FAVORABLE GEOMETRY WITH RESPECT TO FATIGUE.
EFFECT ON ENGINE: CRITICALITY 1 FAILURE
RATIONALE: THE WORST CASE SCENARIO FOR FAILURE OF THE INTERNAL RESTRAINT MECHANISM IN THE LOW PRESSURE FUEL DUCT IS RUPTURE OF THE FLEX JOINT BELLOWS, LEADING TO UNCONTROLLED FIRE AND LOSS OF VEHICLE.
9/30/89 - PROBLEM DEFERRED FOR STS-34 PER RATIONALE E. THE PROBLEM IS TIME/AGE/CYCLE RELATED AND THE FLIGHT UNITS WILL HAVE ACCUMULATED LESS THAN 50% OF THE CRITICAL PARAMETERS AT THE END OF THE NEXT FLIGHT.
11/6/89 - PROBLEM CLOSURE RATIONALE SUBMITTED.
PROBLEM DESCRIPTION: DURING A PLANNED 300 SECOND DURATION TEST ON ENGINE 2206, THE INTERNAL PRESSURE RESTRAINTS IN ONE OF THE FLEX JOINTS IN A LPFP DISCHARGE DUCT FAILED. THE THREE LEGS ATTACHED TO THE BALL SIDE OF THE INTERNAL BALL AND SOCKET MECHANISM DETACHED FROM ITS SUPPORT TRIPOD, ALLOWING THE ONE-HALF POUND BALL (AND THREE LEG "STUBS") TO BE CARRIED BY THE FLOW DOWNSTREAM. AT THE FIRST DUCT ELBOW, IT PUNCTURED THE DUCT WALL, CAUSING A HYDROGEN LEAK UNDER THE INSULATION, WHICH RUPTURED THE NICKEL PLATING OF THE DUCT. THIS RESULTED IN AN ENGINE FIRE, WHICH WAS ESTINGUISHED BEFORE ANY SIGNFICANT ENGINE OR FACILITY DAMAGE OCCURRED. THE POSITION "C" FLEX JOINT (THIRD DOWN

(C O N T I N U A T I O N)

MSFC #: A12281 IFA #: CONTRACTOR #: A008935

STREAM FROM THE INLET FLANGE) EXTENDED ROUGHLY 100% AS A RESULT OF THE LOSS OF RESTRAINT ON THE AXIAL PRESSURIZATION FORCES ACTING ON THE BELLOWS. THE PLASTICALLY STRETCHED BELLOWS DID NOT FAIL OR LEAK.
INVESTIGATION: THE FAILED DUCT HAS BEEN SECTIONED AND EXAMINED, AND THE FRACTURE SURFACES IN THE "C" POSITION FLEX JOINT HAVE BEEN ANALYZED. HIGH CYCLE (NON-PLASTIC) FATIGUE WAS THE PRIMARY FAILURE MECHANISM IN ONE LEG, AND A COMBINATION OF PLASTIC FATIGUE AND DUCTILE OVERLOAD (50%) IN THE OTHER TWO LEGS.
OTHER ARTICULATING DUCT UNITS OF THE SAME AND DIFFERING PART NUMBERS HAVE BEEN SECTIONED AND EXAMINED FOR SIMILAR FAILURE, AND NON-DESTRUCTIVE INSPECTIONS ON EXTERNALLY TIED FLEX JOINTS HAVE BEEN PERFORMED. NO CRACKING HAS BEEN FOUND. IN ADDITION, THE TRIPOD LEGS AND HUBS WITHIN THE SECTIONED LPFP DISCHARGE DUCT JOINTS WERE DIMENSIONALLY EXAMINED. A LIST OF EXAMINED DUCTS IS AS FOLLOWS.

PART NO:	SERIAL NO:	TIME/STARTS
RS007018	4881753	35564/82
RS007018	4887572	25286/64
RS007015	4881352	17100/60
RS007043	4879399	33744/75
RS007034	4881228	31730/69
RS007016	4882257	28947/60
RS007035	4886508	42300/90
RS007037	4881319	22039/37

VENDOR RECORDS HAVE BEEN REVIEWED FOR BOTH FUEL AND LOX INTERNALLY-TIED, TRIPOD-TYPE FLEX JOINTS. (REFERENCE INTERNAL LETTER 89-QE-127.) TWO GENERIC PROBLEMS WITH RS00[illegible] AND RS00[illegible] FLEX JOINTS HAVE BEEN IDENTIFIED. FIRST, A NUMBER OF TRIPOD LEGS WERE FOUND TO HAVE DISCREPANT CROSS-SECTIONS (OVER-RADIUSED LEADING EDGE AND LONG TRAILING EDGE CHAMFER). SECONDLY, THE CRITICAL TRIPOD LEG/TRIPOD HUB TRANSITION "DOGLEG" RADIUS IS NOT INSPECTED AFTER FINAL HAND-BLENDING, AND HAS BEEN FOUND TO BE AS SMALL AS .020" ON AN "A" TYPE FLEX JOINT (BLUEPRINT MINIMUM IS .060"). THIS RADIUS WAS THE CRACK INITIATION SITE ON THE FAILED UNIT. THE "PRIMARY FAILURE" LEG EXHIBITED BOTH DISCREPANT CROSS-SECTION AND UNDERSIZE DOGLEG RADIUS (.029").
EXPERIMENTAL VERIFICATION OF THE FATIGUE CHARACTERISTICS OF 21-6-9 STEEL (USED IN THE LEGS) IS BEING OBTAINED NEAR THE CONDITIONS IN THE FAILED UNIT. PRELIMINARY FINDINGS HAVE BEEN OBTAINED (REFERENCE MATERIALS PROCESSING REPORT 89-1420), AND THEY CORRELATE WITH EXPECTED RESULTS. ADDITIONAL WORK WILL ALSO BE ACCOMPLISHED TO ACQUIRE THESE CHARACTERISTICS NEAR PRINT (TRIPOD LEG RADIUS) CONDITIONS.
PROBLEM CAUSE: THE INFORMATION COLLECTED ON THE FAILED UNIT INDICATED A

HIGH CYCLE FATIGUE TYPE FAILURE IN ONE LEG, LEADING TO BREAKAGE IN THE OTHER TWO LEGS AFTER SOME OPERATIONAL TIME. THE FAILURE WAS DUE TO A COMBINATION OF EXCESSIVE STRESS CONCENTRATION AT THE UNDERSIZE RADIUS, INCREASED STRESS LEVEL AS A RESULT OF THE DECREASED LEG CROSS-SECTION,

MSFC #: A12281 IFA #: CONTRACTOR #: A008935

AND HIGH HOT-FIRE TIME.
THE FAILED UNIT HAD 90 STARTS AND 31,853 SECONDS OF HOT FIRE OPERATION AND WAS THE SECOND HIGHEST FLEET LEADER UNIT IN TIME AND NORMALIZED DAMAGE. EXAMINATION OF THE OTHER LEGS IN THE FAILED UNIT AS WELL AS TRIPOD LEGS FROM TWO OTHER FLEET LEADER UNITS SHOWED THE FAILED TRIPOD LEG TO HAVE THE WORST OBSERVED COMBINATION OF HOT FIRE TIME, DOGLEG RADIUS, AND SECTION MODULUS, AND WAS LOCATED IN THE HIGHEST STRESS FLEX JOINT, "C".
ALL OTHER TYPES OF ARTICULATING DUCTS ARE ACCEPTABLE, BASED ON THEIR MORE FAVORABLE GEOMETRY WITH RESPECT TO FATIGUE.
OTHER REPORTED PROBLEMS: NO OTHER FAILURES OF THIS TYPE HAVE BEEN OBSERVED.
REMEDIAL ACTION: ANALYZING THE STRESSES AND LIFE USING THE POTENTIAL CASE OF A 0.020 RADIUS ON A "C" FLEX JOINT YIELDED A LIFE OF 3,600 EFPL SECONDS. THIS LIFE CORRELATED TO THE ENGINE 2206 FAILURE AND TO THE LIFE OF THE 0.020 TRIPOD ON AN "A" FLEX JOINT ASSUMING FAILURE WOULD HAVE OCCURRED ON THE NEXT TEST IN CONJUNCTION WITH A CORRECTION FOR THE LOWER STRESSES IN AN "A" FLEX JOINT. ALTHOUGH THE PROBABILITY IS EXTREMELY SMALL FOR HAVING A COMBINED SET OF CONDITIONS MORE SEVERE THAN THE ENGINE 2206 FAILURE, AN INTERIM LIMIT OF 3600/2 = 1800 EFPL IS ESTABLISHED AS A LIMIT FOR DUCTS WITH UNKNOWN TRIPOD LEG DOGLEG RADII AND CROSS SECTION IN THE POSITION "C" FLEX JOINT (REFERENCE DAR 2296-R1).
A PROGRAM OF INSPECTING LPF DUCT FLEX JOINT C TRIPOD DOGLEG RADII WAS DEVELOPED IN ORDER TO DETERMINE THE ACTUAL RADIUS AND SECTION PROPERTIES AND THEREBY NOT HAVING TO USE THE WORST CASE VALUES FOR THESE PARAMETERS. THE INSPECTION WAS DESIGNED TO EVALUATE THE RADIUS USING A BORESCOPE COMPARATIVE ANALYSIS TECHNIQUE. THE MAJOR LIMITATION OF THE CURRENT INSPECTION TECHNIQUE HOWEVER, IS THE INABILITY OF DETERMINING A SPECIFIC RADIUS VALUE. THE MOST RELIABLE CRITERION DEVELOPED IS A SIMPLE PASS/NO PASS METHOD IN WHICH THE REPORTED VALUE IS EITHER GREATER THAN 0.030, OR "UNABLE TO VERIFY" GREATER THAN 0.030. CONVERSELY THOUGH, THE THE SECTION PROPERTIES ARE READILY CHARACTERISZED BY BORESCOPE EVALUATION. LIFE LIMITS WERE IMPOSED, BASED ON THIS INSPECTION TECHNIQUE, USING DARS 2296, 2315 (FOR TWO DEVELOPMENT UNITS), AND 2333 (FOR THE ENGINE 0208 TEST BED UNIT).
A NEW TECHNOLOGY VIDEO BORESCOPE HAS BEEN REQUISITIONED WHICH ALLOWS

IMPROVED QUANTIFICATION OF THE TRIPOD LEG RADIUS. THIS SHOULD ALLOW EXTENSION OF THE CONSERVATIVE LIMITS IMPOSED PRESENTLY.
ALL EXISTING FLEX JOINT DETAILS AND FLEX JOINTS NOT PRESENTLY WELDED INTO DUCTS WILL BE INSPECTED FOR PROPER TRIPOD LEG RADIUS AND SECTION PROPERTIES.
RECURRENCE CONTROL: INSPECTION OF THE TRIPOD LEG RADII WILL NOW BE

(C O N T I N U A T I O N)

MSFC #: A12281 IFA #: CONTRACTOR #: A008935

REQUIRED AFTER FINAL HAND BLENDING. VENDOR PLANNING HAS BEEN REVISED ACCORDINGLY (REFERENCE INTERNAL LETTER 90-QE-219).
FMEA/CIL INTERFACES: THIS FAILURE IS A CRITICALITY 1 ITEM. THE WORST CASE SCENARIO FOR FAILURE OF THE INTERNAL RESTRAINT MECHANISM IN THE LOW PRESSURE FUEL DUCT IS RUPTURE OF THE FLEX JOINT BELLOWS, LEADING TO UNCONTROLLED FIRE AND LOSS OF VEHICLE.
BACK-UP DATA:
DAR 2296 R1 A1
DAR 2315
DAR 2333
I.L. 89-QE-127
I.L. 89-QE-219
M.P.R. 89-1420
11/9/89 - PROBLEM CLOSURE DEFERRED WITH ACTION ITEM 253-2, FOR ROCKETDYNE TO EXPOUND THE RECURRENCE CONTROL TO ADDRESS ALL PHASES PAST, PRESENT AND FUTURE. PER RATIONALE E: THE PROBLEM IS TIME/AGE/LIFE CYCLE RELATED AND THE FLIGHT UNITS WILL HAVE ACCUMULATED LESS THAN 50 PERCENT OF THE CRITICAL PARAMETER(S) AT THE END OF THE NEXT FLIGHT.
12/6/89 - RESPONSE FROM ACTION ITEM 253-2
ENGINEERING ADDENDUM: DED. D/529-164, 891204
PER PRB 253, ACTION ITEM 253-2
RE: UCR/FAR A008935
REMEDIAL ACTION: WORDING OF THE REMEDIAL ACTION PORTION OF THE FAR SHOULD BE CHANGED TO READ AS FOLLOWS:
THE FAILED LPF DUCT S/N 4917969 WAS REMOVED FROM ENGINE 2206 AND SECTIONED FOR THE MATERIALS INVESTIGATION.
RECURRENCE CONTROL: WORDING OF THE RECURRENCE CONTROL PORTION OF THE FAR SHOULD BE CHANGED TO READ AS FOLLOWS:
IN RESPONSE TO THE HOT-FIRE TIME RELATED FAILURE EXPERIENCED, LIFE LIMITS WERE IMPOSED ON ALL OTHER LPF DUCTS IN THE FLEET. ANALYSIS THE STRESSES AND LIFE USING THE POTENTIAL CASE OF A 0.020 RADIUS ON A "C" FLEX JOINT YIELDED A LIFE OF 3,600 EFPL SECONDS. THIS LIFE CORRELATED TO THE ENGINE 2206 FAILURE AND TO THE LIFE OF THE 0.020 TRIPOD ON A "A" FLEX JOINT ASSUMING FAILURE WOULD HAVE OCCURRED ON THE NEXT TEST IN

CONJUNCTION WITH A CORRECTION FOR THE LOWER [illegible]ESSES IN AN "A" FLEX JOINT. ALTHOUGH THE PROBABILITY IS EXTREMELY SMALL FOR HAVING A COMBINED SET OF CONDITIONS MORE SEVERE THAN THE ENGINE 2206 FAILURE, AN INTERIM LIMIT OF 3600/2 = 1800 EFPL IS ESTABLISHED AS A LIMIT FOR DUCTS WITH UNKNOWN TRIPOD LEG DOGLEG RADII AND CROSS SECTION IN THE POSITION

(C O N T I N U A T I O N)

MSFC #: A12281 IFA #: CONTRACTOR #: A008935

"C" FLEX JOINT (REFERENCE DAR 2296-R1).
A PROGRAM OF INSPECTING LPF DUCT FLEX JOINT C TRIPOD DOGLEG RADII WAS DEVELOPED IN ORDER TO DETERMINED THE ACTUAL RADIUS AND SECTION PROPERTIES AND THEREBY NOT HAVING TO USE THE WORST CASE VALUES FOR THESE PARAMETERS. THE INSPECTION WAS DESIGNED TO EVALUATE THE RADIUS USING A BORESCOPE COMPARATIVE ANALYSIS TECHNIQUE. THE MAJOR LIMITATION OF THE CURRENT INSPECTION TECHNIQUE HOWEVER, IS THE INABILITY OF DETERMINING A SPECIFIC RADIUS VALUE. THE MOST RELIABLE CRITERION DEVELOPED IS A SIMPLE PASS/NO PASS METHOD IN WHICH THE REPORTED VALUE IS EITHER GREATER THAN 0.030 ON "UNABLE TO VERIFY" GREATER THAN 0.030. CONVERSELY THOUGH, THE SECTION PROPERTIES ARE READILY CHARACTERIZED BY BORESCOPE EVALUATION. LIFE LIMITS WERE IMPOSED, BASED ON THIS INSPECTION TECHNIQUE, USING DARS 2296, 2315 (FOR TWO DEVELOPMENT UNITS), AND 2333 (FOR THE ENGINE 0208 TEST BED UNIT).
A NEW TECHNOLOGY VIDEO BORESCOPE HAS BEEN REQUISITIONED WHICH ALLOWS IMPROVED QUANTIFICATION OF THE TRIPOD LEG RADIUS. THIS SHOULD ALLOW EXTENSION OF THE CONSERVATIVE LIMITS IMPOSED PRESENTLY.
ALL EXISTING FLEX JOINTS DETAILS AND FLEX JOINTS NOT PRESENTLY WELDED INTO DUCTS WILL BE INSPECTED FOR PROPER TRIPOD LEG RADIUS AND SECTION PROPERTIES. THIS INSPECTION WILL BE ACCOMPLISHED BY QUALITY ASSURANCE WORK AUTHORIZATION.
TO ELIMINATE THE INADEQUATE RADIUS CONDITION FROM FUTURE FLEX JOINT UNITS INSPECTION OF THE TRIPOD LEG RADII WILL BE REQUIRED AFTER FINAL HAND BLENDING. VENDOR PLANNING HAS BEEN REVISED ACCORDINGLY (REFERENCE INTERNAL LETTER 89-0E-219). THE RS008981 AND RS008961 DRAWINGS HAVE BEEN REVISED TO CLARIFY INSPECTION REQUIREMENTS FOR THE TRIPOD LEG RADII. REFERENCE DRAWING CHANGE EO 360313.
12/11/89 - PROBLEM CLOSED BY PRB. ACTION ITEM 253-2 CLOSED BY PRB.

MSFC RESPONSE/CONCURRENCE:

MSFC RPT # : A13939
STATUS : CLOSED
FAIL MODE : MC
R/C CODE 1 : 7
NCA NOMEN : BLADE, 2ND STAGE
FAIL DATE : 07/24/91
PROB TITLE : SSME 0215 MAJOR INCIDENT HPFTP (2ND STAGE BLADE FAILURE)
SYSTEM : TURBOMCHNERY
FUNCT CRIT : 1
LOCATION : SSC A1
TEST OPER. : D
NCA PART # : RS007520
MSFC CLOS : 11/12/91
FMEA # : 8200-04
HRDWR CRIT : 1
CAUSE : MP
DEFECT : DC
NCA SERLOT : UNK.

PROB DESCR :

WRITTEN BY: J BRYANT DEPT: 559 000 DATE: 07 24 91
HOTFIRE TEST 901666 HAD PREMATURE ENGINE CUTOFF AT ENGINE START PLUS 4.41 SECONDS.THE FOLLOWING 9 FIDS WERE RECORDED:

15005	CCV CH A ACTUATOR
111301	LPFTP DISCH PR CH A
11302	LPFTP DISCH PR CH B
20003	THRUST LIMITING CONDITIONS
111203	MCC PC CONTROL AND IGNITION CONFIRMATION FIXED LIMIT AND PC REF CH REASONABLENESS CH A
11204	MCC PC CONTROL AND IGNITION CONFIRMATION FIXED LIMIT AND PC REF CH REASONABLENESS CH A
111303	LPFTP DISCH TEMP CH A
11304	LPFTP DISCH TEMP CH B
111101	FUEL FLOWRATE INTRA-CHANNEL TEST CH A

EXTERNAL FIRE IN FUEL PREBURNER AREA WAS OBSERVED AFTER CADS CUT.

WRITTEN BY: P MAY DEPT: 866 214 DATE: 08 01 91
ADDENDUM TO UCR A030973
RS007531 SEAL S/N 8727953 IDCR 1009559
DURING PUMP DISASSEMBLY IT WAS NOTICED THAT THE SEAL HAD NO INTERFERENCE FIT WITH THE 4.994 I.D. OF THE RS007532-091 S/N 4875578 DIFFUSER. WITH SEAL INSTALLED EXCESSIVE MOVEMENT WAS NOTICED. SHOULD HAVE INTERFERENCE FIT PER ASSY SPEC REQTS.
WRITTEN BY: J OLSEN DEPT: 568 351 DATE: 08 13 91

WRITTEN BY: Z HUANG DEPT: 695 351 DATE: 09 05 91
ADDITIONAL INFO. TO UCR A030973: MCC U/N 4010, P/N

(C O N T I N U A T I O N)

MSFC #: A13939 IFA #: CONTRACTOR #: A030973

G15RS009105-531, S/N 4866385 WAS SEVERELY DAMAGED DURING TEST 901-666 DUE TO THE MAJOR INCIDENT. SEVERE EROSION OF THE

NARLOY-Z LINER NOTED FWD OF THE THROAT. THE EDNI IS VISIBLE FROM THE ID. SIDE. TWO BURN THROUGHS EXIST IN THE INCONEL 718 STRUCTURAL JACKET FWD OF THE THROAT. REFER IDCR 1008043.

INVESTIGATION/RESOLUTION :

CLS AND/OR DEFERRAL PROBLEM DESCRIPTION
TEST 901-666 PREMATURE ENGINE SHUTDOWN
WRITTEN BY: S TRAMMELL DEPT: 525 476 DATE: 07 30 91

TEST 901-666 OF PHASE II+ ENGINE 0215 WAS TERMINATED AT START PLUS 4.3 SECONDS OF A PLANNED 513 SECOND DURATION, DUE TO THE DETECTION OF CONTROLLER ELECTRICAL LOCKUP.
WRITTEN BY: A TODISCO DEPT: 568 351 DATE: 07 30 91

WRITTEN BY: E JANNERIAN DEPT: 568 351 DATE: 08 26 91
FAR DEFERRAL: KEVIN CRAMER; 520-170 08/26/91
THE PROBLEM IS DEFERRED FOR STS-48.
TEST 901-666 EXPERIENCED A PREMATURE ENGINE SHUTDOWN AT ENGINE START PLUS 4.33 SECONDS DUE TO DEGRADED ENGINE PERFORMANCE. A LOSS OF FUEL FLOW RESULTED IN EXTENSIVE HOT GAS SYSTEM EROSION. THE TEST HAS BEEN CLASSIFIED AS A MAJOR INCIDENT.
INCIDENT INVESTIGATION OF DEFERRAL:
ENGINE INCIDENT TEAMS WERE FORMED AT BOTH ROCKETDYNE AND MSFC TO DETERMINE THE FAILURE CAUSE. A REVIEW OF BOTH THE TEST DATA AND THE HARDWARE CONCLUDED THAT THE FAILURE INITIATED IN THE TURBINE SECTION OF THE HPFTP (UNIT 5602R1) FURTHER ANALYSIS INDICATED THAT A TURBINE BLADE FAILURE WAS THE INITIAL EVENT. THE INVESTIGATION THEN CONCENTRATED ON THE CAUSE OF THE BLADE FAILURE. A FISHBONE CHART WAS GENERATED TO IDENTIFY ALL POTENTIAL FAILURE MODES (SEE BACK-UP DATA 1). PRO/CON CHARTS WERE THEN CREATED TO INDENTIFY THE MOST LIKELY CAUSES FOR THE BLADE FAILURE.
ANALYSIS OF THE TEST DATA SHOWED THE HPFTP EXHIBITED A SPEED RECOVERY AFTER THE INITIAL LOSS OF POWER. THE SPEED RECOVERY WAS DRIVEN BY AN INCREASE IN TURBINE DELTA PRESSURE WHICH INDICATES SUFFICIENT BLADE MATERIAL WAS REMAINING TO GENERATE POWER.
ME&T ANALYSIS OF THE FIRST STAGE BLADES INDICATES ALL BLADES HAVE LIQUID METAL EMBRITTLEMENT FIRTREE CORNER LOBE CRACKS. THESE CRACKS WERE THERMALLY INDUCED BY THE EXCESSIVE TURBINE INLET TEMPERATURES DURING THE INCIDENT WHICH DEPOSITED MELTED GOLD ON THE FIRTREE CORNERS. NO FIRTREE OVERLOAD CRACKS WERE OBSERVED. EXAMINATION OF THE SECOND STAGE BLADES SHOWED 55 OF 59 BLADES HAS SUCTION SIDE FIRTREE OVERLOAD CRACKS INDICATING THE BLADES WERE IMPACTED. THESE DATA ALONG WITH THE SPEED RECOVERY SUGGESTS THE FAILURE INITIATED IN THE SECOND STAGE.
TWO OF THE SECOND BLADES FRACTURED FLUSH WITH THE DISC OUTSIDE DIAMETER (POSITION 44 AND 48); THE REMAINING [illegible]ADES HAD APPROXIMATELY 75 PERCENT OF THE BLADE SHANK [illegible]AINING.THE BLADE

IN POSITION 44 SHOWED CHARACTERISTICS OF OVERLOAD ON THE

(C O N T I N U A T I O N)

MSFC #: A13939 IFA #: CONTRACTOR #: A030973

FRACTURED SURFACE. THE BLADE IN POSITION 48 EXHIBITED A THUMBNAIL IMPRINT ON THE FRACTURE SURFACE. THE THUMBNAIL COVERED APPROXIMATELY 25 PERCENT OF THE SURFACE AREA AT THE FRACTURE. THE REMAINING SURFACE INDICATED A DUCTILE OVERLOAD FRACTURE. THE FRACTURE SURFACE WAS ERODED AND OXIDIZED, BUT A CLOSE EXAMINATION ALONG WITH SECTIONING OF THE BLADE INDICATED THAT THE THUMBNAIL MAY HAVE BEEN A PRE-EXISTING CRACK IN THE BLADE. INTERDENDRITIC POROSITY WAS OBSERVED ALONG THE CRACK SURFACE. A CRACK WAS NOTED ON THE PRESSURE SIDE OF FIRTREE LOBE #3 OF THE SAME BLADE. THE FRACTURE SURFACE WAS NOT DAMAGED AND THE MATERIAL ANALYSIS OF THIS CRACK INDICATED IT INITIATED SUBSURFACE AND PROPAGATED BY SUSTAINED LOAD HYDROGEN EMBRITTLEMENT. APPROXIMATELY TWENTY-ONE ARREST LINES WERE DISCOVERED. CT SCANS AND SUBSEQUENT SECTIONING OF THE BLADE INDICATED A NETWORK OF SUBSURFACE INTERDENDRITIC POROSITY. HYDROGEN MOST LIKELY ENTERED THOUGH THE NETWORK OF POROSITY AND CAUSED THE MATERIAL TO BECOME BRITTLE. THE CRACK THEN PROPAGATED VIA SUSTAINED LOAD. STRUCTURAL ANALYSIS AND FRACTURE MECHANICS SHOW THAT WITH THE PRE-EXISTING CRACK IN BLADE 48, THE BLADE COULD FAIL UNDER NORMAL OPERATING CONDITIONS. FAILURE OF THIS BLADE IS THE MOST LIKELY FAILURE CAUSE FOR THIS INCIDENT.
TO INVESTIGATE THE POTENTIAL FOR POROSITY IN OTHER BLADE SETS, CT SCAN AND X-RAY TECHNIQUES ARE BEING UTILIZED. ALL SECOND STAGE BLADES FROM 5602R1 WERE INSPECTED BY THESE TECHNIQUES. ONE ADDITIONAL BLADE WAS NOTED TO HAVE POROSITY (POSITION 19). SECTIONING OF THE BLADE INDICATED A POTENTIAL HYDROGEN CRACK ON THE SUCTION SIDE ROOT ABOVE THE SECOND LOBE. THE CRACK INITIATED SUBSURFACE IN AN AREA OF POROSITY. ELEVEN BLADES FROM THIS SET HAVE BEEN SECTIONED AND NO INCIDENCES OF POROSITY OR HYDROGEN CRACKING HAVE BEEN OBSERVED. THE FLEET LEADER SECOND STAGE BLADES (43 STARTS FOR 18242 SECONDS LAST USED IN HPFTP 12108R3) WERE CT SCANNED AND X-RAYED. ONE BLADE WAS DETERMINED TO HAVE POROSITY. THE BLADE WAS SECTIONED AND NO HYDROGEN CRACKS WERE NOTED. OTHER HIGH TIME BLADE SETS WILL BE CT SCANNED AND SECTIONED AS REQUIRED.
WRITTEN BY: L JAVAHERIAN DEPT: 568 351 DATE: 08 29 91
VIA TSO BY: M JACOBSON DEPT: 520 170 DATE: 11/05/91

TEST 901-666 (ENGINE 0215) EXPERIENCED A PREMATURE ENGINE SHUTDOWN DUE TO ELECTRICAL LOCK-UP PRIOR TO SIMULATED SRB IGNITION AT 4.34 SECONDS. A LOSS OF FUEL FLOW RESULTED IN EXTENSIVE HOT GAS SYSTEM EROSION AND AN EXTERNAL FIRE. THE TEST HAS BEEN CLASSIFIED AS A MAJOR INCIDENT.
WRITTEN BY: M JACOBSON DEPT: 520 170 DATE: 11 05 91

INVESTIGATION
TEST 901-666 PREMATURE ENGINE SHUTDOWN
VIA TSO BY: M JACOBSON DEPT: 520 170 DATE: 11/05/91
ENGINE INCIDENT TEAMS WERE FORMED AT BOTH ROCKETDYNE AND MSFC TO DETERMINE THE FAILURE CAUSE. A REVIEW OF BOTH THE TEST DATA AND THE HARDWARE CONCLUDED THAT THE FAILURE INITIATED IN THE TURBINE SECTION OF THE HPFTP (UNIT 5602R1). FURTHER ANALYSIS

(C O N T I N U A T I O N)

MSFC #: A13939 IFA #: CONTRACTOR #: A030973

INDICATED THAT A TURBINE BLADE FAILURE WAS THE INITIAL EVENT. A FISHBONE CHART WAS GENERATED TO IDENTIFY ALL POTENTIAL FAILURE MODES (SEE BACK-UP DATA 1). PRO/CON CHARTS WERE THEN CREATED TO IDENTIFY THE MOST LIKELY CAUSES FOR THE BLADE FAILURE.
ANALYSIS OF THE TEST DATA SHOWED THE HPFTP EXHIBITED A SPEED RECOVERY AFTER THE INITIAL LOSS OF POWER. THE SPEED RECOVERY WAS DRIVEN BY AN INCREASE IN TURBINE DELTA PRESSURE WHICH INDICATES SUFFICIENT BLADE MATERIAL WAS REMAINING TO GENERATE POWER.
ME&T ANALYSIS OF THE FIRST STAGE BLADES INDICATES ALL BLADES HAVE LIQUID METAL EMBRITTLEMENT FIRTREE CORNER LOBE CRACKS. THESE CRACKS WERE THERMALLY INDUCED BY THE EXCESSIVE TURBINE INLET TEMPERATURES DURING THE INCIDENT WHICH DEPOSITED MELTED GOLD ON THE FIRTREE CORNERS. NO FIRTREE OVERLOAD CRACKS WERE OBSERVED. EXAMINATION OF THE SECOND STAGE BLADES SHOWED 55 OF 59 BLADES HAD SUCTION SIDE FIRTREE OVERLOAD CRACKS INDICATING THE BLADES WERE IMPACTED. THESE DATA ALONG WITH THE SPEED RECOVERY SUGGESTS THE FAILURE INITIATED IN THE SECOND STAGE. TWO OF THE SECOND BLADES FRACTURED FLUSH WITH THE DISC OUTSIDE DIAMETER (POSITION 44 AND 48); THE REMAINING BLADES HAD APPROXIMATELY 75 PERCENT OF THE BLADE SHANK REMAINING. THE BLADE IN POSITION 44 SHOWED CHARACTERISTICS OF OVERLOAD ON THE FRACTURED SURFACE. THE BLADE IN POSITION 48 EXHIBITED A THUMBNAIL IMPRINT WHICH COVERED APPROXIMATELY [illegible] PERCENT OF

THE SURFACE AREA AT THE FRACTURE. THE REMAINING SURFACE INDICATED A DUCTILE OVERLOAD FRACTURE. THE FRACTURE SURFACE WAS ERODED AND OXIDIZED, BUT A CLOSE EXAMINATION ALONG WITH SECTIONING OF THE BLADE INDICATED THAT THE THUMBNAIL WAS A PRE-EXISTING CRACK IN THE BLADE. A NETWORK OF INTERDENDRITIC POROSITY WAS OBSERVED ALONG THE CRACK SURFACE AND THROUGHOUT THE FIRTREE CONNECTING TO THE SURFACE . A CRACK WAS NOTED ON THE PRESSURE SIDE OF FIRTREE LOBE #3 OF THE SAME BLADE INITIATED IN THE SAME NETWORK OF POROSITY. THE FRACTURE SURFACE WAS NOT DAMAGED AND THE MATERIAL ANALYSIS OF THIS CRACK INDICATED IT INITIATED SUBSURFACE AND PROPAGATED BY SUSTAINED LOAD HYDROGEN EMBRITTLEMENT. APPROXIMATELY TWENTY ONE ARREST LINES WERE DISCOVERED. HYDROGEN MOST LIKELY ENTERED THROUGH THE NETWORK OF POROSITY AND CAUSED THE MATERIAL TO BECOME BRITTLE. THE CRACK THEN PROPAGATED VIA SUSTAINED LOAD. STRUCTURAL ANALYSIS AND FRACTURE MECHANICS SHOW THAT WITH THE PREEXISTING CRACK IN BLADE 48, THE BLADE COULD FAIL UNDER NORMAL OPERATION CONDITIONS. FAILURE OF THIS BLADE IS THE MOST LIKELY FAILURE CAUSE FOR THIS INCIDENT. THIS BLADE SET HAD ACCUMULATED 35 STARTS FOR 13225 SECONDS.
TO INVESTIGATE THE POTENTIAL FOR POROSITY IN OTHER BLADE SETS, COMPUTER TOMOGRAPHY (CT) SCAN AND X-RAY TECHNIQUES WERE UTILIZED. ALL SECOND STAGE BLADES FROM HPFTP 5602R1 WERE INSPECTED BY THESE TECHNIQUES. ONE ADDITIONAL BLADE WAS NOTED TO HAVE POROSITY (POSITION 19 S/N AL895). SECTIONING OF THE BLADE INDICATED A HYDROGEN CRACK ON THE SUCTION SIDE ROOT

ABOVE THE SECOND LOBE. THE CRACK INITIATED SUBSURFACE IN AN AREA OF POROSITY. SEVENTEEN OTHER BLADES FROM THIS SET WERE SECTIONED AND NO OTHER INCIDENCES OF POROSITY OR HYDROGEN CRACKING WERE OBSERVED.
ADDITIONAL BLADE SETS WERE CT INSPECTED, X-RAYED AND SOME BLADES WERE SECTIONED. A SUMMARY OF THE RESULTS AS OF MID OCTOBER IS SHOWN IN BACKUP DATA 2. APPROXIMATELY 3.2 PERCENT OF THE BLADES INSPECTED HAVE SHOWN EVIDENCE OF INTERNAL POROSITY. SECTIONING OF 113 BLADES HAS REVEALED ONLY ONE ADDITIONAL BLADE (AK925) WITH A SUSPECT HYDROGEN CRACK. THIS WAS ON THE FLEET LEADER SECOND STAGE BLADE SET WHICH ACCUMULATED 43 STARTS FOR 18242 SECONDS. THE CRACK WAS ONLY

0.02 INCH DEEP AND TOO SMALL TO PERFORM METALLURGICAL ANALYSIS. TO DATE, THE POROSITY IN THE FAILED BLADE FROM HPFTP 5602R1 IS THE MOST EXTENSIVE EXPERIENCED.

PROBLEM CAUSE
TEST 901-666 PREMATURE ENGINE SHUTDOWN
VIA TSO BY: M JACOBSON DEPT: 520 170 DATE: 11/05/91
THE ENGINE INCIDENT WAS INITIATED BY A SECOND STAGE BLADE FAILURE IN THE HPFTP. THE BLADE FAILURE WAS A RESULT OF INTERNAL POROSITY WHICH ALLOWED HYDROGEN TO ENTER AND EMBRITTLE THE BLADE MATERIAL. AN INTERNAL CRACK INITIATED AND PROPAGATED BY HYDROGEN ASSISTED LCF DURING THE BLADE TEST HISTORY OF 35 STARTS FOR 13255 SECONDS. THE BLADE FAILED DUE TO THE INABILITY TO CARRY THE OPERATING LOAD WITH THE PRESENCE OF THE CRACK

REMEDIAL ACTION
TEST 901-666 PREMATURE ENGINE SHUTDOWN
VIA TSO BY: M JACOBSON DEPT: 520 170 DATE: 11/05/91
FIRST AND SECOND STAGE BLADE FLIGHT LIFE HAS BEEN RESTRICTED BY DARS 2552R1 AND 2553R1. THE CURRENT LIMIT IS 4300 SECONDS WHICH HAS BEEN APPROVED FOR STS-44. THIS LIMIT WAS DERIVED UTILIZING A LIMITED DATA SAMPLE CONSISTING OF ONLY THE CURRENT CONFIGURATION FIRST AND SECOND STAGE BLADE HISTORIES AND EQUATES TO A THREE ENGINE RELIABILITY OF 0.999. SINCE THE ROOT CAUSE OF THE PROBLEM IS POROSITY GENERATED FROM THE FABRICATION PROCESS, THE ENTIRE BLADE HISTORY (ALL HPFTP CONFIGURATIONS) WOULD BE APPLICABLE TO GENERATE A LIMIT. THE LIMIT MAY BE EXTENDED FOR FUTURE FLIGHTS. FOR GROUND TEST UNITS, A LIMIT OF APPROXIMATELY TWICE THE FLIGHT LIMIT WILL BE ENFORCED.

FMEA/CIL INTERFACE
TEST 901-666 PREMATURE ENGINE SHUTDOWN
VIA TSO BY: M JACOBSON DEPT: 520 170 DATE: 11/05/91
FMEA/CIL B-200 MODE 4- STRUCTURAL FAILURE OF THE TURBINE BLADES
CAUSE A - ROTOR BLADE CRACKS

CRITICALITY CODE - 1
THE CIL WILL BE AMENDED TO REFLECT THE RECURRENCE CONTROL.

BACK-UP TEXT
TEST 901-666 PREMATURE ENGINE SHUTDOWN
VIA TSO BY: M JACOBSON DEPT: 520 170 DATE: 11/05/91
SEE ATTACHED CHARTS 1 AND 2

RECURRENCE CONTROL
TEST 901-666 PREMATURE ENGINE SHUTDOWN
VIA TSO BY: M JACOBSON DEPT: 520 170 DATE: 11/05/91
FOR PRODUCTION UNITS, DAR 2552R1 AND 2553R1 RESTRICT THE FIRST AND SECOND STAGE BLADE FLIGHT LIFE. THE CURRENT LIMIT IS 4300 SECONDS. THIS LIMIT WAS DERIVED UTILIZING A LIMITED DATA SAMPLE CONSISTING OF ONLY THE CURRENT CONFIGURATION FIRST AND SECOND STAGE BLADE HISTORIES AND EQUATES TO A THREE ENGINE RELIABILITY OF 0.999. FOR GROUND TEST UNITS, A LIMIT OF APPROXIMATELY TWICE THE FLIGHT LIMIT WILL BE ENFORCED.
A CT TECHNIQUE HAS BEEN DEVELOPED TO DETECT THE PRESENCE OF INTERNAL POROSITY. THE TECHNIQUE WAS DEVELOPED THROUGH CT SCANS AND SUBSEQUENT SECTIONING OF MULTIPLE BLADE SETS. THE TECHNIQUE HAS BEEN VERIFIED ON SEVERAL DEVELOPMENT UNITS. A SPECIFICATION IS BEING PREPARED TO IMPLEMENT THIS PROCESS ON PRODUCTION UNITS. IN THE INTERIM, PRODUCTION BUILDS WILL HAVE THIS INSPECTION IMPLEMENTED BY HSPOA. WHEN THE FLEET IS RETROFITTED WITH CT INSPECTED BLADES, A NEW FLIGHT LIMIT WILL BE ESTABLISHED.

DEFERRAL RATIONAL TEXT
SSME 0215 MAJOR INCIDENT
WRITTEN BY: S TRAMMELL DEPT: 525 476 DATE: 07 30 91

THIS DEFERRAL IS BASED UPON THE FRR BRIEFING SUBMITTED TO THE LEVEL 1 PRCB ON 7/30/91. THE FOLLOWING IS A SUMMARY OF THIS BRIEFING.

THE INVESTIGATION WORK COMPLETED AS OF THIS DATE HAS DETERMINED THAT THE INCIDENT WAS CAUSED BY A FAILURE OF A HPFTP TURBINE BLADE.

THE MOST LIKELY CAUSES OF THE TURBINE BLADE FAILURE ARE THE CRACKING/DEFLECTION OF THE MAIN HOUSING INNER RING, OR THE INJESTION OF A TURBINE SUPPORT INLET SHEET METAL FRAGMENT. THESE FAILURE MODES WOULD RESULT IN TURBINE BLADE IMPACT OR SEVERE RUBBING.

ENGINE 0215 HPFTP U/N 5602R1 HAD ACCUMMULATED 61 STARTS (66% FLEET LEADER) AND 25,143 SECONDS (64% FLEET LEADER). THE MAIN HOUSING INNER RING HAD TWO TYPE "A" CRACKS AND SIX ADDITIONAL CRACKS. THE HPFTP TURBINE SUPPORT HAD A HISTORY OF EXTENSIVE

SHEET METAL CRACK REPAIRS. THE HPFTP WAS ALSO BEING USED FOR MARGIN DEMONSTRATION OF TURBINE THERMAL CRACKING AND REPAIRS.

RATIONALE FOR FLIGHT:

THE HPFTP'S SCHEDULED FOR STS-43 ARE LOW TIME UNITS AND HAVE NO TYPE "A" CRACKS OF THEIR HOUSING INNER RING. THE PUMPS ALSO HAVE HAD ONLY MINOR TURBINE SUPPORT SHEET METAL CRACK REPAIRS. FABRICATION, INSPECTION AND REPAIR HISTORIES OF THE THREE FLIGHT UNITS WERE REVIEWED AND ARE WITHIN FLIGHT EXPERIENCE.

HPFTP HOUSING:

HPFTP U/N	% FLEET LEADER STARTS / SECONDS	% 5602R1 STARTS / SECONDS
6102R3	11.0 / 14.2	16.4 / 17.6
4007R3	8.8 / 9.6	13.1 / 11.9
6009	2.2 / 2.6	3.3 / 3.3

HPFTP TURBINE SUPPORT:

HPFTP U/N	% FLEET LEADER STARTS / SECONDS	% 5602R1 STARTS / SECONDS
6102R3	7.5 / 13.8	10.7 / 13.8
4007R3	7.5 / 10.5	10.7 / 10.5
6009	5.7 / 7.6	8.0 / 7.6

WORK IS CONTINUING TO DETERMINE THE EXACT CAUSE OF THE INCIDENT. ONCE THE CAUSE IS DETERMINED AN ADDITIONAL UCR WILL BE GENERATED AGAINST THE SUSPECT HARDWARE.

THE CLOSURE OF THIS UCR IS DEFERRED FOR THREE (3) FLIGHTS OR SIX

WRITTEN BY: A TODISCO DEPT: 568 351 DATE: 07 30 91
WRITTEN BY: L JAVAHERIAN DEPT: 568 351 DATE: 08 29 91
WRITTEN BY: L JAVAHERIAN DEPT: 568 351 DATE: 08 29 91
THE ENGINE FAILURE OCCURRED ON A NON FLIGHT CONFIGURATION ENGINE WITH FLEET LEADER OR HIGH TIME TURBINE COMPONENTS. MARGIN TESTING WAS BEING PERFORMED ON SOME COMPONENTS INCLUDING THE MAIN HOUSING, TURBINE BEARING SUPPORT AND THE TURBINE BLADES. DISCOVERY UNITS ARE ACCEPTABLE BASED ON ALL POTENTIAL FAILURE MODES. THE MAJOR TURBINE COMPONENTS ARE LOW TIME WITH RESPECT TO THE FLEET LEADER AND FAILED UNIT (SEE BACKUP DATA 2). FABRICATION, INSPECTION AND PERFORMANCE HISTORIES OF THE DISCOVERY UNITS ARE NOMINAL AND WITHIN PREVIOUS FLIGHT EXPERIENCE. REVIEW OF THE FAILED BLADE PROCESSING INDICATES NO GENERIC PROBLEM WITH BLADES CAST IN THE SAME LOT (ONE BLADE FROM THIS LOT IS ON DISCOVERY). THE CASTING SCRAP RATE IS NORMAL WHEN COMPARED TO OTHER LOTS AND 12 BLADES FROM THE LOT HAVE

(C O N T I N U A T I O N)

MSFC #: A13939 IFA #: CONTRACTOR #: A030973

BEEN CT SCANNED INSPECTED WITH NO POROSITY FOUND.
A PROBABILITY ANALYSIS INDICATES DISCOVERY UNITS HAVE A LOW PROBABILITY OF FAILURE. BASED ON DISCOVERY UNIT BLADE TIMES THE RELIABILITY FOR A THREE ENGINE CLUSTER IS AS FOLLOWS:
FIRST STAGE BLADE RELIABILITY = 0.99993
SECOND STAGE BLADE RELIABILITY = 0.99986

41 SECOND STAGE BLADE SETS HAVE ACCUMULATED MORE STARTS AND 24 SETS HAVE ACCUMULATED MORE TIME THAN THE HIGHEST DISCOVERY UNIT.
71 FIRST STAGE BLADE SETS HAVE ACCUMULATED MORE STARTS AND 41 SETS HAVE ACCUMULATED MORE TIME THAN THE HIGHEST DISCOVERY UNIT.
IN ADDITION, DARS 2552 AND 2553 HAVE BEEN WRITTEN TO LIMIT THE USE OF FLIGHT BLADES TO 4500 SECOND FOR THE SECOND STAGE AND 5500 SECONDS FOR THE FIRST STAGE.
FINALLY, EXTENSIVE FLIGHT OPERATIONAL HISTORY HAS BEEN ACCUMULATED WITH THE FLIGHT CONFIGURATION HPFTP. SIXTY SEVEN BUILDS HAVE BEEN TESTED FOR OVER 430 STARTS AND SECONDS.

MSFC RESPONSE/CONCURRENCE:

7/30/91 - PROBLEM IS DEFERRED BY PRB 334 FOR STS-43 PER RATIONALE E: THE PROBLEM IS TIME/AGE/LIFE CYCLE RELATED AND THE FLIGHT UNITS WILL HAVE ACCUMULATED LESS THAN 50 PERCENT OF THE CRITICAL PARAMETER(S) AT THE END

OF THE NEXT FLIGHT. DEFERRAL IS BASED ON HARD COPIES SENT IN BY ROCKETDYNE. MSFC IS AWAITING ELECTRONIC TRANSFER.

8/1/91 - FAR DEFERRAL RECEIVED BY ELECTRONIC TRANSFER FROM ROCKETDYNE.

08/14/91 - THIS UCR WAS TRANSFERRED TO FUEL TURBOMACHINERY.

9/4/91 PRB - CLOSURE OF THIS PROBLEM WAS DEFERED THROUGH FLIGHT STS-48. DEFERRAL RATIONALE E: "THE PROBLEM IS TIME/AGE/LIFE/CYCLE RELATED AND THE FLIGHT UNITS WILL HAVE ACCUMULATED LESS THAN 50 PERCENT OF THE CRITICAL PARAMETER(S) AT THE END OF THE NEXT FLIGHT."

11/12/91 PRB - THIS PROBLEM WAS OFFICIALLY CLOSED.

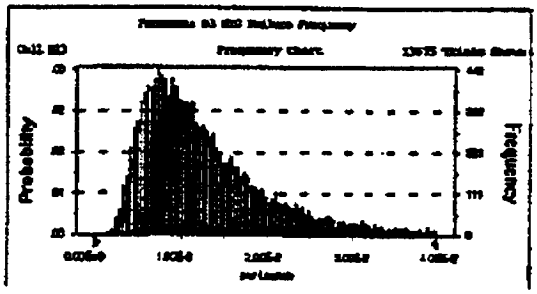
1993 STS Catastrophic Failure Frequency Simulation

Forecast: 93 STS Failure Frequency **Cell: E13**

Summary:

Display Range is from 0.00E+0 to 4.00E-2 per Launch
Entire Range is from 1.54E-3 to 1.62E-1 per Launch
After 20,000 Trials, the Std. Error of the Mean is 0.00

Statistics:	Display Range	Entire Range
Trials	13675	14020
Mean	1.28E-02	1.38E-02
Median (exact)	1.09E-02	1.11E-02
Mode (exact)	1.54E-03	1.54E-03
Standard Deviation	7.29E-03	1.01E-02
Variance	5.31E-05	1.01E-04
Skewness	1.24	(unavailable)
Kurtosis	4.36	(unavailable)
Coeff. of Variability	0.57	0.73
Range Minimum	0.00E+00	1.54E-03
Range Maximum	4.00E-02	1.62E-01
Range Width	4.00E-02	1.60E-01
Mean Std. Error	6.23E-05	8.50E-05



Percentiles for Entire Range (per Launch):

Percentile	93 STS Failure Frequency (exact)
0%	1.54E-03
5%	4.48E-03
10%	5.38E-03
15%	6.12E-03
20%	6.83E-03
25%	7.49E-03
30%	8.13E-03
35%	8.86E-03
40%	9.54E-03
45%	1.03E-02
50%	1.11E-02
55%	1.20E-02
60%	1.29E-02
65%	1.40E-02
70%	1.53E-02
75%	1.67E-02
80%	1.86E-02
85%	2.12E-02
90%	2.49E-02
95%	3.20E-02
100%	1.62E-01

End of Forecast

1993 STS Catastrophic Failure Frequency Simulation

Forecast: 93 STS (Sensitivity 1) Failure Frequency **Cell: E21**

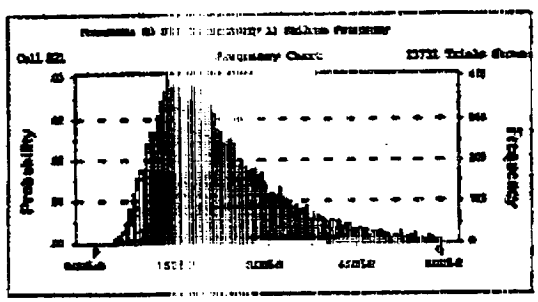
Summary:

Display Range is from 0.00E+0 to 5.00E-2

Entire Range is from 2.52E-3 to 1.66E-1

After 14,020 Trials, the Std. Error of the Mean is 0.00

Statistics:	Display Range	Entire Range
Trials	13731	14020
Mean	2.19E-02	2.26E-02
Median (exact)	1.97E-02	1.94E-02
Mode (exact)	2.52E-03	2.52E-03
Standard Deviation	1.07E-02	1.33E-02
Variance	1.14E-04	1.77E-04
Skewness	1.07	(unavailable)
Kurtosis	3.91	(unavailable)
Coeff. of Variability	0.50	0.59
Range Minimum	0.00E+00	2.52E-03
Range Maximum	5.00E-02	1.66E-01
Range Width	5.00E-02	1.64E-01
Mean Std. Error	9.12E-05	1.12E-04



Percentiles for Entire Range:

Percentile	S (Sensitivity 1) Failure Frequency (exact)
0%	2.52E-03
5%	8.48E-03
10%	1.02E-02
15%	1.16E-02
20%	1.27E-02
25%	1.37E-02
30%	1.48E-02
35%	1.59E-02
40%	1.70E-02
45%	1.82E-02
50%	1.94E-02
55%	2.06E-02
60%	2.21E-02
65%	2.37E-02
70%	2.55E-02
75%	2.78E-02
80%	3.04E-02
85%	3.39E-02
90%	3.89E-02
95%	4.77E-02
100%	1.66E-01

End of Forecast

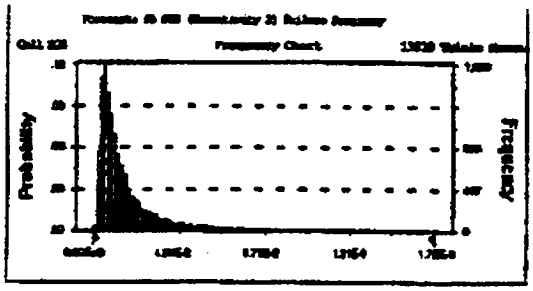
1993 STS Catastrophic Failure Frequency Simulation

Forecast: 93 STS (Sensitivity 2) Failure Frequency **Cell: E28**

Summary:

Display Range is from 0.00E+0 to 1.75E-1
Entire Range is from 9.83E-4 to 1.37E+0
After 14,020 Trials, the Std. Error of the Mean is 0.00

Statistics:	Display Range	Entire Range
Trials	13818	14020
Mean	1.90E-02	2.35E-02
Median (exact)	1.10E-02	1.12E-02
Mode (exact)	9.83E-04	9.83E-04
Standard Deviation	2.32E-02	4.96E-02
Variance	5.38E-04	2.46E-03
Skewness	3.13	(unavailable)
Kurtosis	14.84	(unavailable)
Coeff. of Variability	1.22	2.11
Range Minimum	0.00E+00	9.83E-04
Range Maximum	1.75E-01	1.37E+00
Range Width	1.75E-01	1.37E+00
Mean Std. Error	1.97E-04	4.19E-04



Percentiles for Entire Range:

Percentile	'93 (Sensitivity 2) Failure Frequency (exact)
0%	9.83E-04
5%	3.31E-03
10%	4.13E-03
15%	4.95E-03
20%	5.67E-03
25%	6.41E-03
30%	7.19E-03
35%	8.01E-03
40%	8.96E-03
45%	9.98E-03
50%	1.12E-02
55%	1.25E-02
60%	1.42E-02
65%	1.61E-02
70%	1.85E-02
75%	2.18E-02
80%	2.67E-02
85%	3.36E-02
90%	4.66E-02
95%	7.72E-02
100%	1.37E+00

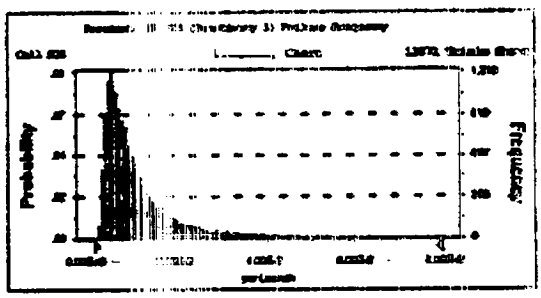
End of Forecast

Forecast: 93 STS (Sensitivity 3) Failure Frequency **Cell: E35**

Summary:

Display Range is from 0.00E+0 to 8.00E-2 per Launch
Entire Range is from 9.00E-4 to 1.09E+0 per Launch
After 14,020 Trials, the Std. Error of the Mean is 0.00

Statistics:	Display Range	Entire Range
Trials	13871	14020
Mean	1.06E-02	1.22E-02
Median (exact)	7.38E-03	7.4[illegible]E-03
Mode (exact)	1.00E-04	9.0[illegible]E-04
Standard Deviation	1.01E-02	2.2[illegible]E-02
Variance	1.02E-04	5.[illegible]E-04
Skewness	2.83	(unavailable)
Kurtosis	13.31	(unavailable)
Coeff. of Variability	0.96	1.[illegible]8
Range Minimum	0.00E+00	9.0[illegible]E-04
Range Maximum	8.00E-02	1.0[illegible]E+00
Range Width	8.00E-02	1.0[illegible]E+00
Mean Std. Error	8.59E-05	1.9[illegible]E-04



Percentiles for Entire Range (per Launch):

Percentile	S (Sensitivity 3) Failure Frequency (exact)
0%	9.0[illegible]E-04
5%	2.5[illegible]E-03
10%	3.1[illegible]E-03
15%	3.6[illegible]E-03
20%	4.1[illegible]E-03
25%	4.6[illegible]E-03
30%	5.0[illegible]E-03
35%	5.5[illegible]E-03
40%	6.1[illegible]E-03
45%	6.8[illegible]E-03
50%	7.4[illegible]E-03
55%	8.1[illegible]E-03
60%	9.0[illegible]E-03
65%	9.9[illegible]E-03
70%	1.11[illegible]E-02
75%	1.2[illegible]E-02
80%	1.4[illegible]E-02
85%	1.7[illegible]E-02
90%	2.2[illegible]E-02
95%	3.3[illegible]E-02
100%	1.0[illegible]E+00

End of Forecast

1993 STS Catastrophic Failure Frequency Simulation

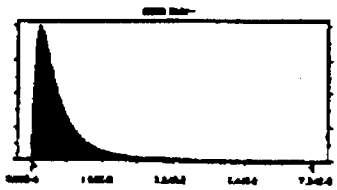
Assumptions

Assumption: RSRB Pair **Cell: E3**

Lognormal distribution with parameters:

Mean	7.80E-03	(=E3)
Standard Dev.	8.28E-03	(=M3)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 7.79E-3

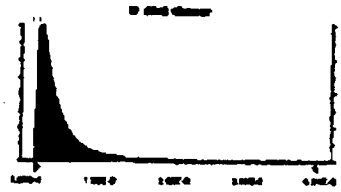


Assumption: 93 SSME Cluster **Cell: E5**

Lognormal distribution with parameters:

Mean	4.68E-03	(=E5)
Standard Dev.	5.74E-03	(=M5)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 4.70E-3

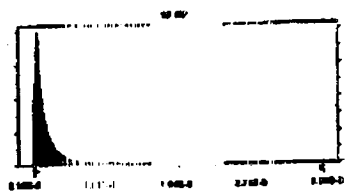


Assumption: 93 ET **Cell: E7**

Lognormal distribution with parameters:

Mean	1.93E-04	(=E7)
Standard Dev.	1.68E-04	(=M7)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 1.90E-4

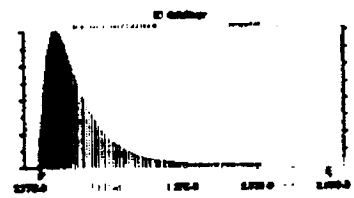


Assumption: 93 Orbiter **Cell: E9**

Lognormal distribution with parameters:

Mean	4.10E-04	(=E9)
Standard Dev.	3.93E-04	(=M9)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 4.11E-4



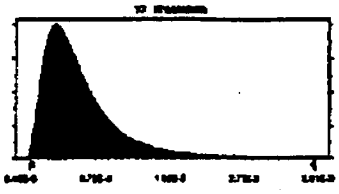
Assumption: 93 Prelaunch **Cell: E11**

Lognormal distribution with parameters:

Mean	7.03E-04	(=E11)
Standard Dev.	6.89E-04	(=M11)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 7.02E-4

Assumption: 93 Prelaunch (cont'd) **Cell: E11**

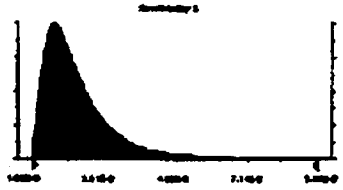


Assumption: Sensitivity 1 **Cell: E19**

Lognormal distribution with parameters:

Mean	1.66E-02	(=E19)
Standard Dev.	1.20E-02	(=M19)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 1.66E-2

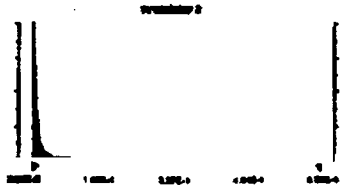


Assumption: Sensitivity 2 **Cell: E26**

Lognormal distribution with parameters:

Mean	1.82E-02	(=E26)
Standard Dev.	6.79E-02	(=M26)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 1.75E-2

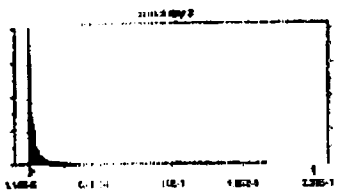


Assumption: Sensitivity 3 **Cell: E33**

Lognormal distribution with parameters:

Mean	6.11E-03	(=E33)
Standard Dev.	2.21E-02	(=M33)

Selected range is from 0.00E+0 to +Infinity
Mean value in simulation was 6.21E-3



End of Assumptions

Appendix H:

Comments on the Differences between the *Galileo* Study Results and *Galileo* - era Results in this Study

Appendix H:

Comments on the differences between the *Galileo* Study Results and *Galileo*-era results in this study.

The first step in the current analysis was to ensure that the updated failure frequency distributions resulted only from additional experience acquired since the *Galileo* study, and not from the inadvertent introduction of different statistical methods, tools, or assumptions. Unfortunately, there was insufficient information in the *Galileo* study report to exactly duplicate the previously published results for the SRBs and the SSMEs. At the central values (mean and median) of the system level failure frequency distributions, the regenerated values match very closely the published *Galileo* study values. Specifically, the *Galileo* study results were 1/78 and 1/55 for the median and mean, respectively. The corresponding values in the current study were 1/74 and 1/54. Since the updated (April 1993) results in this study are not completely consistent with the earlier results (even though they were well within the statistical certainty interval of the *Galileo* study), it was necessary to generate an intermediate set *Galileo*-era results using the original assumptions and data, but using the same statistical methods and tools that were applied in this update. These intermediate results are therefore entirely consistent with the updated results.

Since we were unable to perfectly duplicate the previously published results, it is impossible to know precisely the sources of the differences between the *Galileo* study calculations and the calculations used here. However, the principal source of the discrepancy appears to be a bias toward preserving the extreme values (fifth and ninety-fifth percentiles) of lower level distributions when generating higher level distributions (in the *Galileo* study), as opposed to preserving the central tendency (mean) of a distribution and one extreme (as was done in this study). The problem occurs when aggregating distributions or combining the distributions of risk contributors to generate the failure frequency distribution of the overall system. In general, the lower level distributions my not be well behaved or well modeled functions amenable to sampling for the Monte Carlo or Latin Hypercube simulations. The lower level distributions must therefore be converted to readily sampled distributions, preserving as much information about the original distribution as possible. In general this involves selecting the type of distribution best suited to model the original distribution, and two points from the original distribution to "anchor" the selected distribution type. In both the *Galileo* study and the current study the distribution type used in the simulations was the lognormal. The analysts performing the *Galileo* study appear to have selected the extremes (fifth and ninety-fifth percentiles) of the underlying distributions to anchor their lognormal distributions, allowing the central tendencies of the underlying distribution to "float" to fit the lognormal distribution.

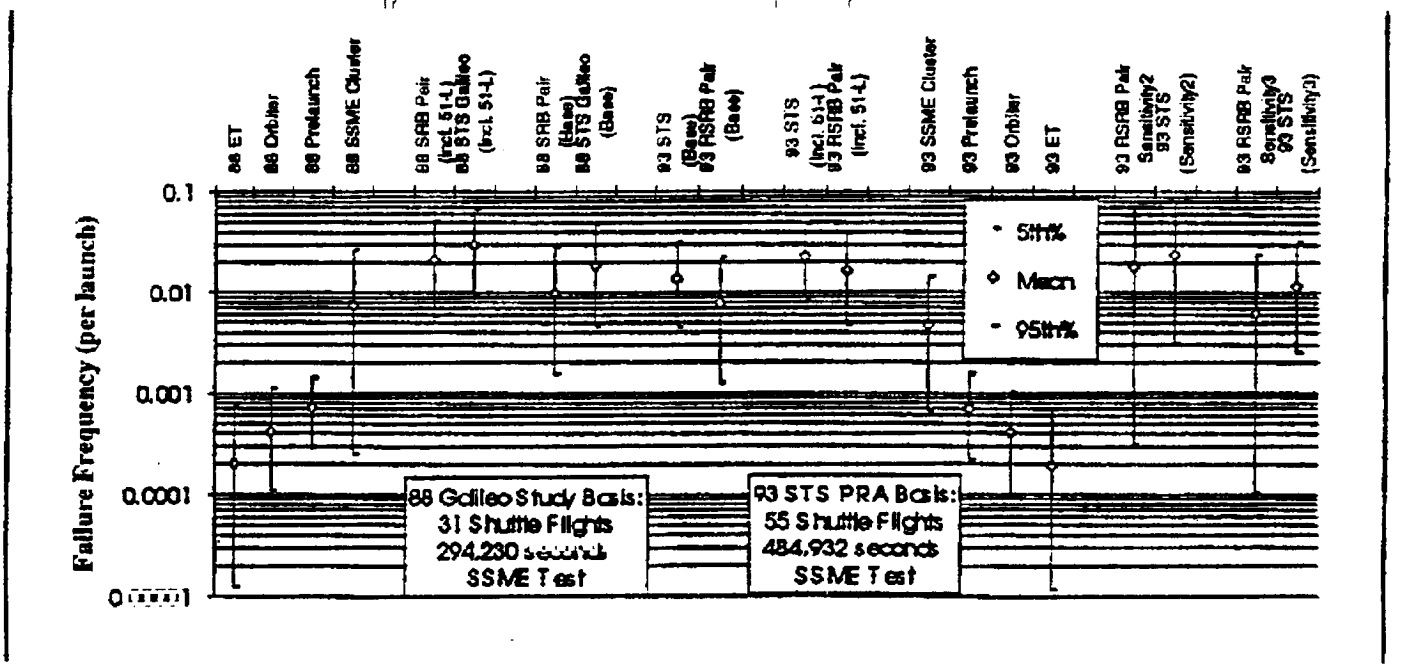
While the process of anchoring the extremes may have been justified for the unique purpose of the *Galileo* study, it was felt that for the purpose of this study, it was much more important that the central tendencies and the worst case tendencies (the mean and ninety-fifth percentiles) be anchored when converting distributions. In this study therefore, all distributions are generated using the maximum likelihood estimator (MLE) as the mean (MLE = failures / exposure), and all distributions are converted to lognormal preserving the mean and the error factor (EF). The error factor is determined by EF = 95th percentile / median. A converted distribution therefore preserves the mean and the relationship between the median and worst-case end of the underlying distribution.

Appendix I:

Determination of Shuttle Catastrophic Failure Frequency Using No Prior (non-Shuttle) Knowledge of SRB Failure Frequency

SAIC was asked to calculate the risk of Shuttle catastrophic ascent failure without using prior (non-Shuttle) knowledge to determine the RSRB failure frequency distribution. This analysis was performed and is shown here for contractual completeness. "Sensitivity 2" shows the estimated risk if the 51-L failure is included as relevant, and "Sensitivity 3" shows the estimated risk if the 51-L failure is discounted.

Figure I-1. Shuttle Failure Frequency Distributions



These cases show the failure frequency distribution for the RSRB pair (and the resulting STS failure frequency distribution) **if no prior knowledge about the reliability of the RSRB is assumed.** In these cases, the uncertainty in the failure frequency arises only from the statistical confidence associated with the data of 1 failure in 110 RSRB-launches (Sensitivity 2 - including the 51-L failure) or 0 failures in 109 RSRB launches (Sensitivity 3 - discounting the 51-L failure). We believe that the RSRB reliability belongs in the set of all U.S. solid rockets reliability, and that the use of the solid rocket prior is therefore justified. The appropriate distributions for general use are therefore the Base case and Sensitivity 1, depending upon the extent to which the decision maker believes that design and operational changes since the 51-L accident have controlled or mitigated the 51-L field joint failure mode.

Appendix J:

Presentation Viewgraphs

Probabilistic Risk Assessment of the Space Shuttle, Phase 1:

Space Shuttle Catastrophic Failure Frequency

An update of the 1988 *Galileo* RTG risk assessment with data through April, 1993.

SAIC®

Shuttle PRA Phase 1:

Shuttle Catastrophic Failure Frequency

- Summary of risk assessment results.
- Summary of risk assessment analysis method.
- Comparison of reliability analysis and risk assessment:
  - difference in objectives,
  - difference in results.
- Detailed risk assessment results:
  - comparison of 1988 Galileo study to current estimates,
  - comparison of risk contributors,
  - comparison of Shuttle with other launch vehicles.
- Conclusion.

SAIC®

Shuttle PRA Phase 1 Summary

- Objective:
  - Update catastrophic ascent failure summary results of the 1988 *Galileo* RTG risk assessment.
- Results:
  - Mean risk of catastrophic failure:
    = 1/73 (up from 1/55 in the *Galileo* Study)
  - Median (50th percentile) of estimate:
    = 1/90 (up from 1/78 in the *Galileo* Study)

SAIC®

Risk of Catastrophic Ascent Failure Comparison of Today with *Galileo* (STS-34)

	5th %	20th %	Median (50th %)	Mean	80th %	95th %
93 Shuttle System (Base)	1 in 223	1 in 146	1 in 90	1 in 73	1 in 54	1 in 31
88 Shuttle System (*Galileo* Base)	1 in 350	1 in 168	1 in 78	1 in 55	1 in 36	1 in 18

Experience since the 1988 *Galileo* RTG study has improved the estimate of mean risk (launches between failures) by 33% and reduced uncertainty by 32%.

Analysis Method

Preserve *Galileo* study methods, data, assumptions.

- Use best avai able data to characterize prior experience, update with operational experience using Bayes' theorem.
  - SSME Risk
    - Prior experience: SSME test experience to date (April 93)
    - Update with operational experience (55 missions, 165 Starts).
  - SRB Risk
    - Prior experience: Aggregate of U.S. solid rocket experience.
    - Base Case Update: Operational experience excluding 51-L failure.
    - Sensitivity Case Update: All operational experience including 51-L.
  - ET, Orbiter, Prelaunch Risk
    - Prior Experience: *Galileo* study results, catastrophic reliability estimate from critical component type and count.
    - Update with operational experience.

SAIC®

Demonstrated Reliability Analysis

vs.

Risk Assessment (1 of 2)

Reliability Analysis Results

- Demonstrated Reliability Analysis - SSME Assessment Team
  - P(SSME Catastrophic Failure) = 1/120 Mean (per flight)
  - "Because the [conventional reliability] analyses cannot and do not take into account the effects of all the special controls and precautions currently taken with the engines prior to clearing them for flight, ***the Team believes that the actual single flight reliability of the engine is higher the the numbers would indicate.****"
    - Report of the SSME Assessment Team, January 1993

* Emphasis added.

Demonstrated Reliability Analysis

vs.

Risk Assessment (2 of 2)

Risk Assessment Results

- Risk Assessment - Space Shutt e PRA Team
  - P(SSME Catastrophic Failure) (per flight)

5th percentile	Median	**Mean**	95th percentile
= 1/1550	1/342	**1/213**	1/71

  - A Risk Assessment atttempts to capture and quantify all significant contributors to the risk. The PRA Team believes this range of estimates captures the current actual probability of catastrophic Shuttle failure during ascent.

SAIC

Demonstrated Reliability Analysis

e.g.: F. Safie, MSFC*; R. Biggs, Rocketdyne*

- Objective: Conservative estimate of reliability demonstrated by the SSME to date.
  - Exclude only failures clearly outside operating envelope at time of failure.
  - Required assumptions are deliberately conservative.
  - Test stand experience equivalent to operational experience.

*Results used by SSME Assessment Team.

SAIC®

Risk Assessment
Phase 1 - Space Shuttle PRA

- Objective: Realistic estimate of the range of current SSME reliabilty.
  - Exclude failures which would not occur or lead to failure in current Shuttle.
  - Make realistic assumptions (neither conservative nor optimistic).
  - Test stand experience is best non-flight indicator of operational performance, but is not equivalent to operational experience.

SAIC

SSME Analysis - Startup

Prior (test experience) = 1 failure / 1260 starts

Update (operational experience) = 0 failures / 165 starts

Updated Posterior Distribution:

5th percentile	Median	Mean	95th percentile
4.78 e-6	7.17 e-5	2.78 e-4	1.08 e-3

catastrophic failures per SSME - launch.

SAIC

SSME Analysis - Mainstage

Test experience =3 failures / 484,932 seconds

P(Shuttle Fail | SSME Fail) = {0, 1/2, 1} for failures ˙ and 2
(uninformative prior)
= ˙ for failure 3

Prior Experience = Aggregate of
(1 failure / 484,932 seconds
2 failures / 484,932 seconds
3 failures / 484,932 seconds)

Update (operational experience)= 0 failures / 85,800 seconds

Updated Posterior Distribution:

5th percentile	Median	Mean	95th percentile
2.66 e-7	1.45 e-6	2.47 e-6	7.91 e-6

catastrophic failures per ssecond of SSME burn.

Burn Duration =520 seconds

SRB Analysis

Prior (Aggregated of U.S. Solid Rocket Experience)
- Castor
- Star
- Minuteman
- Poseidon / Trident
- Titan Solid

→ Homogeneity Analysis - Valid statistical reasons to remove any family from set of priors?
- NO!

Prior	3.03 e-4	5.08 e-3	7.59 e-3	2.11 e-2

Update (Base Case) =0 failures / 109 SRB - flights

Update (Sensitivity Case) =1 failure / 109 SRB - flights

Updated Posterior Distribution:

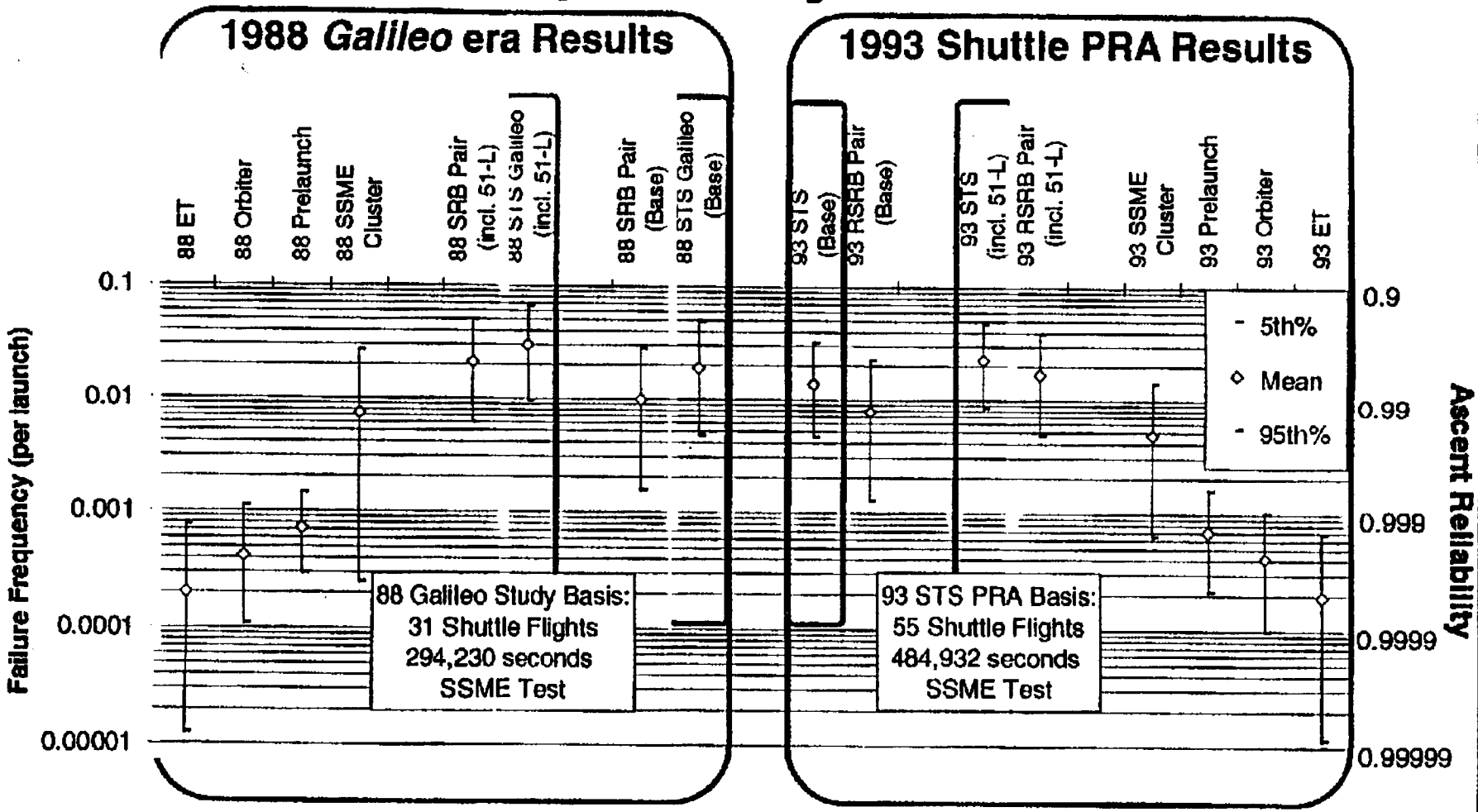
	5th %	Median	Mean	95th %
Base	6.41 e-4	2.67 e-3	3.90 e-3	1.12 e-2
Sensitivity	2.32 e-3	6.74 e-3	8.32 e-3	1.96 e-2

catastrophic failures per SRB - flight.

1993 Risk of Catastrophic Ascent Failure

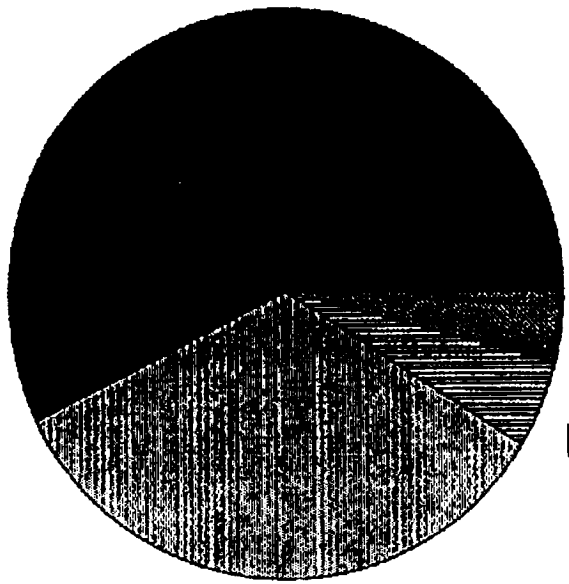
	5th %	20th %	Median (50th %)	Mean	80th %	95th %
93 ET	1 in 86400	1 in 31900	1 in 11200	1 in 5200	1 in 3950	1 in 1460
93 Orbiter	1 in 10100	1 in 5710	1 in 3140	1 in 2440	1 in 1720	1 in 974
93 Prelaunch	1 in 4650	1 in 2860	1 in 1710	1 in 1430	1 in 1030	1 in 631
93 SSME Cluster	1 in 1550	1 in 741	1 in 342	1 in 213	1 in 153	1 in 71
93 SRB Pair (Base) (w/out 51-L)	1 in 782	1 in 388	1 in 187	1 in 128	1 in 90	1 in 45
93 STS Base	**1 in 223**	**1 in 146**	**1 in 90**	**1 in 73**	**1 in 54**	**1 in 31**
93 SRB Pair (Sensitivity 1) (Include 51-L)	1 in 216	1 in 128	1 in 74	1 in 60	1 in 43	1 in 25
93 STS Sensitivity 1 (Include 51-L)	**1 in 118**	**1 in 79**	**1 in 52**	**1 in 44**	**1 in 33**	**1 in 21**

Failure Frequency Distributions



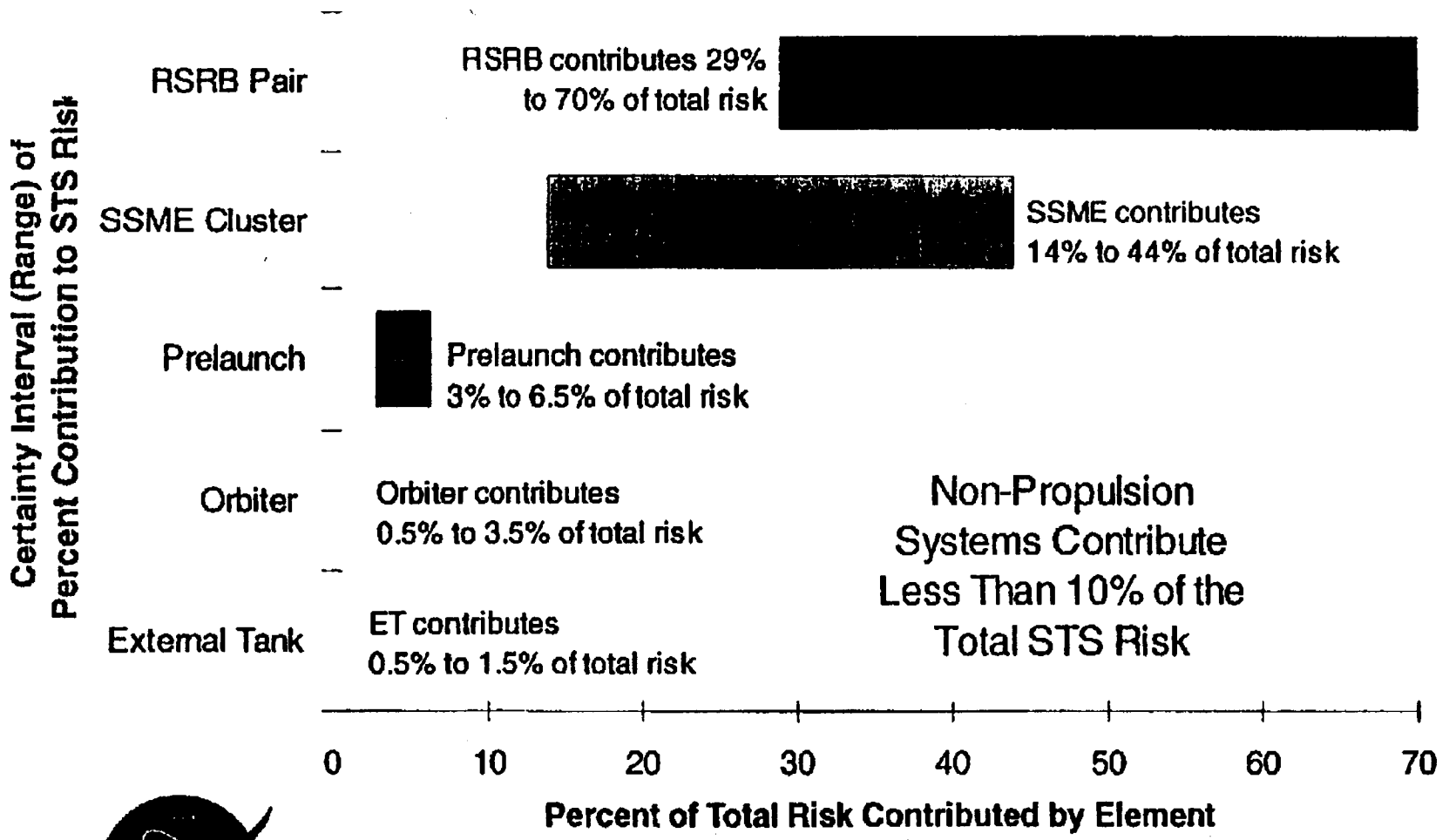
Mean Contribution of STS Elements to Risk of Catastrophic Ascent Failure

Mean Contribution to STS Risk by Element



For the SRB Base Case (51-L failure not included).

Uncertainty in Contribution to Shuttle Risk of Catastrophic Failure



For the SRB Base Case.

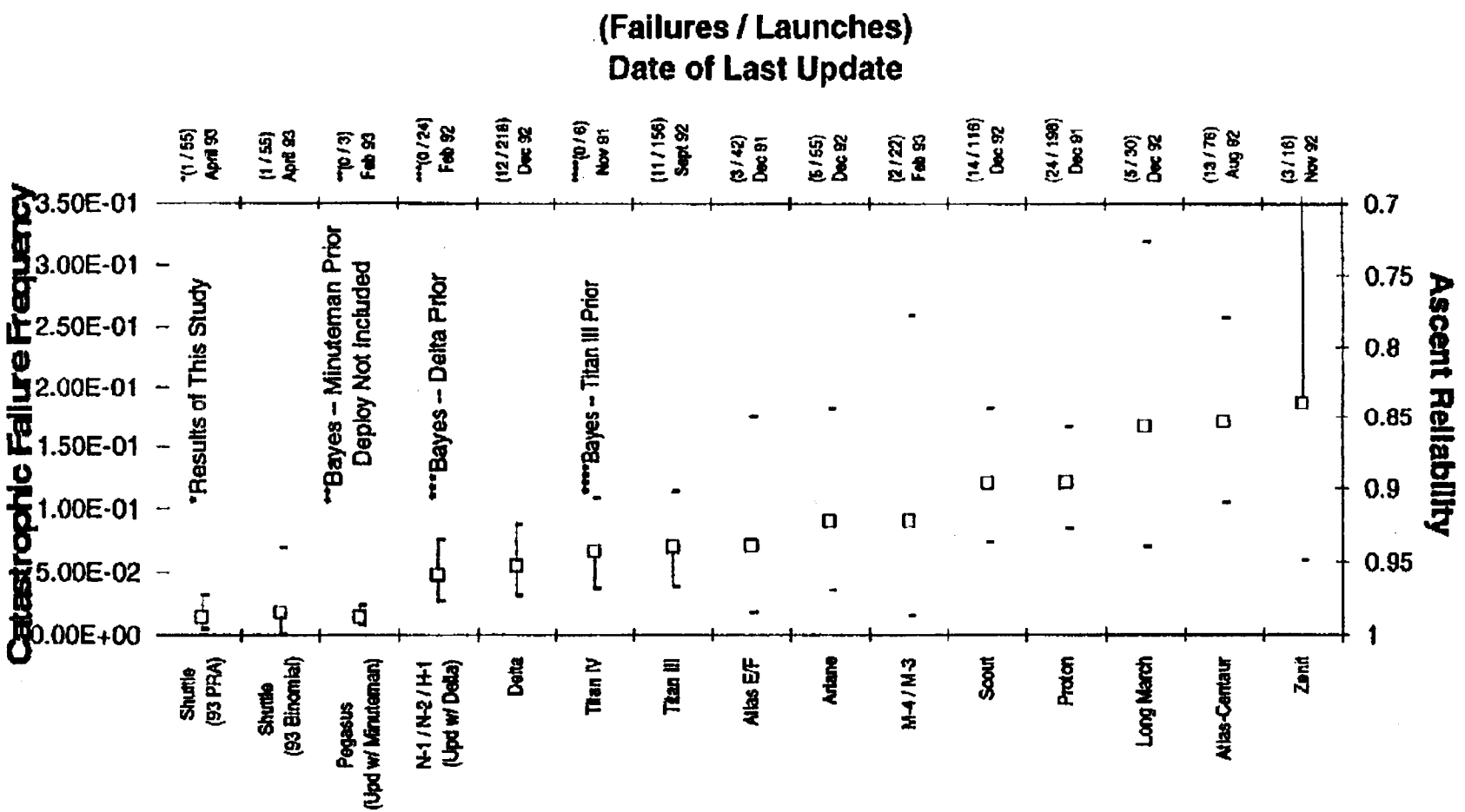
SSME Test Program

- In the Galileo RTG study, risk from SSME cluster was comparable to risk from SRB pair. Since then:
  - No new catastrophic SRB failures,
  - 1 New catastrophic SSME failure (in test).
- Yet estimatec SSME risk today is considerably less than SRB risk - **Why?**
  - Both SRBs and SSMEs have 24 new missions since Galileo study,
  - but new SSME experience includes 471 starts and 190,702 seconds in test - equivalent to over 5 times the additional operational experience.
- With no test failures, test progam reduces estimated SSME risk 5 times faster than operational experience alone.
- Even with failures*, the test program significantly reduces uncertainty associated with SSME risk.

* as long as failure frequency is generally consistent with or better than predictions.

SAIC

Comparison of Active Launch Vehicles



The Shuttle is the most reliable launch system in the world.

Conclusions

- Based on this study, the Space Shuttle today is the worlds most reliable launch vehicle.
- The SSME test program has had a significant positive impact on reducing the estimated Shuttle risk.
- The Redesigned Solid Rocket Booster (RSRB) is currently the most significant contributor to Shuttle risk.

SAIC®

Backup Slides

SAIC

1988 *Galileo* Risk of Ascent Failure

	5th %	20th %	Median (50th %)	Mean	80th %	95th %
88 ET	1 in 8000	1 in 2900	1 in 10000	1 in 5000	1 in 3500	1 in 1300
88 Orbiter	1 in 9200	1 in 5300	1 in 2900	1 in 2400	1 in 1600	1 in 900
88 Prelaunch	1 in 3400	1 in 2600	1 in 1900	1 in 1400	1 in 1300	1 in 700
88 SSME Cluster	1 in 1200	1 in 458	1 in 171	1 in 92	1 in 64	1 in 26
88 SRB Pair (Base) (w/out 51-L)	1 in 1300	1 in 624	1 in 278	1 in 182	1 in 124	1 in 58
88 STS Base	**1 in 350**	**1 in 168**	**1 in 78**	**1 in 55**	**1 in 36**	**1 in 18**
88 SRB Pair (Sensitivity 1) (Include 51-L)	1 in 555	1 in 251	1 in 109	1 in 65	1 in 48	1 in 22
88 STS Sensitivity 1 (Include 51-L)	**1 in 202**	**1 in 102**	**1 in 50**	**1 in 36**	**1 in 24**	**1 in 13**

SAIC®

SSME Data - Failures (1 of 3)

DATE	TEST	ENGINE	FAILURE	DAMAGE	MSFC	PRA	REASON FOR EXCL / INCL.
3/24/77	901-110	3	HPOP Oxidizer Primary Seal Failure	Uncont.			
8/27/77	901-133	4	FPB Housing Burn Through	Uncont.			
9/8/77	901-136	4	HPOP No. 3 Bearing Failure	Uncont.			
11/17/77	902-095	2	HPFP Turbine Blade Failure	Uncont.			
12/1/77	901-147	103	HPFP Turbine Blade Failure	Uncont.			
3/31/78	901-173	2	Main Injector LOX Post Failure	Cont.			
6/5/78	901-183	5	Main Injector LOX Post Failure	Cont.			
6/10/78	902-112	101	Eng. Inlet Fule Supply Blockage (N2)	Uncont.			
7/18/78	902-120	101	HPOP Capacitance Probe Rub	Uncont.			
10/3/78	902-132	6	MOV Improperly Installed	Cont.			
12/6/78	901-222	7	Heat Exchanger Coil Failure	Uncont.			

1988 *Galileo* era Risk of Ascent Failure

	5th %	20th %	Median (50th %)	Mean	80th %	95th %
88 ET	1 in 8000	1 in 2900	1 in 10000	1 in 5000	1 in 3500	1 in 1300
88 Orbiter	1 in 9200	1 in 5300	1 in 2900	1 in 2400	1 in 1600	1 in 900
88 Prelaunch	1 in 3400	1 in 2600	1 in 1900	1 in 1400	1 in 1300	1 in 700
88 SSME Cluster	1 in 4020	1 in 1060	1 in 352	1 in 136	1 in 120	1 in 38
88 SRB Pair (Base) (w/out 51-L)	1 in 642	1 in 305	1 in 147	1 in 101	1 in 71	1 in 35
88 STS Base	**1 in 218**	**1 in 130**	**1 in 74**	**1 in 54**	**1 in 40**	**1 in 21**
88 SRB Pair (Sensitivity 1) (Include 51-L)	1 in 170	1 in 101	1 in 58	1 in 47	1 in 34	1 in 20
88 STS Sensitivity 1 (Include 51-L)	**1 in 103**	**1 in 66**	**1 in 41**	**1 in 34**	**1 in 25**	**1 in 15**

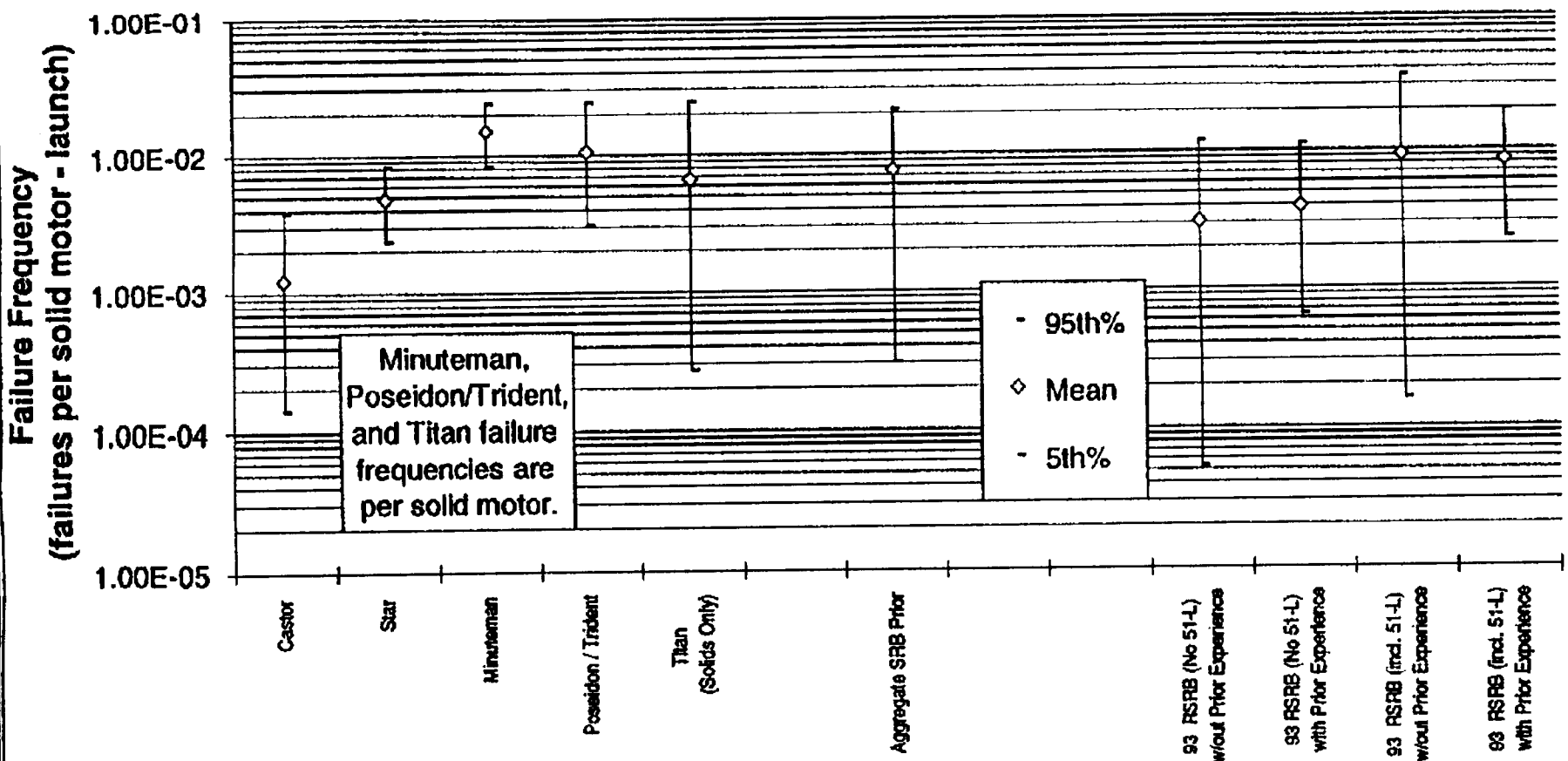
NASA

SAIC

SSME Data - Failures (3 of 3)

DATE	TEST	ENGINE	FAILURE	DAMAGE	MSFC	PRA	Reason for Excl. / Incl.
10/15/81	901-340	107	HPFP Turnaround Duct Failure	Uncont.	N	N	>104%
2/12/82	750-160	110f	Fuel Injector Blockage (Ice)	Uncont.		Y	
4/7/82/	901-364	2013	HPFP Kaiser Hat Nut Failure	Uncont.			
5/15/82	750-168	107	OPOV Leakage During Cutoff	Cont.			
8/27/82	750-175	2208	HPOP Disch. Duct Failure (Ultrasonic FM)	Uncont.			
2/3/84	STS-41C		ASI Erosion				
2/14/84	901-436	208	HPFP Coolant Linear Failure	Uncont.	N	N	>104%
2/4/85	901-468	207	FPB Mainifold Crack	Uncont.			
3/27/85	750-259	2308	MCC Outlet Mainfold Weld Crack	Uncont.	N		>104%
7/1/87	902-428	2106	OPB Injector Element Braze Crack	Cont.	Y		
6/2/89	902-471	2206		Cont.	Y		
6/23/89	904-044	212	HPOP Bearing Failure	Uncont.			
7/24/91	901-666	215	HPFP Second Stage Turbine Blade	Uncont.			
11/6/91	901-674	2032	CCV Coupling Not Installed	Cont.			
6/18/92	902-562	2107	OPOV Failure	Uncont.			
6/2/89	902-471	2206	LPFP Bellows Rupture/Crack	Uncont.			

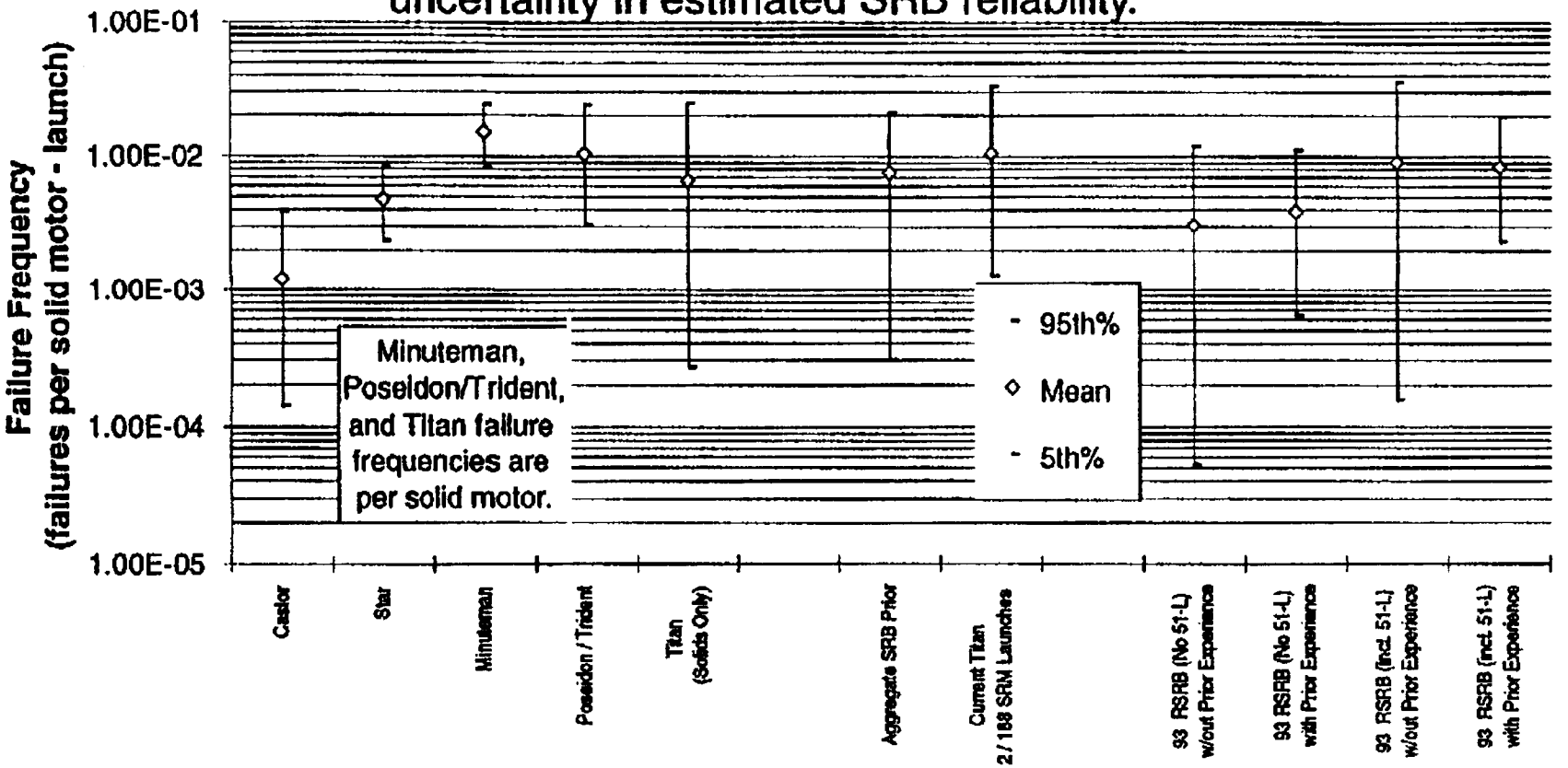
SRB Surrogate and Actual Failure Frequency Distributions



Combining surrogate prior experience with direct SRB experience reduces uncertainty in estimated SRB reliability.

SRB Surrogate and Actual Failure Frequency Distributions

Combining surrogate prior experience with direct SRB experience reduces uncertainty in estimated SRB reliability.



Current Titan SRM includes 2 Aug 1993 failure. This is not included in the aggregate prior, provided for comparison only.

SAIC NASA REPORT 12-001-93RPT
June 8, 1994

Risk Analysis Applied to the Space Shuttle Main Engine:

Demonstration Project for the Main Combustion Chamber Risk Assessment

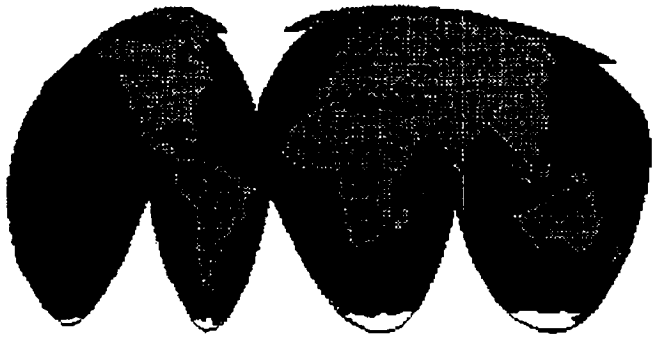
Joseph R. Fragola, Program Manager
Robert E. Kurth, Project Leader
Yu Shen
Mingfa Yang
Jorge Ballesio

SAIC® An Employee-Owned Company
Science Applications International Corporation

C2

Risk Analysis Applied To The Space Shuttle Main Engine:

Main Combustion Chamber (MCC) Analysis



Main Combustion Chamber (MCC) Risk Analysis

The risk analysis of the MCC used standard risk analysis techniques to assess the contribution of MCC failure to the overall risk associated with the space shuttle main engines. These methods included:

Master Logic Diagram (MLD). The MLD is used to identify in a consistent, logical, and exhaustive method all events that could cause failure of the MCC in such a manner *credible* that a loss of vehicle or loss of mission could result. For example, unstable crack growth is included in the MCC analysis but missing bolts on the powerhead and MCC interface is excluded because it is not believed to be credible.

Initiating Event Identification and Evaluation. The initiating events are obtained directly from the MLD. Those events that start the logical sequences leading to MCC failure are grouped into a set of events for further analysis. identified as the initiating events.

Functional Event Sequence Diagram (FESD). The FESD begins at the initiating events and develops the sequence of pivotal events that must proceed to end at either success or the MCC failure point. An example of a FESD is given in Figure 1 for the Flow Recirculation Inhibitor (FRI) system in the MCC. All events are pivotal in the sense that the event must have a yes-no, or on-off, type of output. These events are then quantified by probabilistic analysis: e.g., the yes output occurs 95% of the time, the no output 5%.

Event Tree Analysis. The chain of events developed during the FESD process is placed in an event tree format. This format allows the sequence of events to be quantified as to the contribution of the MCC to the overall SSME risk.

from the list of initiators, the event tree development and quantification, the sensitivity and uncertainty analysis, and, finally, some comments about the main combustion chamber risk.

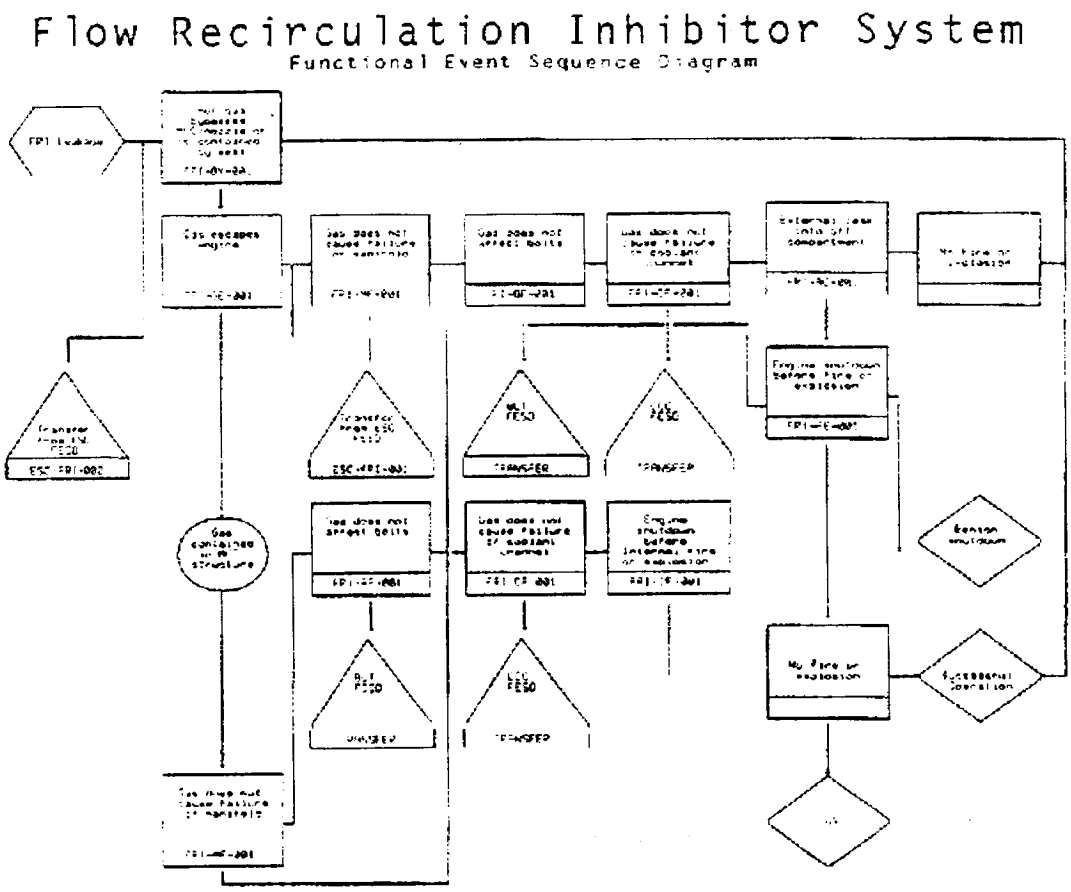


Figure 1. Example Functional Event Sequence Diagram

Each element of this risk assessment is discussed in the following sections. The topics flow naturally from the Master Logic Diagram development to the initiator identification, the development of the initiator frequencies, the construction of the functional event sequence diagrams

Main Combustion Chamber Probabilistic Risk Assessment

Master Logic Diagram Analysis

SAIC® An Employee-Owned Company
Science Applications International Corporation

Introduction

The Probabilistic Risk Assessment (PRA) of the Space Shuttle Main Engine (SSME) Main Combustion Chamber (MCC) has proceeded in a classical PRA development. The analyses began with the development of a Master Logic Diagram (MLD). In this development all potential causes of the top event, loss of the orbiter, are identified by use of a logic flow diagram that captures the logical operation of the SSME and the interaction of SSME components. While the program began by examining the full SSME it was quickly focused on the MCC, as well as the SSME software. The evaluation of the SSME software is the topic of a different task and is not reported here. The MLD, having captured the logic used in the design and operation of the MCC, is evaluated to define all credible causes of a Loss Of Vehicle (LOV) event. It is critical to note that these initiators are not equivalent to CRIT-1 events. CRIT-1 events are failures that lead directly to the loss of the engine. Initiators identified by the MLD may need other events to occur simultaneously or in sequence to have a LOV event. Thus, what is identified in the FMEA as a CRIT-3 event may, under the correct set of circumstances, lead to a CRIT-1 consequence.

After defining the set of initiators each individual initiator is assessed for further development in the Function Event Sequence Diagram (FESD) task. In this assessment the results of previous tests and analyses performed at Rocketdyne and Marshall Space Flight Center (MSFC) are integrated to define the list of initiators that require further development. Those initiators are input to the FESD analyses to identify pivotal events. These events are then formalized in an event tree analyses. Because of the primarily structural nature of the MCC and the lack of mitigating functions for off-nominal events fault tree analyses of the MCC is limited in this study.

Master Logic Diagram (MLD) Results

The development of the MLD for the MCC began with a thorough review of the MCC geometry, flow paths, operations, inputs, outputs, test histories, and failure histories. The MCC design consists of an outer structural jacket forming the shape of the combustion chamber liner and carrying the internal pressure and external loads from the interfacing components. The liner conducts hydrogen coolant in the axial direction and acts as a thermal barrier between the jacket and the combustion gases. It also serves as a heat exchanger to heat the hydrogen used to drive the Low Pressure Fuel TurboPump (LPFTP). The LPFTP is not included in the PRA of the MCC but is critical to the SSME PRA development. The coolant is carried along slotted channels in the liner that are machined from a Narloy-Z material. The channels are closed-out by Electro-Deposited copper (EDCu) and Electro-Deposited nickel (EDNi). The copper is in place to protect the nickel from non-cryogenic hydrogen embrittlement effects. The liner is supported by the high strength (Inconel 718) structural jacket but is attached only at the ends of the jacket. Structurally, the liner is required to strain out to contact the jacket, to react the differential pressure load between the coolant and combustion gases, and to accommodate the cyclic and thermal racheting strain ranges arising from the extreme thermal operating environment. The structural jacket is required to provide external support for the liner

plus react the internal combustion pressure loads as well as the thrust and gimbaling loads. While the liner is not attached all along the jacket the liner motion is restricted by the jacket.

The operating environment for the MCC is severe. Before the SSME firing the entire liner is approximately -400 °F. During steady state operation the hot gas wall of the liner is approximately 1,100 °F while the coolant side near the jacket is -150 °F. Near the throat section of the MCC the coolant pressure is 6,300 psi while the hot wall chamber pressure is 2,100 psi. The coolant channel height (measured radially) is approximately 0.1 inch which implies that a 1,250 °F temperature gradient exists over thickness equivalent to the thickness of a quarter. This temperature differential also introduces a thermal strain mismatch at the Narloy-z/copper/nickel interfaces.

During detailed discussions with the SAIC and MSFC engineers and two on-site meetings the MLD given in Figure 2 was agreed upon. This MLD is used in the following section to identify those initiators for use in the FESD and event tree development.

List Of Initiators and Examination for FESD Development

The results of the MLD evaluation identified a set of initiators that can credibly lead to the LOV event from failures in the MCC. The list of initiators is comprehensive and to the extent possible exclusive. It is important to note that there are overlapping physical conditions that can cause one "initiator" to appear on the event sequence of another initiator. For example, blockage of several coolant channels is an initiator that can lead to a LOV event. It can be the case that it is coupled with cracks in the hot gas wall that under normal cooling conditions are not CRIT-1 events but coupled with large thermal strains become unstable. Therefore, even when an event is listed as an initiator it must be kept in mind that such initiators are dependent on time, the history of the MCC, and the mission requirements. Given these qualifiers the list of initiating events is shown in Table I.

Initiators Identified from MLD
Hot Gas Wall Crack
Coolant Channel Crack
G-15 Bolt Failure
EDNi Separation/Crack
Multiple Channel Blockage
FRI Leakage
Manifold Weld Failure
Actuator Sideload Instability
Loss of Powerhead Bolt Preload
Bent Nozzle Tube at MCC Interface
Combustion/Flow Instability
Loss of Pressure Sensor
Seal Leakage

Table I. Initiators Identified From MLD

Initiator Evaluation

Hot gas wall crack.

If the hot gas wall crack is large enough then the MCC failure will be immediate and catastrophic. However, there is sufficient evidence from previous MSFC data to indicate that the MCC can withstand substantial cracking without catastrophic failure. There are known instances of pinhole and small cracks that have not caused catastrophic failure. A specific example in which a MCC survived with 37 inches (cumulative sum of all cracks, not a single crack length) has been documented. However, since the mechanism for the crack stopping is not well understood the event "crack stops" or "crack is stable" cannot be assessed a 100% probability. Therefore, further investigation of this sequence of events

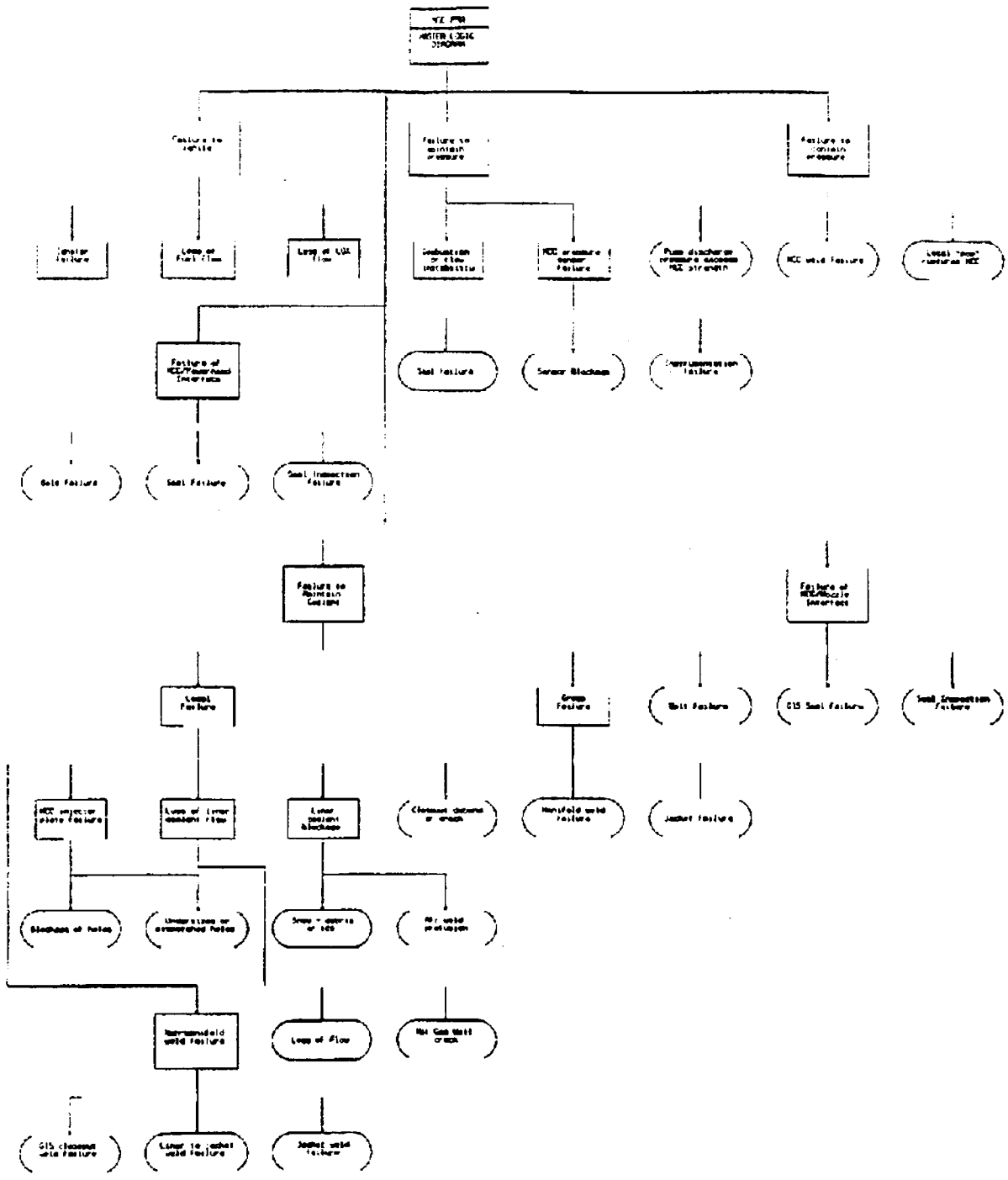


Figure 2. Master Logic Diagram: Main Combustion Chamber For the Space Shuttle Main Engine

is warranted.

Coolant Channel deformation/crack

If the MCC hot gas wall crack is expected to stop growing due to a reduction in thermal stress from H_2 leaking through the crack then it is not possible to neglect the effect of the deformation or cracking of coolant channels. If reduced or lost flow in a coolant channel occurs because of deformation or cracks then a localized hot spot can develop near a crack hot gas wall. In this case the thermal stress may induce large crack growth and the initiator must be developed in the FESD and event tree analysis.

G-15 bolt failure

There is evidence from the MSFC test stand data that a single bolt failure is not a catastrophic event. In the development of the event tree this should be accounted for by a separate path assuming that a report referencing this data is made available.

EDNi closeout separation/crack

The failure of the EDNi closeout has been assumed to be negligible because the hot gas wall is in (primarily) a compressive stress state. However, at the interface of the Narloy-Z, copper, and nickel there are non-negligible shear forces because of the dissimilar materials. The mismatch in shear modulus, Poisson's ratio, and thermal expansion while small still introduces shear forces. The extent of these shear forces is of concern. Also, given a shear force, the frequency of the EDNi failure is of interest. If it can easily be shown that the shear forces will not lead to a failure rate of more than 1 in 10,000 per engine per flight then the overall contribution to the risk will be so small that the pursuit of this failure path is not important.

There are two important failure paths to be concerned with in the consideration of the coolant channel closeout failure. The first is labeled sub-interface failures and the second is labeled interface failures. Either type of failure path can be initiated by a variety of processes:

Manufacturing defects
Voids in the materials
Fatigue
Thermal racheting
Creep

Of course all of these may interact to produce early failures. For this initial scoping effort it is assumed that a defect exists. The question is then: What is the stress state and the potential for defect propagation given that the defect exists?

The answer to this question involves complex, detailed analyses that are time consuming to perform. However, it is possible to assess the stress state in a somewhat simplified analysis to determine if the shear stress is important to the potential failure of the EDNi/Narloy-z closeout.

It is important to emphasize that the shear effect is important because of the dissimilar material bond. It has been shown that a defect in a combined shear and compressive stress field can exhibit Mode I (tensile), as well as Mode II (shear) crack growth depending on the materials and crack orientation. For a defect in the interface the crack acts as a "bubble" in which the effect of increasing the compressive force is to increase the crack growth rate - exactly the opposite effect of what is expected from single material crack growth analysis.

To assess the effect of the MCC stress state on interface and sub-interface crack growth rates two tasks must be considered. First, an anlysis of the frequency of debond failures in the MCC liner must be performed. If the

frequency of debond is high enough then it is necessary to perform some stress analyses of the dissimiliar material interface area to determine if the area is suceptible to larger crack growth rates than was previously expected.

The basic conclusion is that the EDNi and Narloy-z interface must be studied in more detail. The following sections provide the debond rate data analysis and simplified stress analyses.

Multiple coolant channel blockage

Because of the concern over the thermal loading of the MCC liner wall, the closeout, and the hot gas wall cooling via thermal stress reduction from cooling, the possibility of coolant channels becoming blocked, even partially, could affect the fracture behavior or crack growth characteristics in these other areas. While a priori it is expected that these events will have very little chance of causing a loss of MCC event they must still be examined.

FRI system failure

The FRI system protects the MCC interface with the nozzle from exhaust gas re-circulation during mainstage firing. The increased thermal stresses from such a re-circulation pattern could affect the nozzle tubes, the MCC liner turn around duct, or the MCC to nozzle bolts. This initiator must be included in functional event sequence diagram analyses.

Manifold weld failure

Clealy, the failure of the manifold weld is of critical concern. It is believed that the manifold weld failure caused a catastrophic failure of an engine during testing. The evidence was not 100% conclusive because of the large scale destruction of the engine. However, even a belief that the weld failure could have lead to a loss of the SSME requires that it be included in further risk assessment studies.

Actuator sideload instability

MSFC engineers have stated that the force that the actuator develops during any flight is insufficient to cause a buckling of the MCC. This analysis was carried out by Rocketdyne and, pending the receipt of this report, it is not considered further.

Loss of powerhead bolt preload

There is some recent test stand data that indicates that the MCC could survive the loss of a single bolt. This will certainly reduce the frequency with which one reaches a loss of MCC event from this initiator but since it is not known if there is a zero probability of the loss of the MCC this initiator must be evaluated by FESD analysis.

Bent nozzle tubes at MCC/nozzle interface

After meeting with MSFC engineers it was concluded that this initiator, while near the MCC and nozzle interface, was outside the scope of a risk assessment of the MCC. Therefore, this initiator was not considered further because it is out of scope.

Combustion/flow instability

During meetings with MSFC and by careful consideration of the MLD it was concluded that combustion or flow instabilities are not true intiators but rather are the result of some other initiating event. They will be pivotal events in the FESD construction. however, the combustion or flow instabilities result from causes outside the MCC or from other, already

identified. initiating events within the MCC boundaries.

Loss of pressure sensor

When the sequence of events after the loss of the pressure sensor are examined it becomes clear that there are no events within the MCC as a result of this sensor failure. If the sensor becomes plugged then it is within the bounds of the MCC but all events occur at the controller and turbomachinery. Therefore, the loss of pressure sensor was not included during the FESD development.

Based on these examinations there are seven initiators which warrant more detailed investigation in the functional event sequence diagram analysis. These are listed in Table II. Before proceeding to the FESD construction the frequency with each initiator occurs is estimated using the existing data from MSFC tests and orbiter flight data bases.

Summary and Conclusions

The evaluation of the frequency of initiating and pivotal event frequencies indicated that the debond and/or cracking of the Electro-Deposited Nickel (EDNi) close-out layer of the MCC liner is occurring more frequently. There are difficulties in evaluating these data. First, there are relatively few failures of the MCC and, therefore, the associated uncertainties are large. Second, when there are catastrophic failures of the MCC the design is usually changed to remove these sources of failure. In this case it is necessary to discount (i.e. count them as less than unity probability of occurrence) previous failures or show through analysis how these design changes or operational changes have affected the MCC performance. To perform such analysis it is necessary to understand the MCC construction and the function of the liner. To show how physical and/or phenomenological models are used to quantify the failure frequency of initiating or pivotal events the EDNi layer debond is investigated.

Initiators Included in FESD Analysis
Hot Gas Wall Cracks
Coolant Channel Cracks
Coolant Channel Blockage
EDNi Separation or Crack
Bolt Failure
Manifold weld failure
FRI Failure

Table II. Initiating Events For Functional Event Sequence Diagram Analysis

Stress Analyses and Crack Growth:

Application To The MCC Liner

The SSME MCC configuration and cross-section are shown in Figures 3 and 4. The MCC design consists of an outer structural jacket forming the shape of the combustion chamber liner and carrying the internal pressure loads and the external loads from interfacing components. The liner is attached to the jacket at the ends of the structure. The liner is made of Narloy-Z with coolant channels machined into the liner in the axial direction. The coolant channels are closed out by a thin copper layer to protect the nickel material from hydrogen embrittlement. The liner is supported by a high-strength (Inconel 718) jacket that restricts liner motion during engine operation. Thus, although the liner is not attached to the jacket all along the MCC, its motion is restricted. During steady state operation the liner hot gas surface is nominally at 1,100°F and the back wall on the jacket side is typically -150°F. During start and cutoff the complete liner temperature reaches -400°F. Near the MCC throat area, the hot wall chamber pressure is approximately 2,100 psi, while the internal pressure of the coolant hydrogen is 6,300 psi.

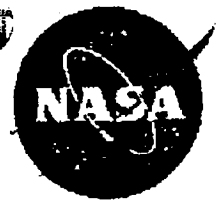
The damage accumulation process in the MCC liner has been previously analyzed as composed primarily of creep and thermal racheting. The effort in the past has focused on wall thinning and crack growth in the hot gas wall side of the liner, because there has been test data taken in which the hot gas wall has developed through-wall cracks.

The failure of the EDNi closeout has been assumed to be negligible because the hot gas wall is (primarily) in a compressive stress state. Under *pressure only* loading conditions, this is valid. In fact, for a single material, under both pressure and temperature loading, the stress field may be primarily compressive. However, at the interface of the Narloy-Z, copper, and nickel, there are non-negligible shear forces because of the dissimilar materials.

The mismatch in shear modulus, Poisson's ratio, and thermal expansion, while small, still introduces shear forces. The extent of these shear forces is of concern. Also, given a shear force, the frequency of the EDNi failure is of interest. If it can easily be shown that the shear forces will not lead to a failure rate of more than one in 50,000 per engine, then the overall contribution to the risk will be so small that the pursuit of this failure path is not important.

There are two important failure paths to consider regarding the coolant channel closeout failure: sub-interface failures and interface failures. Either failure path can be initiated by a variety of processes:

- Manufacturing defects
- Voids in the materials



- Fatigue
- Thermal racheting
- Creep

Of course all these may interact to produce early failures. For this initial scoping effort it is assumed that a defect exists. The question is then: What are the stress state and potential for defect propagation, given that the defect exists?

The answer to this question involves complex, detailed analyses that are time consuming to perform. However, it is possible to assess the stress state in a simplified analysis to determine if the shear stress is important to the potential failure of the EDNi/Narloy-Z closeout.

It is important to emphasize that the shear effect is significant because of the dissimilar weld. It has been shown that a defect in a combined shear and compressive stress field can exhibit Mode I (tensile), as well as Mode II (shear) crack growth depending on the materials and crack orientation. For a defect in the interface, the crack acts as a "bubble" in which the effect of increasing the compressive force is to increase the crack growth rate -- exactly the opposite effect of what is expected from single material crack growth analysis.

To assess the effect of the MCC stress state on interface and sub-interface crack growth rates, a simplified stress analysis has been performed. This analysis examines a realistic MCC geometry and calculates the stress in the liner cavity. The details of this analysis are provided in the following section.

Stress Analysis of MCC Liner

The stress analysis of the MCC liner includes the geometry shown in Figure 4. This geometry is analyzed to determine the stress state near the interface of the EDNi closeout of the Narloy-Z liner material. To provide a realistic approximation to the actual stress state, both the thermal and mechanical stress states must be calculated. Because of the approximate nature of this analysis, previous thermal analysis of the MCC will be used to define the temperature profile in the MCC liner. The temperature profiles are obtained from references [1] and [2]. The temperature profile induces thermal stresses in the Narloy-Z material, which is where the primary heat transfer occurs. The cold wall side of the liner also has a temperature field profile although the gradient is substantially smaller than on the hot wall side. Figure 5 shows the temperature profile as calculated in reference [1]. The profile shown in Figure 5 is for the area of the liner approximately one inch upstream from the throat. The temperature profile is assumed to be the same for the liner at all axial points, except the wall boundary condition. Thus, a simple ratio is used to determine the liner distribution throughout the liner channel at locations away from the throat. When both temperature and pressure loading are considered simultaneously, then there is a non-negligible shear stress introduced near the interface layer.

The Narloy-Z material is strong enough to withstand this combined stress field, and there are many thousands of seconds of test data to

prove this claim. The area of greatest concern comes from the introduction of a defect at, or near, the interface of the Narloy-Z and nickel. The introduction of a crack-like defect causes different behavior and stress loading on the crack tips due to the dissimilar material effect. An important effect has been observed for a sub-interface crack with crack face contact zone in a combined compressive and shear field[3]. Increasing the level of the *compressive* stress may result in an increase of the stress intensity factor K_I at one of the crack tips.[2] The actual value of the stress intensity factor will depend on many parameters including the elastic modulus, Poisson's ratio, the distance from the near crack tip to the interface, the orientation of the major crack axis compared to the interface, and the normal and shear stress levels. Thus, there is a need to demonstrate that the stress field does contain shear forces and estimate this effect on the crack behavior.

To estimate the normal and shear stress fields in the material, a simplified, but realistic, finite element analysis of the MCC liner was undertaken. The geometry for this analysis is assumed to be axisymmetric as shown in Figure 6. The boundary conditions for the analysis are a combined pressure and temperature loading. The two layers modeled were of Narloy-Z and nickel. The elastic modulus, Poisson's ratio, and thermal expansion coefficient are all functions of temperature.[4] For this study, the effect of the thermal variation in material properties was not included to limit the analyses to a linear problem. Thus, the material property data used was for the temperature condition at the MCC throat. By solving the linear problem the principle of superposition can be used to combine the pressure and temperature conditions due to changing power levels.

Figure 7 shows the root mean square total strain state for a typical analysis. The label "prob: shear-03" in Figure 7 implies that both the MCC pressure and temperature field have been imposed on this problem. The pressure is that of steady-state operation. Figure 8 shows the results of the stress analysis when only the pressure field is applied. Because of the calculation procedure used in the COSMOS® finite element package, the "shear" stress reported is the stress in the x-y coordinate system. Since we are interested in the interface layer stress, a post-processing program was developed to change coordinate systems and obtain the interface shear stress. This result is shown in Figure 10. As this Figure indicates, the shear force at the interface is not negligible and must be accounted for in the crack growth analysis.

To estimate the effect on the crack growth, the results of calculations by Yang and Kim[5] are used. In this analysis the stress intensity factor, K_I, is calculated. One of the results is the estimate of K_I as a function of the ratio of the normal stress to the shear stress σ_N, σ_τ. For the nickel and Narloy-Z material properties of interest, the Dunder's parameters given in reference [4] are most closely approximated by of 0.4 and of 0.125. Figure 10 shows a plot of K_I normalized by the stress intensity factor for a crack in an infinite plate versus σ_N/σ_τ. As this

Figure indicates, even for compressive stresses (negative), the value of K_t can be as high as 60% of the stress intensity factor for the crack in an infinite plate under *tensile* loading.

The crack growth rate is given by where C and m are material constants, N is the number of applied stress cycles, and K is the range of the stress intensity factor. If a value of 1×10^{-5} is used for C and 4 for m, then we can calculate the stress level necessary to double the crack length over one cycle. If the initial crack size is 0.005 inches then it will double in size if the stress level is approximately 35 ksi. If the crack is half the width of the land then it will double if the stress is 25 ksi. These must be viewed only as estimates because the stress levels are outside the linear region and therefore equation (1) is not accurate. Also, a doubling of the half-width crack would require that edge effects be incorporated. Given these caveats, these stress ranges are within ranges calculated in a previous Rocketdyne report.[6]

Summary and Conclusions

The MCC liner has been investigated for fatigue and crack growth at, or near, the Narloy-Z and EDNi interface. It was found that sufficient shear-to-compressive stress ratios exist to cause defects to grow during steady state operation due to low cycle fatigue. The stress analysis indicates that K_t can be as large as 60% of the K_t value under normal tensile loads in an infinite plate *even when the hot gas wall is in compression.* Local hot spots, throttle down, and throttle up can cause a change in the crack length. As with all material fracture the larger the initial crack size the larger the growth rate.

From a risk standpoint, the growth of cracks in the closeout area is of concern if the inspection for these cracks is inefficient and if the leak rate is large enough to deform the divergent section of the nozzle. Efficient inspection procedures can substantially reduce the risk.

To fully integrate the effect of the EDNi closeout failure on MCC risk requires that the initial distribution of defects, due to either debond or cracking, is quantified. From the SSME data-base it is possible to define the frequency of the defect rate. An assumption about the size of these defects is needed to fully quantify how many of these defects can cause an initiating event for the failure of the MCC and LOV event.

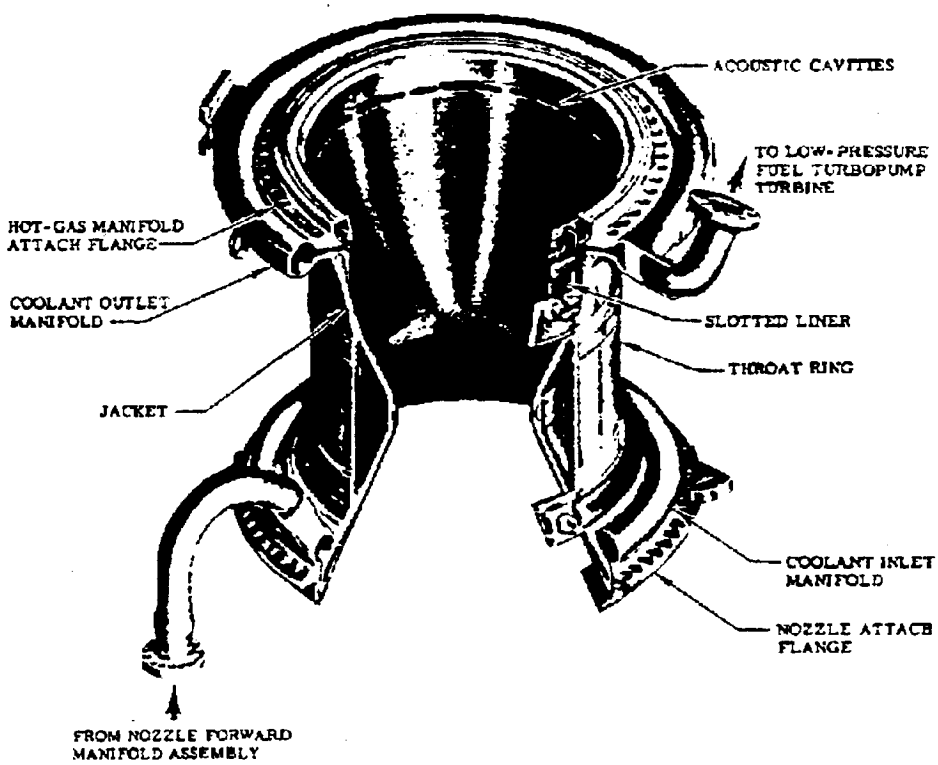


Figure 3. Space Shuttle Main Engine Main Combustion Chamber Configuration

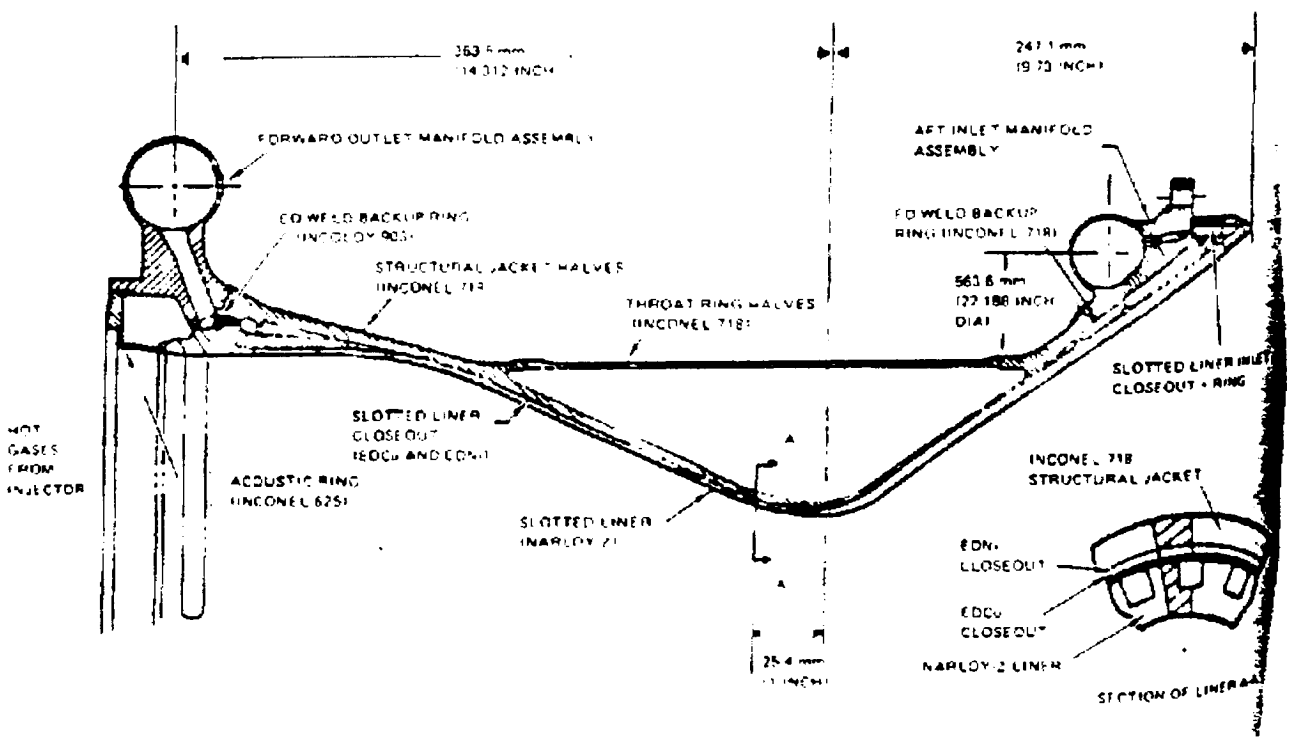


Figure 4. Space Shuttle Main Engine Main Combustion Chamber Cross-Section

Coolant Channel Thermal Distribution (110% FPL hg)

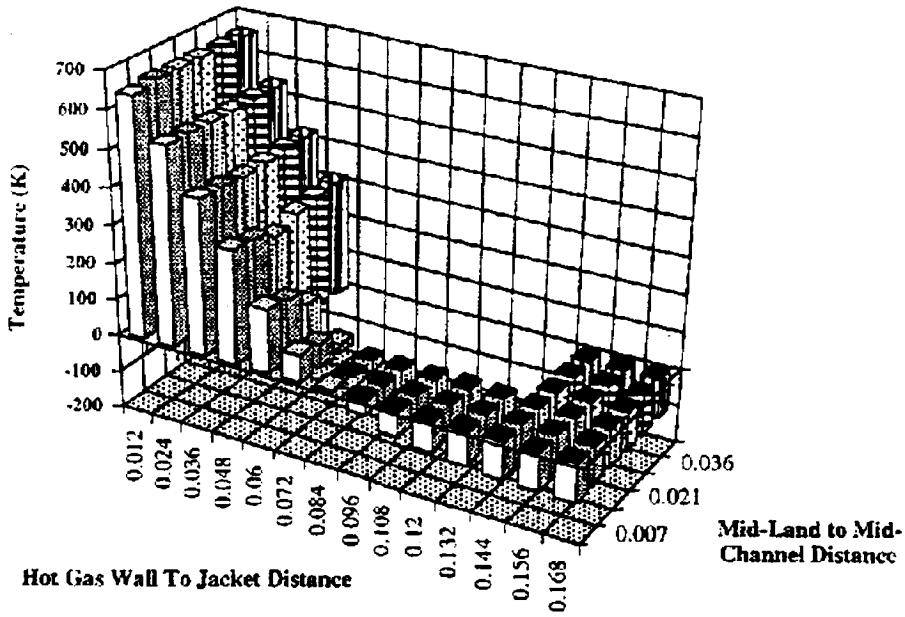


Figure 5. Main Combustion Chamber Liner Temperature Profile

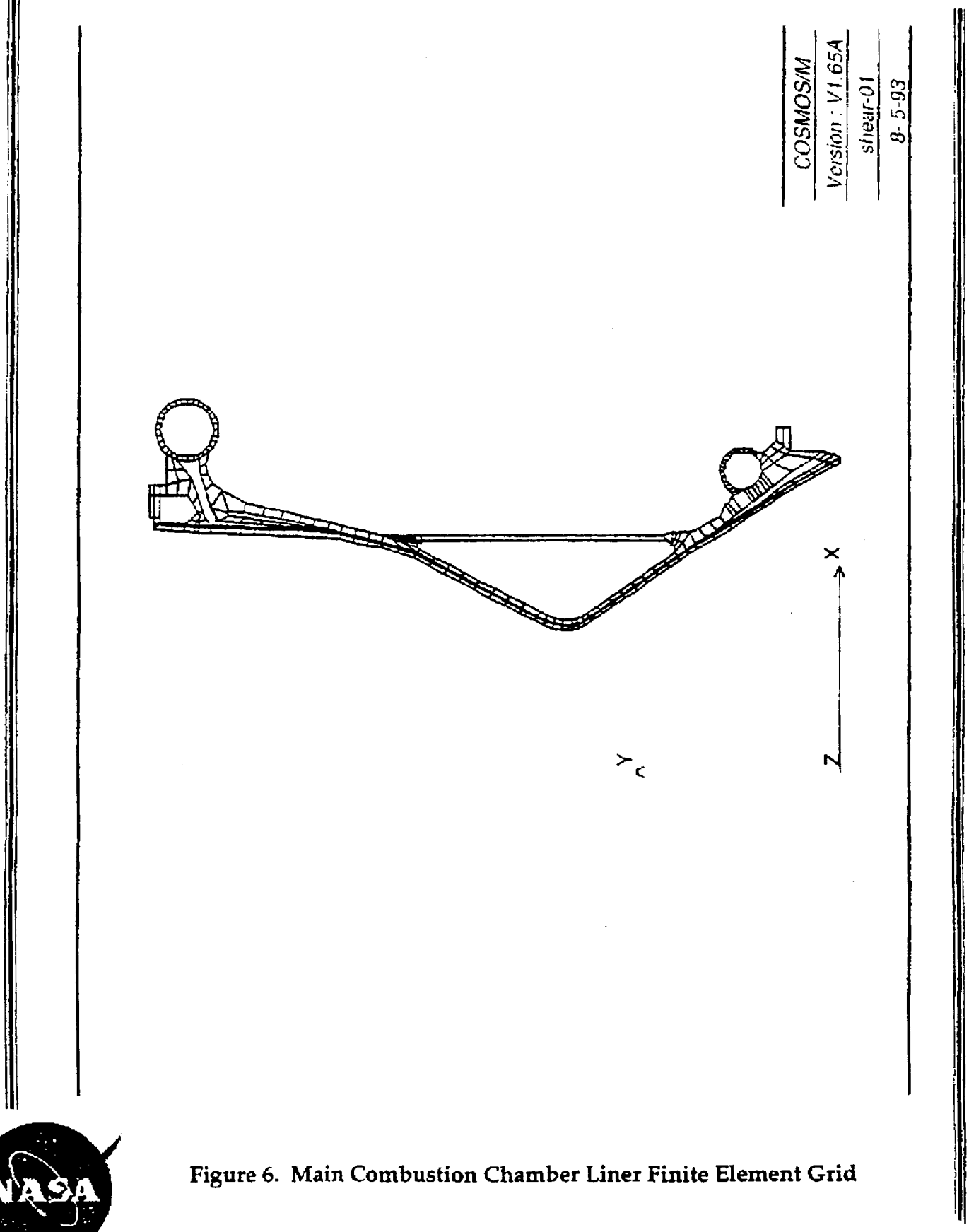


Figure 6. Main Combustion Chamber Liner Finite Element Grid

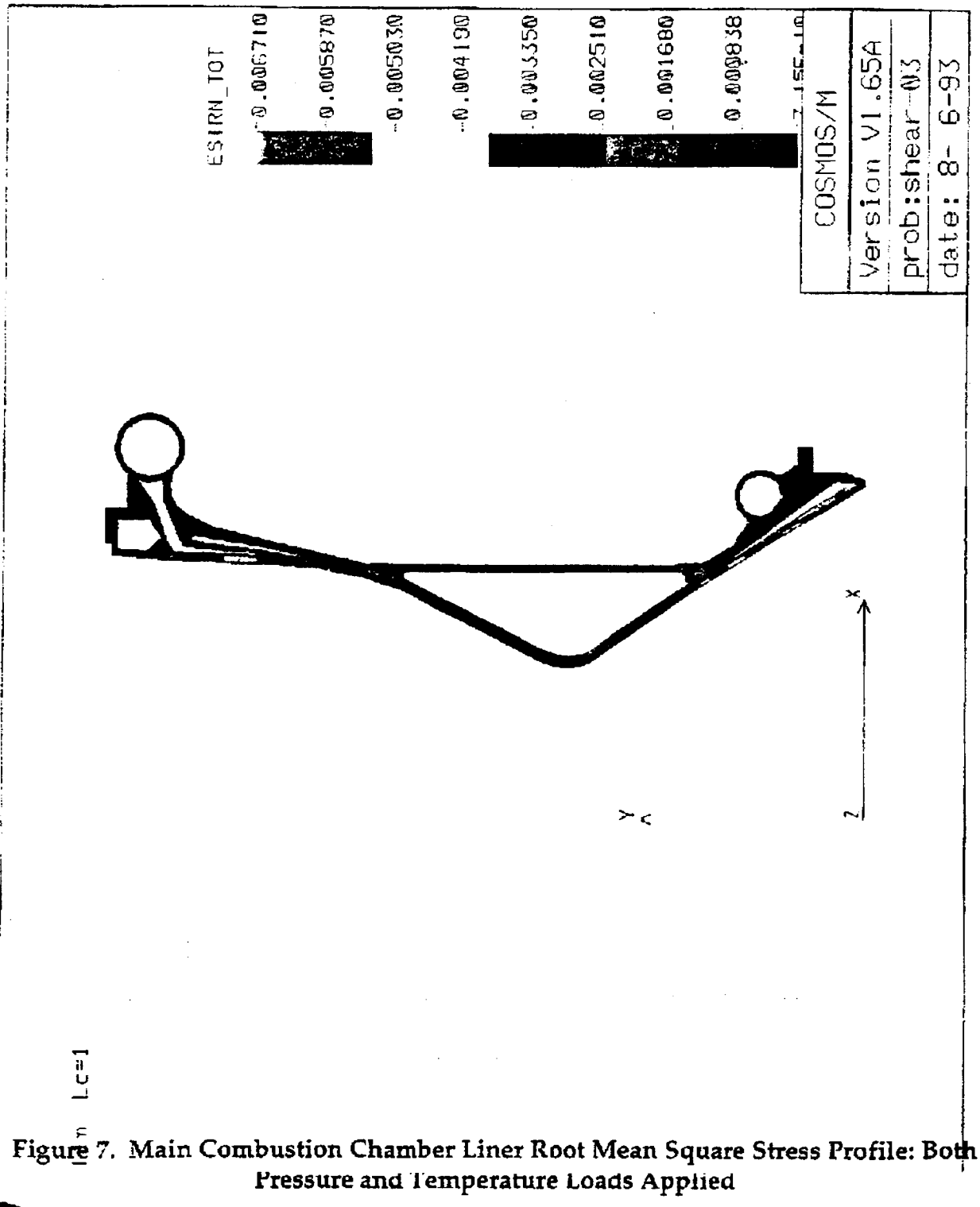


Figure 7. Main Combustion Chamber Liner Root Mean Square Stress Profile: Both Pressure and Temperature Loads Applied

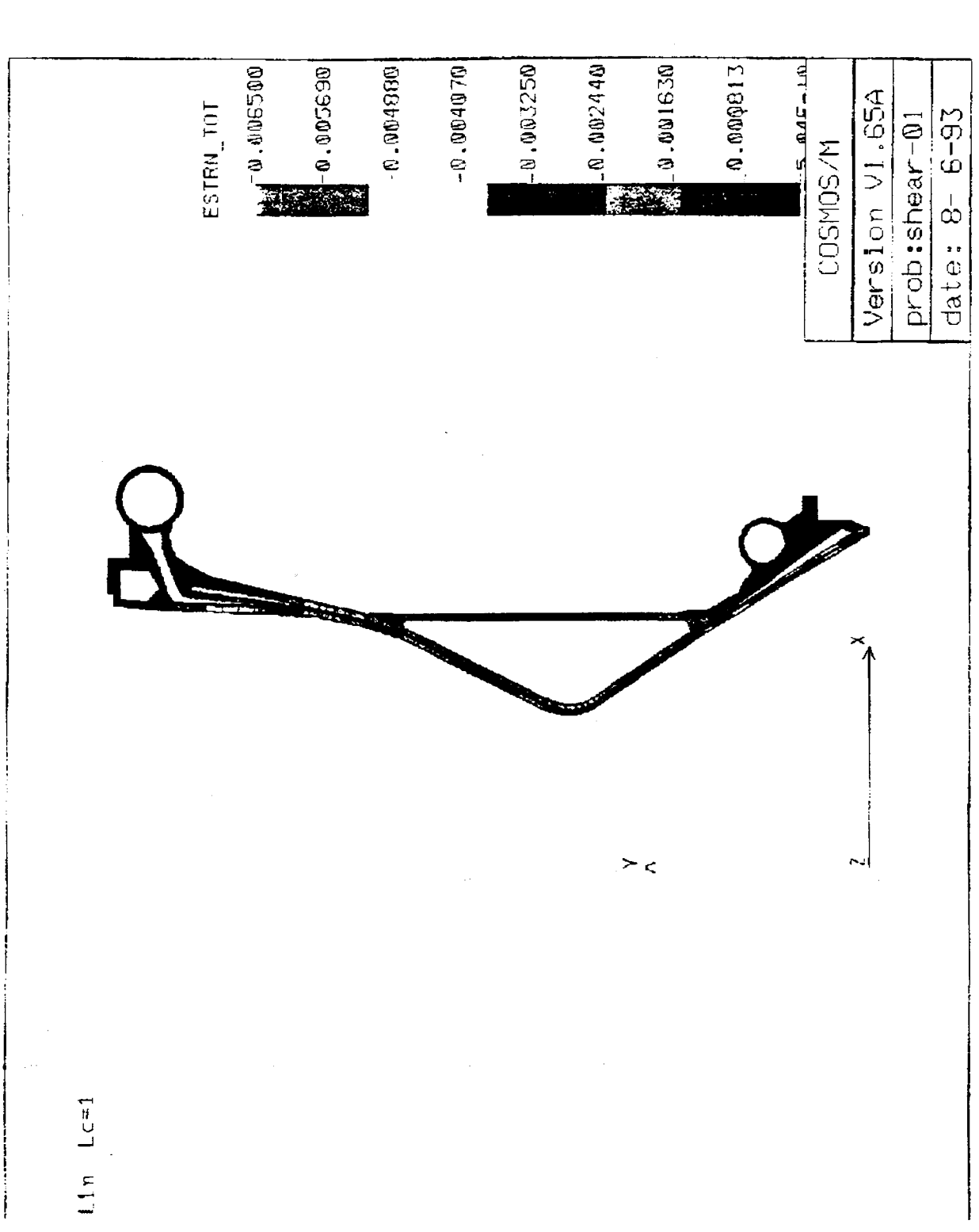


Figure 8. Main Combustion Chamber Liner Root Mean Square Stress Profile: Only Pressure Loads Applied

Calculated Shear Strains For MCC Liner Wall

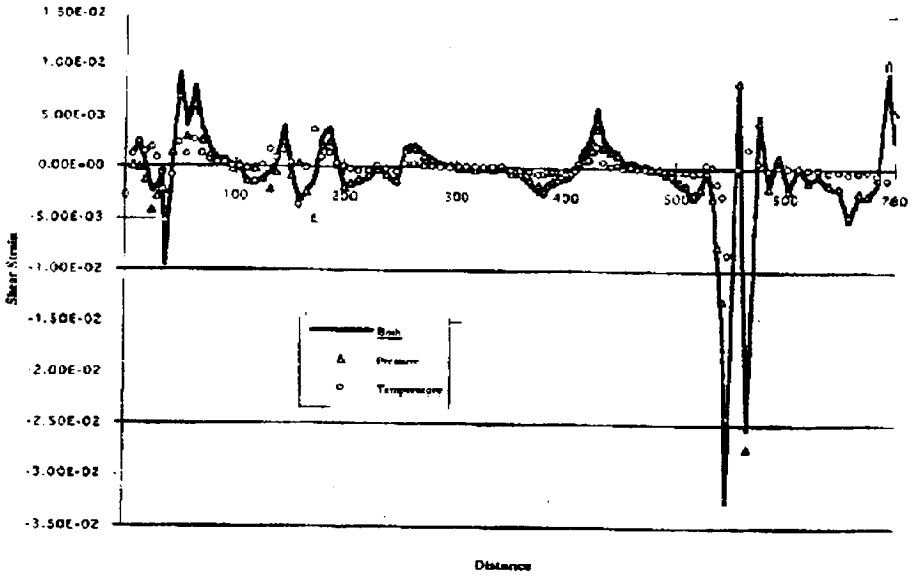


Figure 9. Main Combustion Chamber Liner Interface Shear Stress Profile

Mode I Stress Intensity Factor Versus
Normal To Shear Stress Ratio

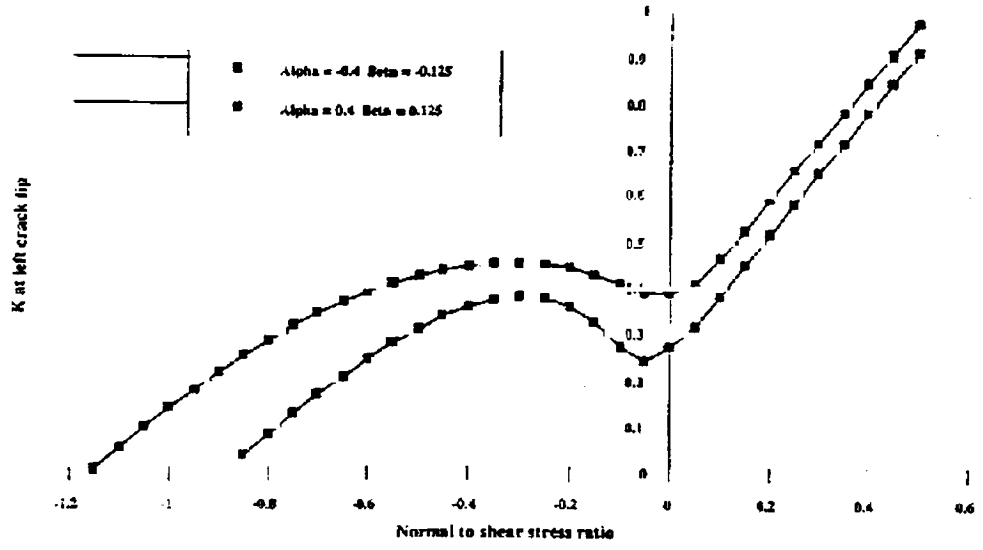


Figure 10. K_I as a Function of the Ratio of the Normal to Shear, σ_N/σ_τ

References

[1]. Rocketdyne report

[2]. data report

[3]. M. Yang and R.E. Kurth, *Stress Intensity Factors for Subinterface Cracks with Crack-Face Contact Zone, Mechanics of Composite Materials -- Nonlinear Effects*, AMD-Vol. 159, 1093, pp 273-282.

[4]. Rockwell International, Rocketdyne Division: *Materials Property Manual* as reported in NASA CR-168215

[5]. M. Yang and K-S Kim, *The Behavior of Subinterface Cracks With Crack-Face Contact*, Eng Frac Mech, 44, pp 155-165

[6]. Cook, R.T., Fryk, E.E., and Newell,J.F., *NASA Final Report: SSME Main Combustion Chamber Life Prediction*, NASA CR-168215, 1983

[7] AGREE Report, "Reliability of Military Electronic Equipment", Office of the Assistant Secretary of Defense, Washington, DC, GPO, 1957.

[8]Yu Shen, "SSME Reliability Analysis", SAIC, Division 265, January, 1990.

MCC PRA:
Initiating Event Frequency Estimation

INTRODUCTION

Classically, most data analyses are only concerned with failure data and failure rates. Because this is a demonstration project it must remain clear that an initiating event does represent a *failure* of a sub-component. However, it *does not* imply the failure of the MCC. Therefore, in this chapter we will refer to sub-component failures, e.g. hot gas wall cracks, as anomalies rather than failures. Then when one sees an anomaly rate it will not be mistaken for an MCC failure rate.

This study proceeded in two phases. The data received by SAIC contained data from January 1983 through April of 1993. The first step in the data analyses is the examination of the data as it exists to estimate initiating event frequencies and pivotal event frequencies. An examination of the raw data also helps to provide closure to the MLD analyses since any events not previously considered should appear in the data base if they are truly important. Therefore, the first part of this chapter provides an overview of the methods and analyses performed on the SSME data as received. The second portion of this chapter then re-organizes the data into a form more suited for the event tree analyses to be performed later.

PRACA Data Base Analyses

The anomaly data (both test and flight) for MCC (Main Combustion Chamber) from 1/14/1983 to 4/6/1993 have been studied. Because of the limited data base, some assumptions are necessary: First, since the successful test data between the anomalies are not available at the present time, the accumulated MCC testing time for each year are assumed to be same. Second, the environments for different MCC tests such as Qualification/certification test, Alert, development test, in-flight, acceptance test and manufacturing are not discriminated in this study. Third, anomalies caused by different anomaly modes are assumed to have the same consequence. Based on these assumptions, the MCC anomalies are categorized into nine anomaly modes. The contributions to the MCC anomaly made by each anomaly mode are estimated. By applying the basic concept of "AGREE Allocation Method" [7], the anomaly occurrence rates of each MCC anomaly mode are also calculated.

MCC Anomaly Modes

There are eight anomaly modes in the original MCC data base. They are:

ET: Measurement Anomaly
EV: Not-To-Specification
MS: Structure
MT: Pressure/Temperature High or Low
MU: Mechanical Tolerance
MV: External Leak
MW: Internal Leak
UC: Unsatisfactory condition

A large portion of MCC anomalies are related to contamination, blanching, and surface roughness which are not identified as initiating events from the MLD analysis. Also, many inconsistencies exist in categorizing anomaly modes in the original MCC data base. For example, anomalies caused by material crack were placed in anomaly category UC from 1983 to 1985, but in anomaly mode missing copper or debond from 1986 to 1988. Therefore, the original data base is re-categorized into the following nine groups:

YEAR	Blanching or surface roughness	Crack and pinhole	Contamination	Leak: Internal and External	Structure: Missing copper or debond	Pressure or Temperature either High or Low	Mechanical tolerance	Random individual	Weld failure	TOTAL
1983	9	14	6	5	2	2	5	1	7	51
1984	8	8	1	1	0	0	2	1	0	21
1985	7	10	1	3	4	0	1	2	5	33
1986	0	6	2	1	3	1	0	0	6	19
1987	0	8	2	0	0	0	0	1	0	11
1988	0	5	0	1	0	0	0	1	0	7
1989	1	1	1	1	0	1	0	1	0	6
1990	0	0	1	0	7	0	0	2	0	10
1991	3	1	6	0	0	0	0	7	0	17
1992	2	2	0	1	1	0	0	2	0	8
TOTAL	30	55	20	13	17	4	8	18	18	183

Table III. Number of Failures Per Year For SSME MCC

BS: Blanching/Surface Roughness
CK: Crack and Pin Hole (Channel, 24%; Liner, 22%; Weld, 27%; Hot Gas Wall, 11%)
CT: Contamination
LK: Leak - internal and external (Burst Diaphragm leakage, 54%)
MS: Structure (Missing Copper, 44%; De-bond, 39%)
MT: Pressure/Temperature Hi or Low
MU: Mechanical Tolerance
WL: Weld Anomaly (not including crack)
RI: Random Individual Anomaly

MCC Anomaly Mode Contribution Estimation

Based on these new categories the number of anomalies for each anomaly mode during each year are listed in Table III.

The average annual anomaly number (anomalies/year) caused by different anomaly modes are estimated by using the following formulas [8]

$$\lambda_{1,2} = (\lambda_1 + \beta\lambda_2)/(1+\beta)$$

$$\lambda_{1,2,3} = (\lambda_{1,2} + \beta\lambda_3)/(1+\beta)$$

$$\lambda_{1,2,\ldots,n} = (\lambda_{1,2,\ldots,n-1} + \beta\lambda_n)/(1+\beta)$$

where

β: Weight factor (=1.5 in the present study)
λ_1: Anomaly occurrence rate for the first year
λ_2: Anomaly occurrence rate for the second year
$\lambda_{1,2}$: Average anomaly occurrence rate for the 1st and 2nd year
$\lambda_{1,\ldots,n}$: Average anomaly occurrence rate for the 1st through nth year

The Annual anomaly numbers versus years for MCC and the top four anomaly contributors (cracks and pinhole leaks, contamination, blanching or surface roughness, and random, individual anomaly) are illustrated in Figures 11, 12, 13, 14, 15 and 16.

The contributions to the MCC anomaly made by different anomaly modes are listed in Table IV. The top three contributors to the MCC anomalies versus years is shown in Figure 17.

Anomaly occurrence rate Estimation for MCC Anomaly Modes

The anomaly occurrence rates for each MCC anomaly mode are estimated by using the basic concept of the *AGREE allocation method* [7]. The anomaly occurrence rate to the MCC

MCC ANNUAL ANOMALY NUMBER (TOTAL)

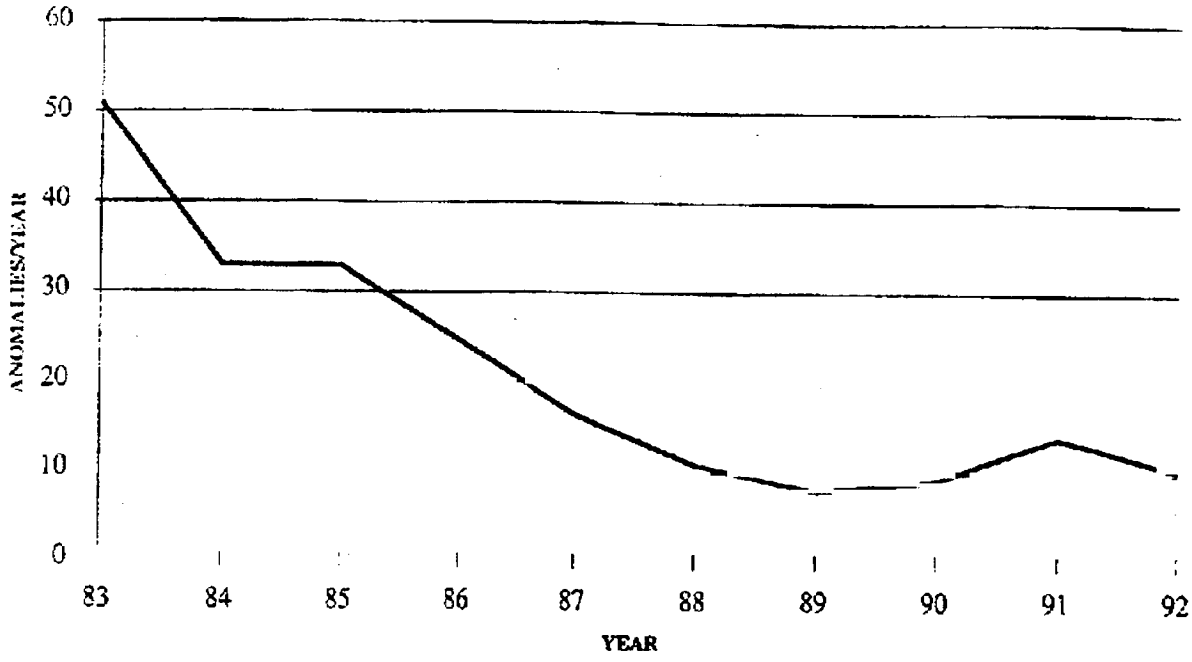


FIGURE 11. MCC Total Anomaly Number

CRACK (CK) ANNUAL ANOMALY NUMBER

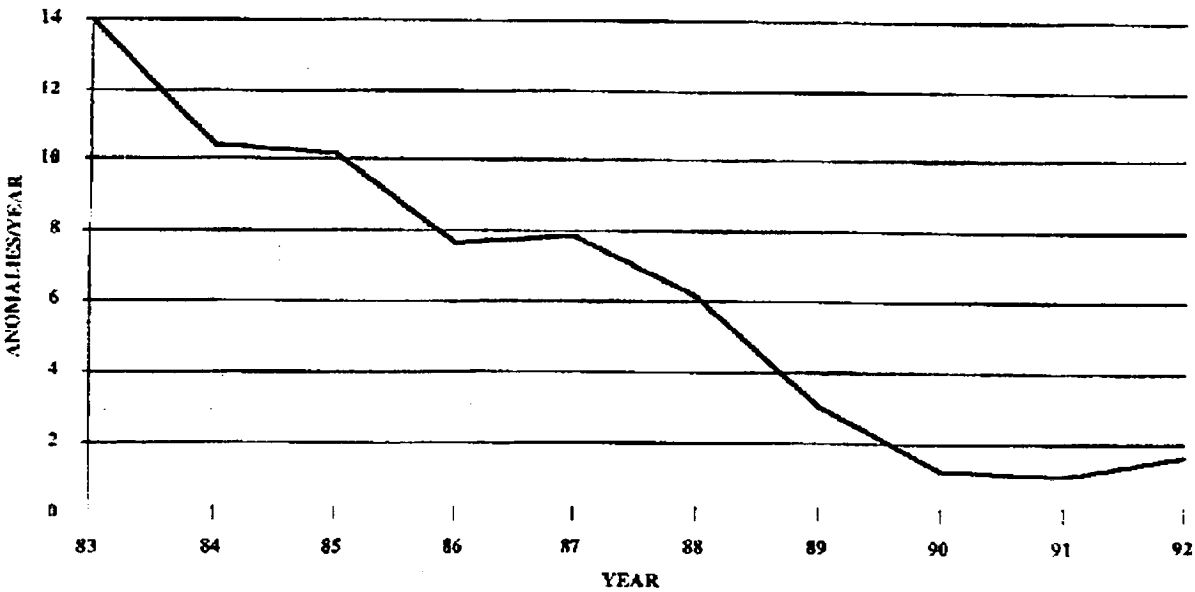


FIGURE 12. MCC Cracking Anomaly Number

CONTAMINATION (CT) ANNUAL ANOMALY NUMBER

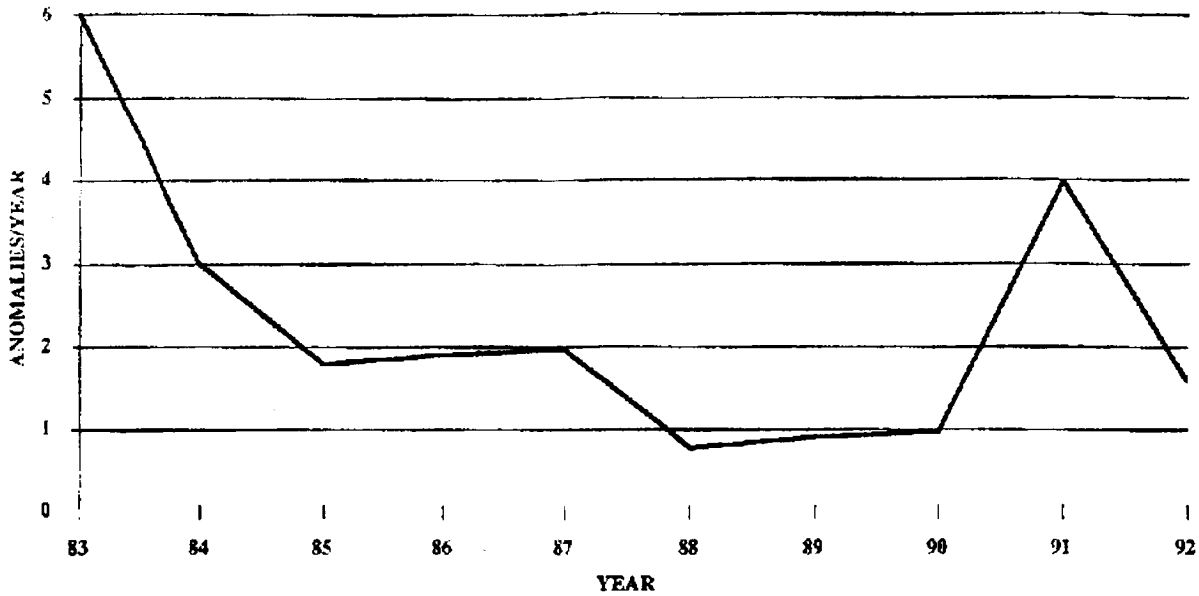


FIGURE 13. Contamination Annual Anomaly Number

BLANCHING/SURFACE ROUGHNESS (BS) ANNUAL ANOMALY NUMBER

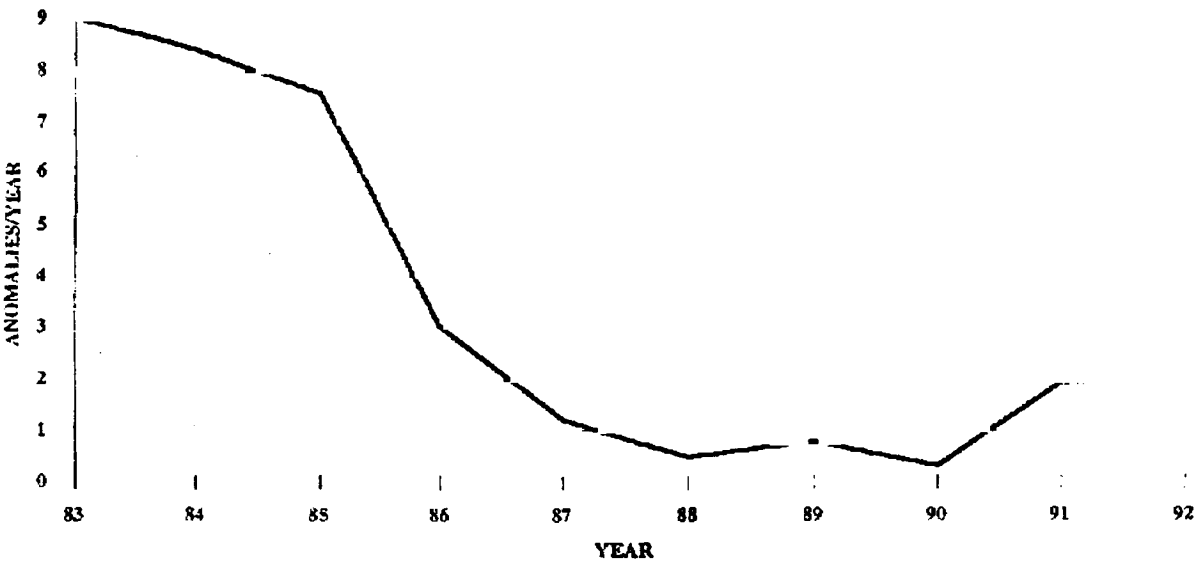


FIGURE 14. Blanching/Surface Roughness Annual Anomaly Number

RANDOM INDIVIDUAL FAILURE GROUP (RI) ANNUAL ANOMALY NUMBER

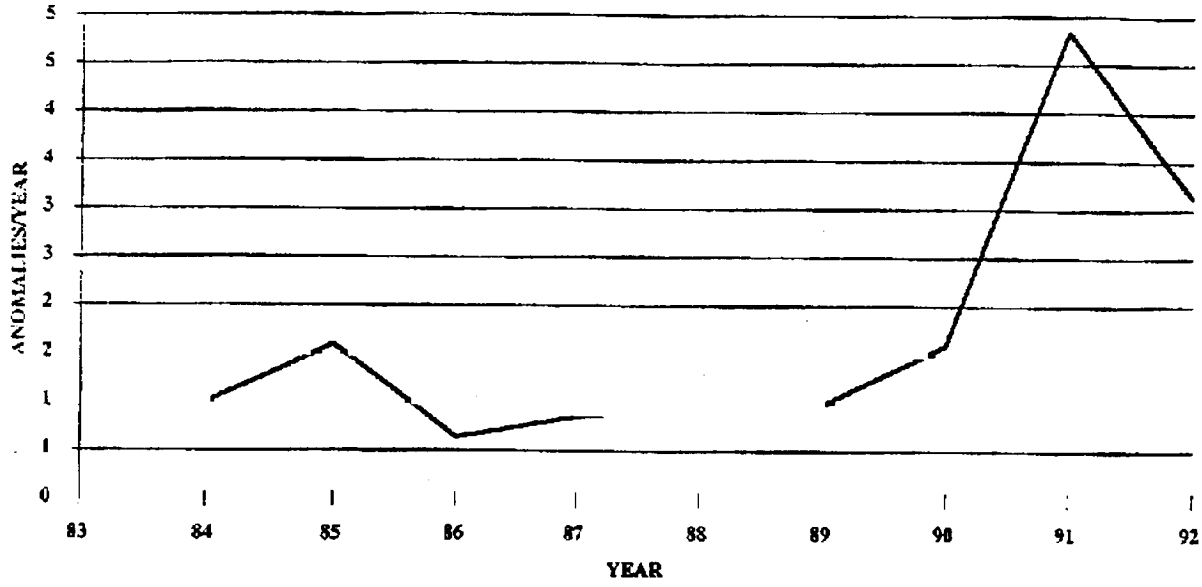


FIGURE 15. Random Individual Annual Anomaly Number

CONTRIBUTIONS TO MCC ANOMALY MADE BY MODES BS, CK , CT AND RI

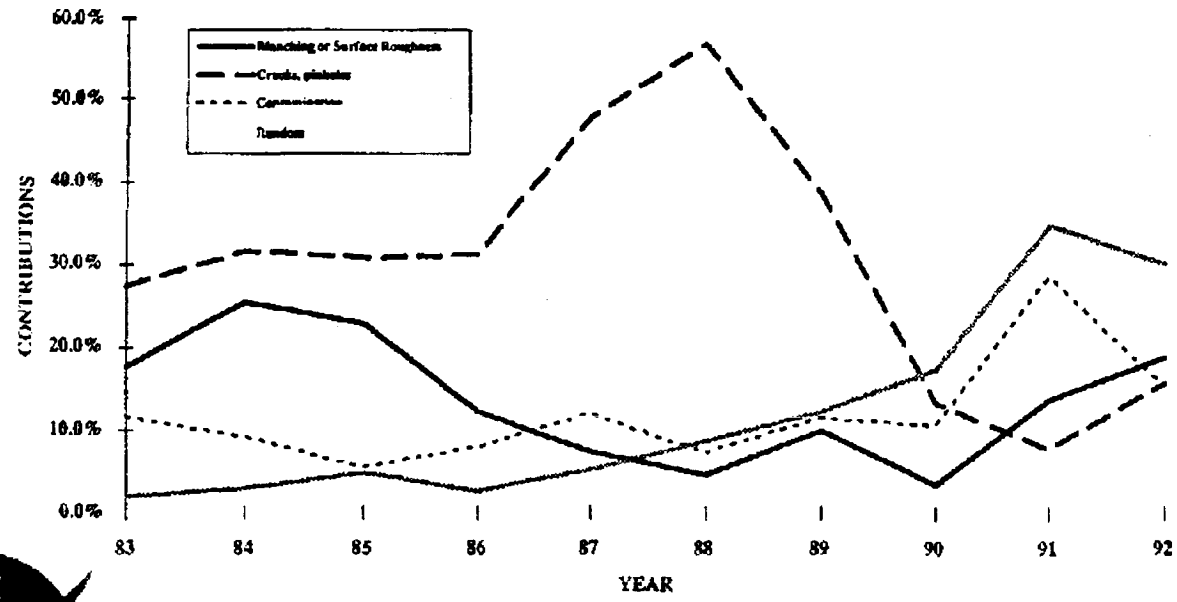


FIGURE 16. Contributors to Anomaly Number

TOP THREE MCC INITIATOR CONTRIBUTORS

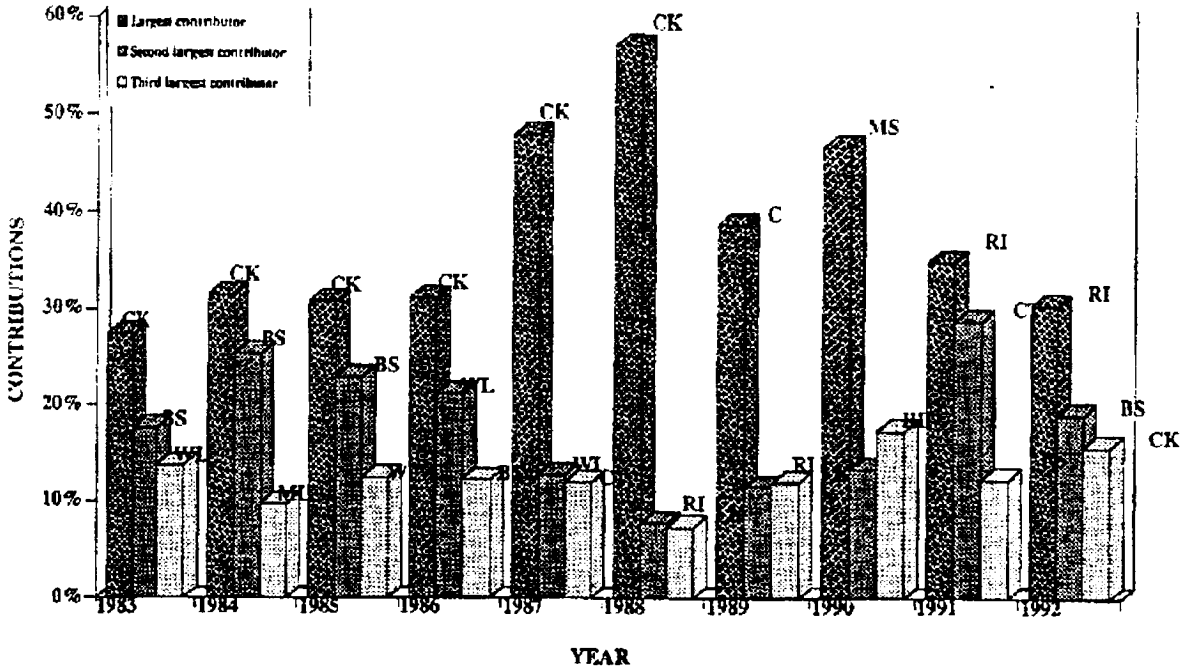


FIGURE 17. Top Three Contributors to Annual Anomaly Number

anomaly mode is given by

$$\lambda = C(-\ln(R(t))/\omega t$$

where

t: mission time
C: contribution of the anomaly mode
ω: importance factor for the anomaly mode P[MCC anomaly | anomaly caused by the anomaly mode]
$R_{(t)}$: MCC reliability for mission time t

For a mission time of 520 seconds, the contribution of different anomaly modes can be obtained from Table V. The importance factor for each anomaly mode is 1 (based on the third assumption described in the introduction).

The estimated anomaly occurrence rates for MCC anomaly modes in 1992 are listed in the Table VI.

Discussion and Summary

The average annual anomaly number for MCC dropped almost 80% from 1983 to 1992. Based on the results obtained from this study, the trend of the MCC reliability growth is toward stable.

Anomaly Modes Cracks and Pinhole Leaks (CK), Contamination (CT), and Blanching or Surface Roughness (BS)

The average annual anomaly numbers for the anomaly modes cracks and pinhole leaks, contamination, and blanching or surface roughness dropped 88%, 73% and 78% respectively (Figures 12, 13 and 14), but their contributions to the total MCC anomaly are still in the important positions (cracks and pinhole leaks 16%, contamination 15%, blanching or surface roughness 19% for 1992).

YEAR	Blanching or surface roughness	Crack and pinhole	Contamination	Leak: Internal and External	Structure: Missing copper or debond	Pressure or Temperature either High or Low	Mechanical tolerance	Random individual	Weld failure	TOTAL
83	9	14	6	5	2	2	5	1	7	51
84	8.4000	10.4000	3.0000	2.6000	0.8000	0.8000	3.2000	1.0000	2.8000	33.0000
85	7.5600	10.1600	1.8000	2.8400	2.7200	0.3200	1.8800	1.6000	4.1200	33.0000
86	3.0240	7.6640	1.9200	1.7360	2.8880	0.7280	0.7520	0.6400	5.2480	24.6000
87	1.2096	7.8656	1.9680	0.6944	1.1552	0.2912	0.3008	0.8560	2.0992	16.4400
88	0.4838	6.1462	0.7872	0.8778	0.4621	0.1165	0.1203	0.9424	0.8397	10.7760
89	0.7935	3.0585	0.9149	0.9511	0.1848	0.6466	0.0481	0.9770	0.3359	7.9104
90	0.3174	1.2234	0.9660	0.3804	4.2739	0.2586	0.0193	1.5908	0.1343	9.1642
91	1.9270	1.0894	3.9864	0.1522	1.7096	0.1035	0.0077	4.8363	0.0537	13.8657
92	1.9708	1.6357	1.5946	0.6609	1.2838	0.0414	0.0031	3.1345	0.0215	10.3463

Table IV. Weighted MCC Annual Anomaly Number (Anomalies/Year)

Anomaly Mode Random, Individual Anomaly (RI)

The annual anomaly number for the anomaly mode random, individual anomaly increased 213% from 1983 to 1992. Since dealing with random, individual anomalies is a much more difficult task than other anomaly modes (which are more specifically defined), it is expected to see random individual anomalies take a more important position for the MCC reliability improvement in the later MCC performance period.

Anomaly Modes: Internal or External Leak (LK) and Missing Copper or Debond (MS)

The MCC anomalies caused by internal or external leak were dominated by "Burst Diaphragm Leak" from 1983 to 1986. The latest three anomalies (1988, 1989, and 1992) are not related to "Burst Diaphragm Leak". The anomaly mode internal or external leak contributes 6% of the total MCC anomalies for 1992.

YEAR	Blanching or Surface Roughness	Cracks and pinholes	Contamination	Leaks: Internal And External	Structure: Missing copper or debond	Pressure or temperature either high or low	Mechanical Tolerance	Random	Weld failure
83	17.6%	27.5%	11.8%	9.8%	3.9%	3.9%	9.8%	2.0%	13.7%
84	25.5%	31.5%	9.1%	7.9%	2.4%	2.4%	9.7%	3.0%	8.5%
85	22.9%	30.8%	5.5%	8.6%	8.2%	1.0%	5.7%	4.8%	12.5%
86	12.3%	31.2%	7.8%	7.1%	11.7%	3.0%	3.1%	2.6%	21.3%
87	7.4%	47.8%	12.0%	4.2%	7.0%	1.8%	1.8%	5.2%	12.8%
88	4.5%	57.0%	7.3%	8.1%	4.3%	1.1%	1.1%	8.7%	7.8%
89	10.0%	38.7%	11.6%	12.0%	2.3%	8.2%	0.6%	12.4%	4.2%
90	3.5%	13.3%	10.5%	4.2%	46.6%	2.8%	0.2%	17.4%	1.5%
91	13.9%	7.9%	28.8%	1.1%	12.3%	0.7%	0.1%	34.9%	0.4%
92	19.0%	15.8%	15.4%	6.4%	12.4%	0.4%	0.0%	30.3%	0.2%

Table V. Anomaly Mode Contributions to the MCC Anomaly Rate

There are 7 MCC anomalies caused by anomaly mode missing copper or debond in 1990, that drove the MS annual anomaly number high.

Year	Blanching or Surface Roughness	Cracks and pinholes	Contamination	Leaks: Internal And Structure: External	Missing copper or debond
1992	5.75E-08	4.77E-08	4.65E-08	1.93E-08	3.75E-08
	1 in 33,438 missions	1 in 40,287 missions	1 in 41,328 missions	1 in 99,717 missions	1 in 51,331 missions

Year	Pressure or temperature either high or low	Mechanical Tolerance	Random	Weld failure	TOTAL
1992	1.21E-09	8.99E-11	9.15E-08	6.27E-10	2.09E-07
	1 in 1,592,479 missions	1 in 21,394,699 missions	1 in 21,024 missions	1 in 3,065,704 missions	1 in 9,222 missions

Table VI. 1992 Estimated MCC Anomaly Rate

More than 83% of the missing copper or debond anomalies were caused by " Missing Copper and Debond". The anomaly mode missing copper or debond contributes 12% of the total MCC anomalies for 1992.

Anomaly Modes Pressure/Temperature High or Low (MT), Mechanical Tolerance (MU), and Weld Anomaly (WL)

The contributions to the MCC anomaly made by pressure/temperature high or low, mechanical tolerance and weld anomaly are relatively low in the recent years (Totally less than 1% of the MCC anomalies are contributed by these three anomaly modes in 1992).

Estimating MLD Initiating Event Frequencies

The previous analysis demonstrated that events that are related to the initiating events identified from the MLD are occurring frequently enough to warrant further, detailed study.

Unfortunately, the detailed records needed to study the thirteen initiators identified by the Master Logic Diagram only are available from 1988 to 1992. Previous data did not contain enough information to separate the data into MLD initiating event categories. The annual events attributed to each initiating event is listed in Table VII. The average annual initiating event frequencies are based on two considerations:

The accumulated MCC testing or flight time for each year, and
The "*reliability growth effect*".

The following formulas have been used to estimate the average annual initiating event frequencies:

$$F_{1,2} = (T_{1,2}F_1 + \beta F_2)/(1 + \beta)$$
$$F_{1,2,3} = (T_{2,3}F_{1,2} + \beta F_3)/(1 + \beta)$$
$$F_{1,\ldots,n} = (T_{n-1,n}F_{1,\ldots,n-1} + \beta F_n)/(1 + \beta)$$

where

β: weight factor, 1.5 in present study
F_i: Number of events in i^{th} year
$T_{i,j}$: Time factor, $T_{i,j} = T_j/T_i$

The accumulated test/flight time use for the $T_{i,j}$ values are shown in Table VIII. The values for F are calculated based on the data in Tables VII and VIII. The results are shown in Table IX.

It is now possible to estimate the individual initiating event frequencies from Tables VII through IX. Using the *AGREE allocation method* the initiating event frequency for event i is calculated by the following formula:

$$\lambda_i = (C_i\lambda_{MCC})/\omega_i$$

YEAR	Largest contributor		Second largest contributor		Third largest contributor	
1983	27%	Cracks, pinholes	18%	Blanching or Surface Roughness	14%	Weld failure
1984	31%	Cracks, pinholes	24%	Blanching or Surface Roughness	10%	Contamination
1985	30%	Cracks, pinholes	22%	Blanching or Surface Roughness	12%	Weld failure
1986	31%	Cracks, pinholes	19%	Weld failure	14%	Blanching or Surface Roughness
1987	43%	Cracks, pinholes	14%	Weld failure	11%	Contamination
1988	51%	Cracks, pinholes	10%	Weld failure	8%	Contamination
1989	40%	Cracks, pinholes	11%	Contamination	11%	Leaks: Internal And External
1990	38%	Structure: Missing copper/debond	19%	Cracks, pinholes	15%	Random
1991	32%	Random	26%	Contamination	14%	Structure: Missing copper/debond
1992	29%	Random	18%	Blanching or Surface Roughness	16%	Cracks, pinholes

Table VII. Largest Contributors to MCC Anomaly Rate

where

λ_i : Initiating event frequency estimate
C_i: Contribution of i^{th} initiator
λ_{MCC}: Frequency of all MCC initiating events
ω_i: Importance factor for the i^{th} initiator
P(MCC failure | failure cause by the i^{th} initiator)

The estimate for λ_{MCC} in 1992 is 1.61×10^{-4} per second. This estimate is obtained by dividing the total number of recorded anomalies by the total equivalent test (or hot-fire) time. If it is assumed that the average mission time is 520 seconds the value of λ_{MCC} implies an initiator occurs about every 12 missions. This frequency is probably too low, that is initiating events occur more frequently, but a more detailed data analysis could improve this accuracy. However, the purpose of this study is a demonstration of the method, it is not to calculate the detailed risk. Therefore, while the initiating event frequency is believed to be realistic the current scope of the program does not allow a more detailed analysis of data received after this initial analysis was completed. The estimates for the initiating event frequencies are provided in Table XI.

Based on these results, it was decided after examining the event tree diagrams (to be presented in the following chapter) that more detailed analyses of the data was warranted for the initiating event frequencies. These results are presented in the following section.

YEAR	Hot Gas Wall Crack	Coolant Channel Crack	G-15 Bolt Failure	EDNI Separation/Crack	Multiple Channel Blockage	FRI Leakage	Manifold Weld Failure
1988	0	1	0	0	0	0	3
1989	0	2	0	4	1	0	0
1990	3	0	2	5	2	0	0
1991	1	1	1	1	1	0	0
1992	1	1	0	3	0	0	0
TOTAL	5	5	3	13	4	0	3

YEAR	Actautor Sideload Instability	Loss of Powerhead Bolt Preload	Bent Nozzle Tube at MCC Interface	Combustion/Flow Instability	Loss of Pressure Sensor	Seal Leakage	TOTAL
1988	0	0	1	1	0	2	8
1989	0	0	0	0	0	4	11
1990	0	0	0	0	0	1	13
1991	1	0	0	1	0	1	8
1992	0	0	0	0	1	0	6
TOTAL	1	0	1	2	1	8	46

Table VIII. Events Used to Estimate MLD Initiating Event Frequency

YEAR	88				
Flight/Test seconds	45,268	44,166	52,407	40,614	47,475
Time factor	0.9757	1.1866	0.7750	1.1689	1.0000
β	1.5	1.5	1.5	1.5	1.5

Table IX. Test/Flight Time Used to Estimate MLD Initiating Event Frequency

YEAR	Hot Gas Wall Crack	Coolant Channel Crack	G-15 Bolt Failure	EDNI Separation/Crack	Multiple Channel Blockage	FRI Leakage	Manifold Weld Failure
1988	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	3.0000
1989	0.0000	1.5903	0.0000	2.4000	0.6000	0.0000	1.1708
1990	1.8000	0.7548	1.2000	4.1391	1.4848	0.0000	0.5557
1991	1.1580	0.8340	0.9720	1.8831	1.0603	0.0000	0.1723
1992	1.1414	0.9899	0.4545	2.6805	0.4958	0.0000	0.0805
TOTAL	4.0994	5.1690	2.6265	11.1027	3.6408	0.0000	4.9793

YEAR	Actautor Sideload Instability	Loss of Powerhead Bolt Preload	Bent Nozzle Tube at MCC Interface	Combustion/Flow Instability	Loss of Pressure Sensor	Seal Leakage	TOTAL
1988	0.0000	0.0000	1.0000	1.0000	0.0000	2.0000	8
1989	0.0000	0.0000	0.3903	0.3903	0.0000	3.1805	9.7220892
1990	0.0000	0.0000	0.1852	0.1852	0.0000	2.1096	12.414522
1991	0.6000	0.0000	0.0574	0.6574	0.0000	1.2539	8.6483123
1992	0.2805	0.0000	0.0268	0.3074	0.6000	0.5863	7.6437225
TOTAL	0.8805	0.0000	1.6598	2.5403	0.6000	9.1304	46.4286

Table X. Average Annual Initiating Events For MLD Initiators

YEAR	Hot Gas Wall Crack	Coolant Channel Crack	G-15 Bolt Failure	EDNi Separation/Crack	Multiple Channel Blockage	FRI Leakage	Manifold Weld Failure
1988	Large	1 in 96	Large	Large	Large	Large	1 in 32
1989	Large	1 in 73	Large	1 in 48	1 in 194	Large	1 in 99
1990	1 in 82	1 in 196	1 in 124	1 in 36	1 in 100	Large	1 in 267
1991	1 in 89	1 in 124	1 in 106	1 in 55	1 in 97	Large	1 in 600
1992	1 in 80	1 in 92	1 in 201	1 in 34	1 in 184	Large	1 in 1,134

YEAR	Actautor Sideload Instability	Loss of Powerhead Bolt Preload	Bent Nozzle Tube at MCC Interface	Combustion/Flow Instability	Loss of Pressure Sensor	Seal Leakage	TOTAL
1988	Large	Large	1 in 96	1 in 96	Large	1 in 48	1 in 12
1989	Large	Large	1 in 298	1 in 298	Large	1 in 37	1 in 12
1990	Large	Large	1 in 801	1 in 801	Large	1 in 70	1 in 12
1991	1 in 172	Large	1 in 1,799	1 in 157	Large	1 in 82	1 in 12
1992	1 in 325	Large	1 in 3,401	1 in 297	1 in 152	1 in 156	1 in 12

Table XI. Estimated Initiating Event Frequencies For MLD Initiators

Re-Examination of PRACA Data Base For MCC Initiating Frequencies

The MCC data bases used in this analysis are
MSFC Report,
SSME FRR Report, and
SSME Historical Data (NASA/MFSC).

MCC Data Analysis

The following assumptions were utilized during the re-examination of the available SSME data.

HGW: Hot Gas Wall Crack

The pinholes and cracks on the hot gas wall are counted.

The sizes and locations of the pinholes or cracks are not distinguished.

Surface roughness, blanching, or blister are not counted.

Abnormal data that are not representative of the population as a whole, for example, MCC 4011 had 141 holes and cracks in only 8 starts, are eliminated from this analysis.

PBF: Bolt failure

Bolt failure such as bolt stretch, crack or fracture are counted (obtained from SSME FRR Report).

ESC: EDNi crack - not aft end

The cold wall cracks which are not at the aft end are counted.

Leakage in weld joint 15(EDNi close out) causing the MCC liner cavity pressure increase are counted.

EAE: EDNi crack - aft end

MCC cold wall cracks or debonds at the aft end are counted.

FRI: Flow recirculation inhibitor system leakage

The FRI failures such as seal leak and seal overheating are counted (obtained from SSME

FRR Report).

MWF: Manifold weld failure

Manifold weld cracks are counted.

Lack of fusion, microcracks (acceptable per the weld spec.) in welds are not counted as weld failures.

CCC: Coolant channel deformation/crack, and
CCB: Multiple coolant channel blockage,

Contaminations which do not cause blockage are not counted as a failure.

Based on the existing data base, the MCC failures caused by CCC or CCB can not be explicitly identified, and are eliminated in this analysis.

The MCC failure data (both test and flight) from 1/5/88 to 4/6/93 has been used for this study.

Note: The total number of pinholes/cracks on MCC 2024 were 30. These occurred over 5 years. The number of the HGW events for each year in this case is assumed to be 6.

MCC Initiator Frequency Estimation

The method developed for the MCC initiator frequency estimation is based on the following assumptions:

The MCCs considered in this analysis are assumed to have same physical conditions. They are not discriminated.

The environments for different MCC tests such as Qualification/certification test, Alert, development test, in flight, acceptance test and manufacturing are not distinguished in this study.

In order to evaluate the MCC "reliability growth effect", a weight factor has been used in this study. The basic concept of using this weight factor is to place more weight on the current MCC initiating event than on the earlier MCC initiating event in the MCC initiating event frequency estimation. For example, the MCC initiating events which occurred in 1992 are weighted more than the MCC initiating events which occurred in 1991. In this analysis, $\beta=1$ (no reliability growth effect), $b=1.5$, and $\beta=2$ (strong reliability growth effect) has been tested.

Since the successful test/flight data between the MCC anomalies are not available at the present time, the frequencies of MCC initiators are estimated on a yearly basis (the accumulated MCC test/flight time for each year are available). The MCC initiating event frequencies are assumed to be proportional to the length of the accumulated MCC test/flight time.

For this set of assumptions the analysis of the previous section is repeated. Using a standard χ^2 distribution uncertainty ranges can be formed. These results are presented in Tables IV-A, V-A, and VI-A.

YEAR	Hot Gas Wall Crack	Coolant Channel Crack	G-15 Bolt Failure	EDNI Separation/Crack	Multiple Channel Blockage	FRI Leakage	Manifold Weld Failure
1988	9	0	0	1	0	1	7
1989	19	0	0	2	1	4	0
1990	6	0	2	0	2	1	0
1991	6	0	1	0	1	1	0
1992	7	0	0	0	0	0	0
TOTAL	47	0	3	3	4	7	7

YEAR	Actuator Sideload Instability	Loss of Powerhead Bolt Preload	EDNI Aft End Separation/Crack	Combustion/Flow Instability	Loss of Pressure Sensor	Seal Leakage	TOTAL
1988	0	0	0	1	0	2	21
1989	0	0	1	0	0	4	31
1990	0	2	5	0	0	1	19
1991	1	1	0	1	0	1	13
1992	0	0	1	0	1	0	9
TOTAL	1	3	7	2	1	8	93

Table IV-A. Weighted MCC Annual Anomaly Number (Anomalies/Year)

YEAR	Hot Gas Wall Crack	Coolant Channel Crack	G-15 Bolt Failure	EDNI Separation/Crack	Multiple Channel Blockage	FRI Leakage	Manifold Weld Failure
1988	9.0000	0.0000	0.0000	1.0000	0.0000	1.0000	7.0000
1989	14.9124	0.0000	0.0000	1.5903	0.6000	2.7903	2.7318
1990	10.6780	0.0000	1.2000	0.7548	1.4848	1.9244	1.2966
1991	6.9100	0.0000	0.9720	0.2340	1.0603	1.1965	0.4019
1992	7.4309	0.0000	0.4545	0.1094	0.4958	0.5595	0.1879
TOTAL	48.9314	0.0000	2.6265	3.6884	3.6408	7.4706	11.6183

YEAR	Actuator Sideload Instability	Loss of Powerhead Bolt Preload	Rear Nozzle Tube at MCC Interface	Combustion/Flow Instability	Loss of Pressure Sensor	Seal Leakage	TOTAL
1988	0.0000	0.0000	0.0000	1.0000	0.0000	2.0000	21
1989	0.0000	0.0000	0.6000	0.3903	0.0000	3.1805	26.79548402
1990	0.0000	1.2000	3.2848	0.1852	0.0000	2.1096	24.11829082
1991	0.6000	0.9720	1.0182	0.6574	0.0000	1.2539	15.2763018
1992	0.2805	0.4545	1.0761	0.3074	0.6000	0.5863	12.54279549
TOTAL	0.8805	2.6265	5.9791	2.5403	0.6000	9.1304	99.7329

Table V-A. Individual Anomaly Mode Contributions to the MCC Anomaly Rate

YEAR	Hot Gas Wall Crack	Coolant Channel Crack	G-15 Bolt Failure	EDM Separation/Crack	Multiple Channel Blockage	FRI Leakage	Manifold Weld Failure
1988	1 in 10	1 in 1,500	1 in 1,500	1 in 87	1 in 1,500	1 in 87	1 in 12
1989	1 in 5	1 in 1,500	1 in 1,500	1 in 46	1 in 122	1 in 26	1 in 27
1990	1 in 12	1 in 1,500	1 in 107	1 in 169	1 in 86	1 in 66	1 in 99
1991	1 in 13	1 in 1,500	1 in 94	1 in 392	1 in 87	1 in 77	1 in 228
1992	1 in 17	1 in 1,500	1 in 280	1 in 1,163	1 in 257	1 in 227	1 in 677

YEAR	Actuator Sideload Instability	Loss of Powerhead Bolt Preload	EDM All End Separation/Crack	Combustion/Flow Instability	Loss of Pressure Sensor	Seal Leakage	TOTAL
1988	1 in 1,500	1 in 1,500	1 in 1,500	1 in 87	1 in 1,500	1 in 44	1 in 4
1989	1 in 1,500	1 in 1,500	1 in 122	1 in 188	1 in 1,500	1 in 23	1 in 3
1990	1 in 1,500	1 in 107	1 in 39	1 in 691	1 in 1,500	1 in 61	1 in 5
1991	1 in 153	1 in 94	1 in 90	1 in 140	1 in 1,500	1 in 73	1 in 6
1992	1 in 454	1 in 280	1 in 118	1 in 414	1 in 212	1 in 217	1 in 10

Table VI-A. 1992 Estimated MCC Anomaly Rate

Functional Event Sequence Diagrams (FESD's):

Application To The MCC

Manifold Weld Anomaly Functional Event Sequence Diagram

The functional event sequence diagram for the Manifold Weld Anomaly, identified MWF in the FESD, is shown in Figure 18. The entry condition for this FESD is a crack of any size existing in the weld material of Heat Affected Zone (HAZ) of the parent material. Given that a crack exists, the first question to ask is if it is large enough to be detected, MWF-CD-001? If it is large enough to be detected then it is assumed that a repair of the crack is attempted. If the repair is effective, a positive response to event MWF-RE-001, then there is a successful operation. If the repair is not effective then a crack still exists in the structure and the FESD must return to the path that examines the size of the crack. If the crack in the weld or HAZ is small enough to not grow to a critical size over one mission, a positive response to MWF-LC-001, then there is successful operation. If the crack grows to a critical size then there would be a loss of vehicle.

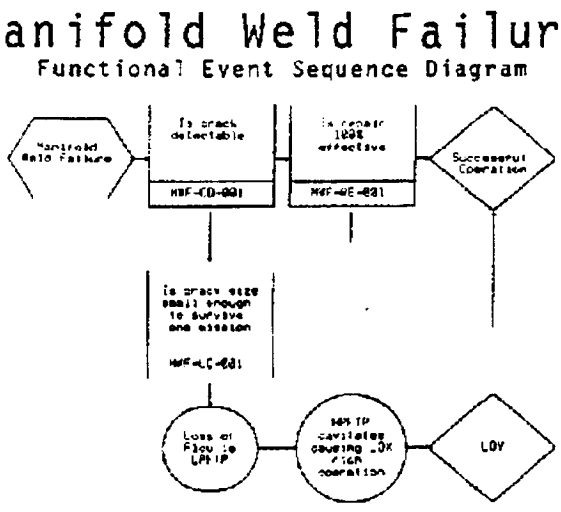


Figure 18. Manifold Weld Anomaly FESD

Bolt Anomaly Functional Event Sequence Diagram

The functional event sequence diagram for the Bolt Anomaly, identified PBF in the FESD, is shown in Figure 19. The entry point for this FESD is that the pre-load on the bolt is outside the MSFC specifications. The evidence from

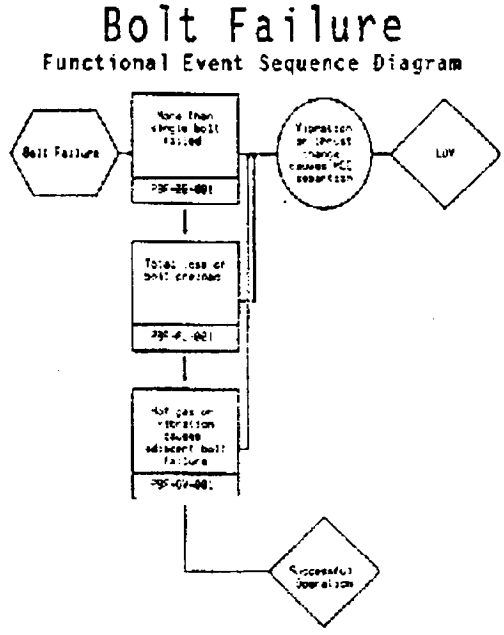


Figure 19. Bolt Anomaly FESD

MSFC is that a single bolt failure due to incorrect torque being applied, bolt stretch, or bolt shear, is insufficient to affect the operation of the MCC. Therefore, the first question to be asked is if more than a single bolt has failed, PBF-BB-001. If more than a single bolt has failed, it is

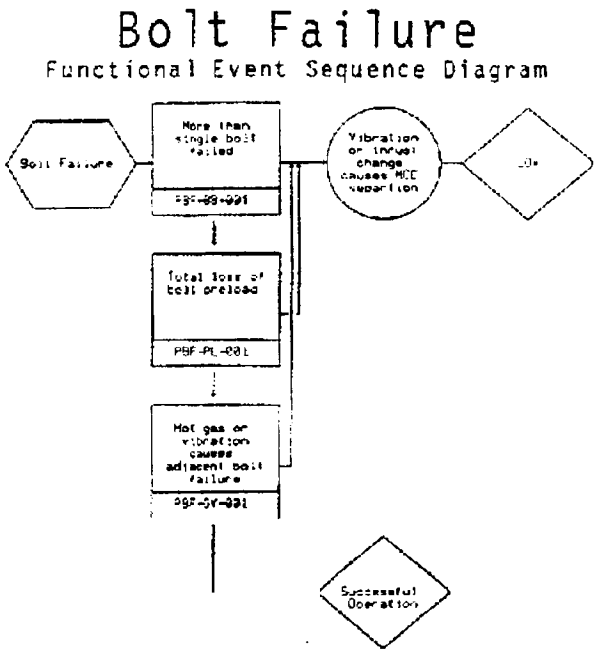


Figure 20. Updated Bolt Anomaly FESD

assumed that the leakage and/or vibration loading will lead to an LOV event. If only a single bolt fails then a total loss of the bolt could also lead to a leakage path causing LOV. If there is not a total loss of the bolt, a negative response to PBF-PL-001, then it is possible that the added loading, both mechanical and thermal, on adjacent bolts could cause their failure. The initial FESD for the bolt loss included a branch for the combustion or flow instability; however, MSFC personnel stated in an August 24, 1993 meeting that this is not possible for a partial loss of a

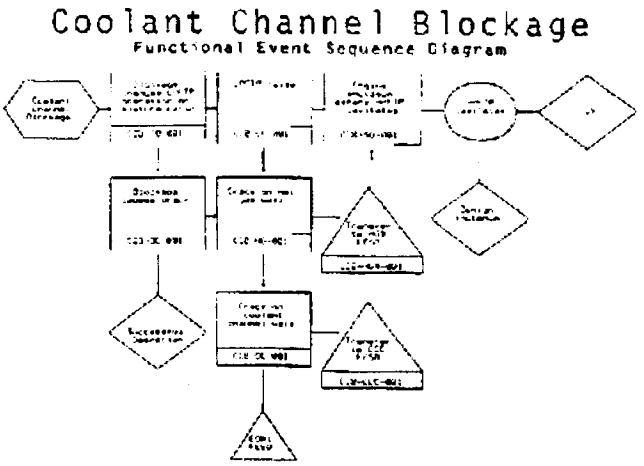


Figure 21. Coolant Channel Blockage FESD

single bolt. The events PBF-CI-001 and PBF-SW-001 have been deleted from the PBF FESD. This updated FESD is shown in Figure 20.

Coolant Channel Blockage Functional Event Sequence Diagram

The functional event sequence diagram for the Coolant Channel Blockage Anomaly, identified CCB in the FESD, is shown in Figure 21. The entry condition for this FESD is loss of flow in one or more channels.

The first event is whether enough blockage occurs to starve the LPFTP or change the mixture ratio enough to cause the controller to change the oxidizer valve position, event CCB-CD-001. If the LPFTP receives insufficient flow then the engine must be shutdown or there will

be an LOV event, CCB-SD-001. If the blockage is insufficient to cause the LPFTP to fail then the next event to check is whether the blockage causes a crack in the liner, identified as CCB-DC-001. If no crack is caused then the flow path has been changed but there is no significant effect on the MCC operation and there is successful operation. If the blockage does cause a crack, then the question, CCB-HG-001, is if there is a crack on the hot gas wall. If there is a crack, a positive response to CCB-HG-001, then the sequence must either transfer to the coolant

The functional event sequence diagram for the Coolant Channel Cracking Anomaly, identified CCC in the FESD, is shown in Figure 22. The entry point for this FESD is a crack of any size within the land area of the Narloy liner. This is an important definition for the remainder of the FESD discussion. Cracks on the hot gas wall of the Narloy or in the Narloy-copper-nickel interface and nickel closeout are treated separately in

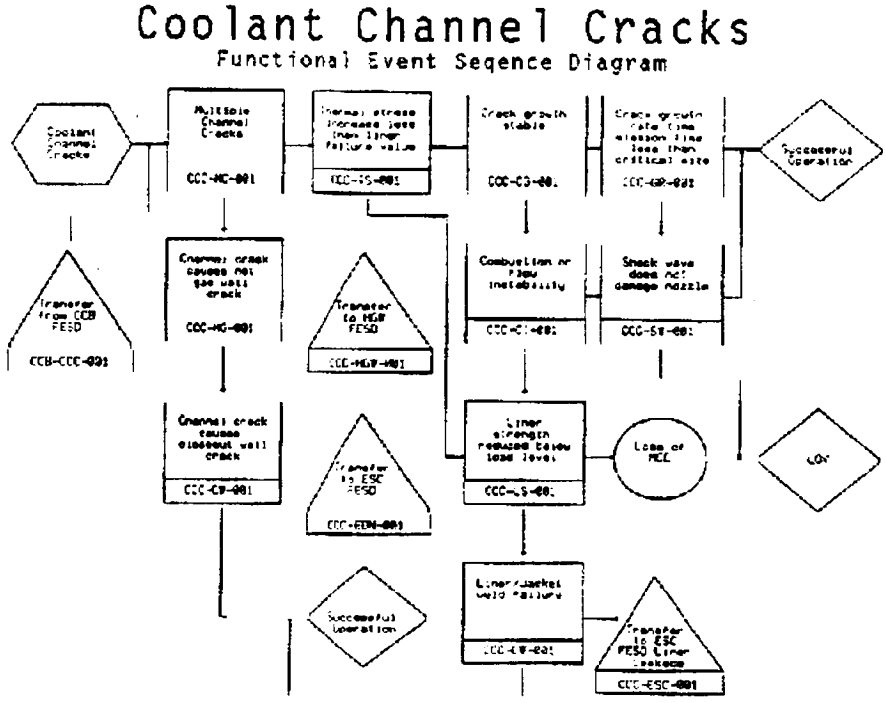


Figure 22. Coolant Channel Cracks FESD

channel crack, the EDNi closeout crack, or the hot gas wall crack FESD.

Coolant Channel Cracks Functional Event Sequence Diagram

this study. Thus, if the coolant channel crack occurs and it grows all the way through the land the net effect is to have turned two coolant channels into one coolant channel since a flow path between the channels has now been created. Because the fuel is undergoing a transition from a liquid to gaseous phase there is the potential for a mass flow rate reduction due to the com-

pressible nature of the fluid. Therefore, the heat transfer characteristics of this type of anomaly must be quantified through a separate FESD.

The first event that is examined is whether there are multiple cracks in the coolant channel land CCC-MC-001. If there are then the liner strength is examined to determine if it has fallen below the load level, CCC-LS-001. If it has then there is a loss of cooling to the MCC, MCC failure, and LOV. If the strength is not less than the load level then the crack growth is examined for stability. If the crack growth is dynamic it is possible to change the liner geometry due to bulging and cause a combustion and/or flow instability, this branch identified as CCC-CI-001. Such an instability could cause a shock wave that would damage the nozzle and cause an LOV. If a shock wave or flow instability is not caused then the effect of a dynamic crack on the overall liner strength must be examined. If the ripping of the multiple channel lands reduces the strength below the load level then there is a loss of the MCC and LOV.

Note that several branches of the CCC FESD converge to the point CCC-LS-001. This is because the phenomenological sequence after a no response to CCC-TS-001, CCC-CI-001, and CCC-SW-001 are all identical. If the liner strength remains above the load level then the effect of the dynamic crack on the liner-to-jacket weld must be examined. If the impact of the dynamic crack on this weld causes weld failure there will be leakage into the liner/jacket cavity. This leakage will transfer to a point in the EDNi FESD, just prior to ESC-BD-001. If the liner-to-jacket weld does not fail then there is no adverse effect of multiple coolant channel cracks on the MCC and there is successful operation.

If there are not multiple channel cracks, a no response to CCC-MC-001, then the next event examined is if the coolant channel crack transfers load to the hot gas wall causing a hot gas wall crack, CCC-HG-001. A yes response to this event causes a transfer into the HGW FESD. If not then the same question is posed for the closeout wall, CCC-CW-001. Again a positive response causes a transfer to the ESC FESD. A no response implies successful operation.

Flow Recirculation Inhibitor Functional Event Sequence Diagram

The functional event sequence diagram for the Flow Recirculation Inhibitor Anomaly, identified FRI in the FESD, is shown in Figure 23. It must be noted that all seal leakage events have been collapsed into this FESD. The other seal leakage locations are: pressure port seal; contracting seal at the MCC and powerhead interface; and the seal at the MCC and injector plate interface. The pressure port seal leads to events that are outside the scope of the MCC restrictions placed on this study. As discussed with MSFC staff at the August 23 and 24, 1993 meetings the powerhead seals are not actual seals. The contracting seal is not meant to contain gas but rather to provide a space for the contraction and expansion during cool-down and engine firing. The inter-propel-

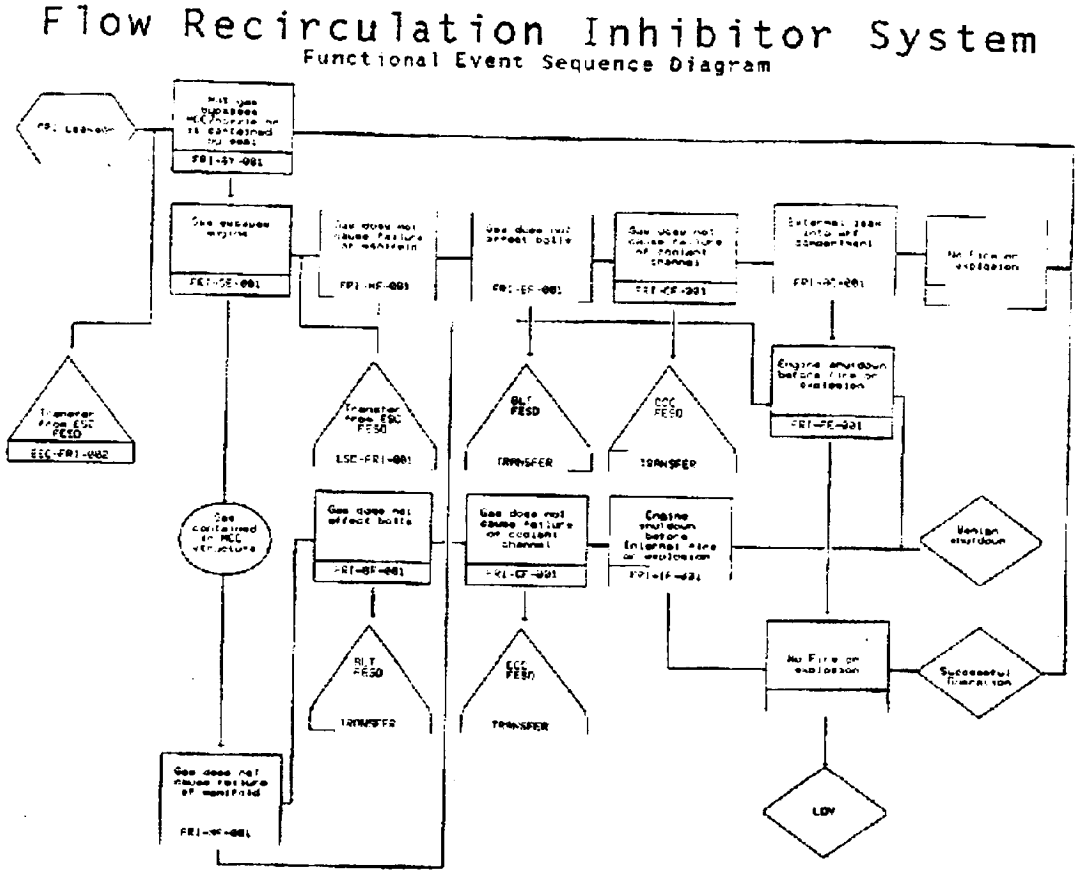


Figure 23. Flow Recirculation Inhibitor Anomaly FESD

lant face seal already has a leak path provided by the holes drilled in the plate. Therefore, any anomaly causing leakage will only act to cool the hot gas wall and will actually be beneficial. Thus, the only seal of concern is the G15 bellows seal. Since the FRI must fail before any G15 anomaly would have any effect on the MCC operation the FRI system leads to all seal leakage problems.

Given that the FRI has failed the first event to consider is whether the hot gas bypasses the G15 seal or whether it recirculates in the gap between the MCC and nozzle, event FRI-BY-001. If it does bypass the G15 seal then the engine is operating as designed and this is successful operation. If the gas does not bypass the G15 seal then the sequence may proceed by failing the G15 seal and allowing gas to escape, a positive response to FRI-GE-001, or the seal may contain the gas within the engine. Whether the gas is contained or not the next three events are identical in concept but their probability of occurrence is different. For example, if the gas is escaping the engine the force and temperature change on the manifold may cause its failure, event FRI-MF-001. If the gas is contained

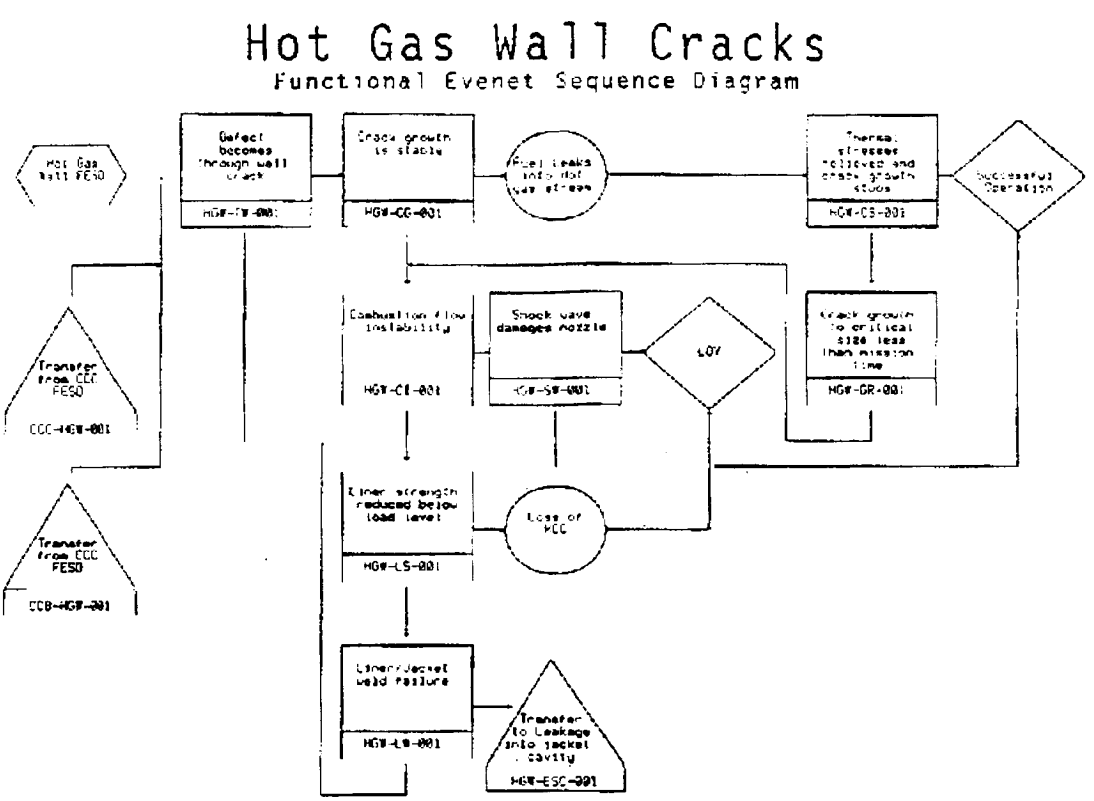


Figure 24. Hot Gas Wall Cracks FESD

within the engine then the manifold may still fail because of the change in the thermal stress from the FRI failure but the hot gas will not be in direct contact causing a lower probability of occurrence.

Hot Gas Wall Cracks Functional Event Sequence Diagram

The functional event sequence diagram for the Hot Gas Wall Cracks Anomaly, identified HGW in the FESD, is shown in Figure 24. The entry point for this FESD is any crack on the hot gas wall surface of the MCC. The first event, HGW-TW-001, is when the crack becomes a through-wall crack. If the crack is not a through-wall crack then there is successful operation. When the crack becomes a through-wall crack, it can undergo stable or unstable crack growth, represented by event HGW-CG-001. In the situation in which the crack growth is unstable or dynamic, a similar set of event sequences as in the coolant channel blockage and crack FESD's is considered. In this sequence the possibility of a combustion or flow instability, HGW-CI-001, is examined which if it does not occur then the possibility of the liner strength being reduced below the load level, HGW-LS-001, is considered. If the HGW-LS-001 event does occur then

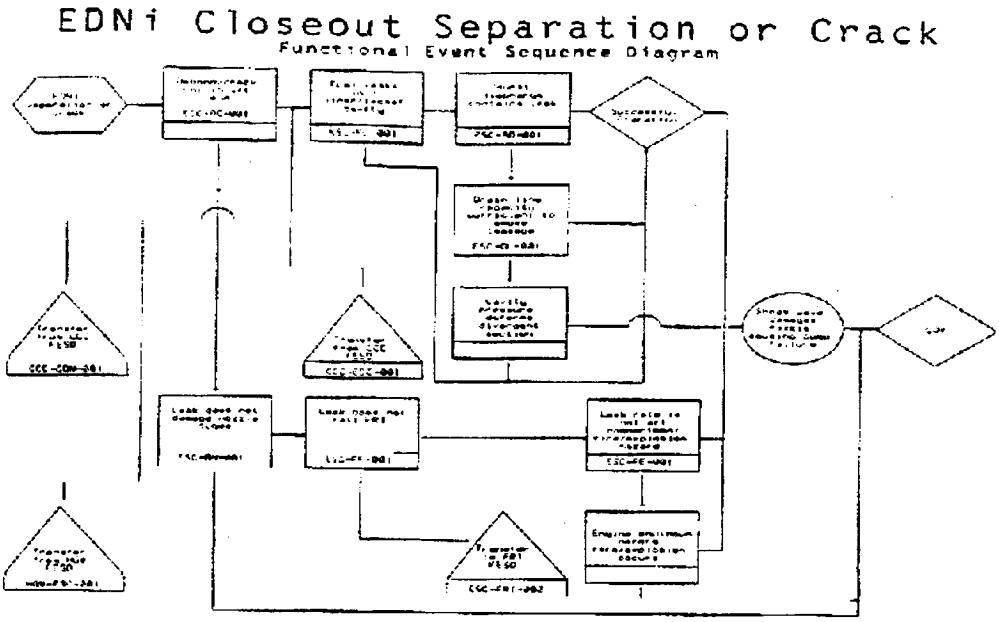


Figure 25. EDNi Closeout Separation/Crack FESD

there is a loss of the MCC and LOV. If not, then the effect of an unstable crack being stopped at the liner to jacket weld is examined by event HGW-LW-001. If the weld fails, then there is a transfer into the EDNi closeout separation or crack FESD via transfer HGW-ESC-001. If either the shock wave does not damage the nozzle or the liner to jacket weld does not fail, negative outputs from either event HGW-SW-001 or HGW-LW-001, then there is successful operation.

If the crack is growing stably, a yes to event HGW-CG-001, then the next event is fuel leaks through the crack to relieve the thermal strain and stop the crack growth, HGW-CS-001. If this occurs then there is successful operation. If it does not stop the crack growth then the event crack growth rate to critical size is less than mission time is examined, event HGW-GR-001. If this event occurs, there is successful operation, otherwise there is a loss of the MCC and subsequent LOV.

EDNi Closeout Separation/Crack Functional Event Sequence Diagram

The functional event sequence diagram for the EDNi Closeout Separation/Crack Anomaly, identified ESC in the FESD, is shown in Figure 25. The entry point for this FESD is any debond of the Narloy-copper-nickel interface, a crack within the shear zone of the interface in the Narloy, or a crack in the nickel material. The FESD for this event has been modified by the MSFC engineers to account for the fact that there can be a different path if the debond occurs

in the aft end of the liner. These changes are reflected in ?

Thus, the first event is the debond does not occur in the aft end of the liner, event ESC-AE-001. If this is fails, then the sequence of events is to check if the fuel jet does not cause a burn through of the nozzle, ESC-BN-001. If it does cause a burn through, a negative response to ESC-BN-001, then there is a loss of vehicle event. If no nozzle burn through occurs then the next event is the after EDNi leak does not fail the G15 bellows seal, ESC-FB-001. If it does, a no branch to this event, then a transfer into the ESC FESD is made. If it does not fail the bellows then the FRI system integrity is checked via event ESC-FF-001. This event is FRI system does not fail, which if true requires that the leak rate into the aft compartment be checked. If the leak rate does not pose a fire/explosion hazard, a positive output from event then there is successful operation.

Because of changes to the EDNi closeout FESD there are also changes that must reflect the new transfer points in the FRI FESD. These changes are shown in Figure 26.

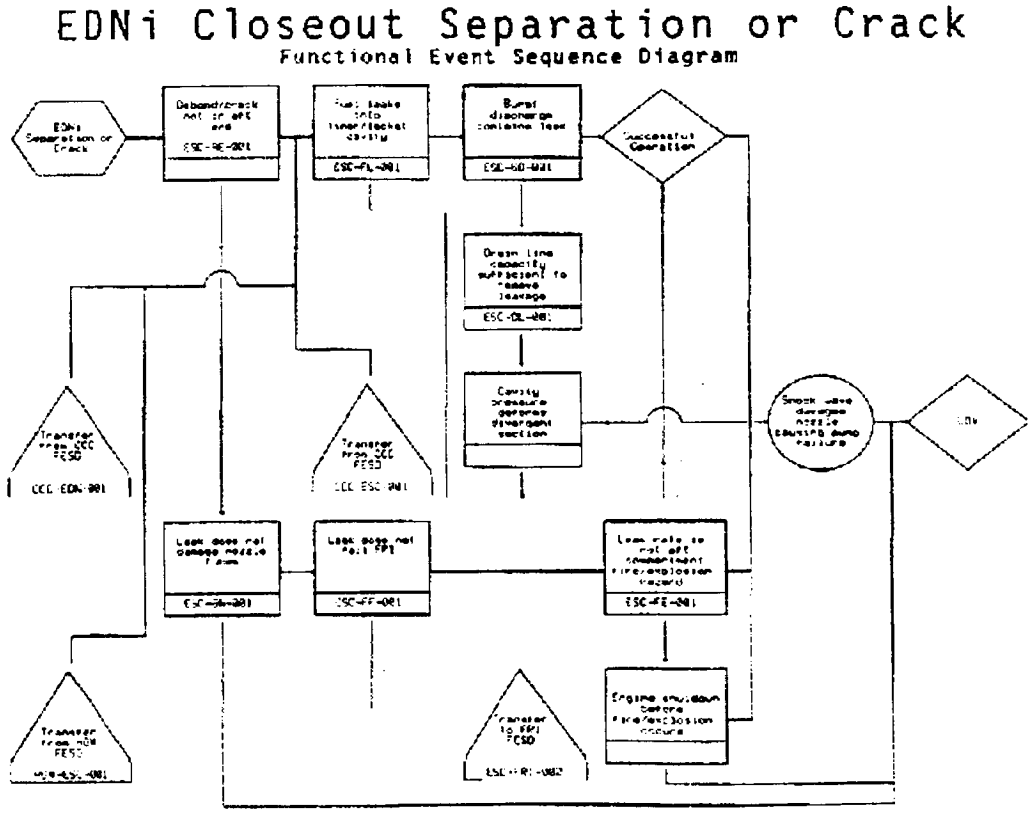
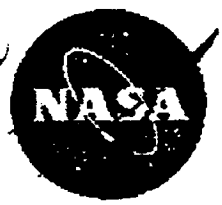


Figure 26. Updated EDNi Closeout Separation/Crack FESD

Summary

The FESD's that have been constructed by applying a structure to the logical sequence of events can now be cast into a form that is amenable to computer analysis. This form is the event tree format mentioned previously. Based on the FESD's just developed, the event trees can be constructed in a relatively easy manner. In order to quantify the event trees we first need to perform some data analysis to define the frequency with which different events occur or states exist. The following section gives the data quantification for the initiating events.



Event Tree Analysis:
Application To The MCC

Event Tree Event Frequency Evaluations

The FESD diagrams have been converted to an event tree format. Quantitatively, there is no essential difference between the event tree and the corresponding FESD. Qualitatively, the format is significantly different, and computationally, there are several computer programs which allow for easy calculation of the top event frequency given the pivotal event frequency.

The next step in the analysis must be the assignment of event tree probabilities to each pivotal event. In the cases where data exist to calculate these frequencies, reasonable estimates can be made. Unfortunately, there is very little data available to estimate the frequency of most pivotal events. This implies that expert opinion must be employed. In those cases in which expert opinion is used, the estimates are meant to be conservative.

The pivotal event frequencies for each event tree are given in Table XII. The frequencies are based on previous meetings with SAIC and MSFC engineers as well as data from the PRACA data base. Some general comments about each of the event trees are made in the following sections.

Event Tree Event Probabilities			
CCB	Mix Ratio OK	99.0%	CCB-CD-001
	No Cracks	5.0%	CCB-DC-001
	HGW OK	90.0%	CCB-HG-001
	CC Wall OK	90.0%	CCB-CC-001
	LPFTP OK	90.0%	CCB-LF-001
	Shutdown	0.0%	CCB-SD-001
CCC	Single Channel	10.0%	CCC-MC-001
	No HGW crack	10.0%	CCC-HG-001
	No ESC crack	90.0%	CCC-CW-001
	Thermal stress < Failure	99.0%	CCC-TS-001
	Stable crack	99.0%	CCC-CC-001
	Time > mission	99.9%	CCC-GR-001
	Flow stable	99.0%	CCC-CI-001
	Nozzle ok	95.0%	CCC-SW-001
	Liner strength < Load	10.0%	CCC-CS-001
	No liner/jacket weld fail	10.0%	CCC-LW-001
MWF	Crack Detectable	90.0%	MWF-CD-001
	Repair Effective	90.0%	MWF-RE-001
	Small Crack	10.0%	MWF-LC-001
PBF	Single Bolt Fails	99.0%	PBF-DB-001
	Preload OK	99.0%	PBF-PL-001
	No Ad Heat	99.0%	PBF-OV-001
HGW	Surface crack	5.0%	HGW-LW-001
	Thermal stress < Failure	99.0%	HG-GG-001
	Stable crack	99.0%	HGW-CS-001
	Time > mission	99.9%	HGW-GR-001
	Flow stable	90.0%	HGW-CI-001
	Nozzle ok	95.0%	HGW-SW-001
	Liner strength > Load	90.0%	HGW-LS-001
	No liner/jacket weld fail	0.0%	HGW-LW-001
FRI	Gas bypass	99.0%	FRI-BY-001
	Gas escapes engine	99.8%	FRI-GR-001
	Manifold OK	100.0%	FRI-MF-001
	Bolts OK	100.0%	FRI-BF-001
	Coolant channel OK	100.0%	FRI-CF-001
	No leak aft compt.	0.0%	FRI-AC-001
	Engine shutdown	0.0%	FRI-SD-001
	FS fires/explodes	0.0%	FRI-FE-001
ESC	Nozzle OK	99.0%	ESC-BH-001
	FRI OK	99.995%	ESC-FF-001
	Aft Compartment OK	0.0%	ESC-FE-001
	Engine Shutdown	0.0%	ESC-SD-001
ESC	No fuel in cavity	99.0%	ESC-FL-001
	Burst diaphragm OK	25.0%	ESC-BD-001
	Leak Drained	50.0%	ESC-DL-001
	No divergent section change	0.0%	ESC-DD-001

Table XII. Pivotal Event Frequencies

Coolant Channel Blockage Pivotal Event Frequencies

The pivotal events listed in Table XI for the Coolant Channel Blockage event tree are listed under the nomenclature CCB. It is assumed that the blockage of the coolant channel will have a negligible effect on the mixture ratio 99% of the time. However, if there is coolant channel

blockage, the probability of high thermal stresses inducing cracks is significant. Therefore, the event "no cracks" is assumed to occur only 5% of the time. Because we are interested only in the those cracks that are initiated by CCB, the hot gas wall (HGW) and coolant channel (CC) wall cracks are assumed to occur only 10% of the time in which there is blockage. It is important to point out this is *not* representative of the hot gas wall cracking frequency but rather is caused by the event of channel blockage either from deformation or contamination. A conservative frequency estimate in which the LPFTP is affected due to reduced H_2 flow of 10% is used. In reality it is expected that the amount of blockage of the coolant channel will be low enough that there will be no effect on the LPFTP with a much higher frequency, say 99.9% of the time. Finally, in a consistent manner throughout the entire quantification, the effect of engine shutdown is not accounted for in this study. This implies that the frequency of the ***loss of the MCC***, as opposed to the frequency of the ***loss of vehicle***, is being examined. The event tree is shown in Figure 27.

Coolant Channel Cracking Pivotal Event Frequencies

The coolant channel cracking event frequencies are similar to the CCB frequencies, with the exception of considerating stable and unstable crack growth. All events associated with the stable growth of cracks are assigned a 99% frequency of occurrence. That is, 1 in 100 cracks will grow unstably, will have a stable crack growth time less than the mission time, and so forth. Each of these pivotal events is listed as CCC. The event tree is shown in Figure 28.

Manifold Weld Anomaly Pivotal Event Frequencies

An anomaly of the manifold weld is relatively straightfoward. Either a crack exists or it does not. If it exists and is large then it can cause an anomaly. Of course, if it is large then it is also more easily detectable. Thus, the events MWF-CD-001 and MWF-LC-001 are *not* independent. If it is assumed that the crack in the manifold weld area has a small chance of being detected, then there is a corresponding increase in the likelihood that the crack is small. If a crack is detected, it is assumed that a repair is always attempted. However, it is further assumed that this repair is effective only 90% of the time. This repair rate is conservative and attempts to encompass the probability of introducing a flaw as well as an incomplete repair. The event tree is shown in Figure 29.

Bolt Anomaly Pivotal Event Frequencies

Recent evidence from MSFC tests has indicted that the single bolt anomaly sequence is unlikely to a cause significant likelihood of catastrophic engine failure. Therefore, pivotal events in this tree are assumed to be relatively high reliability occurring only 1 in 1,000 times. The event tree is shown in Figure 30.

Hot Gas Wall Pivotal Event Frequencies

The hot gas wall pivotal events have led to many discussions between MSFC and SAIC staff about what does and does not constitute a credible event. Therefore, at this time some discussion is warranted regarding test and flight histories and their relevance to risk analysis.

In many of the developmental and flight MCC's there have been many instances of cracking. These cracks have reached in size from "pin-

hole" cracks to cracks eight inches long. In every case to date, a crack has never been observed to grow beyond the MCC throat area. Because this has never been observed, the occurrence of a crack which extends beyond the throat is viewed as an incredible event by the MSFC staff. However, if the load needed to drive the crack through the throat area only occurs, on the average, once in every one hundred missions then there is a high probability that this event simply has not been observed yet.

To demonstrate this, let us make some conservative assumptions. First, assume that the entire MCC test and flight history is equivalent to 500 missions. Second, assume that in one half of these missions there is a crack is near the throat area. Third, assume that all of the missions have the same statistical load spectrum. Finally, assume that the load necessary to drive the crack through the throat area occurs at a probability of 1%. In this case the probability of the crack not extending beyond the throat area is 91.8%. There is still a 8.2% probability that the event simply has not been observed! If only in one fourth of the missions is the MCC cracked then there is a 28.5% probability that the event will not have been observed. While a substantial number of MCC's have been cracked, this is still less than a one-in-four mission probability.

Examined another way, if the frequency of cracked MCC's is less than one in seven missions, then there is *at least* a 50% probability that a crack growing beyond the throat area simply has not been observed. Of course, the data can also be used to help determine what the load level probability to grow a crack beyond the throat area.

For example, assume that the probability of the load level needed to drive a crack beyond the throat area is 10%. With all other assumptions being the same, the probability that a crack growing through the throat area simply not having been observed is 3.6×10^{-12}. If the incidence of MCC cracking is one in four missions, this probability is still 1.9×10^{-12}. Therefore, it is safe to assume that the frequency of this load is substantially less than 10%.

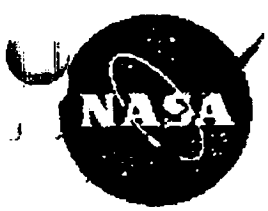
This is the logic used to establish the probabilities for the HGW crack event tree. The event tree is shown in Figure 31.

Flow Recirculation Inhibitor (FRI) System Pivotal Event Frequencies

The failure of the FRI system will not necessarily ensure that gas will recirculate in the MCC and nozzle interface. For this study, it is assumed that this occurs 10% of the time. Since the FRI has failed, there is a high probability that the exhaust gas will leave the normal gas stream, i.e. the gas will not recirculate into the normal exhaust. However, based on MSFC expertise, it is assumed that, for 99.99% of the time, the manifold, bolts, and coolant channel at the turnaround weld are not induced to fail by this gas path. The event tree is shown in Figure 32.

EDNi Closeout Separation/Crack

The EDNi closeout is divided into two event trees. The first, EAE, is for the case when the closeout fails in the aft end. This was a concern raised by MSFC structural engineers. The second event tree, ESC, follows the events more closely associated with the previous FMEA. The event trees are shown in Figure 33 and Figure 34.



Coolant Channel Blockage	LPFTP and Mix Ratio OK	No Cracks	HGW OK	CC Wall OK	LPFTP OK	Shutdown	Scenario Number	End State or Transfer
CCB-IE	CCB-CD-001	CCB-DC-001	CCB-HG-001	CCB-CC-001	CCB-LF-001	CCB-SD-001		
			na	na	na	na	1	OK
					na	na	2	X-ESC
							3	X-CCC
				na	na	na	4	X-HGW
			na	na			5	OK
							6	OK
							7	LOV
							8	X-ESC
							9	X-ESC
							10	LOV
							11	X-CCC
							12	X-CCC
							13	LOV
				na			14	X-HGW
							15	X-HGW
							16	LOV

Figure 27. Coolant Channel Blockage Event Tree

Coolant Channel Cracking	Single Channel	No HGW crack	No ESC crack	Thermal stress < Failure	Stable crack	Time > mission	Flow stable	Nozzle ok	Liner strength > Load	No liner/jacket weld fail	Scenario Number	End State or Transfer
CCC-IE	CCC-MC-001	CCC-HG-001	CCC-CW-001	CCC-TS-001	CCC-CG-001	CCC-GR-001	CCC-CI-001	CCC-SW-001	CCC-CS-001	CCC-LW-001		
											1	OK
											2	X-ESC
											3	X-HGW
											4	OK
											5	OK
											6	X-ESC
											7	LOV
											8	OK
											9	LOV
											10	OK
											11	X-ESC
											12	LOV
											13	OK
											14	LOV
											15	OK
											16	X-ESC
											17	LOV

Figure 28. Coolant Channel Cracking Event Tree

Manifold Weld Failure	Crack Detectable	Repair Efective	Small Crack	Scenario Number	End State or Transfer
MWF-IE	MWF-CD-001	MWF-RE-001	MWF-LC-001		
				1	OK
				2	OK
				3	LOV
		na		4	OK
				5	LOV

Figure 29. Manifold Weld Anomaly Event Tree

Bolt Failure PBF-IE	Single Bolt Fails PBF-BB-001	Preload OK PBF-PL-001	No Adjacent PBF-GV-001	Scenario Number	End State or Transfer
				1	OK
				2	LOV
			na	3	LOV
		na	na	4	LOV

Figure 30. Bolt Anomaly Event Tree

Hot Gas Wall Cracks	Surface crack	Thermal stress < Failure	Stable crack	Time > mission	Flow stable	Nozzle ok	Liner strength > Load	No liner/jacket weld fail	Scenario Number	End State or Transfer
HGW-IE	HGW-TW-001	HGW-GG-001	HGW-CS-001	HGW-GR-001	HGW-CI-00	HGW-SW-001	HGW-LS-001	HGW-LW-001		
		na	na	na	na	na	na	na	1	OK
				na	na	na	na	na	2	OK
					na	na	na	na	3	OK
						na			4	OK
									5	X-ESC
									6	LOV
							na	na	7	OK
							na	na	8	LOV
			na	na		na			9	OK
									10	X-ESC
									11	LOV
							na	na	12	OK
							na	na	13	LOV

Figure 31. Hot Gas Wall Crack Event Tree

Flow Recirculation Inhibitor Leakage FRI-IE	Gas bypasses nozzle interface FRI-BY-001	Gas escapes engine FRI-GE-001	Manifold OK FRI-MF-001	Bolts OK FRI-BF-001	Coolant channel OK FRI-CF-001	No leak in aft compartment FRI-AC-001	Engine shutdown FRI-SD-001	No fire/explosion FRI-FE-001	Scenario Number FRI	End State or Transfer
		na	na	na	na	na	na	na	1	OK
								na	2	OK
									3	OK
									4	LOV
									5	OK
									6	OK
									7	LOV
						na	na	na	8	X-CCC
					na	na	na	na	9	X-PBF
				na	na	na		na	10	OK
									11	OK
									12	LOV
						na		na	13	OK
									14	OK
									15	LOV
						na	na	na	16	X-CCC
					na	na	na	na	17	X-PBF
				na	na	na		na	18	OK
									19	OK
									20	LOV

Figure 32. Flow Recirculation System Event Tree

EDNi Crack Aft End EAE-IE	Nozzle OK ESC-BH-001	FRI OK ESC-FF-001	Aft Compartment OK OK ESC-FE-001	Engine Shutdown ESC-SD-001	Scenario Number	End State or Transfer
			na	na	1	OK
				na	2	X-FRI
					3	X-FRI
					4	LOV
		na	na	na	5	LOV

Figure 33. EDNi Crack: Aft End Event Tree

EDNi Crack: Not Aft End ESC-IE	No fuel in cavity ESC-FL-001	Burst diaphragm OK ESC-BD-001	Leak Drained ESC-DL-001	No divergent section change ESC-DD-001	Scenario Number	End State or Transfer
		na	na	na	1	OK
			na	na	2	OK
				na	3	LOV
					4	X-FRI
					5	LOV

Figure 34. EDNi Crack: Not in Aft End Event Tree

Event Tree Quantification

The data in Table XII was put into the event trees given in Figures 27 through 34. The calculations were made using Microsoft Excel®. The results are shown in Table XIII, and they are graphically depicted in Figure 35. The end result is that the loss of the MCC is estimated at approximately a 1 in 1,500 chance of occurrence per mission.

Loss of MCC Frequencies		
FRI LOMCC Frequency	1 in 21,710 missions	4.61E-05
Manifold weld LOMCC Frequency	1 in 3,959 missions	2.53E-04
Bolt failure LOMCC Frequency	1 in 9,426 missions	1.06E-04
Coolant Channel blockage LOMCC Frequency	1 in 256,654 missions	3.90E-06
Coolant Channel cracking LOMCC Frequency	1 in 89,128 missions	1.12E-05
Hot gas wall cracking LOMCC Frequency	1 in 18,898 missions	5.29E-05
EDNi debond (not aft) LOMCC Frequency	1 in 163,230 missions	6.13E-06
EDNi aft end debond LOMCC Frequency	1 in 5,899 missions	1.70E-04
TOTAL LOMCC FREQUENCY	1 in 1,542 missions	6.48E-04

Table XIII. Loss of MCC Frequencies

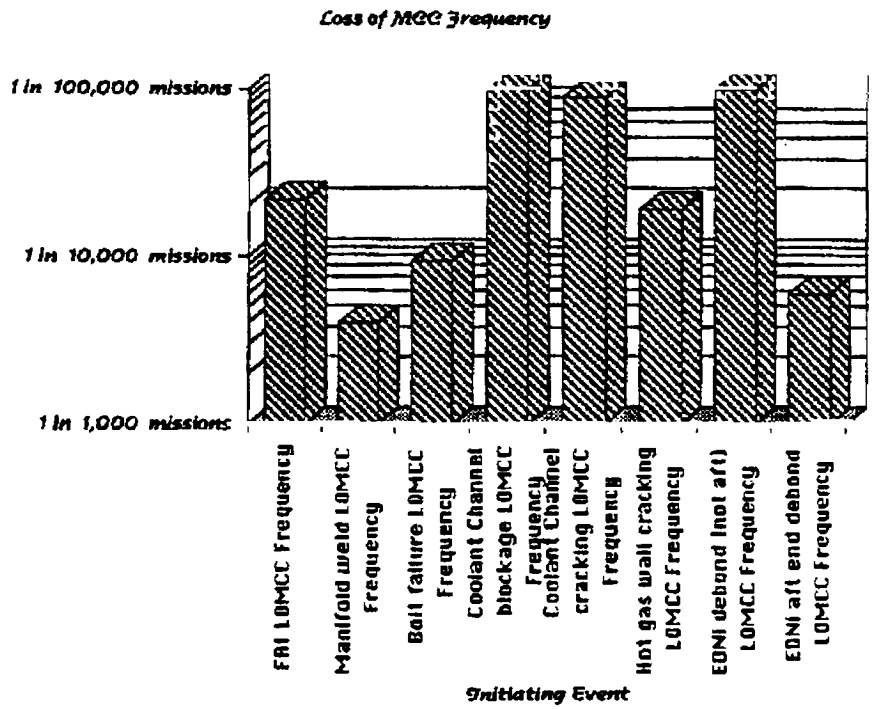


Figure 35. Loss of MCC Frequencies

Event Tree Uncertainty Analysis

Introduction

The uncertainty analyses of the MCC event trees and risk models requires that the frequency of each pivotal event be represented by a distribution. These distributions were developed, to the extent possible, based on data obtained from MSFC. Primarily, these data were based on the PRACA database. The assumptions and results of these analyses are contained in the chapter on initiating event frequencies. This chapter recalls the results of that data analysis and provides the output of an uncertainty analysis that was performed for the risk significant event trees.

Input Distributions

The event trees discussed in the previous sections were evaluated using a probabilistic methodology for uncertainty analysis. The distribution fitting for the data was determined to be *not* critical. Thus, if a lognormal or Weibull distribution is selected for use in the analyses, the effect of the selected distribution on the uncertainty results is minimal. The selected distributions are then one of three types:

Uniform. These are used for the values of constants. For example, the engine shutdown is assumed to never occur, i.e. no credit is given for controller logic since it is outside the scope of the MCC and thus this study. Since it occurs with 0% probability it is assigned a uniform distribution with both the lower and upper limits set to 0, i.e. a constant.

Normal. This is the standard normal density or bell shaped curve.

Weibull distribution. This is used to approximate data that exhibits "long tails"; that is, there is a significant probability of the pivotal event occurring with high frequency. It is important to re-emphasize at this point that there are two numbers of interest during an uncertainty evaluation: the frequency of an event occurring and the probability that the frequency selected is the

Variable	Distribution	Mean	5th Percentile	95th Percentile
CCC-IE	Weibull	1 in 1,500	1 in 6,085	1 in 856
CCC-MC-001	Normal	10.00%	4.86%	14.61%
CCC-TS-001	Normal	99.00%	98.33%	99.29%
CCC-SW-001	Normal	95.00%	90.00%	96.67%
CCC-CI-001	Normal	99.00%	98.33%	99.29%
CCC-CS-001	Normal	10.00%	4.86%	14.61%
CCC-CG-001	Normal	99.00%	98.33%	99.29%
CCC-GR-001	Normal	99.90%	99.89%	99.91%
FRI-IE	Weibull	1 in 191	1 in 772	1 in 109
FRI-SY-001	Normal	99.00%	98.33%	99.29%
FRI-GE-001	Normal	99.00%	98.33%	99.29%
FRI-MF-001	Normal	99.99%	99.99%	99.99%
FRI-SI-001	Normal	99.99%	99.99%	99.99%
FRI-CF-001	Normal	99.99%	99.99%	99.99%
FRI-AC-001	Uniform	0.00%	0.00%	0.00%
FRI-SD-001	Uniform	0.00%	0.00%	0.00%
FRI-IE-001	Uniform	0.00%	0.00%	0.00%
HGW-IE	Weibull	1 in 18	1 in 70	1 in 11
HGW-TW-001	Normal	5.00%	2.56%	7.32%
HGW-TS-001	Normal	99.00%	98.33%	99.29%
HGW-CS-001	Normal	99.00%	98.33%	99.29%
HGW-GR-001	Normal	99.90%	99.89%	99.91%
HGW-CI-001	Normal	90.00%	83.33%	92.86%
HGW-SW-001	Normal	95.00%	90.00%	96.67%
HGW-LS-001	Normal	90.00%	80.00%	93.33%
EAE-IE	Weibull	1 in 124	1 in 500	1 in 71
EAE-BH-001	Normal	99.00%	98.50%	99.33%
EAE-FF-001	Weibull	100.00%	99.99%	100.00%
EAE-FE-001	Uniform	0.00%	0.00%	0.00%
EAE-SD-001	Uniform	0.00%	0.00%	0.00%
ESC-IE	Weibull	1 in 706	1 in 2,662	1 in 403
ESC-FL-001	Normal	99.00%	98.75%	99.17%
ESC-BD-001	Normal	25.00%	11.76%	34.78%
ESC-DL-001	Normal	50.00%	28.57%	61.54%
ESC-DB-001	Normal	10.00%	2.76%	19.24%
MWF-IE	Weibull	1 in 308	1 in 1,247	1 in 176
MWF-CD-001	Normal	80.00%	67.50%	151.67%
MWF-RE-001	Normal	90.00%	83.33%	92.86%
MWF-CC-001	Normal	10.00%	6.35%	11.58%
PBF-IE	Weibull	1 in 272	1 in 1,101	1 in 156
PBF-BB-001	Normal	99.00%	98.33%	99.29%
PBF-PL-001	Normal	99.00%	98.33%	99.29%
PBF-SV-001	Normal	99.00%	98.33%	99.29%

Table XIV. Uncertainty Analysis Inputs For MCC Event Trees

"true" frequency. For example, from Table XIII the mean, or average, value of the initiating event frequency for the FRI is 1 in 191 missions. However, there is a wide spread in the data and, therefore, while we believe this to be an average value, we also believe that the value could be between 1 in 109 and 1 in 772 missions. This uncertainty in our degree of knowledge of the true FRI initiating event frequency is represented by the probability density function, in this case a Weibull distribution.

Table XIV gives the results of all of the distribution fits used in the uncertainty analyses.

Event Tree Uncertainty Analyses Results

The distributions shown in Table XIV were input to the uncertainty analysis code for evaluation. The result of the complete uncertainty analysis is given in Figure 36. In this Figure we see that the estimated loss of MCC frequency is between 1 in 3,000 missions and 1 in 800 missions. The 50% value (which is ***not*** the mean value) is near 1 in 1,500 missions. This does compare very favorably to the point estimate, indicating that the distributions are not causing a significant skewing effect and that many are contributing equally to the overall uncertainty. This is best seen by an examination of the individual event tree uncertainty analyses.

Figure 37 shows the results of the individual event tree uncertainty analyses. In this Figure the overall uncertainty analyses, shown in Figure 36, are also superimposed. The individual event tree uncertainty analyses indicate that the manifold weld anomaly, aft end debond of the liner, and the bolt anomaly make up a significant portion of the uncertainty. The most effective way to reduce the MCC risk is better inspections or repairs of the manifold weld.

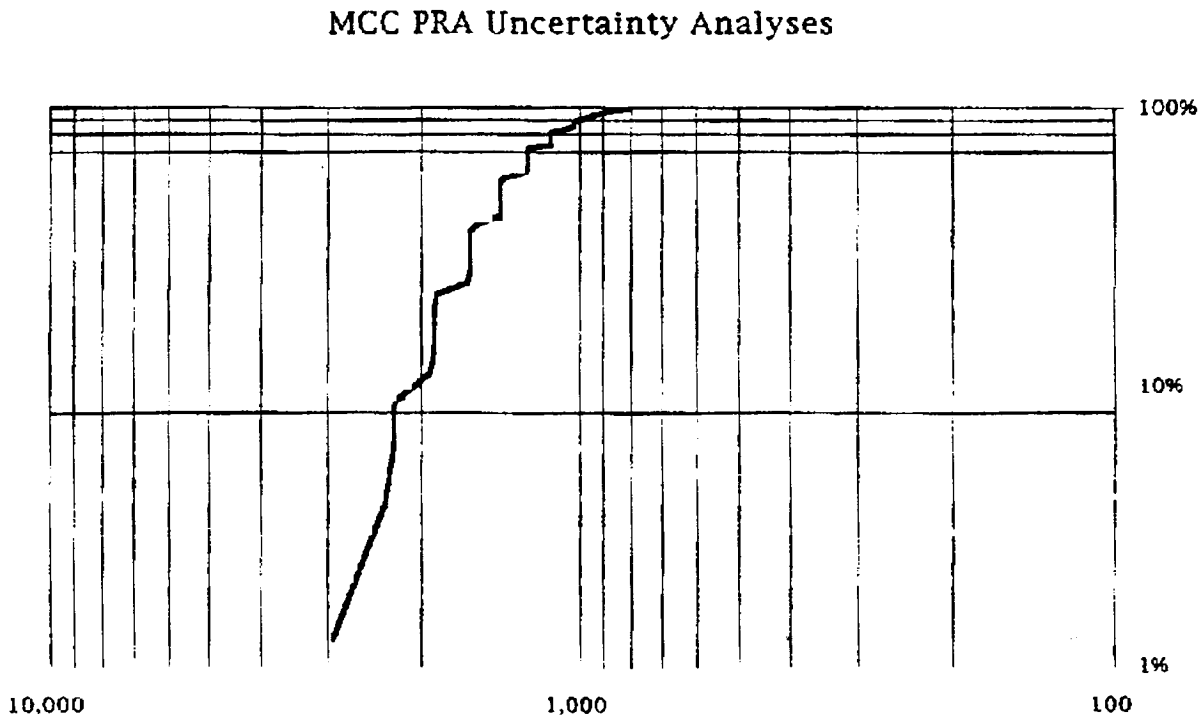


Figure 36. MCC Event Tree Uncertainty Analyses

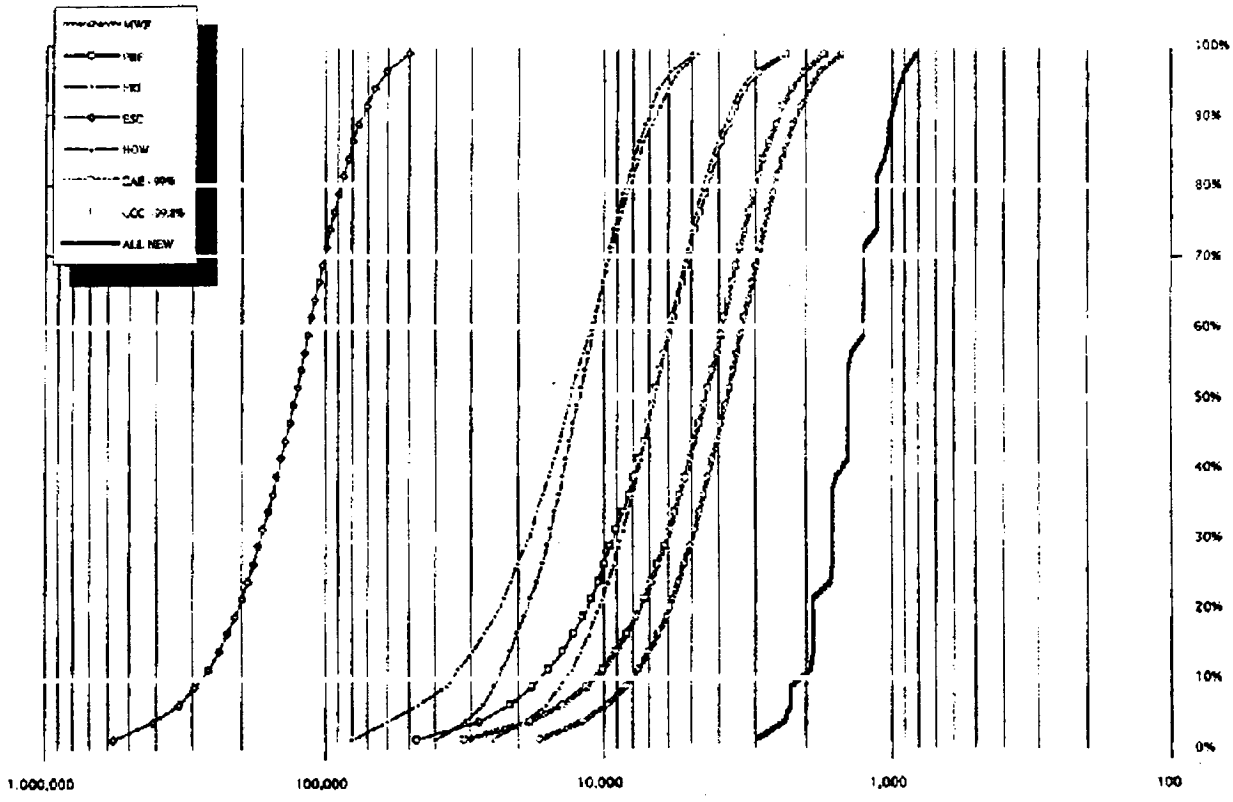


Figure 37. MCC Individual Event Tree Uncertainty Analyses

APPENDIX A

DATA BASE FOR ANOMALY AND FAULTS USED TO DEVELOP INITIATING EVENT AND EVENT FREQUENCIES

MSFC RPT #	Test/Operability	NCA PART #	FAIL DATE	PROBLEM TITLE
A09973	Development Test	2XRS009170-041	10/27/79	CLASS 3 LEAK IN MCC LINER
A05396	Field Postuse	8R00C9105-21	9/4/91	FOREIGN OBJECT DETECTED ON MAIN INJECTOR
A05526	Development Test	8R00C9105-21	1/26/91	MCC SURFACE FINISH UNACCEPTABLE
A05522	Development Test	8R00091C5-21	2/5/91	CONTAMINATION AT PORT CGIF
A05553	Development Test	8R00091C5-21	1/24/92	CRACK IN MCC ACOUSTIC CAVITY RING
A04585	In Flight	9RS009105-11	1/31/91	PART FAILED FLOW TEST DUE TO CRACK IN HOT WALL
A13274	Qualification or Certification Test	9RS009105-21	4/6/93	MCC BONDLINE DEBOND
A04608	Manufacturing	G13RS009105-431	7/23/90	DEBONDING OF NICKEL NARLOY
A05574	Development Test	G13RS009105-431	2/25/92	MCC COPPER LOSS
A05035	Development Test	G14RS009105-471	3/7/91	MCC BLANCHING AFTER ENLARGING COOLANT HOLES.
A05040	Development Test	G14RS009105-471	3/28/91	MCC AFT LIP EROSION
A05767	Manufacturing - Depot Maintenance	G16RS009105-541	12/22/92	SSME 0220 MCC BLANCHING
A10266	Development Test	G2RSC09170-921	1/3/82	SURFACE IRREGULARITIES ON HOT GAS WALL
A06906	Development Test	G5RS009170-381	4/22/81	SECONDARY EDCU PLATING PEALING ON MCC
A06973	Development Test	G5RS009170-381	4/25/81	HIGH PERFORMANCE BAFFLES NIBBLING
A07034	Development Test	G5RS009170-381	5/26/81	BLANCHED AREA BELOW ELEMENT 16
A08417	Development Test	G5RS009170-381	9/15/81	BLANCHED AREA WITH PINHOLES ON MCC WALL
A10340	Development Test	G6RS009170-391	10/13/81	ROUGH CHAMBER WALL HOT SPOTS
A11779	Development Test	G6RS009170-391	10/14/81	POSITIVE PRESSURE ON THE MCC LINER CAVITY
A12112	Development Test	G6RS009170-391	10/15/81	MCC DIAPHRAGM DAMAGED
A06618	Development Test	G6RS009170-391	11/6/81	SURFACE ROUGHNESS: HOT SPOTS
A06720	Development Test	G6RS009170-391	11/7/81	CHANNEL CRACK; ROUGHNESS
A08482	Development Test	G6RS009170-391	11/8/81	SURFACE ROUGHNESS, HOT SPOTS AND CHANNEL CRACKING
A09605	Development Test	G6RS009170-391	11/20/81	CHANNEL CRACK AT ELEM 85
A06599	Development Test	G7RS009105	7/29/82	MCC LINER EROSION
A02500	Development Test	GRS009105-441	7/22/87	CONTAMINATION ON F16 FLANGE
A06972	Development Test	GSRS009170-381	5/5/81	AREA BENEATH 2 ELEMENTS CRACKING
A10096	Development Test	MRS009176-001	9/25/79	BURST DIAPHRAGM RUPTURED
A10991	Development Test	MRS009176-001	3/13/80	RUPTURED BURST DIAPHRAGM
A12485	Development Test	R0011640-001	4/21/79	MCC BURST DIAPHRAGM RUPTURED
A03891	Qualification or Certification Test	R035518-1	5/4/89	OXIDIZER REPRESSURIZING LINE CONTAMINATION
A03519	Qualification or Certification Test	RS008861-015	9/16/88	GIS SEAL HAS MINOR DISCOLORATION - NON PROBLEM
A03868	Qualification or Certification Test	RS008861-015	4/20/89	DISCOLORED BELLOWS SEAL AT JOINT G1S-IFA-STS-29-E-2
A03864	Qualification or Certification Test	RS009105	3/19/89	MCC BONDLINE LEAK - IFA STS 29E1
A13670	Development Test	RS009105-0341	8/27/84	CRACKS & PINHOLES ON HOT GAS WALL
A13346	In Flight	RS009105-071	5/11/84	MCC LINER SURFACE FINISH OUT OF SPEC
A02501	Development Test	RS009105-1	9/12/87	LINER CRACKS AND PINHOLES
A02570	Development Test	RS009105-1	9/21/87	MCC LINER CRACKS
A11169	Acceptance Test	RS009105-301TSA	6/11/80	LEAKAGE ON HOT GAS WALL, DELAMINTN OF EDCU CONSTRAINT: NONE
A08061	Development Test	RS009105-341	2/12/83	SURFACE ROUGHNESS BLANCHING & THROAT CRACKS
A13823	In Flight	RS009105-341	8/8/84	CONTAMINATION/COOLANT CHANNELS
A14315	In Flight	RS009105-341	9/20/84	CRACK IN WELD JOINT
A00965	Development Test	RS009105-341	10/22/85	MISSING COPPER IN OUTLET NECK
A01849	Alert	RS009105-341	9/11/86	CRACKS AND LACK OF FUSION IN INLET WELDS, MCC (U/N 0007), INSPECTION
A07745	Acceptance Test	RS009105-351	12/7/82	SURFACE ROUGHNESS AND BLANCHING IN ROW 13
A08673	In Flight	RS009105-351	4/18/83	MCC CHANNEL CRACK
A08975	In Flight	RS009105-351	4/21/83	ROUGH SURFACE FINISH
A09570	In Flight	RS009105-351	7/25/83	WELD MISMATCHES IN JOINT 11, 13, 14 AND 16
A09695	In Flight	RS009105-351	9/12/83	MCC CHANNEL CRACKS

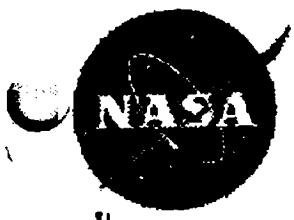
MSFC RPT #	Test/Operability	MCA PART #	FAIL DATE	PROBLEM TITLE
A09802	In Flight	RS009105-351	9/27/83	SURFACE ROUGHNESS EXCEEDS MAX ALLOWABLE
A09986	In Flight	RS009105-351	10/7/83	DIMENSIONAL DISCREPANCY
A10086	In Flight	RS009105-351	10/15/83	NI/NARLOY UNBOND
A13165	In Flight	RS009105-351	2/16/84	SURFACE ROUGHNESS EXCEEDS MAX LIMITATION
A14192	In Flight	RS009105-351	3/15/84	MCC AFT END DIMENSION OVERSIZE
A14316	Development Test	RS009105-351	3/24/84	CRACKS & PIN HOLES ON HOT GAS WALL
A14334	In Flight	RS009105-351	1/28/85	CONTAMINATION ON CHAMBER WALL
A14345	In Flight	RS009105-351	2/5/85	CHANNEL CRACKS
A14426	In Flight	RS009105-351	2/5/85	SURFACE ROUGHNESS EXCEEDS LIMIT
A14922	Development Test	RS009105-351	3/27/85	RUPTURE IN MCC OUTLET - ENGINE DESTROYED
A15141	In Flight	RS009105-351	4/23/85	SURFACE ROUGHNESS EXCEEDS LIMIT
A11424	In Flight	RS009105-351	7/3/85	CHANNEL CRACK DOWNSTREAM ELEMENT 42
A00481	Development Test	RS009105-351	8/3/85	CLASS III LEAK AT BURST-DIAPHRAGM
A00764	Alert	RS009105-351	10/19/85	LACK OF FUSION IN WELD 10
A00703	Development Test	RS009105-351	10/19/85	CRACK IN MCC LINER
A01001	Alert	RS009105-351	10/25/85	WELD 3, LACK OF FUSION; WELD1, SHARP FOLD
A01087	Development Test	RS009105-351	10/26/85	MISSING COPPER IN OUTLET NECK
A01305	Alert	RS009105-351	3/25/86	CRACKS/POROSITY IN ELBOW OUTLET WELDS 3 AND 5
A01704	Alert	RS009105-351	4/2/86	WELD THICKNESS FOR WELD 5 AND 22 NOT PER SPECIFICATION
A01885	Development Test	RS009105-351	10/16/86	1 INCH HIGH BULGE ON HOT GAS WALL, MCC, POST-TEST
A02260	Development Test	RS009105-351	10/16/86	PREMATURE CUTOFF; REDLINE ON MCC CAVITY PRESSURE, HOT FIRE
A12725	Manufacturing	RS009105-351TSA	8/14/80	MCC DAMAGED DURING PRESSURE TEST
A06388	Acceptance Test	RS009105-351TSA	2/3/81	HOT GAS WALL RUPTURE
A08607	Acceptance Test	RS009105-351TSA	4/1/83	MCC CONTAMINATION
A06389	Manufacturing	RS009105-371	6/23/82	PROOF PRESSURE FAILURE
A08680	Acceptance Test	RS009105-371	4/19/83	RAISED AREA ON THE HOT GAS WALL
A08701	Acceptance Test	RS009105-371	4/19/83	GOLD SPLATTER ON MCC WALL AND MAIN INJECTOR
A08973	Acceptance Test	RS009105-371	5/19/83	DIMENSIONAL DISCREPANCY AT CENTER THROAT
A08974	Acceptance Test	RS009105-371	5/23/83	INTERMITTENT MACHINE STEP AT CENTER LINE
A09734	Acceptance Test	RS009105-371	5/25/83	LEAK IN THE LINER CAVITY
A09160	Acceptance Test	RS009105-371	6/4/83	DIMENSION NOT PER DRAWING REQUIREMENTS
A09152	Acceptance Test	RS009105-371	6/6/83	LINER BLANCHING/MINUTE DAMAGE
A09194	Acceptance Test	RS009105-371	6/13/83	COOLANT INLET WELD MISMATCH
A09195	Acceptance Test	RS009105-371	6/20/83	HEAVY BLANCHING/MINOR SURFACE EROSION
A09281	Acceptance Test	RS009105-371	6/21/83	CAVITY PRESSURE RISE
A09643	Field Preuse	RS009105-371	8/11/83	WELD MISMATCHES AT COOLANT INLET LINE
A11308	In Flight	RS009105-371	1/3/84	MCC SURFACE ROUGHNESS
A11888	In Flight	RS009105-371	1/3/84	MCC SURFACE ROUGHNESS
A12192	In Flight	RS009105-371	1/3/84	MCC SURFACE ROUGHNESS ABOVE MAX ALLOWED
A13450	Acceptance Test	RS009105-371	5/22/84	CHANNEL CRACK
A13531	Qualification or Certification Test	RS009105-371	5/29/84	EDNI REINFORCEMENT DIM. REQ. NOT/SPEC.
A13765	In Flight	RS009105-371	9/17/84	SURFACE ROUGHNESS EXCEEDS MAX LIMIT
A14029	Development Test	RS009105-371	9/26/84	PIN HOLE & CRACK IN BLANCHED AREAS
A14078	Development Test	RS009105-371	10/8/84	CRACK & PINHOLES W/IN BLANCHED AREAS
A14700	Development Test	RS009105-371	11/5/84	DAMAGE ON NARLOY & NICKLE SURFACE ON MCC
A14258	Development Test	RS009105-371	11/13/84	PINHOLES IN BLANCHED AREAS
A14503	In Flight	RS009105-371	2/5/85	CHANNEL CRACKS & PIN HOLES IN MCC
A14520	In Flight	RS009105-371	2/5/85	SURFACE ROUGHNESS EXCEEDS LIMIT
A11412	In Flight	RS009105-371	5/16/85	SURFACE ROUGHNESS EXCEEDS MAX LIMIT
A15357	In Flight	RS009105-371	5/16/85	SURFACE ROUGHNESS EXCEEDS MAX LIMIT

MSFC RPT #	Test/Operability	NCA PART #	FAIL DATE	PROBLEM TITLE
A00203	In Flight	RS009105-371	7/6/85	CRACK IN MCC HOTWALL
A00152	Acceptance Test	RS009105-371	7/18/85	BLISTERS IN LINER
A00637	Alert	RS009105-371	10/15/85	MISSING COPPER & DEPRESSED AREA IN MCC NECK
A00767	Alert	RS009105-371	10/19/85	LACK OF FUSION IN WELDS 2 & 3
A00970	Alert	RS009105-371	10/25/85	LACK OF FUSION IN WELDS 3, 5 AND 11
A01399	Alert	RS009105-371	3/11/86	METALLIC CONTAMINATION FOUND IN OUTLET ELBOW
A01225	Alert	RS009105-371	3/16/86	COPPER EROSION/BLISTERS/DISCOLORATION ON SPLITTER WELD
A01243	Alert	RS009105-371	3/17/86	MISSING COPPER IN OUTLET NECK
A01255	Qualification or Certification Test	RS009105-371	3/18/86	WELD THICKNESS FOR WELDS 5 AND 22 NOT PER SPECIFICATION
A01263	Alert	RS009105-371	3/19/86	TWO PORES IN WELD 2; CRACK IN WELD 22
A01619	Alert	RS009105-371	3/27/86	POROSITY IN ELBOW OUTLET WELDS 5 AND 10
A03498	#N/A	RS009105-371	3/31/86	WELD THICKNESS FOR WELDS 5 AND 22 NOT PER SPECIFICATION
A01825	Manufacturing	RS009105-371	5/14/86	7600 +150/-000 PROOF TEST REVEALS LEAK. WELD 11
A14884	Development Test	RS009105-381	3/7/85	BLISTERS IN LINER
A15102	Acceptance Test	RS009105-381	4/18/85	CHANNEL CRACK IN BLANCHED AREA/BLISTERS
A00405	Development Test	RS009105-381	7/20/85	CHANNEL CRACKS IN MCC LINER
A01153	Acceptance Test	RS009105-401	12/20/85	3 PIMPLES WITH THROUGH CRACKS IN LINER
A01151	Alert	RS009105-401	1/9/86	CRACKS & POROSITY IN WELDS
A01775	Alert	RS009105-401	5/13/86	MINIMUM WALL THICKNESS FOR OUTLET ELBOW IS UNDERSIZE
A01830	In Flight	RS009105-401	5/22/86	METALLIC PARTICLE CONTAMINATION. JOINT F16
A02800	Development Test	RS009105-431	12/23/87	CHANNEL CRACKS FOUND ON LINER
A02975	Qualification or Certification Test	RS009105-431	4/22/88	LACK OF WELD PENETRATION - NON PROBLEM
A02982	Qualification or Certification Test	RS009105-431	4/26/88	MCC AFT ACTUATOR SUPPORT LUGS OUT OF TOLERANCE - NON PROBLEM
A03771	Qualification or Certification Test	RS009105-431	10/5/88	LEAK IN NOZZLE TUBE/JOINT AREA - STS-26-E-2
A04239	Qualification or Certification Test	RS009105-431	1/9/90	MCC GOUGE ENGINE 2028
A14310	Development Test	RS009105-441	2/4/85	SHEAR LIP DIAMETER OVERSIZE APPROXIMATELY .020 INCH
A02338	Development Test	RS009105-441	6/2/87	CRACKS IN VICINITY OF WELD JOINT 19
A04004	Qualification or Certification Test	RS009105-441	8/11/89	BLANCHED MCC LINER BELOW MAIN INJECTOR
A04204	Qualification or Certification Test	RS009105-441	1/9/90	MCC LINE DEBOND
A04578	Qualification or Certification Test	RS009105-441	4/12/90	MCC DENTS CAUSED BY HAMMERING TOOL
A04906		RS009105-441	10/12/90	MCC ROUGHNESS EXCEEDS 150 MICRO INCHES
A04957	Development Test	RS009105-441	1/30/91	MCC AFT LIP EROSION
A05185	Development Test	RS009105-441	5/1/91	GIMBAL BRG POP
A05186	Field Preuse	RS009105-441	6/5/91	CONTAMINATION
A05366	Development Test	RS009105-441	11/7/91	MCC LINEAR INDICATION
A05872	Development Test	RS009105-441	2/3/93	SSME 0218 MCC AFT LIP DYE PENT INDICATIONS
A03499	Development Test	RS009105-451	8/29/88	THREE CRACKS BELOW WELD 19
A04001	Qualification or Certification Test	RS009105-451	6/20/89	MCC LINER ELEVEN MAJOR CHANNEL CRACKS
A05184	Field Preuse	RS009105-451	4/28/91	CONTAMINATION
A02164	Development Test	RS009105-461	10/25/86	PIN HOLES THROUGH MCC HOT WALL. MCC ASSY. POST-TEST
A02253	Development Test	RS009105-461	11/26/86	SEVERAL CRACKED CHANNELS, MCC, POSTTEST
A02340	Development Test	RS009105-461	4/14/87	CRACKS AND HOLES IN MCC LINER
A02484	Development Test	RS009105-461	6/4/87	CRACKS IN MCC LINER
A05481	Development Test	RS009105-461	9/16/87	LEE JET UNSEATED AT CG2DP AND CG2EP
A02641	Qualification or Certification Test	RS009105-461	10/1/87	CONTAMINATION DOWN STREAM OF SPLITTER VANE
A02550	Development Test	RS009105-461	10/10/87	TWO CHANNEL CRACKS
A02719	Qualification or Certification Test	RS009105-461	11/19/87	CRACKS IN WELD 3 AND WELD 22
A02803	Development Test	RS009105-461	1/5/88	CHANNEL CRACKS FOUND ON LINER
A03453	Qualification or Certification Test	RS009105-461	5/4/88	MCC CRACKS ADJACENT TO WELD 19
A04453	Qualification or Certification Test	RS009105-461	2/28/90	MCC LINER DEPRESSIONS

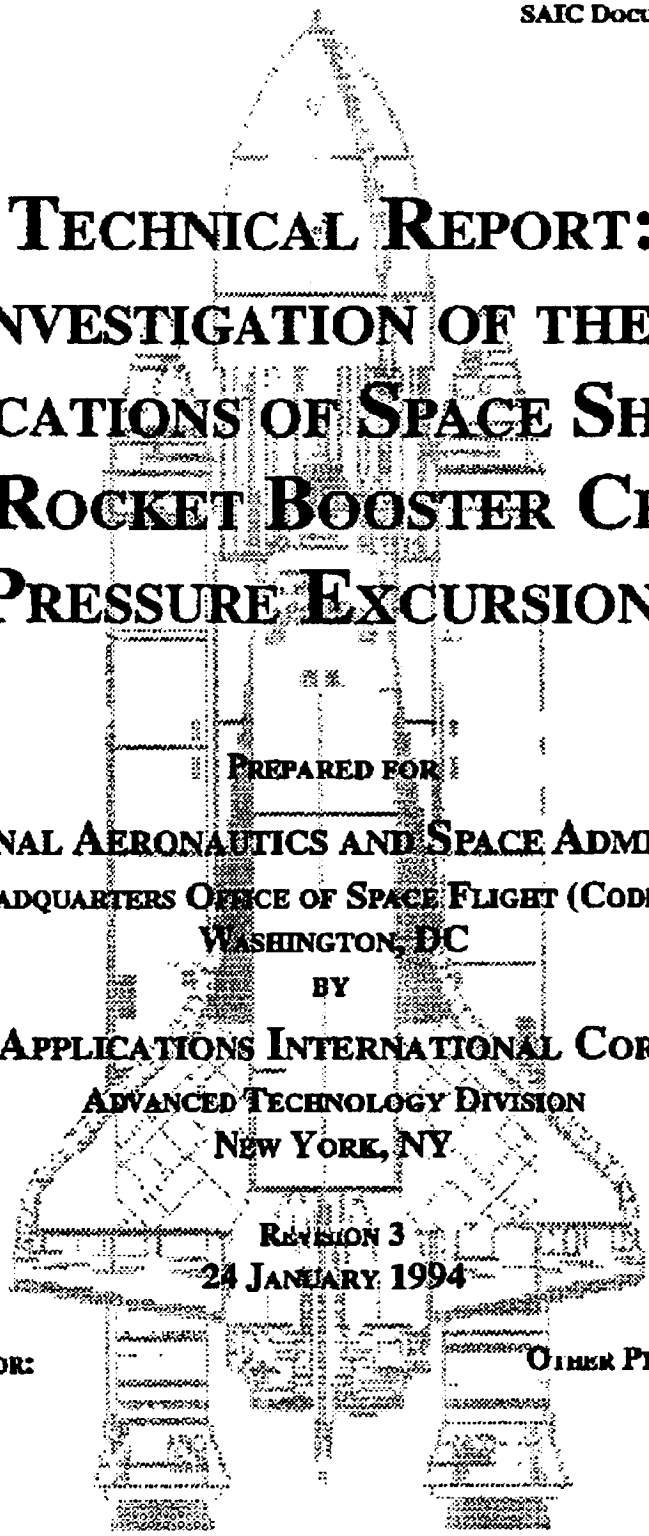
MSFC RPT #	Test/Operability	NCA PART #	FAIL DATE	PROBLEM TITLE
A05188	Field Preuse	RSC09105-461	6/5/91	CONTAMINATION
A05408	Field Postuse	RSC09105-461	9/12/91	MCC CONTAMINATION
A05477	In Flight	RSC09105-461	1/24/91	MCC PC CHANNEL B INDICATED HIGHER THAN CHANNEL A
A05544	Field Postuse	RS009105-461	1/22/92	BLANCHING
A05580	Field Preuse	RS009105-461	5/7/92	MCC BODY DAMAGE
A05667	Field Postuse	RS009105-461	7/31/92	MCC LINER CRACKS
A02847	Development Test	RS009105-471	2/25/88	CRACK IN WELD 1S - NON PROBLEM
A05256	Field Preuse	RS009105-501	3/13/91	CONTAMINATION
A04005	Qualification or Certification Test	RS009105-531	3/16/89	MCC PRESSURE SPIKE, BURST DIAPHRAGM RUPTURE
A04042	Qualification or Certification Test	RS009105-531	1/9/90	MCC GOUGE - ENGINE 2024
A04545	Qualification or Certification Test	RS009105-531	3/30/90	DEBONDED AREA NEAR END OF - MCC LINER
A04808	In Flight	RS009105-531	6/24/90	MCC HOT GAS WALL NICKS & DINGS
A04893	Development Test	RS009105-531	10/2/90	SSME 2032 JT F16 CONTAMINATION
A04964	Field Postuse	RS009105-531	12/13/90	MCC UNBOND
A05155	Development Test	RS009105-531	4/2/91	ACOUSTIC CAVITY BLOCKED
A05442	Development Test	RS009105-531	11/20/91	SSME 2032 MCC LINER SURFACE FINISH
A06565	Field Postuse	RS009105-531	7/31/92	MCC LINER LEAK
A05777	Qualification or Certification Test	RS009105-531	12/2/92	MCC PC SENSE LINE BLOCK
A07367	Manufacturing	RS009105-043SDI	11/2/82	WALL LINER RUPTURE
A09988	Development Test	RS009116-001	10/3/79	BLOWN OUT BURST DIAPHRAGM PETALS
A10424	Development Test	RS009116-001	1/12/80	SMALL RATE LEAKAGE FROM THE DIAPHRAGM
A11027	Development Test	RS009116-011	9/29/79	MCC BURST DIAPHRAGM RUPTURED
A09862	Development Test	RS009116-011	10/1/79	MCC BURST DIAPHRAGM RUPTURED
A10352	Development Test	RS009116-011	1/14/80	BLOWN BURST DIAPHRAGM
A10802	Development Test	RS009116-011	3/8/80	DIAPHRAGM BURST PETALS EXPANDED
A03471	Qualification or Certification Test	RS009122-1301	6/20/88	MCC INJECTOR CRACKED AND RETAINER BROKEN
A00638	Development Test	RS009168-351	10/7/85	LINER CRACK IN MCC ASSY
A09136	Development Test	RS009170-001	6/30/81	SLIGHT BULGING ON HOT GAS WALL
A10791	Development Test	RS009170-191	2/22/80	CRACKED MCC LINER
A07587	Development Test	RS009170-191	1/7/81	SMALL CRACK BELOW MAIN INJ
A14313	Acceptance Test	RS009170-291	5/25/79	DELAMINATION OR CRACK IN MAIN COMBUSTION CHAMBER
A09993	Development Test	RS009170-291	10/30/79	BLANCHED/CRACK ON INJECTOR FACEPLATE
A10391	Development Test	RS009170-291	1/23/80	PLUGGED PORT (JOINT G8.3 TAP CG2CP)
A10434	Development Test	RS009170-291	2/9/80	RUPTURED BURST DIAPHRAGM
A09987	Development Test	RS009170-311	6/25/79	BLISTERING AND MINOR SURFACE CRACKING
A09989	Development Test	RS009170-311	6/25/79	BLISTERING AND SURFACE CRACKING IN MCC
A10685	Development Test	RS009170-311	2/22/80	BULGES/RIPPLES IN WALL
A10004	Development Test	RS009170-321	10/13/79	SMALL CRACK IN THROAT AREA
A11570	Acceptance Test	RS009170-351	7/7/80	JOINT G8.1 CONTAMINATED CONSTRAINT: NONE
A12309	Development Test	RS009170-351	8/1/80	PORT CG2CP (LEE JET) DAMAGED OR MISDRILLED (C010)
A12724	Acceptance Test	RS009170-351	8/23/80	ORIFICE INSTALLED NOT PER PRINT - LEE JET
A12829	Development Test	RS009170-351	10/23/80	HOT SPOTS IN THROAT BELOW ELEMENTS
A06218	In Flight	RS009170-351	4/5/82	MCC ACOUSTIC CAVITY CONTAMINATION
A09314	In Flight	RS009170-351	7/8/83	MCC THROAT CENTERLINE CRACK
A11695	Development Test	RS009170-371	7/23/80	ACOUSTIC CAVITY ERODED
A12848	Development Test	RS009170-391	10/25/80	HORZ CRACK ABOVE MCC THROAT
A12890	Development Test	RS009170-391	11/13/80	CRACKS ON MCC LINER
A06341	Development Test	RS009170-391	1/19/81	EXPANDER PIN & LEE JET BODY OUT OF TOLERANCE
A10351	Development Test	RS009170-391	1/19/81	CONTAMINATION EXTRUDING OUT OF ORIFICE
A06570	Development Test	RS009170-391	2/24/81	OVERSIZED LEE JET ORIFICE INSERT

IMSFC RPT #	Test/Operability	NCA PART #	FAIL DATE	PROBLEM TITLE
A06688	Field Preuse	RS009170-391	3/2/81	LOCALIZED ROUGH REGIONS IN THE LINER
A06736	Development Test	RS009170-391	3/18/81	OVERHEATING IN THE UPPER CONVERGENT ZONE
A06305	Development Test	RS009170-391	5/29/81	BLANCHED AREA DOWNSTREAM POST 19 ROW 13
A06960	Development Test	RS009170-391	6/17/81	LEAK BETWEEN TUBES 870-900 AND JOINT G-15
A10335	Development Test	RS009170-391	6/17/81	HOT SPOT WITH ROUGH FINISH IN ELEM 2
A06419	In Flight	RS009170-391	7/23/82	ROUGH SURFACE FINISH
A06433	In Flight	RS009170-391	7/23/82	ROUGH SURFACE FINISH
A06478	In Flight	RS009170-391	7/23/82	ROUGH SURFACE AREA
A07392	Development Test	RS009170-391	11/7/82	STRUT ASSY LUG CRACKS
A07954	Development Test	RS009170-391	2/4/83	BLANCHING AT THROAT AREA
A08268	In Flight	RS009170-391	3/3/83	MCC CONTAMINATION
A08585	In Flight	RS009170-391	4/6/83	MICROCRACKS AT WELD JOINTS
A08663	In Flight	RS009170-391	4/6/83	MICROCRACKS ON WELD JOINTS
A08664	In Flight	RS009170-391	4/8/83	ELBOW WALL THICKNESS UNDERSIZE
A08667	In Flight	RS009170-391	4/8/83	INTERNAL CRACK ON ELBOW (WELD JT11
A08821	In Flight	RS009170-391	4/20/83	MCC CONTAMINATION
A08971	In Flight	RS009170-391	5/19/83	CRACK ON WELD S3 AND S5
A14314	In Flight	RS009170-391	9/14/84	SURFACE ROUGHENSS EXCEEDS MAX LIMIT
A07937	Development Test	RS009170-391TSA	2/11/83	MCC CONTAMINATION
A11426	Development Test	RS009170-401	6/27/80	ROUGH LINER SURFACE/GOUGE & RAISED SURFACE
A06578	Development Test	RS009170-401	2/4/81	HOLE IN THE RAISED METAL TOWARD EXIT MANIFOLD
A06626	Development Test	RS009170-401	6/20/81	BLANCHING/BLISTERING ON MAIN COMBUSTION CHAMBER
A06023	Development Test	RS009170-401	1/4/82	ACOUSTIC CAVITY EROSION
A06052	Development Test	RS009170-401	3/1/82	HOLES/CRACKS ON THROAT AREA
A06135	Development Test	RS009170-401	3/23/82	BLANCHED/CRACK CHAMBER WALL
A06303	Development Test	RS009170-401	5/25/82	ROUGH SURFACE/FINISH; BLANCHED AREAS
A06366	Development Test	RS009170-401	5/29/82	ROUGH SURFACE FINISH; BLANCH AREAS
A06367	Development Test	RS009170-401	6/6/82	CRACK PROPAGATION
A06369	Development Test	RS009170-401	6/6/82	BLANCHING AND ROUGH SURFACE AREAS
A06342	Development Test	RS009170-401	6/15/82	BLANCHING/ROUGH SURFACE FINISH
A06370	Development Test	RS009170-401	6/22/82	CRACK BETWEEN ELEMENTS
A06418	Development Test	RS009170-401	7/22/82	BLANCHING/ROUGH SURFACE; CHANNEL CRACKING
A06522	Development Test	RS009170-401	7/27/82	CHANNEL CRACKS
A06669	Acceptance Test	RS009170-401	8/27/82	SPLIT RING DIMENSIONS NOT PER PRINT
A06586	Development Test	RS009170-401	8/27/82	CRACK AT ELEMENT 72-73
A06730	Acceptance Test	RS009170-401	8/28/82	DIMENSIONS NOT PER PRINT
A06839	Acceptance Test	RS009170-401	9/10/82	RUPTURED BURST DIAPHRAGM
A06846	Acceptance Test	RS009170-401	9/18/82	BORE MISALIGNMENT
A06953	Acceptance Test	RS009170-401	9/23/82	LEE JET EXPANDER PIN OUT OF POSITION
A07115	Acceptance Test	RS009170-401	9/25/82	SURFACE EROSION, ROUGHNESS AND BLANCHING
A07129	Acceptance Test	RS009170-401	9/28/82	BLOCKED COOLANT CHANNEL
A07169	Acceptance Test	RS009170-401	10/4/82	SURFACE ROUGHNESS, BLANCHING AND CRACKS
A07165	Acceptance Test	RS009170-401	10/8/82	MCC THROAT CRACK
A07170	Acceptance Test	RS009170-401	10/9/82	SURFACE ROUGHNESS/BLANCHING
A07354	Acceptance Test	RS009170-401	10/21/82	MINOR CHAMBER LINER EROSION
A08052	Development Test	RS009170-401	11/9/82	CRACK PROPAGATED
A07748	Development Test	RS009170-401	1/14/83	MCC CONTAMINATION
A07771	Acceptance Test	RS009170-401	1/18/83	OUTLET FLANGE COPPER DELAMINATION
A08289	Field Preuse	RS009170-401	3/28/83	LEAK/THERMAL CRACK IN THE HOT GAS WALL
A08794	In Flight	RS009170-401	4/19/83	MCC HOT GAS WALL CRACK

MSFC RPT #	Test/Operability	NCA PART #	FAIL DATE	PROBLEM TITLE
A08951	In Flight	RS009170-401	4/20/83	MCC SURFACE ROUGHNESS
A08968	In Flight	RS009170-401	5/5/83	SURFACE FLAWS ON WELDS 5 AND 22
A09736	In Flight	RS009170-401	7/8/83	MCC THROAT CENTERLINE CRACK
A09692	Development Test	RS009170-401	7/25/83	BLANCHING/SURFACE ROUGHNESS
A09693	In Flight	RS009170-401	7/25/83	WELD MISMATCHES IN JOINT 11,13,14 & 16
A09683	Development Test	RS009170-401	8/30/83	ROUGHNESS/BLANCHING SURFACE
A09685	Acceptance Test	RS009170-401	9/2/83	MCC LINER CRACK
A09684	In Flight	RS009170-401	9/12/83	PIN HOLES AT MCC CHANNEL
A09723	In Flight	RS009170-401	9/12/83	MCC CHANNEL CRACKS
A09697	In Flight	RS009170-401	9/22/83	SURFACE ROUGHNESS EXCEEDS MAX ALLOWABLE
A12249	Development Test	RS009170-401	1/27/84	MCC CHANNEL CRACKS
A13093	In Flight	RS009170-401	2/13/84	MCC SURFACE ROUGHNESS EXCEEDS MAX LIM
A14704	In Flight	RS009170-401	2/5/85	SURFACE ROUGHNESS EXCEEDS LIMIT
A15210	In Flight	RS009170-401	4/23/85	SURFACE ROUGHNESS EXCEEDS LIMIT
A00200	In Flight	RS009170-401	7/3/85	PINHOLES; ADJ. TO ELEMENTS 68 & 66
A00645	Alert	RS009170-401	10/16/85	MISSING COPPER IN OUTLET NECK
A00916	Alert	RS009170-401	10/19/85	WELD 22, LACK OF FUSION; WELD 6 CONCAVITY
A07866	Field Preuse	RS009170-401 TSA-1	11/29/83	LEAK IN MCC TURBINE DRIVE SUPPLY MANIFOLD
A09277	Development Test	RS009170-401TSA	6/22/83	WELD MISMATCHES AT COOLANT INLET LINE
A09353	In Flight	RS009170-401TSA	7/15/83	WELD MISMATCH AT MCC INLET WELD 11
A06244	Development Test	RS009170-901	5/11/82	HEAVY BLANCHED AREA AND EROSION BELOW ELEMENT 8
A11093	Development Test	RS009170-921	3/24/80	SEVERAL ROUGH AREAS/CRACKS IN THE MCC
A12432	Qualification or Certification Test	RS009170-921	8/5/80	RETAINER RING NOT PROPERLY INSTALLED
A12726	Qualification or Certification Test	RS009170-921	8/15/80	LEE JET SNAP RING & WASHER MISSING
A07328	Qualification or Certification Test	RS009170-921	12/6/80	CRACK AND PIN HOLES IN NARLOY LINER
A10007	Development Test	RS009170-931	8/1/79	MCC EROSION AND CRACK
A07473	Qualification or Certification Test	RS009170-931	12/6/80	CRACKS IN NARLOY LINER
A09994	Development Test	RS009176-001	12/27/79	EXPENDED MCC BURST DISC PETALS
A13010	Development Test	RS009176-001	3/14/80	RUPTURED BURST DIAPHRAGM
A06368	Development Test	RS009176-001	3/27/82	BURST DIAPHRAGM LEAKING
A09137	Acceptance Test	RS009176-001	5/27/83	BURST DIAPHRAGM EXCESSIVE LEAKAGE
A09694	Development Test	RS009176-001	9/17/83	BURST DIAPHRAGM PRESSURE LOSS
A10901	Development Test	RS009176-001	10/19/83	BURST DIAPHRAGM LEAKAGE
A11029	Development Test	RS009176-001	11/10/83	BURST DIAPHRAGM LEAK
A13615	Development Test	RS009176-001	7/23/84	BURST DIAPHRAGM LEAK
A00733	Development Test	RS009176-001	10/18/85	BURST-DIAPHRAGM LEAKS
A11041	Development Test	RS009176-011	3/15/80	BLOWING LEAK IN THE RTV/RUPTURED DIAPHRAGM
A11158	Development Test	RS009190-353	4/2/80	VOID IN THE MCC PARENT METAL
A02029	Development Test	RS009211-003	10/4/86	BURST DIAPHRAGM LEAKS, MCC, POST-TEST



CONTINUATION OF SPACE SHUTTLE
PROBABILISTIC RISK ASSESSMENT, TASK 1
SAIC DOCUMENT NO. SAIC NY94-01-10



TECHNICAL REPORT: AN INVESTIGATION OF THE RISK IMPLICATIONS OF SPACE SHUTTLE SOLID ROCKET BOOSTER CHAMBER PRESSURE EXCURSIONS

PREPARED FOR

US NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
HEADQUARTERS OFFICE OF SPACE FLIGHT (CODE M)
WASHINGTON, DC

BY

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
ADVANCED TECHNOLOGY DIVISION
NEW YORK, NY

REVISION 3
24 JANUARY 1994

PRINCIPAL INVESTIGATOR:
JOSEPH R. FRAGOLA

OTHER PRINCIPAL CONTRIBUTORS:
MICHAEL V. FRANK*
JAMES J. KARNS
GASPARE MAGGIO
RICHARD H. MCFADDEN

* SAFETY FACTOR ASSOCIATES, INC.
ENCINITAS, CA

C 3

SAIC An Employee-Owned Company
Science Applications International Corporation

CONTINUATION OF SPACE SHUTTLE PROBABILISTIC RISK ASSESSMENT, TASK 1 -

TECHNICAL REPORT:
AN INVESTIGATION OF THE RISK IMPLICATIONS OF SPACE SHUTTLE SOLID ROCKET BOOSTER CHAMBER PRESSURE EXCURSIONS

1.0. INTRODUCTION AND BACKGROUND.

This document is a technical report on work by the Advanced Technology Division of Science Applications International Corporation (SAIC), New York, NY and SAIC's subcontractor Safety Factor Associates, Encinitas, CA to support an investigation of the risk implications of pressure excursions observed on Space Shuttle Solid Rocket Boosters. The SRB Pressure Excursion Assessment described herein is Task 1 of the continuation of the Space Shuttle Probabilistic Risk Assessment (PRA) program sponsored by the Headquarters Office of Space Flight (Code M) of the US National Aeronautics and Space Administration.

1.1. Background.

Post-flight analysis of the telemetry data on solid rocket booster internal pressure from Space Shuttle Mission STS-54 in January 1993 revealed an apparent pressure excursion of approximately 13 psi* peak magnitude above nominal pressure and four seconds total duration on the "B" booster, beginning at 67 seconds after SRB ignition. While slight pressure variations are a normal feature of the solid-fuel-rocket burn process, pressure excursions in solid-fuel rocket motors translate to thrust excursions, and therefore can impose a variety of hazards on the Shuttle vehicle if they exceed a safe magnitude. Since the pressure transients appeared to be increasing flight-to-flight in size, frequency, and variability, NASA became concerned about their potential flight safety implications, and initiated a series of investigations of their cause(s) and effects on the Shuttle.

Analysis of chamber pressure data from previous firings of the High-Performance Motor (HPM) SRB and the post-*Challenger*-accident Redesigned Solid Rocket Booster (RSRB) revealed that similar, although smaller, pressure excursions had occurred fairly frequently in both flight and ground-test motors. A statistical analysis of this experience led NASA to conclude that the pressure transient was well within the envelope of the experience base of earlier flights, and that therefore the next scheduled mission (STS-55) would be safe to fly. While STS-55 did in fact fly successfully, its "A" booster experienced a 13 psi* pressure excursion at approximately 72 seconds. This repetition added urgency to the need to understand and, if necessary, to find a way to mitigate the pressure transient phenomenon.

A number of candidate mechanisms for generating pressure transients have been postulated and evaluated; attempts have been made to establish upper bounds on the magnitude of the associated thrust excursions through a combination of statistical, analytical, and empirical methods; ground tests of SRBs with special instrumentation for the pressure transient investigation have been conducted; and increasingly refined analyses have been performed to assess the effects of the upper-bound thrust on structural stress margins and vehicle dynamics. The study described in this report continues this work by bringing a probabilistic risk assessment perspective to the SRB pressure excursion investigation.

Note: these were the pressure observations initially reported, based on a 2-per-second sampling rate. 12.5-per-second data that became available later showed peak excursions up to 15 psi.

1.2. Objectives.

The general objectives of the SRB Pressure Excursion Assessment were to support the independent internal review of the SRB pressure excursion phenomenon chartered by the NASA Administrator by providing insights into the risk implications of the pressure excursion situation, to prepare information on SRB risks that will be needed to support the more-comprehensive Space Shuttle PRA that is now under way, and to demonstrate the benefits of probabilistic-risk-based thinking processes to the civil space enterprise.

2.0. Discussion of Project Subtasks.

2.1. Subtask 1. Information Review and Risk Framework Development.

In Subtask 1 the SAIC-Safety Factor Associates (SFA) team obtained and reviewed the information furnished by the Shuttle program to the NASA independent review team that met at Marshall Space Flight Center during the week of 3 January 1994. In brief summary, this data set contained briefing materials from pre- and post-flight reviews of the STS-55, STS-57, and STS-58 missions; information on the TEM-10 and TEM-11 ground tests; briefing materials and responses to questions prepared for both the independent internal review requested by the Administrator and the external (Paget committee) review; and a variety of background information. Together with the program's answers to clarifying questions, this information gave the SAIC-SFA team a reasonably complete and detailed understanding of the process and results of the SRB pressure excursion investigation.

The information the team reviewed does not — and is not intended to — deal with the pressure excursion phenomenon as one of many potential contributors to total Shuttle accident risk. NASA and its contractors quite properly focused on the causes and effects of the pressure transient phenomenon rather than its top-level risk implications. However, understanding the relative contributions of potential accident initiators to total risk is essential to making sound decisions concerning the allocation of scarce resources among candidate risk-reduction approaches. This is one of the key reasons for performing a PRA on the Shuttle.

The SAIC-SFA team began the process of placing the SRB pressure excursion data within a PRA risk scenario structure by developing a preliminary Master Logic Diagram for catastrophic Shuttle accidents during the mission phase in question. A Master Logic Diagram (MLD) is a specialized logic tree that identifies all of the credible accident initiating events that lead to the "top event," but addresses neither pivotal events that can alter the progress of cause-effect sequences for better or worse, nor interactions among initiators and event sequences, nor the probabilities of the initiating events. (These items are dealt with in later stages of the analysis). The MLD is the first step in constructing accident sequences or scenarios that can then be analyzed to obtain quantitative information on the total risk and the relative contributions of risk factors.

Appendix 1 contains the top-level MLD for the boost phase of Shuttle ascent, showing the role of SRB pressure and thrust transients as potential initiators of Loss of Vehicle. As the reader will note, these are the only initiators that are called out specifically on this preliminary MLD; the other potential initiators are left undeveloped (as denoted by the diamond-shaped symbols), and will be developed later during the main Shuttle PRA. The lower-level branches that are not shown explicitly in Appendix 1 (denoted by triangular off-page-connector symbols containing numbers, e.g., ⚠) are similar to the analogous branches of NASA's "fault tree" for the pressure excursion event (which is itself actually an MLD, as we note below). Appendix 2 contains the NASA "fault tree."

2.2. Subtask 2. Correlation of Solid Rocket Booster Pedigree Information with Pressure Excursions.

Subtask 2 is a correlation analysis that searched for significant relationships between the magnitude, frequency, and variability of observed SRB chamber pressure transients, and the pedigree and history of the SRBs that had experienced transients. The SAIC-SFA team investigated potential correlations between the following factors and pressure excursion phenomena on the basis of the information furnished by NASA and its SRB contractors:

- Casting sequence
- Firing sequence
- Storage time (interval between casting and firing)
- Ammonium perchlorate (AP) vendor
- Aluminum powder vendor
- SRB TVC gimballing just before or during pressure excursions.

Combinations of several factors were considered in some cases.

Figures 1 and 2 show some of the most interesting and potentially significant results of this subtask. Figure 1 is a scatter plot of peak pressure transient magnitude versus casting date for SRBs containing ammonium perchlorate (AP) from the three vendors, Pacific Engineering (PE), Kerr-McGee (KM), and Western Electrochemical (WE, successor to PE after the PE plant was destroyed in an accidental explosion.) Figure 1 clearly shows that boosters loaded with WE AP exhibit considerably higher pressure-transient magnitudes than those containing other venders' AP, as also noted in a number of NASA analyses. (A *T*-test, a standard statistical test of significance, demonstrates that the differences among vendors are statistically significant at more than 99% confidence.)

Figures 2a and 2b on page 5 are plots of a five-booster moving average of recorded pressure transient peaks versus propellant motor identification number (arranged in order of casting date) for SRBs containing AP from KM and WE respectively. (Averaging over five motors highlights

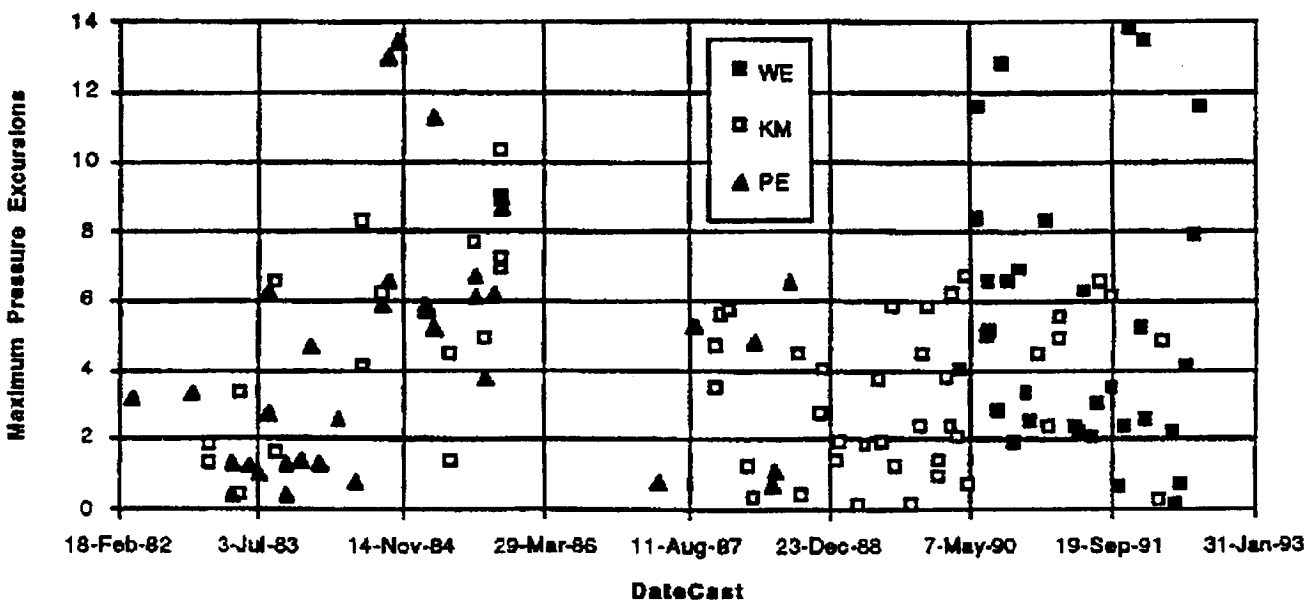


Figure 1. Scatter Plot of Peak Pressure Transient Versus Casting Date for SRBs Containing Ammonium Perchlorate from Three Vendors.

trends in the data by filtering out small motor-to-motor variations.) Note the difference in trends between the two plots. Pressure excursion magnitudes in KM SRBs have trended gradually upward, and seem to have become somewhat more variable recently. However, WE SRB pressure excursions were trending gradually downward until they showed a sudden and sharp increase beginning at motor number 29B. This suggests that a significant change occurred in some characteristic that affects chamber pressure stability at that point. It is not yet clear whether the change involved the AP material itself, its processing into finished SRBs, the treatment of the SRBs between manufacture and launching, or the characteristics of the flights during which the excursions occurred (or perhaps some combination of these).

2.3. Subtask 3. Development of Parameter Uncertainty Distributions.

It is clear that thrust is the solid rocket booster performance parameter of greatest flight-safety risk significance, at least in the present context of risk imposed by SRB pressure excursions. Therefore the SAIC-SFA team concentrated on developing uncertainty distributions for thrust. The basis of this analysis is the following mission-specific SRM thrust equation that has been presented in several of the briefing packages (e.g. "MSFC RSRM Pressure Blip and Dispersions," 11/10/93, reproduced in Appendix 3 of this report), and that is apparently used to compute the normal and upper-bound SRB thrust for flight certification of the external tank (ET).

$$F = F_{BLOCK} + \Delta F_{BURN\ RATE} + \Delta F_{PMBT} + \Delta F_{OSC\ MEAN} + \Delta F_{IMB\ MEAN} + \tag{1}$$

$$\sqrt{\Delta F^2_{SCALE\ FACTOR} + \Delta F^2_{NOM} + \Delta F^2_{PMBT\ UNC} + \Delta F^2_{SHAPE} + \Delta F^2_{F/P} + \Delta F^2_{OSC\ DISP}}$$

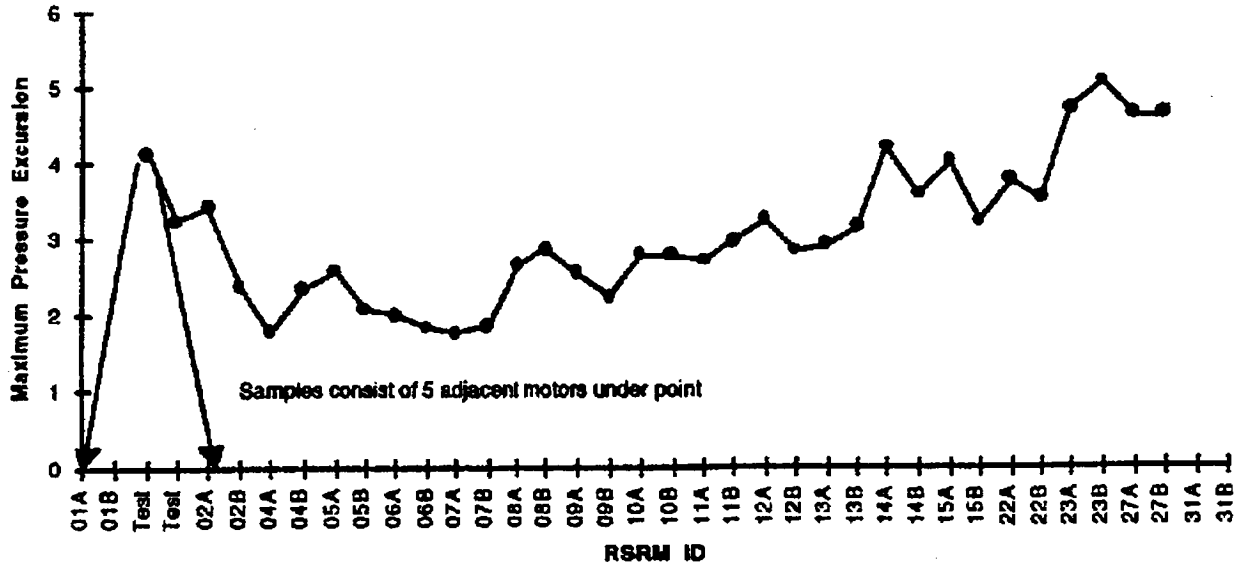


Figure 2a. Five-Motor Moving Average of Peak Pressure Transient Versus Casting Sequence Number for SRBs Containing Kerr-McGee Ammonium Perchlorate.

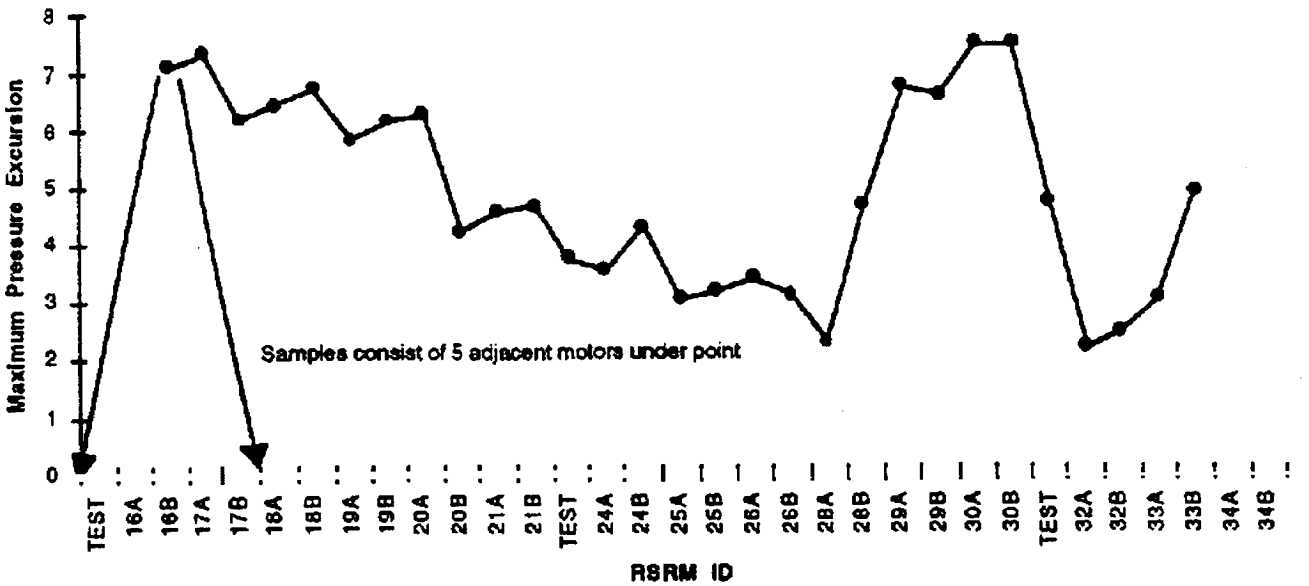


Figure 2b. Five-Motor Moving Average of Peak Pressure Transient Versus Casting Sequence Number for SRBs Containing Western Electrochemical Ammonium Perchlorate.

(The nomenclature is defined in Appendix 3.) This equation appears to be an essentially empirical relation combining nominal ("block") thrust; several quasi-constant terms which adjust for expected variations from nominal thrust due to propellant temperature, burn rate variability, etc.; and terms reflecting uncertainties in most of the other terms. The latter set of terms is combined by using the "root-of-the-sum-of-the-squares" (RSS) method into a single uncertainty term that is summed with the others . (The SAIC-SFA team questions the appropriateness of the RSS method in this case, as discussed in paragraph 3.3 below, but we will reserve that issue for later.)

In order to develop an uncertainty distribution for total SRB thrust, the uncertainty terms were represented as distributions around a mean, and grouped with the terms that represent their respective means. In this way the equation is restated as...

$$F = (F_{BLOCK} \pm \Delta F_{NOM}) + (\Delta F_{BURN\ RATE} \pm \Delta F_{SCALE\ FACTOR}) + (\Delta F_{PMBT} \pm \Delta F_{PMBT\ UNC}) + (\Delta F_{OSC\ MEAN} \pm \Delta F_{OSC\ DISP}) + (0 \pm \Delta F_{SHAPE}) + (0 \pm \Delta F_{F/P}) + \Delta F_{IMB\ MEAN} \quad (2)$$

Consistently with NASA's practice, and in the absence of contrary evidence, the distributions on the uncertainty terms were assumed to be normal or Gaussian. The standard deviations assigned to the distributions depended on the specific circumstances. This equation was set up in an Excel 4.0™ spreadsheet, and the distributions of the uncertain terms propagated through the equation to form the total thrust distribution by Monte Carlo simulation using Crystal Ball™, a commercial Monte Carlo simulation tool that interfaces directly with Excel. Figures 4a and 4b in paragraph 3.3 show outputs for several simulation cases, and the accompanying text explains their significance.

3.0. KEY RISK ISSUES.

The SRB Pressure Excursion Assessment was performed partly in order to develop risk-based insights into both the SRB pressure transient phenomenon and the Shuttle flight safety decision-making process. Accordingly the SAIC-SFA team identified a number of key risk issues which are presented below.

3.1. Fault Tree (Master Logic Diagram).

Early in its investigation, NASA prepared what was characterized as a "fault tree" in order to systematically identify and track all credible potential mechanisms for the production of SRB pressure transients. This tree was presented in "STS-54 RSRM-29 Chamber Pressure Observation Overview," 4 February 1993, and is reproduced in Appendix 2. After reviewing the "fault tree," the SAIC-SFA team concluded that while it is not really a fault tree in the sense in which that term is normally used in the risk assessment community, it is in fact a reasonably comprehensive and well-founded Master Logic Diagram for the "top event" of SRB pressure transients. (As discussed previously, an MLD identifies all of the credible events that can lead to the top event, but ignores pivotal events, interactions among initiators and event sequences, and event probabilities.) Therefore it will be possible to transfer much of the basic-events information and logic from the NASA "fault tree" directly into the MLD for the main Shuttle Probabilistic Risk Assessment.

3.2. Deciding on the Acceptability of Pressure Excursions Based on Statistical Analysis of Pressure Excursion Experience.

NASA has consistently used a statistical analysis of the experience base of pressure excursions observed during flight and ground test firings of SRBs to determine what pressure transients (and indirectly what thrust transients) are considered "normal" and thus acceptable. (See, for example, the briefing materials reproduced in Appendix 4.) In essence, the procedure is to fit an assumed Gaussian probability distribution to the pressure excursion observations to date, and take the upper bound of "normal" pressure excursions to be the mean of this distribution plus a factor k times the standard deviation, where k is selected to assure an acceptably low probability that the bound will be exceeded at an acceptably high statistical confidence level. In some instances $k=3.0$ is used, as in standard aerospace practice, while in others k appears to have been selected to achieve acceptable confidence. Whether "3σ" or "$k\sigma$" is used is irrelevant to the point at hand.

The effect of this approach is to widen the envelope of pressure excursions that are considered normal and acceptable every time a transient occurs that significantly exceeds the range of recent observations. Figure 3 illustrates this. It depicts the pressure excursions observed on SRBs loaded with WE ammonium perchlorate, plotted against motor identification number in order of casting sequence. For each SRB, the mean and the 3σ bounds of a normal distribution fitted to the set of pressure transients observed on motors up to and including the motor in question are also plotted.

Consider the example of boosters 29B and 30A, which flew on Missions STS-54 and STS-55 respectively. Just before STS-54, the 3σ limit was approximately 14.5 psi. When the STS-54 observation was added it grew to about 16 psi. This was taken to mean that the 13 psi excursion on STS-54, while unprecedentedly large, was within the range to be expected considering the experience base, and therefore was not a matter of serious concern. When the second 13 psi transient on STS-55 was absorbed into the experience base, the 3σ limit rose to about 17.5 psi, implying that the STS-55 transient was even farther from the outer bound based on experience and thus even less of a concern than the similar transient on the previous mission.

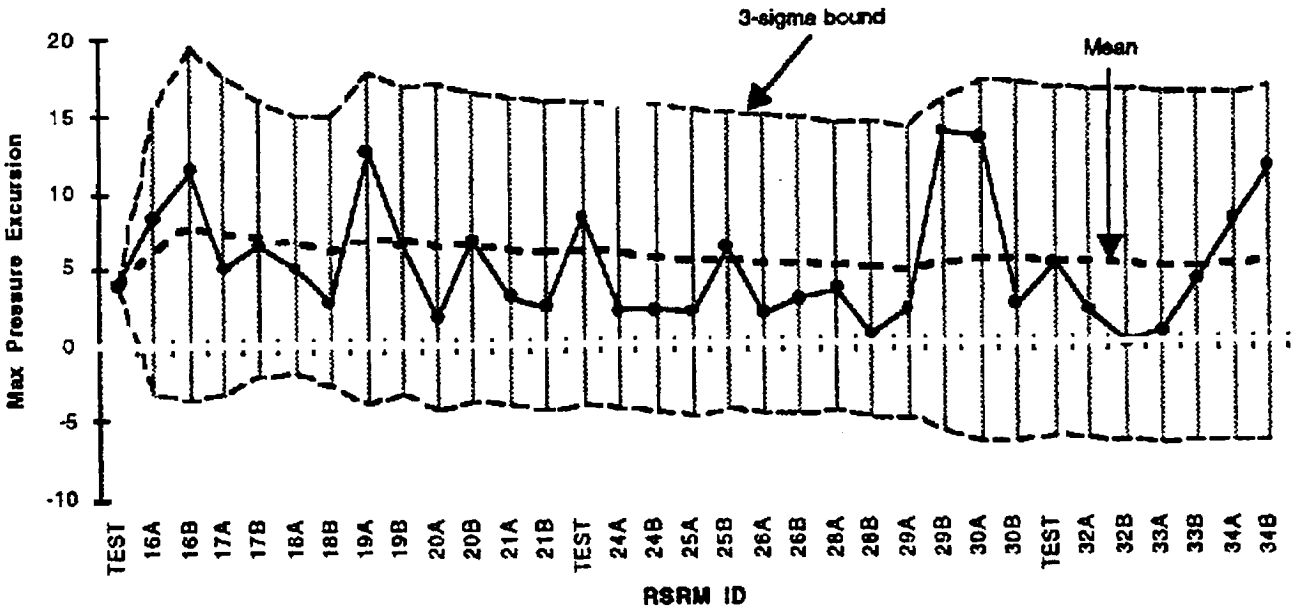


Figure 3. Pressure Excursion Experience of SRBs Loaded with WE AP, with "3σ" Bounds of Experience Distributions.

This approach presents three problems. First, it is based on the unstated assumption that all pressure excursions are part of a single population differing only in magnitude. However, the large positive pressure excursions that are the subject of this study appear to be qualitatively different from the minor fluctuations around the nominal pressure that comprise most of the experience base. This implies that incidents of these two kinds are not part of the same population and should not be treated statistically as if they were. Second and more generally, the approach provides a mechanism for safety margins to be gradually eroded through a series of incremental decisions without a thorough engineering review of the overall risk implications of each decision. Third, it tends to mask genuine failure precursors by making them appear to be part of a continuum of normal experience. (A "failure precursor" is any observed abnormal condition that can credibly lead to catastrophic failure if it occurs again with somewhat greater severity or when the ability of the system to respond to it is impaired.)

3.3. Solid Rocket Motor Thrust Equation.

As mentioned earlier, the dispersed thrust equation NASA uses to estimate SRB thrust loading for structural and dynamics calculations uses the root-sum-square (RSS) method to combine the variabilities of the thrust components that are subject to variability into a single term, which is then summed with several other terms. However, the validity of the root-sum-square (RSS) method of combining variabilities depends on the variabilities' being random, symmetrically distributed, and independent. As far as the SAIC-SFA team can determine, none of these conditions is necessarily satisfied for the uncertainty terms of the SRB thrust equation for the following reasons. First, the sources of uncertainty appear to contain some systematic variations, e.g., the variation of thrust excursion magnitude and frequency with AP vendor, and therefore the variabilities are not necessarily random. Second, the sources of uncertainty appear to arise from physical causes which may not necessarily be characterized by symmetrical distributions. Third, several of the uncertainty terms appear likely to be correlated rather than independent. Furthermore, the violations of the

conditions for using RSS are non-conservative in most cases. It seems clear that the RSS method is not appropriate for this case, and using it potentially can increase risk by understating the upper bound of expected thrust and thus decreasing structural margins of safety.

As discussed in paragraph 2.3 above, in order to investigate the risk implications of this situation the SAIC-SFA team formed explicit uncertainty distributions for SRB thrust by constructing uncertainty distributions for the variability terms of the thrust equation and propagating them through a reformulated version of the thrust equation using Monte Carlo simulation. The first, base-case simulation replicated NASA's RSS calculations for the numbers given in the example in Appendix 3, taking the "Δ" terms to be the 3σ values of normal distributions. This case demonstrates that the RSS method gives correct results if the necessary conditions for its use are fulfilled. The team then investigated the impact of violating the conditions by running several sensitivity cases in which distributions that were (1) constant over part of their ranges (hence not random), (2) skewed (hence not symmetrical), and (3) mutually correlated (hence not independent) were substituted for the independent Gaussian distributions of ΔF_{NOM} and $\Delta F_{SCALE\ FACTOR}$, the two largest variability terms in the original simulation. Comparing the resulting thrust distributions with each other and with the base case that replicated the RSS calculations showed that non-randomness and non-symmetry of the distributions had very little effect on the outcome, at least with the moderate violations assumed in this study, but that non-correlation had a substantial impact on the critical right-hand "tail" of the thrust distribution. Furthermore, the effect of using the RSS method to combine correlated variability terms is always non-conservative (i.e., resulting in lower predicted thrust than the Monte Carlo simulation that accounts for correlation). These topics are discussed in detail in Appendix 5.

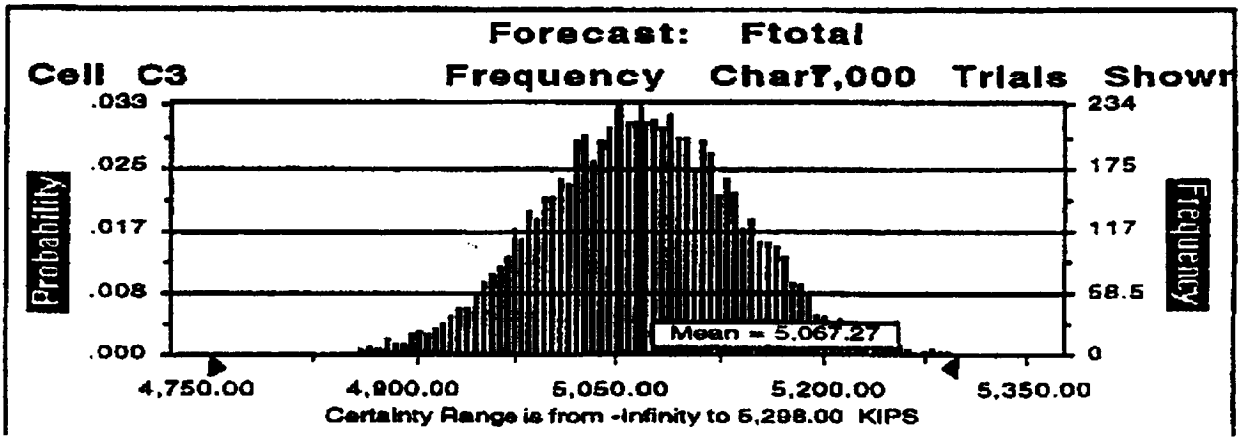


Figure 4a. Dispersed Thrust Uncertainty Distribution for the Base Simulation Case Replicating the Example That Uses the RSS Method.

Figures 4a and 4b show the frequency distributions of dispersed SRB thrust for the base case and the correlated-terms case respectively, as generated by the Crystal Ball Monte Carlo simulation tool. The base and correlated-terms distributions in these figures superficially appear similar, but Figures 5a and 5b highlight the critical difference between them by illustrating how the non-conservative error of using the RSS method to combine correlated variabilities can affect the margin of safety of the critical parts of the external tank structure. The three distributions in 5a and 5b are Gaussian distributions plotted from the parameters given by three Monte Carlo simulation cases. In each figure the distribution labeled "uncorrelated" was derived from the base case that replicates the RSS version of the thrust equation (Figure 4a); the "somewhat correlated" distribution came from the case shown in Figure 4b, where ΔF_{NOM} and $\Delta F_{SCALE\ FACTOR}$ were assumed to be 75% correlated; and

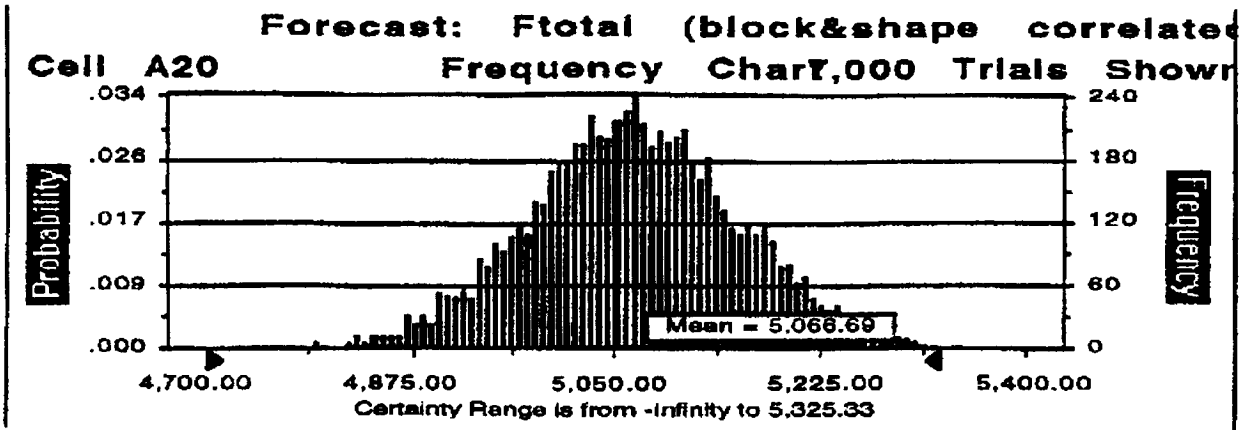


Figure 4b. Dispersed Thrust Uncertainty Distribution for the Sensitivity Simulation Case in which ΔF_{NOM} and $\Delta F_{SCALE\ FACTOR}$ Are Assumed Correlated at 75% Correlation Factor.

the "100% correlated" distribution was based on a case in which all uncertainty terms in the thrust equation were assumed fully correlated with one another. (The latter case puts an upper bound on the factor-of-safety effect to be expected from replacing the RSS method with a more rigorous method of propagating uncertainties.) Figure 5a shows the thrust distributions on a large scale, while Figure 5b focuses in on the right-hand "tails."

Looking first at Figure 5a, note that — as expected — increasing the correlation among variability terms increases the dispersion of the thrust distribution and thus raises the 3σ upper bound on thrust. The rightmost vertical arrow at approximately 6.8×10^6 lbs in Figure 5a represents the ultimate failure-point thrust used in NASA's example, which corresponds to a safety factor of 1.28 applied to the 3σ point of the base RSS-derived thrust. Also shown are the 3σ (99.87%) upper thrust bounds for the uncorrelated, somewhat correlated, and 100% correlated cases. Now refer to Figure 5b, which shows the right-hand "tails" of the thrust distributions in more detail. Note that when two variability terms of the thrust equation are assumed to be somewhat correlated, the factor of safety drops from 1.28 (the minimum requirement in the example) to 1.276. In the worst case in which all variability terms are assumed 100% correlated, the factor of safety is only 1.217. The key point here is that if the minimum acceptable factor of safety is 1.28 based on the 3σ value of the thrust, and the thrust calculated by the RSS method barely satisfies this requirement, then the thrust calculated by a method such as Monte Carlo simulation that correctly accounts for correlations among sources of variability provides a negative margin of safety.

In addition to the inappropriateness of the RSS method, the SAIC-SFA team has serious concerns about the validity of the method used to establish the 3σ upper bound for the ΔF_{SHAPE} term in the thrust equation. NASA appears to have performed a statistical analysis of 66 previous RSRM pressure traces to derive a 3σ upper bound for future pressure spikes. As best the team can reconstruct, the following procedure was followed:

1. The sample population pressure traces were divided into one-second increments.

2. A normal distribution was assumed for the pressure distribution over 66 motors at each time increment.

3. A mean and standard deviation (σ) were obtained at each pressure increment.

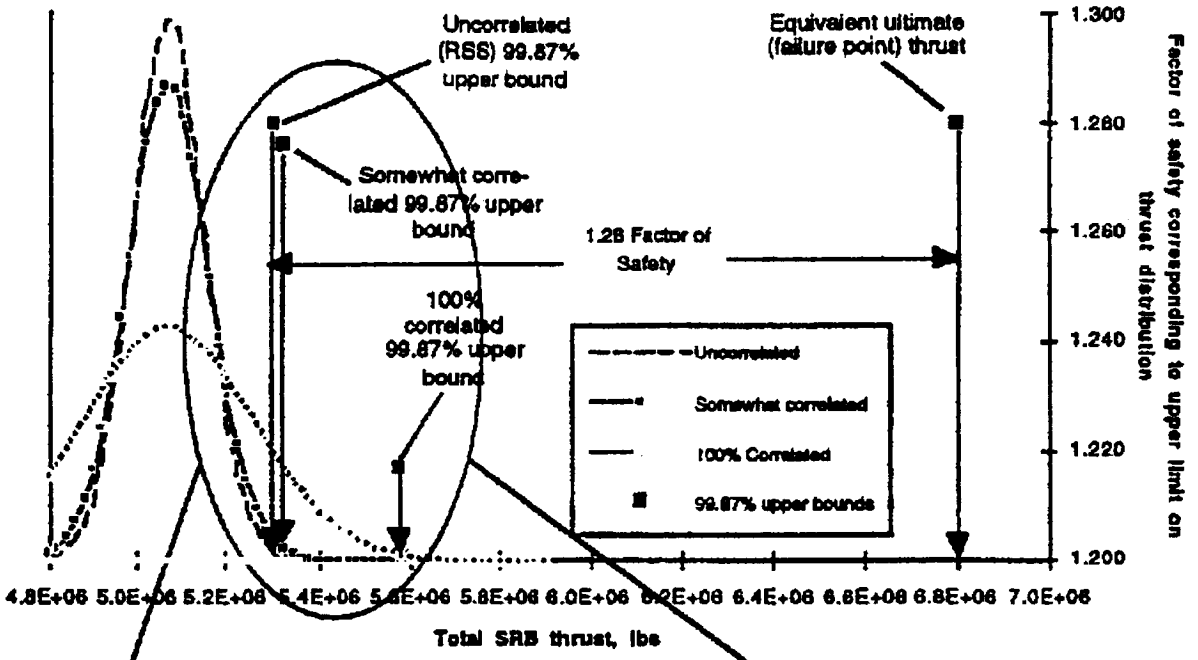


Figure 5a. Comparison of SRB Dispersed Thrust Distributions for Correlated and Uncorrelated Sources of Variation.

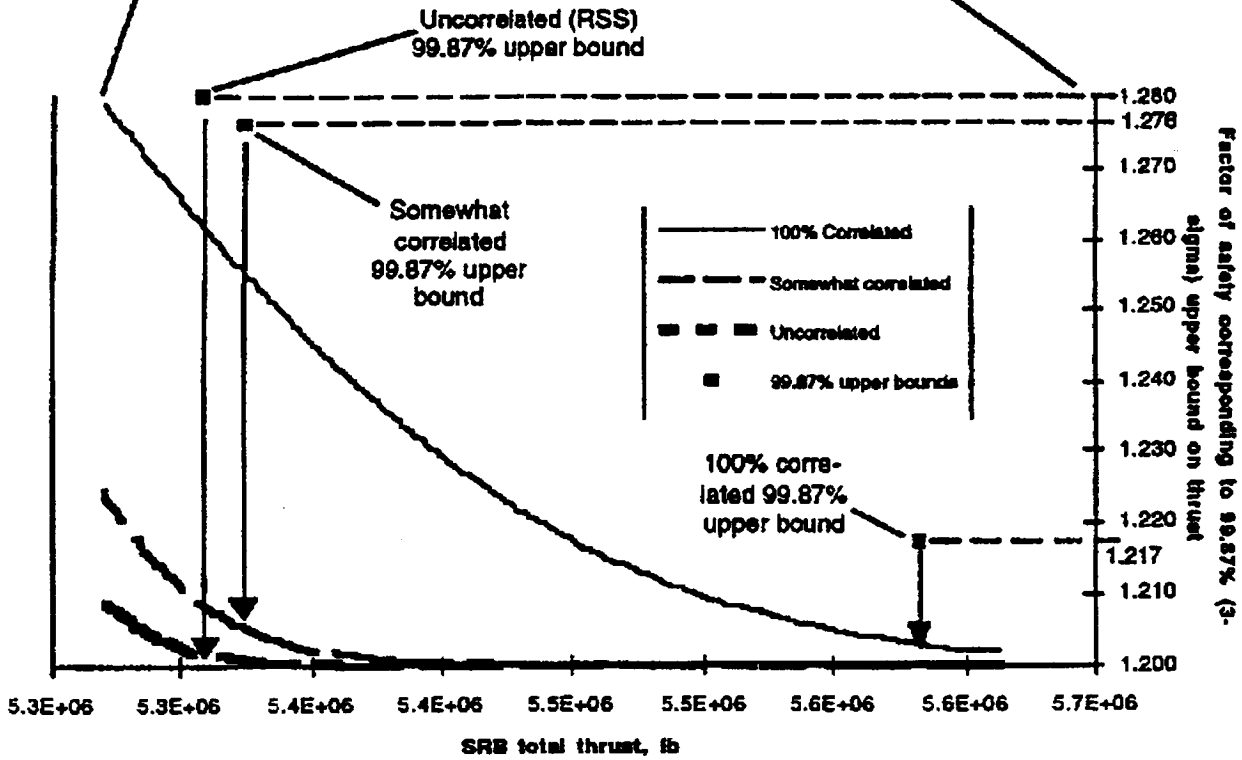


Figure 5b. Right-Hand "Tails" of the Correlated and Uncorrelated Thrust Distributions, with Corresponding Factors of Safety

4. The maximum 3σ value occurred at time 69 seconds. This was 20 psi above the mean.

5. It was assumed that this 20 psi excursion could be generated at any time increment.

6. The ratio of the 3σ value to the sample mean at each time increment was calculated and plotted as a percentage.

7. At 69 and 71 seconds this ratio was about 3.2%. This was converted to thrust (about 80,000 lb) and was used in the empirical thrust equation as the ΔF_{SHAPE} term discussed above.

The SAIC-SFA team performed an independent statistical assessment assuming a normal distribution at 69 and 71 seconds using the pressure plots found in the review material (reproduced in Appendix 6). The mean values were found to be 632 and 634 psi respectively, which correspond to the plotted mean values from the program. The standard deviation at 69 seconds was found to be $\sigma(69) = 4.6$ psi. The standard deviation at 71 seconds was found to be $\sigma(71) = 4.4$ psi. Combining both populations provided a $\sigma = 4.5$. The 20 psi "upper bound" pressure transient used by the program corresponds to about 4.4σ, not 3σ. There is no apparent explanation for this discrepancy; perhaps a normal distribution was not used (although it was stated that a normal was used).

Furthermore, if a 20 psi transient is a 4.4σ event, then a 13 psi excursion is approximately a 3σ event (assuming a normal distribution was in fact used), which implies that its frequency is approximately 1.4×10^{-3} per firing, or less than one in 700 firings. This appears incompatible with the observed experience of two 13 psi excursions in 123 flight and test firings of the HPM and RSRM generations of the Shuttle SRB.

Finally, the NASA analysis divided the population into one-second increments. This implies that each time increment was considered an independent population. This assumption is very difficult to justify. The data shows that the time to each pressure transient is nearly random in the time interval 64 to 80 seconds, which suggests that all data within at least that time interval should be combined. Furthermore, phenomenological investigations indicate good reasons for the slag/slosh scenario to produce transients during this interval, but independently of time during the interval. The reasons stem from propellant burn patterns that begin to allow slag to collect in the bore or nozzle beginning at about 65 seconds, as well as considerations of pitch and gimballing that provide a mechanism for spilling the slag. Again the team sees no reason to believe that each time increment is an independent population. It is likely that a statistical study that combines the data over the 64 to 80-second interval would be valid and would produce a larger 3σ "upper bound."

3.4. Handling of External Tank Structural Safety Factors.

NASA's current method of determining the required safety factor (SF) for limits on external tank (ET) structural loads involves scaling the SF between 1.40 and 1.25 according to the proportion of the total load that is "not well understood" (i.e., highly uncertain) versus "well understood" (i.e., relatively certain.) (Refer to the briefing materials in Appendix 7 for an explanation of the procedure.) However, the NASA method appears to proportion the safety factors according to the magnitude of the expected load, not to the uncertainty of the load, although the SF is intended to account for the variability above the expected load rather than its magnitude. It seems clear that if SFs are to be scaled by some general rule related to load uncertainty, they should be proportioned according to an appropriate uncertainty measure — perhaps standard deviation or variance — instead of load magnitude.

4.0. CONCLUSIONS AND RECOMMENDATIONS.

This section contains the conclusions and recommendations of the SRB Pressure Excursion Assessment. It must be emphasized that they came out of a quick-response analysis driven by urgent Shuttle flight schedule considerations. Some of them may be modified by a more comprehensive and systematic risk analysis such as the main Shuttle Probabilistic Risk Assessment of which this study is a preliminary part.

4.1 Conclusions.

1. The SRB pressure excursion phenomenon increases Shuttle flight safety risk to some degree by potentially initiating at least the accident scenarios listed below.

(a) A transient over-thrust in one or both SRBs which exceeds the structural capabilities of the external tank causes vehicle breakup.

(b) A severe transient thrust imbalance between the two SRBs that exceeds the structural capabilities of the external tank causes vehicle breakup.

(c) A severe transient thrust imbalance between the two SRBs that is not recoverable by flight controls results in an unacceptable flight attitude, causing vehicle breakup due to excessive aerodynamic forces.

(d) A severe, sustained transient thrust imbalance between the two SRBs that is not recoverable by flight controls results in loss of directional control, exceedance of range safety guidelines, and flight termination by the range safety officer.

(e) A severe chamber pressure transient induces a hot-gas leak at an SRB joint that impinges on the ET, causing an ET explosion.

(f) A severe chamber pressure transient ruptures the SRB case.

2. It is impossible to quantify the risks of these scenarios with the limited information available to the SAIC-SFA team in Task 1. (The main Shuttle probabilistic risk assessment is intended to accomplish this.) However, scenarios (c) through (f) appear to be of negligible probability, at least to the extent that they are initiated by SRB pressure excursions, chiefly because it is difficult to conceive of a mechanism for producing thrust or pressure excursions of the necessary magnitude and duration.

3. There is a statistically-significant correlation between the use of ammonium perchlorate supplied by Western Electrochemical (WE) in SRB solid fuel, and the frequency of large, positive pressure transients. The SAIC-SFA team could not draw any conclusions about the reason(s) for this correlation from the data available to us.

4. Trending of peak pressure excursions against the SRB casting sequence suggests that an abrupt change in some characteristic of motors containing WE ammonium perchlorate that affects internal pressure occurred at motor number 29B. The available data do not support any conclusions as to what this change might have been.

5. Based on the material provided for review, the SAIC-SFA team has conceptual and technical concerns about NASA's methodology in these four specific areas:

(a) treating all pressure excursions in the SRB experience base as a single population for the purpose of statistical analysis in order to determine what pressure transients (and indirectly what thrust transients) are considered "normal" and thus acceptable, although the large positive pressure excursions that are the subject of this study appear to be qualitatively different from the minor fluctuations around the nominal pressure that comprise most of the experience base;

(b) using of the "root-of-the-sum-of-the-squares" (RSS) method to combine the variabilities of the terms of the SRB dispersed thrust equation that account for uncertainties in thrust, although there is considerable doubt that the necessary conditions for the validity of that method are fulfilled;

(c) dividing the SRB pressure trace experience base into one-second time increments which were analyzed separately, which implies that the pressure traces in these increments comprise separate populations, although both historical data and phenomenology suggest that the set of pressure traces within the interval when pressure transients occur is part of a common population; and

(d) establishing the minimum structural safety factor for the external tank by scaling the SF between 1.40 and 1.25 according to the proportion of the total load magnitude that is "not well understood" (i.e., highly uncertain) versus "well understood" (i.e., relatively certain), rather than according to a quantitative measure of the uncertainty of these categories of loads.

All of these problems can potentially lead to non-conservative assessments of safety and hence to increases in Shuttle flight risk.

6. More generally, the team had concerns with the flight safety decision process as depicted in the review materials. NASA appears to have used a "3σ" or "$k\sigma$" envelope derived by fitting an assumed Gaussian distribution to the record of pressure observations in order to define the limits of "normal" and thus acceptable SRB pressure transients. (The SAIC-SFA team's experience suggests that this is a common practice that is not restricted to the SRB pressure excursion issue.) The problem with this approach is that each anomalous occurrence becomes part of the experience base and thus widens the range of behavior considered normal, which can mask genuine failure precursors by making them appear to be part of a continuum of normal experience. Making flight safety decisions on this basis provides a mechanism for safety margins to be gradually eroded through a series of incremental decisions without a thorough engineering review of the overall risk implications of each decision.

7. Still more generally, while NASA and its contractors have done an excellent root cause analysis of the SRB pressure transient phenomenon, with the wisdom of hindsight the issue seems to have been handled in a somewhat disorganized, *ad hoc* fashion that was driven largely by the need to make timely flight readiness decisions in the absence of complete information. The SAIC-SFA team believes that much of the disorganization could have been avoided if the Shuttle program had been able to take advantage of a flight-safety decision process based on a systematic, quantitative consideration of risk.

4.1. Recommendations.

1. NASA should consider the conceptual and technical concerns raised in Section 3.0, "Key Risk Issues," some of which appear to be generic to the agency and its contractors. Specifically, the SAIC-SFA team recommends that NASA consider the following changes in its current practices as described in the data furnished for the SRB Pressure Excursion Assessment:

(a) NASA should reformulate the dispersed thrust equation that is used to determine SRB thrust loadings on the external tank structure in a way that avoids using the RSS method unless that method is rigorously shown to be valid, and fully accounts for the observed and potential actually

occurring pressure transients.

(b) NASA should perform a statistical analysis of historical SRB pressure data that uses 12.5-samples-per-second data in lieu of 2-samples-per-second data and treats the data in the 64 to 80 second time interval as a single population.

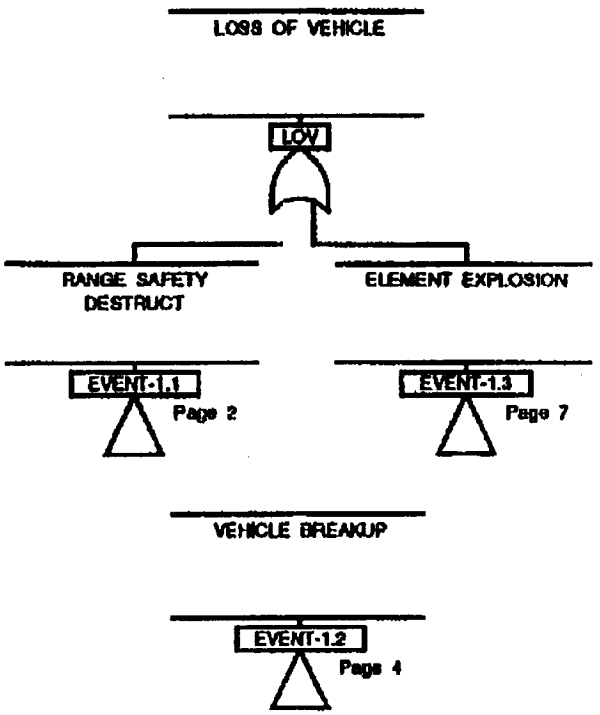
(c) At a minimum, NASA should revise its method of determining minimum structural safety factors for the external tank so as to apportion safety factors according to the ratio of uncertainties in the "well-understood" and "not-well-understood" load categories, rather than according to the magnitudes of the expected loads.

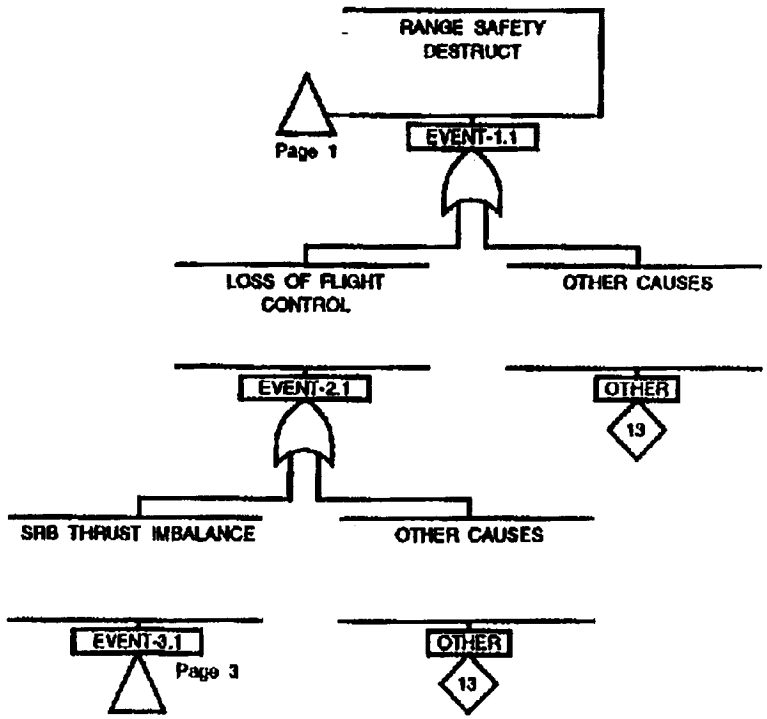
(d) Better still, in view of the progress in our understanding of probabilistic structural mechanics and the development of powerful probabilistic structural analysis tools since the inception of the Shuttle program, NASA should abandon the safety factor concept in favor of rigorous structure-by-structure probabilistic structural analysis as a basis for Shuttle flight certification. This recommendation will become especially important if — as seems likely — the external tank is further lightened by cutting back on structural margins or the Shuttle is called on to fly more structurally-demanding trajectories.

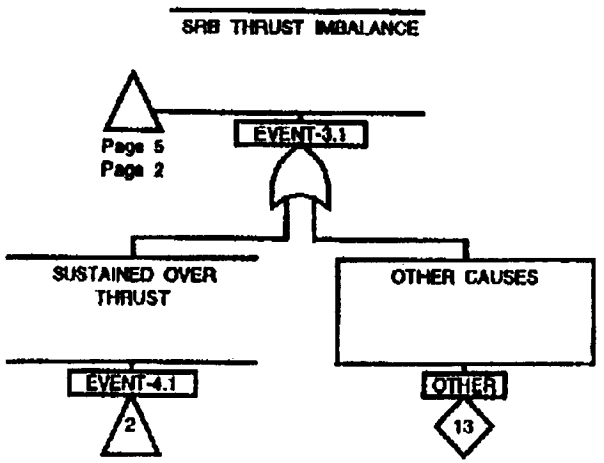
2. Because ET structural failure appears to be the dominant mechanism of potential Shuttle loss due to SRB chamber pressure excursions, and SRB thrust rather than chamber pressure is the direct driver of structural failure, NASA should consider installing high-fidelity force (thrust) instrumentation on the forward attachments between the SRBs and the ET for the next few flights in order to better characterize the thrust transient phenomenon.

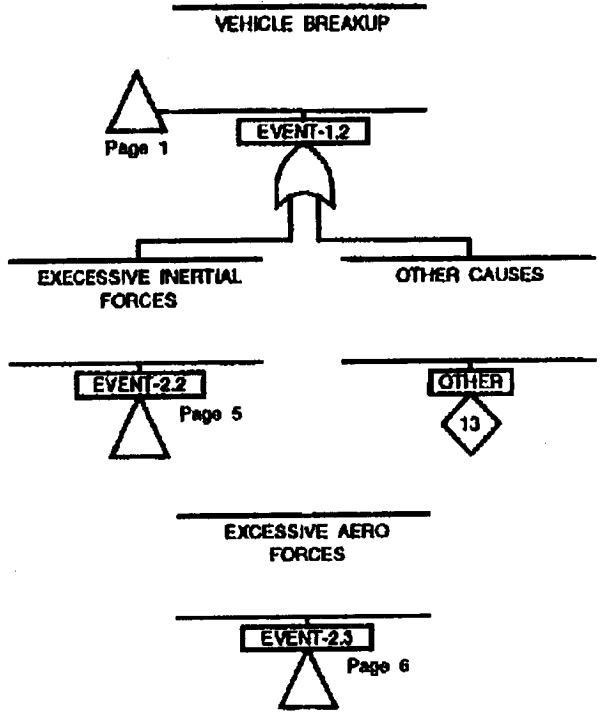
3. In view of the conclusions above, NASA should proceed expeditiously with its planned comprehensive probabilistic risk assessment of the Shuttle system. This study will determine how SRB pressure transients rank relative to other risk contributors, and thus whether continuing expensive and time-consuming efforts to investigate them is a good investment of limited resources; more generally, it will lay a sound foundation for a quantitative risk-based flight readiness decision process for the future.

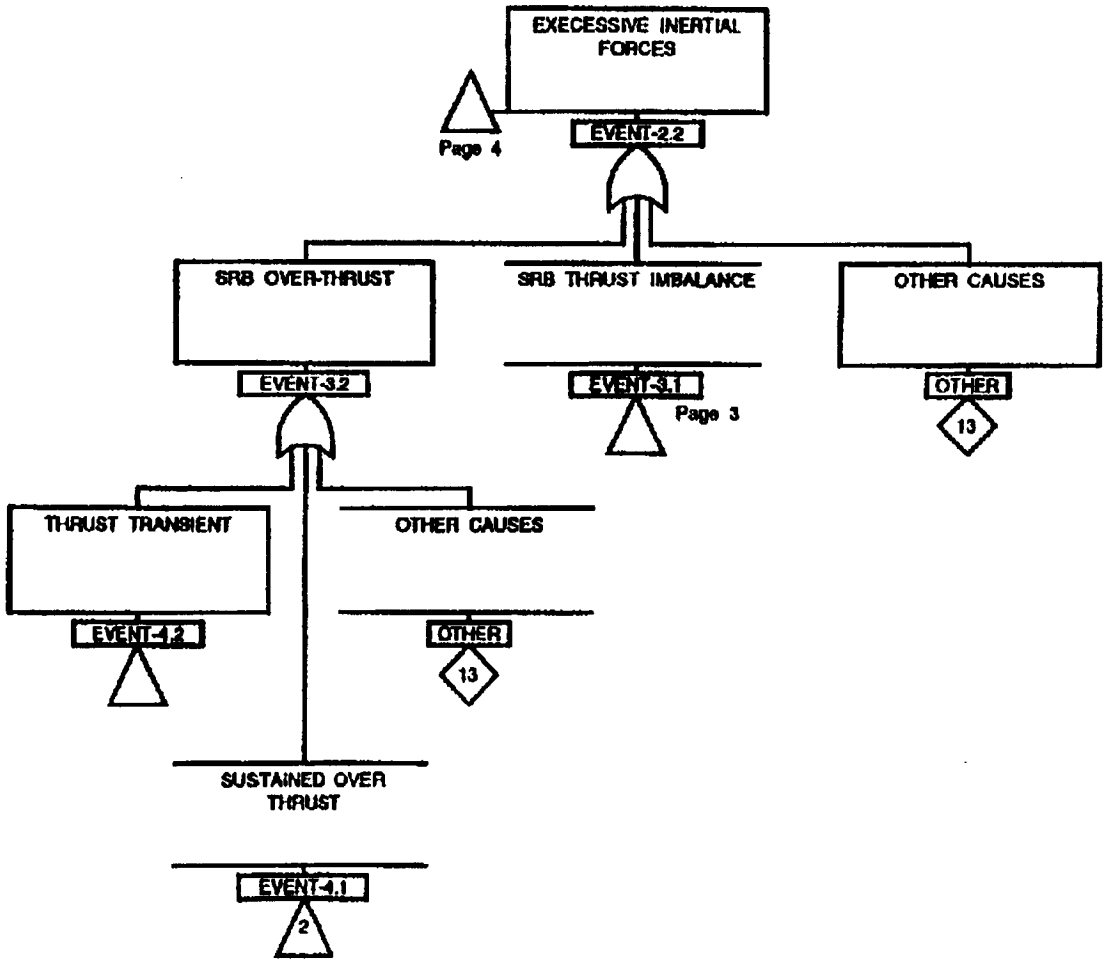
Appendix 1.
Preliminary Top-Level Master Logic Diagram for Loss of Shuttle Vehicle during Shuttle Boost-Phase Ascent, Highlighting SRB Pressure and Thrust Transients as Accident Sequence Initiators.

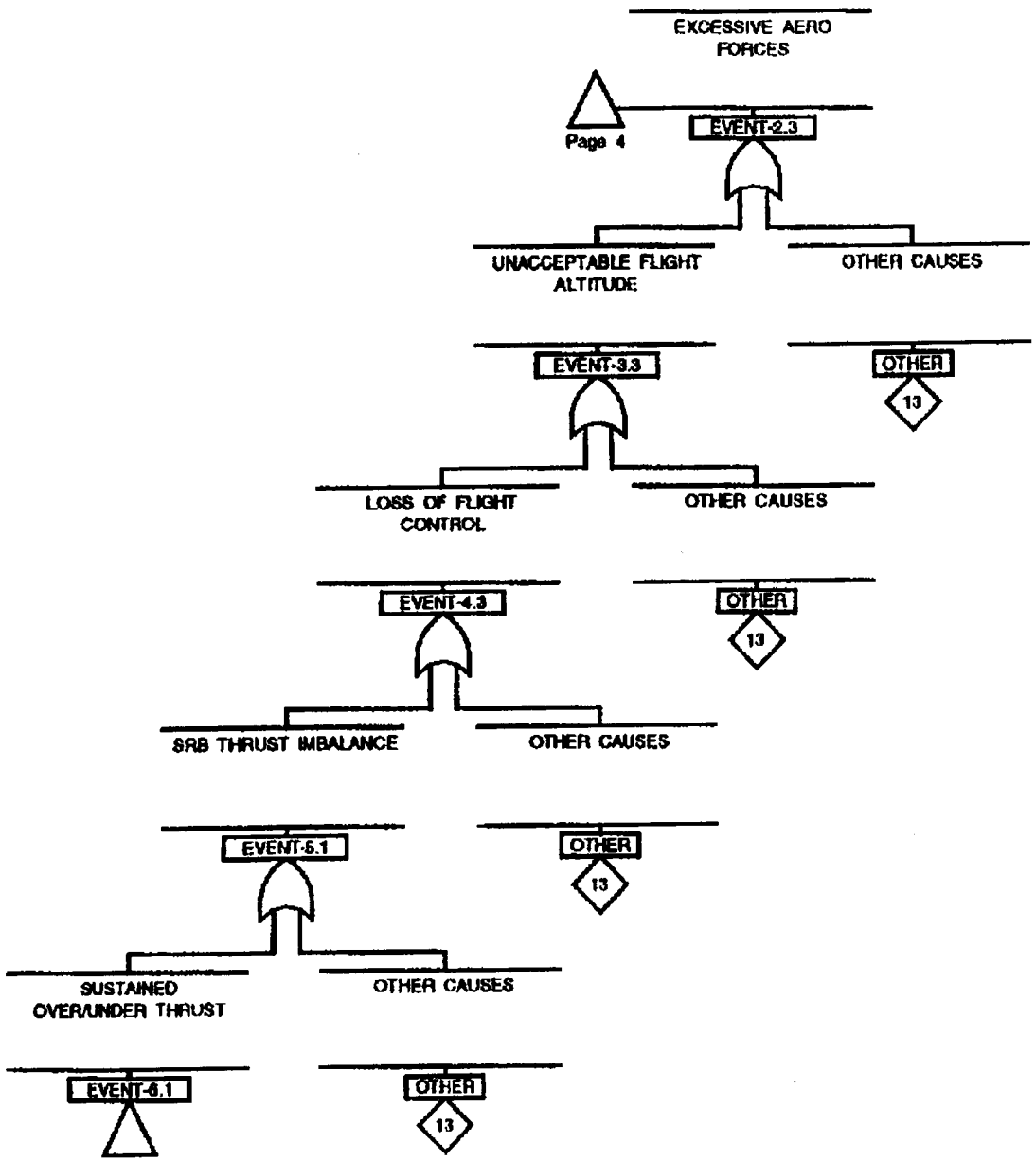

LOSS OF VEHICLE
LOV
RANGE SAFETY DESTRUCT
ELEMENT EXPLOSION
EVENT-1.1
Page 2
EVENT-1.3
Page 7
VEHICLE BREAKUP
EVENT-1.2
Page 4

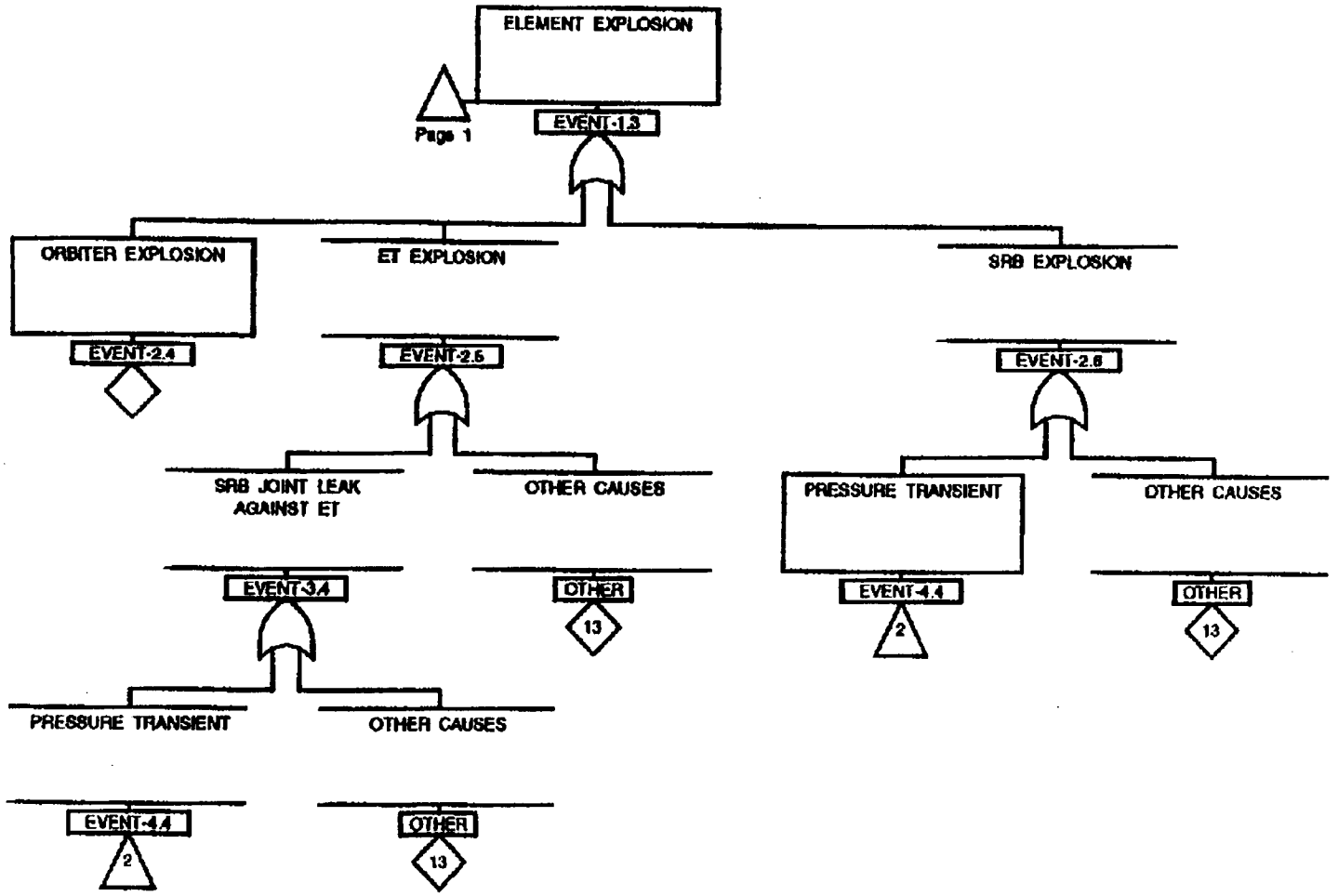

RANGE SAFETY DESTRUCT
Page 1
EVENT-1.1
LOSS OF FLIGHT CONTROL
OTHER CAUSES
EVENT-2.1
OTHER
13
SRB THRUST IMBALANCE
OTHER CAUSES
EVENT-3.1
Page 3
OTHER
13


SRB THRUST IMBALANCE
Page 5
Page 2
EVENT-3.1
SUSTAINED OVER THRUST
OTHER CAUSES
EVENT-4.1
OTHER
2
13

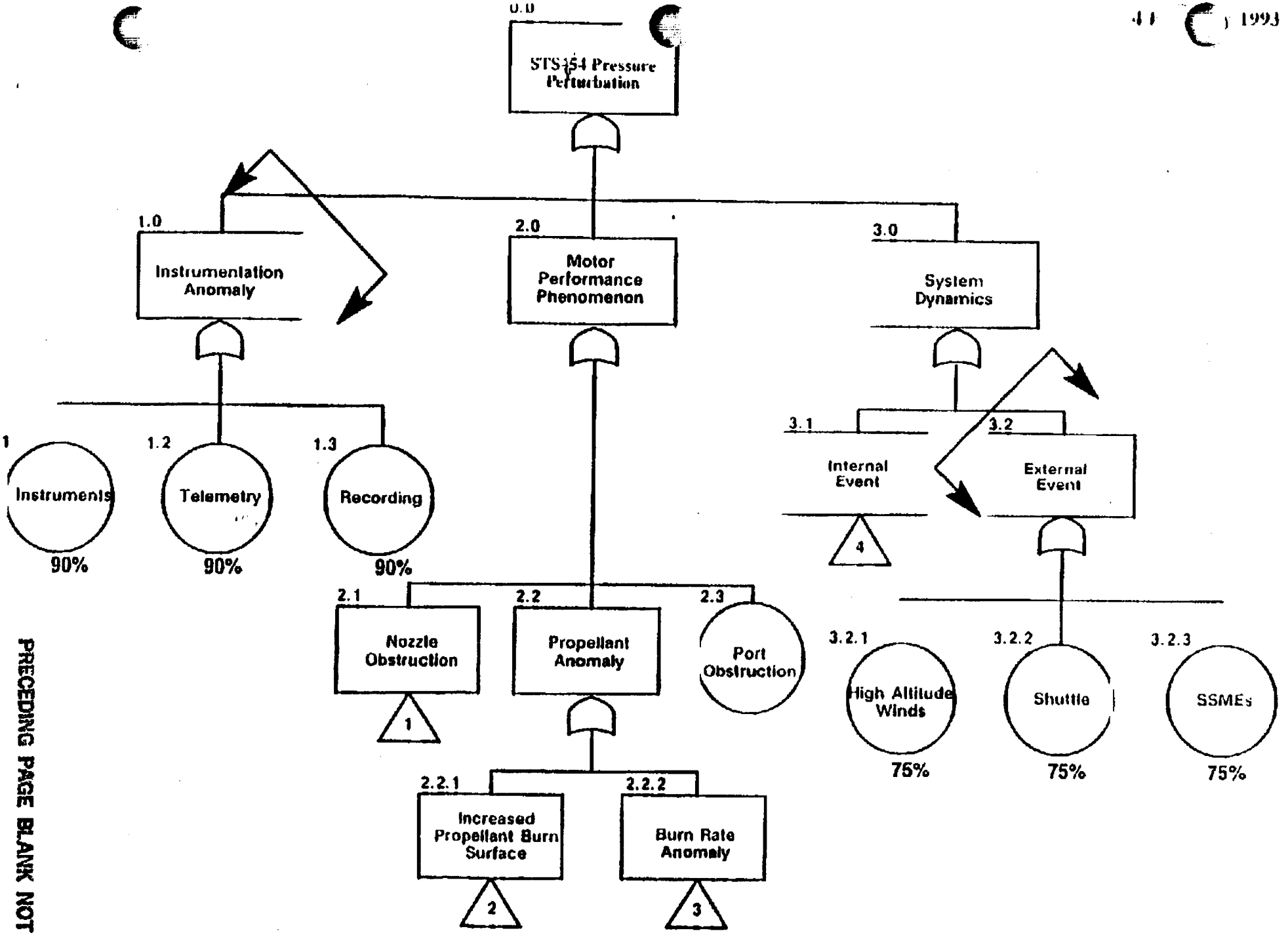

VEHICLE BREAKUP
Page 1
EVENT-1.2
EXECESSIVE INERTIAL FORCES
OTHER CAUSES
EVENT-2.2
Page 5
OTHER
13
EXCESSIVE AERO FORCES
EVENT-2.3
Page 6


EXECESSIVE INERTIAL FORCES
Page 4
EVENT-2.2
SRB OVER-THRUST
SRB THRUST IMBALANCE
OTHER CAUSES
EVENT-3.2
EVENT-3.1
Page 3
OTHER
13
THRUST TRANSIENT
OTHER CAUSES
EVENT-4.2
OTHER
13
SUSTAINED OVER THRUST
EVENT-4.1
2

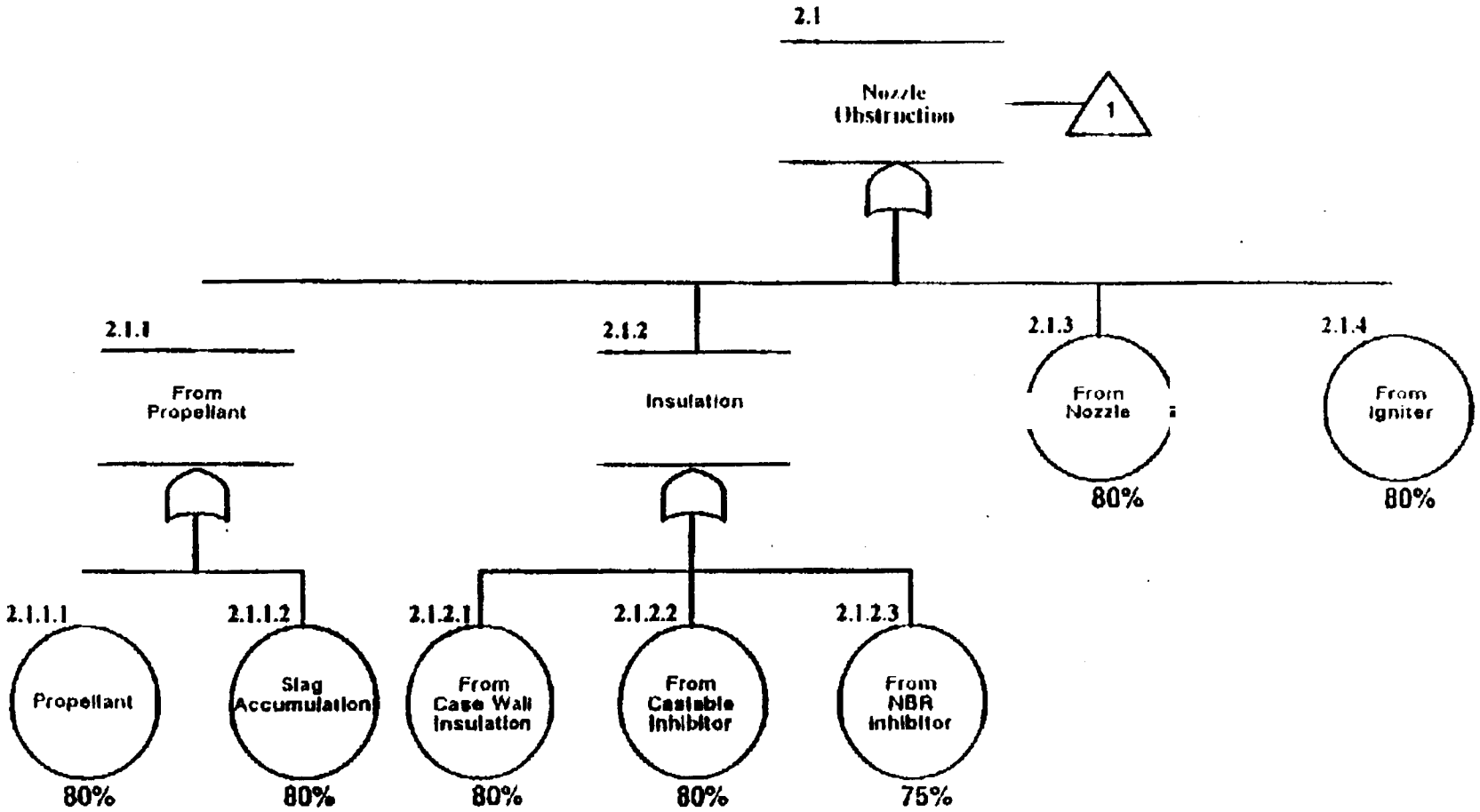

EXCESSIVE AERO FORCES
Page 4
EVENT-2.3
UNACCEPTABLE FLIGHT ALTITUDE
OTHER CAUSES
EVENT-3.3
OTHER
13
LOSS OF FLIGHT CONTROL
OTHER CAUSES
EVENT-4.3
OTHER
13
SRB THRUST IMBALANCE
OTHER CAUSES
EVENT-5.1
OTHER
13
SUSTAINED OVER/UNDER THRUST
OTHER CAUSES
EVENT-6.1
OTHER
13


ELEMENT EXPLOSION
Page 1
EVENT-1.3
ORBITER EXPLOSION
ET EXPLOSION
SRB EXPLOSION
EVENT-2.4
EVENT-2.5
EVENT-2.6
SRB JOINT LEAK AGAINST ET
OTHER CAUSES
PRESSURE TRANSIENT
OTHER CAUSES
EVENT-3.4
OTHER
13
EVENT-4.4
2
OTHER
13
PRESSURE TRANSIENT
OTHER CAUSES
EVENT-4.4
2
OTHER
13

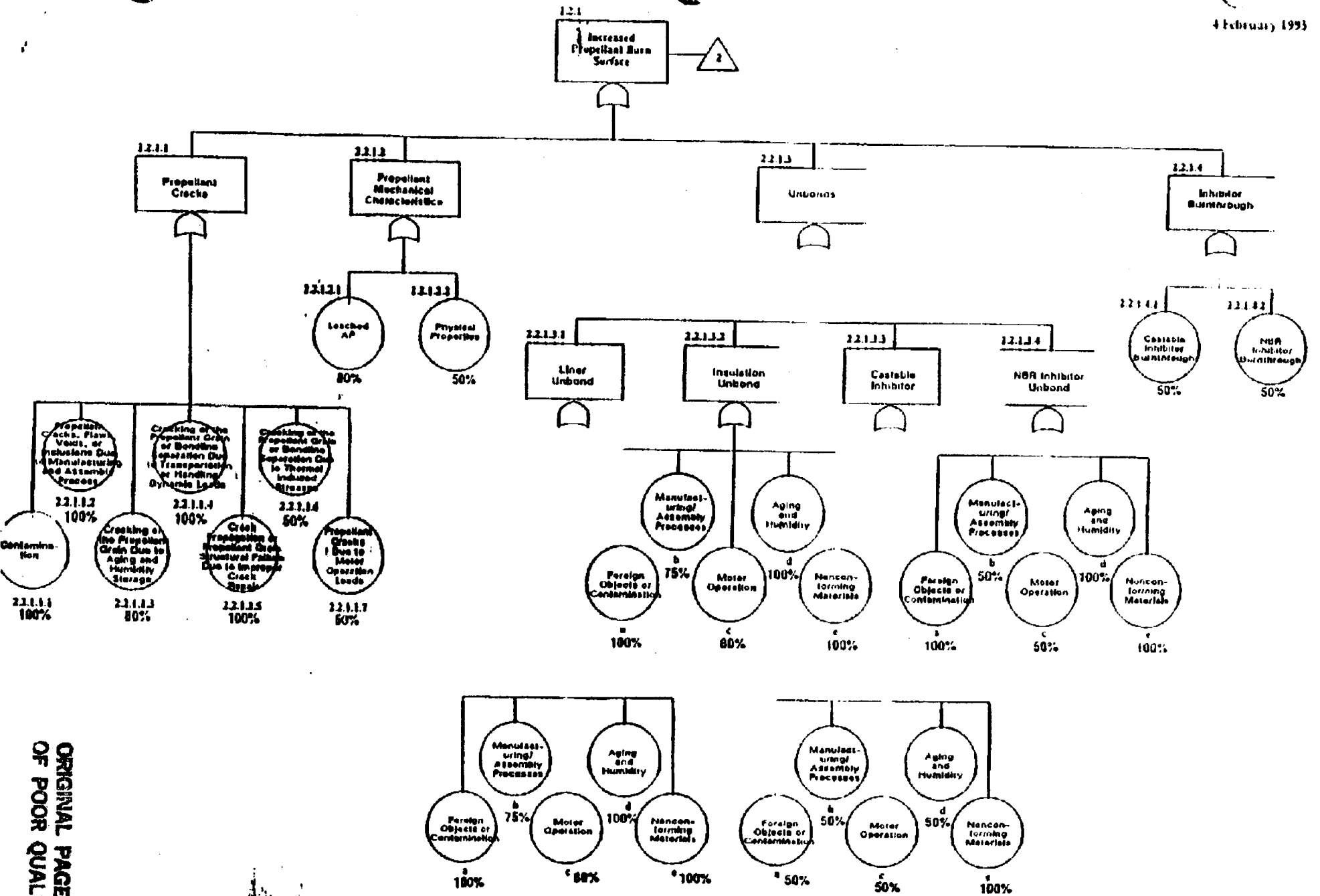
Appendix 2.
NASA "Fault Tree" (Master Logic Diagram) for Pressure Excursions (excerpt from "STS-54 RSRM-29 Chamber Pressure Observation Overview," 4 February 1993



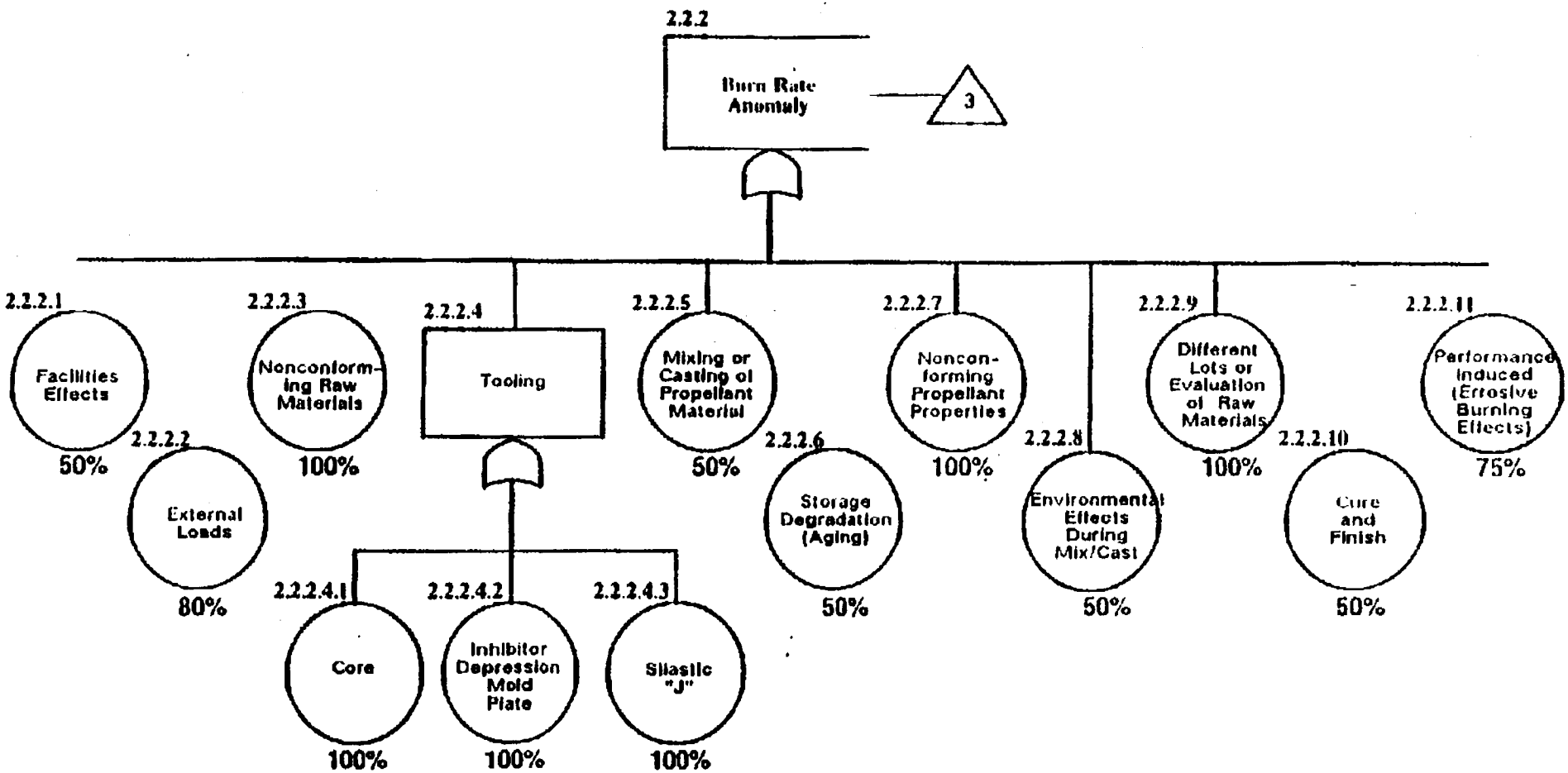
STS-54 Pressure Perturbation Fault Tree



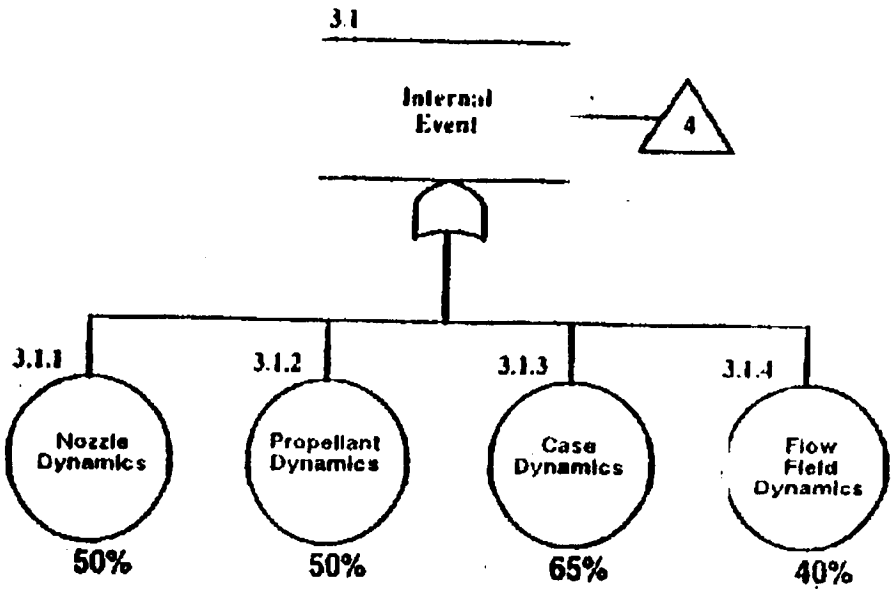
STS-54 Pressure Perturbation Fault Tree



STS–54 Pressure Perturbation Fault Tree



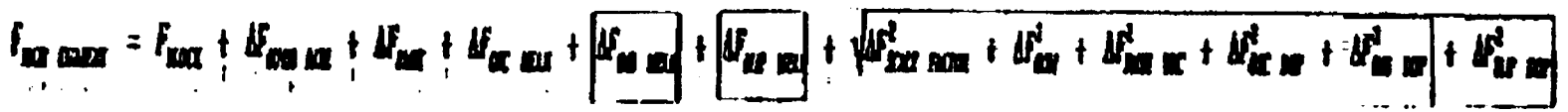
STS-54 Pressure Perturbation Fault Tree

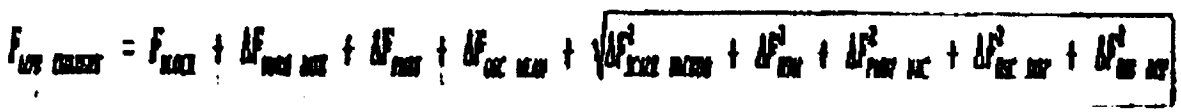


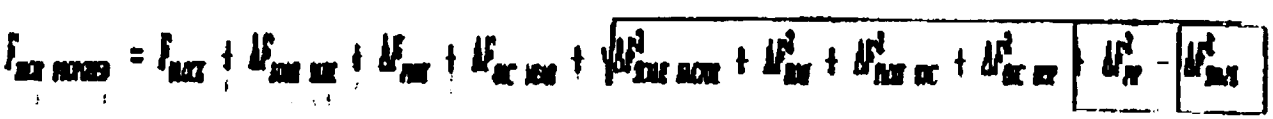
STS-54 Pressure Perturbation Fault Tree

Appendix 3.
SRM Dispersed Thrust Equation and Example of Thrust Calculation (excerpt from "MSFC RSRM Pressure Blip and Dispersions," 10 November 1993)

EQUATION FOR HIGH/LOW MOTORS OF THE PAIR







CURRENT		PROPOSED	
$\Delta F_{SLIP\ MEAN}$	= 17K	$\Delta F_{SLIP\ MEAN}$	= N/A
$\Delta F_{SLIP\ DISP}$	= 107K	$\Delta F_{SLIP\ DISP}$	= N/A
ΔF_{SHAPE}	= N/A	ΔF_{SHAPE}	= 3.2% (80K AT 69 SECS)
ΔF_{FIT}	= N/A	ΔF_{FIT}	= 0.5% (13K AT 69 SECS)
$\Delta F_{BAB\ DISP}$	= 33K	$\Delta F_{BAB\ DISP}$	= N/A
$\Delta F_{BAB\ MEAN}$	= 20K	$\Delta F_{BAB\ MEAN}$	= 20K

EQUATION FOR HIGH/LOW MOTORS OF THE PAIR

$$F_{HIGH} = F_{BLOCK} + \Delta F_{BURN\ RATE} + \Delta F_{PMBT} + \Delta F_{OSC\ MEAN} + \Delta F_{IMB\ MEAN} + \sqrt{\Delta F^2_{SCALE\ FACTOR} + \Delta F^2_{NOM} + \Delta F^2_{PMBT\ UNC} + \Delta F^2_{SHAPE} + \Delta F^2_{F/P} + \Delta F^2_{OSC\ DISP}}$$

F_{BLOCK} = BLOCK MOTOR THRUST AT STANDARD CONDITIONS

$\Delta F_{BURN\ RATE}$ = THRUST DUE TO BURN RATE DEVIATION FROM BLOCK MOTOR

ΔF_{PMBT} = THRUST DUE TO PMBT DEVIATION FROM BLOCK MOTOR

$\Delta F_{OSC\ MEAN}$ = THRUST DUE TO MEAN PRESSURE OSCILLATIONS

$\Delta F_{SCALE\ FACTOR}$ = THRUST DUE TO UNCERTAINTY IN BURN RATE SCALING

ΔF_{NOM} = THRUST DUE TO UNCERTAINTY IN NOMINAL

$\Delta F_{PMBT\ UNC}$ = THRUST DUE TO UNCERTAINTY IN PMBT

ΔF_{SHAPE} = THRUST DUE TO VARIATION ABOUT THE NOMINAL

$\Delta F_{F/P}$ = THRUST DUE TO UNCERTAINTY IN F/P

$\Delta F_{OSC\ DISP}$ = THRUST DUE TO DISPERSED PRESSURE OSCILLATIONS

$\Delta F_{IMB\ MEAN}$ = 0 FOR HIGH MOTOR ; -MEAN IMBALANCE FOR LOW MOTOR

MAGNITUDE OF TERMS FOR SPECIFIC APPLICATIONS

F_{BLOCK} = FUNCTION OF TIME BASED ON TCR-236-89 (60 DEG F & 0.368 IPS)

$\Delta F_{BURN\ RATE}$ = PREDICTED BURN RATE BASED ON 5" CP DATA

ΔF_{PMBT} = PREDICTED PMBT BASED ON L-9 DAY DATA

$\Delta F_{OSC\ MEAN}$ = 1% BASED ON MEAN OSCILLATIONS

$\Delta F_{SCALE\ FACTOR}$ = 2.6% BASED ON SCALE FACTOR K-SIGMA VARIATION OF 1.6%

ΔF_{NOM} = 2% BASED ON MAX EXPECTED DEVIATION IN THE NOMINAL

$\Delta F_{PMBT\ UNC}$ = 1% BASED ON 9 DEG UNCERTAINTY

ΔF_{SHAPE} = 3.2% BASED ON K-SIGMA FOR FLIGHT HISTORY

ΔF_{FIT} = 0.5% ESTIMATE BASED ON STATIC TEST

$\Delta F_{OSC\ DISP}$ = 1% BASED ON DISPERSED OSCILLATIONS

$\Delta F_{IMB\ MEAN}$ = BASED ON PREDICTED BURN RATE DIFFERENCE BETWEEN PAIRS (MIN 20K)

MAGNITUDE OF TERMS FOR GENERIC APPLICATIONS

F_{BLOCK} = FUNCTION OF TIME BASED ON TCR-236-89 (60 DEG F & 0.368 IPS)

$\Delta F_{BURN\ RATE}$ = 5 MILS DELTA (0.373 IPS) BASED ON K-SIGMA SUBSCALE BURN RATE

ΔF_{PMBT} = 22 DEG DELTA (82 DEG F) BASED ON HOTTEST AVERAGE KSC HISTORY

$\Delta F_{OSC\ MEAN}$ = 1% BASED ON MEAN OSCILLATIONS

$\Delta F_{SCALE\ FACTOR}$ = 2.6% BASED ON SCALE FACTOR K-SIGMA VARIATION OF 1.6%

ΔF_{NOM} = 2% BASED ON MAX EXPECTED DEVIATION IN THE NOMINAL

$\Delta F_{PMBT\ UNC}$ = 1% BASED ON 9 DEG UNCERTAINTY

ΔF_{SHAPE} = 3.2% BASED ON K-SIGMA FOR FLIGHT HISTORY

ΔF_{FIP} = 0.5% ESTIMATE BASED ON STATIC TEST

$\Delta F_{OSC\ DISP}$ = 1% BASED ON DISPERSED OSCILLATIONS

$\Delta F_{IMB\ MEAN}$ = 20 KIPS BASED ON FLIGHT HISTORY

STS-55 EXAMPLE CALCULATION AT 65 SECONDS

$$F_{HIGH\ SPECIFIC\ OLD} = 2510 + 17 + 0 + 25 + 20 + 17 + \sqrt{65^2 + 50^2 + 25^2 + 25^2 + 33^2 + 107^2} = 2732 \text{ KIPS}$$

$$F_{LOW\ SPECIFIC\ OLD} = 2510 + 0 + 0 + 25 + 0 + 0 + \sqrt{65^2 + 50^2 + 25^2 + 25^2 + 33^2 + 0^2} = 2630 \text{ KIPS}$$

$$F_{TOTAL} = 5362 \text{ KIPS}$$

$$F_{TOTAL} = 5297 \text{ KIPS WITHOUT BLIP}$$

$$F_{HIGH\ SPECIFIC\ NEW} = 2510 + 17 + 0 + 25 + 0 + \sqrt{65^2 + 50^2 + 25^2 + 80^2 + 13^2 + 25^2} = 2673 \text{ KIPS}$$

$$F_{LOW\ SPECIFIC\ NEW} = 2510 + 0 + 0 + 25 - 20 + \sqrt{65^2 + 50^2 + 25^2 + 80^2 + 13^2 + 25^2} = 2636 \text{ KIPS}$$

$$F_{TOTAL} = 5309 \text{ KIPS}$$

NOTE: EXAMPLE IS FOR ILLUSTRATIVE PURPOSES ONLY
THE ACTUAL LOADS CALCULATION METHODOLOGY IS MUCH MORE INVOLVED

Appendix 4.
Examples of Use of Statistical Analysis of SRB Pressure Transient History in Flight Safety Decisions

Excerpts from:

- **"STS-54 Pressure Perturbation Investigation PRCB Presentation," 4 February 1993**
- **"In-Flight Anomaly Summary" for STS-54 Right RSRM Chamber Pressure Spike**

SUMMARY OF FINDINGS

- SRM, HPM, FWC, AND RSRM MOTORS HAVE EXHIBITED PRESSURE VARIATIONS AFTER 50 SECONDS INTO MOTOR BURN TIME
  - MEASURED OCCURRENCES HAVE DIFFERENCES IN TIME AND MAGNITUDE
- PRESSURE PERTURBATIONS AFTER 50 SECONDS IS A GENERAL CHARACTERISTIC OF THE MOTOR BALLISTICS
  - PRESSURE VARIATIONS EXHIBITED WITH VARIOUS DESIGN, MATERIAL, PROCESS, VENDOR VARIATIONS; AS WELL AS COLD, NOMINAL, AND HOT CONDITIONS
  - EXISTED ON FLIGHT AND STATIC MOTORS WITH AND WITHOUT NOZZLE VECTORING DUTY CYCLES
- STS-54B MOTOR MET ALL PERFORMANCE REQUIREMENTS
  - PERFORMANCE WAS WITHIN K SIGMA BAND OF RSRM HISTORY
- NO RSRM POST-TEST HARDWARE CONDITION ASSESSMENTS HAVE BEEN ASSOCIATED WITH PRESSURE PERTURBATIONS
  - POST-FLIGHT HARDWARE CONDITION OF STS-54B ALSO WITHIN DATABASE

FS-54B PRESSURE PERTURBATION INVESTIGATION

SUMMARY OF FINDINGS (CONT.)

- NO UNIQUE DESIGN, MATERIAL, OR MANUFACTURING PROCESSING HAVE BEEN SHOWN CONNECTABLE TO PRESSURE PERTURBATIONS
- NUMBER AND DIVERSITY OF PRESSURE VARIATIONS SUGGEST A RANDOM COMBINATION OF SOURCES SUCH AS ACOUSTICS, SLAG PARTICLES, MIX-TO-MIX BURN RATE VARIATIONS, INSULATION AND PROPELLANT GEOMETRY CHANGES, NOZZLE VECTORING, PROPELLANT NONHOMOGENIETY, ETC.
- FREQUENCY OF HIGH MAGNITUDE OCCURRENCES HAS INCREASED SINCE STS-37 (RSRM-14)
  - 55% OF MOTORS (18 OF 33 MOTORS) HAVE EXHIBITED THIS PHENOMENON SINCE STS-37
  - DETAILED REVIEW OF MATERIAL AND FABRICATION CHANGES AND INSPECTION DATA ON ALL RSRM MOTORS HAS NOT IDENTIFIED ANY PARAMETERS THAT PROVIDE ANOMALOUS CONDITIONS
- PLAUSIBLE SCENARIO OF CASTABLE INHIBITOR ANOMALY WITH BORE BLOCKAGE (SCENARIO 1) IS BOUNDED
  - A CONSERVATIVE UPPER BOUND THRUST IMBALANCE OF 151 KLB (EXCEEDS THE CEI SPEC LIMIT OF 85 KLB IN THE 1-79 SEC TIME INTERVAL)
  - INTERNAL INSULATION IS DESIGNED TO ACCOMMODATE CASTABLE INHIBITOR FAILURE

STS-54B PRESSURE PERTURBATION INVESTIGATION

FLIGHT RATIONALE

- PRESSURE PERTURBATIONS CONCLUDED TO BE A GENERAL CHARACTERISTIC OF THE MOTOR BALLISTICS
  - FLIGHT PERFORMANCE HAS MET REQUIREMENTS FOR THE RSRM PROGRAM
- STS-55 HAS NO UNIQUE DESIGN, MATERIAL, FABRICATION HISTORY IDENTIFIABLE WITH PRODUCING PRESSURE PERTURBATIONS
- CONSERVATIVE UPPER BOUND OF SCENARIO INDUCING PRESSURE PERTURBATIONS (SPECIAL CAUSE OF FORWARD SEGMENT CASTABLE INHIBITOR SHEDDING) IS
  - THRUST IMBALANCE: 151 KLB
- WITH THE SHUTTLE SYSTEM CAPABILITY TO ACCEPT A 151 KLB THRUST IMBALANCE, STS-55 IS SAFE TO FLY

IN-FLIGHT ANOMALY SUMMARY
(CONTINUATION SHEET)

12. INVESTIGATION SUMMARY (continued): RSRM-29B occurrence is very low. This suggests that either the castable inhibitor comes off in large pieces or that a combined scenario (propellant flaw with bore blockage) is required.

In order to bound this scenario, a conservative approach was developed, where it was assumed that the higher pressure perturbation on RSRM-29B was due to a special cause of variation. To arrive at an upper limit thrust imbalance for this scenario, the following thrust imbalance data were used:

- Castable inhibitor loss exposing the propellant - 74 klb
- Bore blockage - 100 klb

RSS - 124 klb

This scenario is bounded by the amount of castable inhibitor that can be expelled out of the nozzle and the maximum propellant unbonded which adds surface area burning with higher pressure in addition to restricting the bore.

13. PROBLEM SOLUTION: In general, the occurrence of the pressure spike is not a concern for the following reasons:

1) A review of SRM, HPM, FWC, and RSRM motor pressure traces show that each type of motor has exhibited pressure variations after 50 seconds from ignition. The measured occurrences vary in time and magnitude. However, all pressure traces show the "blip" phenomenon and have remained within specification limits. All flight motor pressure perturbations greater than 4 psi have occurred in the 65- to 75-second burn time range. Pressure perturbations are characteristic of the motor ballistics and are exhibited over all the design, material, process and vendor variations. Pressure perturbations are observed with cold, nominal, and hot conditions and have existed on flight and static test motors with and without nozzle vectoring duty cycles. Assessment of flight history shows that the frequency and magnitude of pressure perturbations has increased subsequent to the STS-35 (RSRM-11) time frame.

2) Pressure trace data of flight motors exhibiting blips compare favorably to static test motors, showing excellent correlation. All flight motors are within the expected pressure range. RSRM-29B was within family of RSRM history and met all performance requirements.

3) A review of fabrication and associated inspection data found no shifts or trends that could contribute to pressure perturbations.

4) The observation of high magnitude pressure blips has increased in frequency since RSRM-14. Out of 33 motors, 18 have exhibited this condition.

IN-FLIGHT ANOMALY SUMMARY
(CONTINUATION SHEET)

13. PROBLEM SOLUTION (continued):

5) A statistical analysis of a conservative 3 sigma event (RSRM-29B was 2.3 sigma) shows that the maximum potential pressure perturbation is 18.6 psi. The thrust imbalance associated with that perturbation is 75 klb. The probability of one SRB having a spike event is 1.35×10^{-3} or one in 740 motors. The probability of a pressure spike occurring on both SRBs of a flight set is 1.8×10^{-6} or one in 550,000 flights. The probability of a pressure spike occurring on both motors at the same time is 1.8×10^{-8} or one in 55,000,000 flights.

All RSRM process and materials changes and variations that could contribute to the observed pressure perturbations are under review. Additional tests and analysis efforts have been initiated to understand material and process parameters that influence the generation of pressure perturbations.

- Material and process characterization tests on the castable inhibitor
- Additional TEM-10 instrumentation
  - Real Time radiography (RTR)
  - Infrared cameras
  - Additional accelerometers
  - Additional strain gages
  - High speed cameras
- Cold flow tests and computational fluid dynamics analyses

The results of these tests and studies will be used to define process or material corrective actions that could reduce pressure trace roughness.

The problem report has been deferred based on the following conclusions:

- It is concluded that pressure perturbations are a general characteristic of motor ballistics. Flight performance has not violated requirements for the RSRM Program.
- A review of the build records of all loaded RSRM flight motors found no unique design, material, or fabrication history that can be correlated with producing pressure perturbations. All motors are predicted to meet flight requirements.

IN-FLIGHT ANOMALY SUMMARY
(CONTINUATION SHEET)

13. PROBLEM SOLUTION (continued):

- Using the most probable scenario, a conservative 3 sigma thrust imbalance upper bound is 75 klb. The shuttle system is capable of accepting a 75 klb thrust imbalance.

(Reference PRCBD No. S052158C)

The IFA was closed on 03-19-93 with signatures obtained outside the board on PRCBD No. S044892E. The problem report has been closed for the next three flights or six months, whichever comes first. Deferred.

Appendix 5.
Comparison of Methods for Calculating the Effect of Pressure Perturbations on SRB Thrust

Comparison of methods for calculating the effect of pressure perturbations on SRB thrust.

SUMMARY:

1. **The NASA RSS solution to the SRB thrust equation is NOT conservative if the sources of variation in SRB thrust are correlated.**

2. **The RSS method of solution, which assumes symmetric distributions, is more conservative than propagating skewed (e.g.: lognormal) probability distributions for the existing pressure spike data.**

3. **The RSS example (based on 2 sample / second data) produces a higher (more conservative) total thrust than is indicated by analysis of the raw 12.5 sample / second data.**

4. **The correlation of maximum pressure peaks between left and right motors is more likely due to normal inter- and intra- motor pressure variations than to pressure spike variations associated with slag "sloshing" and ejection.**

NASA uses a Root-Sum-Squares (RSS) method to combine uncertainties in the terms of the SRB thrust equation NASA to determine the upper bound of thrust for calculating Factors of Safety. Two of the key assumptions in the RSS approach are independent sources of variation and symmetrically distributed variations. The extent to which these assumptions are not met, and the impact of not meeting them were examined by solving the SRB thrust equation by propagating uncertainty distributions (in Monte Carlo simulation).

The NASA RSS solution is NOT conservative if the sources of variation are correlated (not independent). The assumed factor of safety for the SRB thrust equation example (RSS) provided by NASA was 1.280. Using the same data but assuming a reasonable correlation between two terms of the SRB thrust equation resulted in a calculated factor of safety of 1.276. In the limiting case of all terms perfectly correlated the calculated factor of safety is 1.217.

The assumption of symmetrically (normally) distributed pressure spike variations resulted in a more conservative (higher) upper bound on thrust than the alternative lognormal distributions developed by F. Safie (MSFC) or those developed by SAIC for this analysis. In general, assuming a skewed distribution for the pressure spikes (blips) results in a slightly asymmetric total thrust distribution with a higher mean but a smaller 99.87% (one-sided upper) certainty bound than the normal distribution implied by the RSS solution. Since the factor of safety calculation is based on the 99.87% certainty bound, the asymmetric solutions result in a higher factor of safety than the symmetric (RSS) assumption. For the various distributions examined here, **the NASA RSS method is**

therefore more conservative than propagating skewed distributions which better reflect the actual distribution of the pressure spike data.

SAIC analyzed the 12.5 sample per second SRB pressure data by separating the inter-motor variations (mean pressure variations from motor to motor), the nominal intra-motor variations (normally distributed variations in pressure within each motor of relatively low amplitude), and the pressure spike variations (strictly positive relatively high amplitude variations above the nominal intra-motor population) for the 66 to 76 second period of interest. Straightforward analysis of this data indicated that **the NASA RSS example (based on 2 sample / second data) produces a higher (more conservative) total thrust than is indicated by the raw data.**

This analysis also found that there is a significant correlation in both inter- (0.42) and intra- (0.68) motor variation between the left and right motors, but little correlation in the pressure spike variations (0.265) between left and right motors. It has been noted that 6 of the 8 highest maximum pressure peaks occurred in the left and right motors on 3 flights. This lead to speculation that slag accumulation and ejection (the postulated cause for the high pressure spikes) may be related to flight dynamics or other mission-specific characteristics. The relatively low correlation between left and right motor pressure spike populations suggests that **the correlation between of max pressure peaks between left and right motors is more likely due to inter- and intra- motor pressure variations than to pressure spike variations associated with slag ejection.**

Discussion:

Most analyses of the SRB pressure spike phenomenon have focused on the effect of pressure spikes (blips) on SRB thrust, and the resulting change in the static load factor of safety. The static load factor of safety (FOS) is defined as the load at which the structure is expected to fail divided by the maximum plausible load to which the structure will be subjected. Determining the maximum plausible total SRB thrust is the essential element of these analyses. This analysis compares the current (RSS) method of determining maximum plausible thrust to the fully probabilistic method of adding distributions in simulation.

The current method combines the sources of SRB thrust variation by adding the square-root of the sum of the squares (root-sum-square -- RSS) of maximum plausible variations to the nominal thrust to find the maximum plausible thrust. It has been pointed out elsewhere that the underlying assumptions of the RSS process, notably the independence, symmetry, and equal probability of the variations, may have been violated. This analysis shows how the method of propagating uncertainty distributions can readily accommodate the violation of those assumptions, and illustrates the impact of these violations on the computed factor of safety.

Objectives:

This analysis has four objectives: (1) Illustrate the method of propagating uncertainty distributions and show its equivalence to the RSS method in the limit that RSS assumptions are valid. (2) Show how a violation of the RSS independence assumption affects the calculated factor of safety. (3) Determine whether there is any significant change in computed factor of safety when the underlying distributions in the thrust equation are not symmetric. (4) Examine the 12.5 sample / second data provided by NASA to determine whether there is any significant change in computed factor of safety compared to the thrust equation solutions.

Analysis and Results:

Objective 1:

Using the values in the example provided by NASA (Table 1), the RSS form of the thrust equation (Equation 1) yields 5,309,000 lbf as the 3-σ upper bound of total SRB thrust. A 1.28 factor of safety implies that the ultimate load (nominal failure point of the structure) is equivalent to 6,795,520 lbf thrust. This relationship is shown graphically in Figure 1.

Equation 1. RSS form of the SRB thrust equation:

$$F_{high} = F_{block} + \Delta F_{burnrate} + \Delta F_{PMBT} + \Delta F_{osc\ mean} + (\Delta F_{nom}^2 + \Delta F_{scale}^2 + \Delta F_{PMBT\ unc}^2 + \Delta F_{osc\ unc}^2 + \Delta F_{shape}^2 + \Delta F_{f/p}^2)^{1/2}$$

$$F_{low} = F_{block} + \Delta F_{burnrate} + \Delta F_{PMBT} + \Delta F_{osc\ mean} + \Delta F_{imb\ mean} + (\Delta F_{nom}^2 + \Delta F_{scale}^2 + \Delta F_{PMBT\ unc}^2 + \Delta F_{osc\ unc}^2 + \Delta F_{shape}^2 + \Delta F_{f/p}^2)^{1/2}$$

$$F_{total} = F_{high} + F_{low}$$

Note: Adding the 3-sigma upper bound values of F_{high} and F_{low} results in an F_{total} upper bound significantly higher than the 3-sigma upper bound on F_{total} (for F_{high} and F_{low} uncorrelated). It is equivalent to assuming that the variations in the high motor are perfectly correlated with the variations in the low motor. Since the uncertainty among terms for each SRB are treated as uncorrelated this may have been inadvertent, but it results in a very conservative estimate of total SRB maximum plausible thrust as shown in Table 1. In the example calculation provided by NASA it is noted: "EXAMPLE IS FOR ILLUSTRATIVE PURPOSES ONLY. THE ACTUAL LOADS CALCULATION METHODOLOGY IS MUCH MORE INVOLVED". If the "actual loads methodology calculation" differs significantly from the example, in particular, if the actual methodology does not simply add the upper bounds on high and low thrust to determine the upper bound on total thrust, then statements made in this analysis regarding the relative conservatism of the RSS solution are invalid. *Except where explicitly noted, all of the distributions shown in this analysis retain the conservative assumption of correlation*

between the high and low motors in order to keep the results comparable with the thrust equation RSS solution.

Figure 1. Relationship between RSS 3-sigma Thrust, Factor of Safety, and Ultimate Load

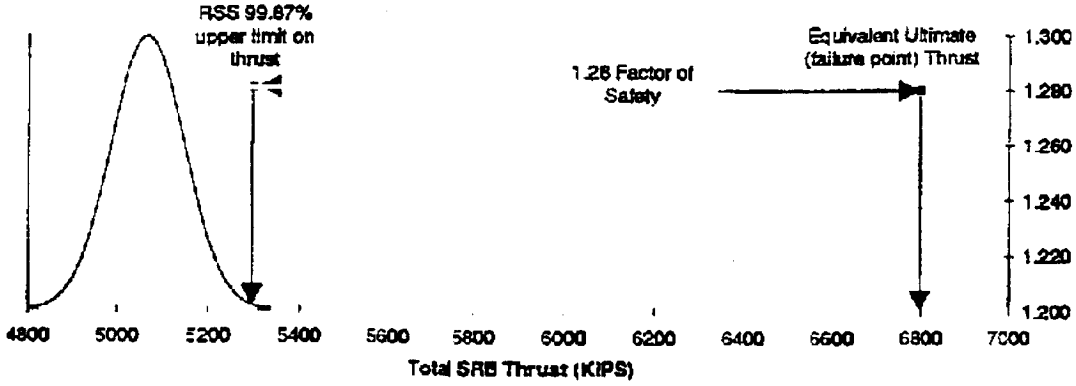


Table 1: Values Used in the SRB Thrust Equation (*1000 lbf)

Term	High Value	Low Value	Corresponding Sigma
F_{block}	2510	2510	N/A
$\Delta F_{t\ldots\ldots}$	17	0	N/A
$\Delta F_{\ldots\ldots}$	0	0	N/A
$\Delta F_{\ldots\ldots}$	25.1	25.1	N/A
$\Delta F_{\ldots\ldots}$		-20	N/A
$\Delta F_{\ldots\ldots}$	50	50	16.67
$\Delta F_{\ldots\ldots}$	65	65	21.67
$\Delta F_{\ldots\ldots}$	25	25	8.33
$\Delta F_{\ldots\ldots}$	25	25	8.33
$\Delta F_{\ldots\ldots}$	80	80	26.67
$\Delta F_{\ldots\ldots}$	13	13	4.33
Thrust Upper Bound	2673	2636	
			Corresponding Factor of Safety
F_{total} Upper Bound (as calculated)	5309		1.280
F_{total} Upper Bound (high & low uncorrelated)	5238		1.297
F_{total} Upper Bound (all terms fully correlated)	5583		1.217

Implicit in the RSS thrust equation is the concept of an underlying (normal) distribution of thrust with a mean equal to the sum of the non-RSSed terms, and standard deviation equal to 1/3 of the RSSed variation terms. This is the distribution is depicted in Figure 1 and in

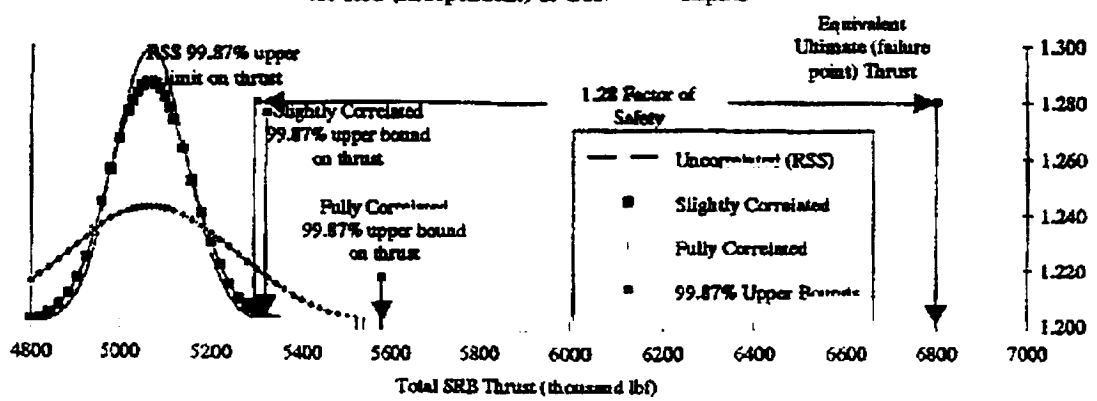
Figure 2 as the "Uncorrelated (RSS)" distribution. Despite the nomenclature "Uncorrelated", this distribution includes the correlation between the high and low motors implicite in the example RSS calculation for the SRB thrust equation. (See the note under Equation 1).

The RSS thrust equation can be arranged in a form suitable for propagating uncertainty distributions by grouping terms. Solving the distribution form of the thrust equation (using Monte Carlo simulation) results in a distribution identical to the one implied by the RSS thrust equation. The ability to produce a distribution with the same mean, standard deviation, and 3-sigma (99.87%) upper bound as the RSS method by propagating uncertainty distributions using Monte Carlo simulation demonstrates that method of propagating uncertainties and the RSS method are equivalent in the limit that the RSS assumptions of symmetry and independence are valid.

Objective 2.

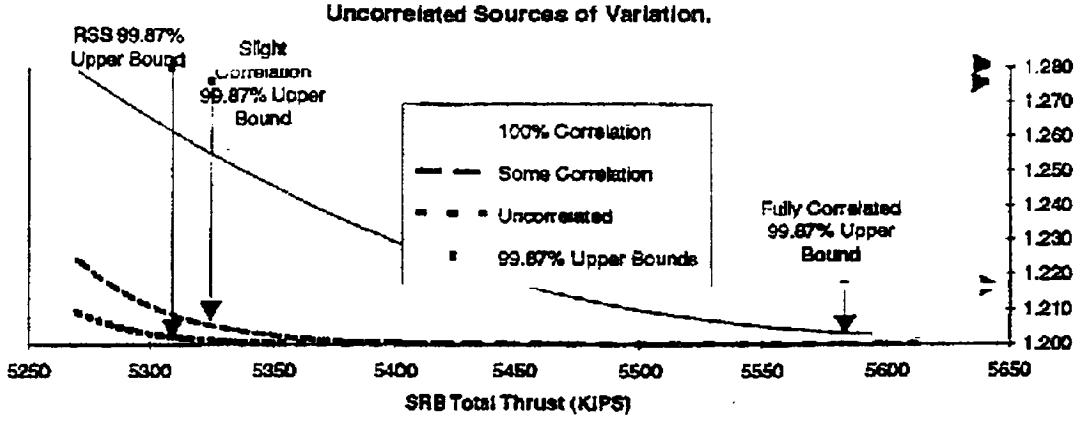
If two or more terms in the RSS thrust equation are known (or believed) to be correlated, then the RSS method does not produce a conservative result. While a rigorously correct derivation of the RSS thrust equation could be developed to handle correlated factors, the propagation method handles correlation quite easily, by specifying a correlation coefficient between two or more factors for the Monte Carlo simulation. Figure 2 shows the original (uncorrelated) total thrust distribution and the total thrust distribution which would result if two factors (F_{block} and ΔF_{shape}) were correlated (correlation coefficient = 0.75). The extreme case of non-independence, in which all factors in the SRB thrust equation are fully correlated is also shown. Figure 3 illustrates these relationships in greater detail by focusing on the upper tails of the distributions. The axis on the right hand side of the Figures shows the factor of safety associated with the 99.87% upper certainty bound on the distributions.

Figure 2. Relationship Between 3-Sigma Thrust, Factor of Safety, and Ultimate Load for RSS (Independent) & Correlated Inputs



The RSS solution to the thrust equation is clearly not conservative if the variation in the terms of the thrust equation are correlated.

Figure 3. Comparison of SRB Thrust Distributions for Correlated and Uncorrelated Sources of Variation.



Objective 3.

Most (if not all) of the analysts and reviewers of the SRB pressure "blip" data noted that there appear to be different sub-populations of pressure variations embedded in the data. It was almost universally noted that positive pressure blips were larger than negative "dips", and appeared to have a different physical root cause than symmetric random variations about the nominal pressure profile.

The RSS solution to the SRB thrust equation is incapable of handling asymmetric (skewed) variations. Implicit in the idea of RSSing variation terms is the demand that every positive pressure excursion is (on average) matched by some combination of negative pressure excursions, and vice-versa. Furthermore, the RSS method demands that the probability of all sources of variation occurring be equal. The observed pressure blips do not appear to occur with the same frequency as other random variations in the pressure profile, so it is likely that the source of the blips does not have the same probability as other random (and symmetric) variations.

Figures 4 through 8 depict the results of propagating the skewed pressure blip distributions developed by F. Safie of MSFC. While Safie's work provides some insight into the effect of segregating the population of pressure variations, he did not show the impact on total SRB thrust or factor of safety. To measure that impact we replaced the ΔF_{shape} term in the thrust equation with the distributions proposed by Safie. The results are uniformly higher factors of safety (smaller upper bounds on thrust).

Figure 4. Lognormal Distribution for Pressure Blips
All RSRMs

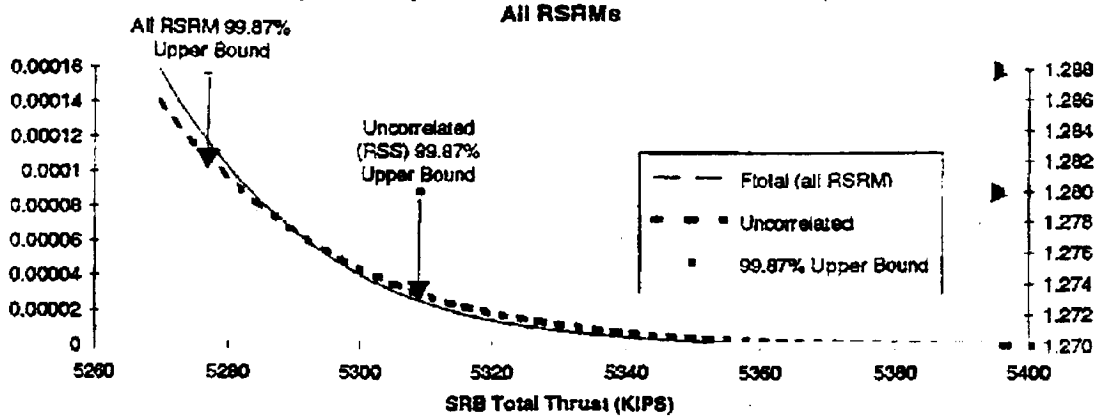


Figure 5. Lognormal Distribution for Pressure Blips
All RSRMs w/out Top 4

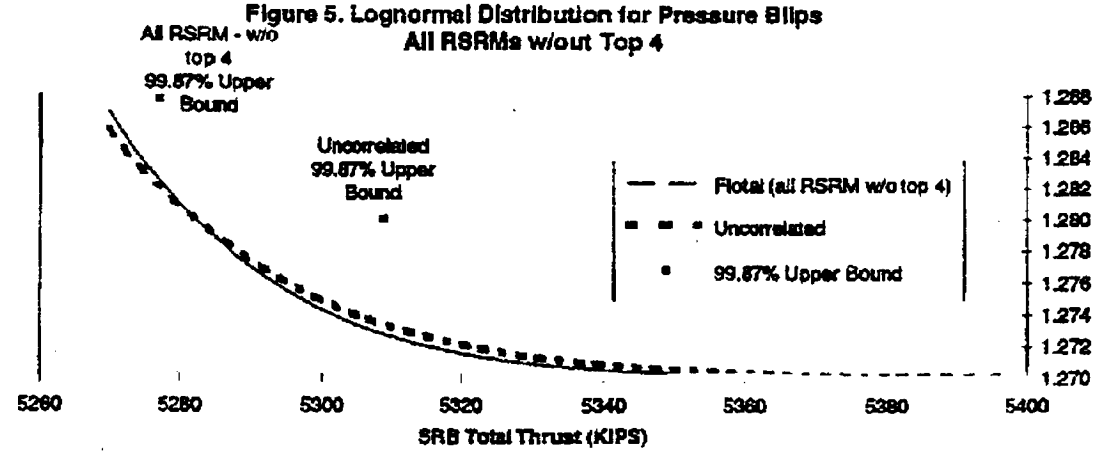


Figure 6. Lognormal Distribution for Pressure Blips
All WECCO

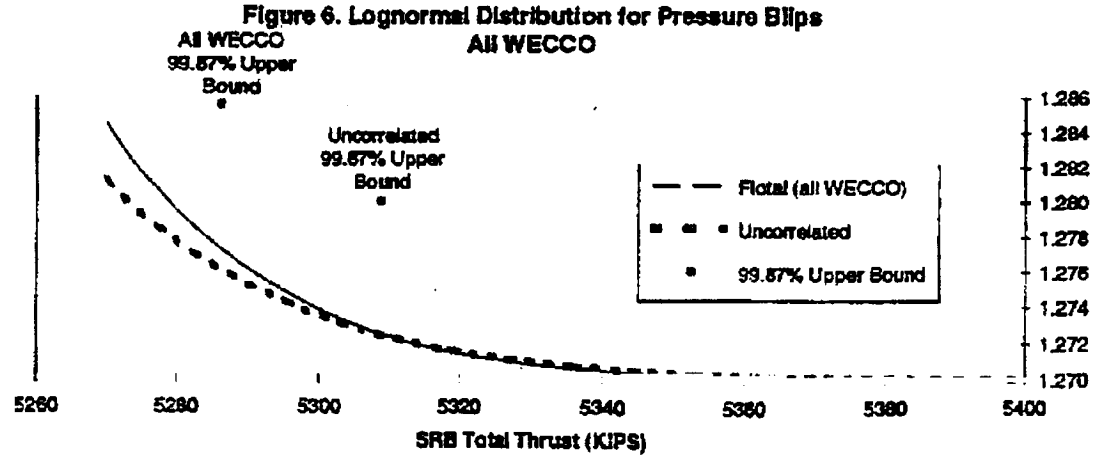


Figure 7. Lognormal Distribution for Pressure Blips
All WECCO w/outu Top 4

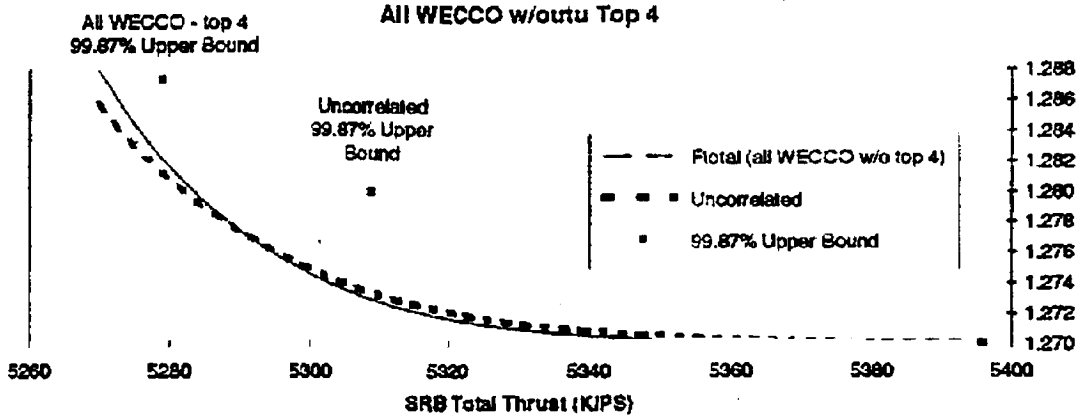
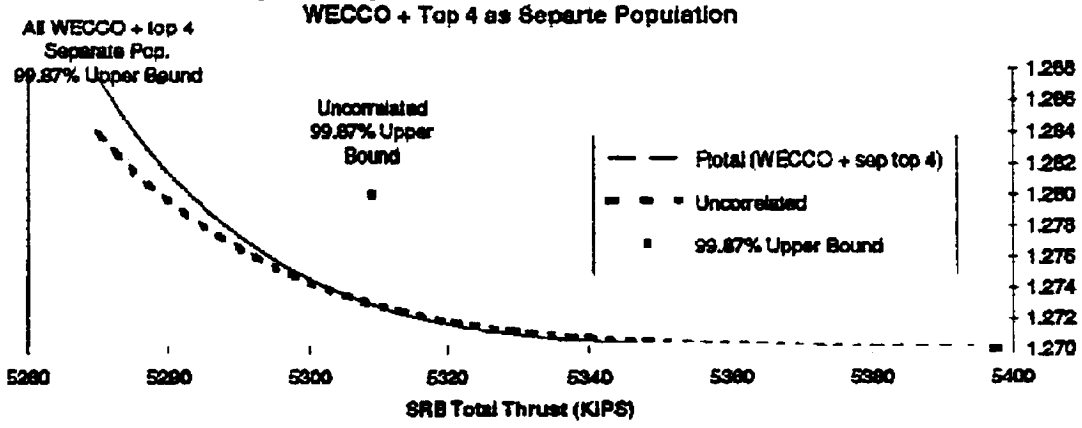


Figure 8. Lognormal Distribution for Pressure Blips
WECCO + Top 4 as Separte Population



Although the lognormal distribution is strictly greater than 0, the upper bound on thrust for these distributions is smaller than the upper bound associated with the normal distribution used to fit the same pressure blip data. This apparent anomaly is due to the fact that the lognormal distribution provides a closer fit to the pressure spike data than the normal distribution. The result on the overall SRB thrust distribution increase the probability density in the region between the mean and the 99.87% upper bound, shifting the mean higher but pulling the 99.87-th percentile closer in, resulting in a smaller upper bound on thrust and consequently, and higher factor of safety.

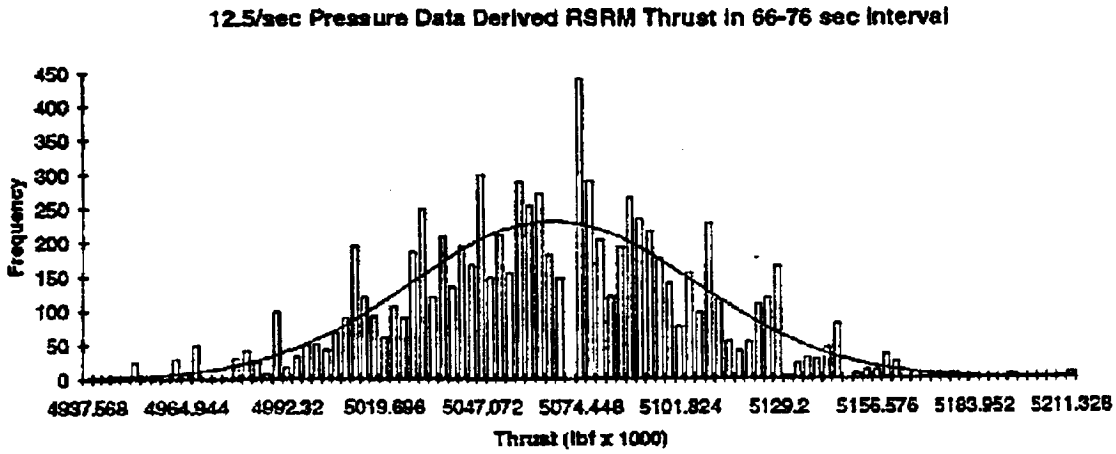
Objective 4.

It is not clear that the thrust equation captures all sources of uncertainty in SRB thrust, or that the values given to the terms of the equation (which were derived from 2 sample / second data) capture the same range as the 12.5 sample / second data. In principle, the thrust equation should capture the uncertainty in SRB thrust from a variety of sources, only one of which is observed variability in the SRB pressure profile. An important

"sanity check" on the thrust equation is to ensure that the maximum plausible thrust (99.87-th percentile) generated by the equation is at least as conservative as an upper bound on thrust generated from the pressure data alone.

SAIC examined the 12.5 sample / second data and developed a segregated data set which would allow an alternate approach to the SRB thrust equation to determine the "maximum plausible thrust" based only on variability in the data and uncertainty in converting pressure to thrust. In this approach, only the pressure variations during the 65 to 76 second interval were examined, since all physical mechanisms for the occurrence of the pressure "blips" are postulated to occur in that time frame. The data was segregated to examine motor-to-motor (inter-motor) pressure variations, symmetric variations about the nominal value in a given motor (intra-motor), and the skewed pressure variations associated with the pressure "blips". Figures 8 through 12 depict these distributions.

Figure 8. "Raw" Combined SRB Thrust Distribution Based on 12.5 Sample / Second Pressure Data



Note on Figure 8 that a normal curve based on the mean and standard deviation of the data is not a good fit The underlying data shown in the histogram appears to have a normally distributed component with a somewhat smaller mean than fitted curve, and an additional component for pressure spikes above the mean. SAIC found that an excellent fit to the data was given by resolving the data into three components: Normally distributed Motor-to-Motor variations in nominal pressure (Inter-Motor); Normally distributed variations within a motor (Intra-Motor); and Lognormally distributed pressure spikes remaining when the normally distributed Intra- and Inter- Motor variations were removed.

Figure 9. Inter-Motor (Motor to Motor) Variation in SRB Pressure

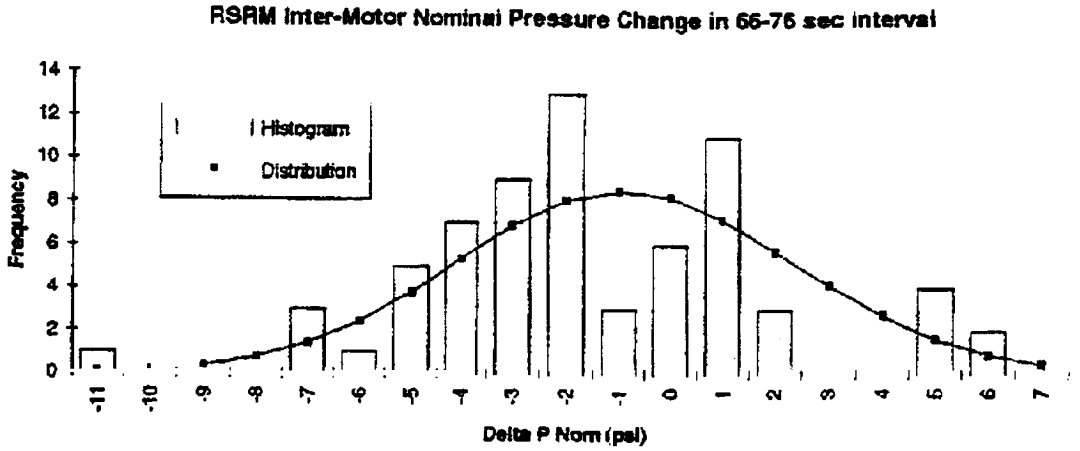


Figure 10. Inter-Motor Left / Right Pressure Differential

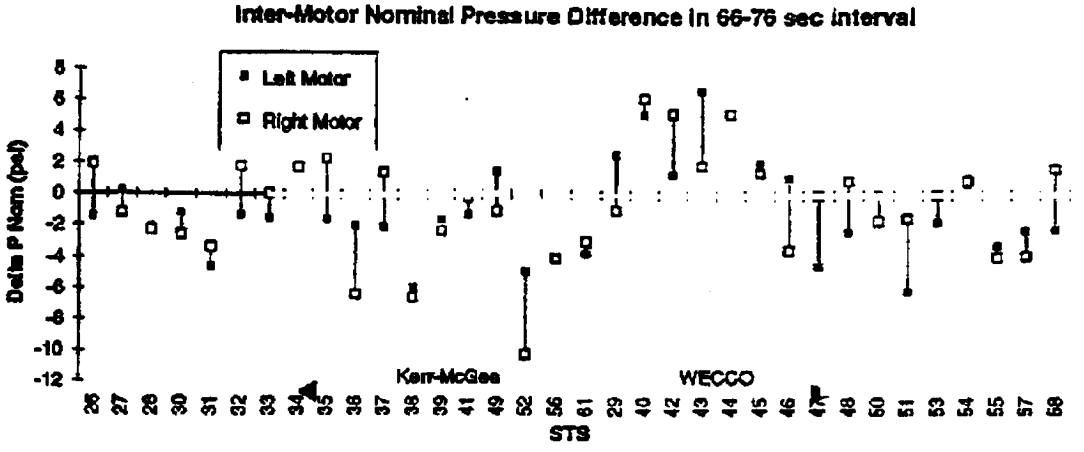


Figure 11. Maximum Pressure Excursions Adjusted for Inter-Motor Variation

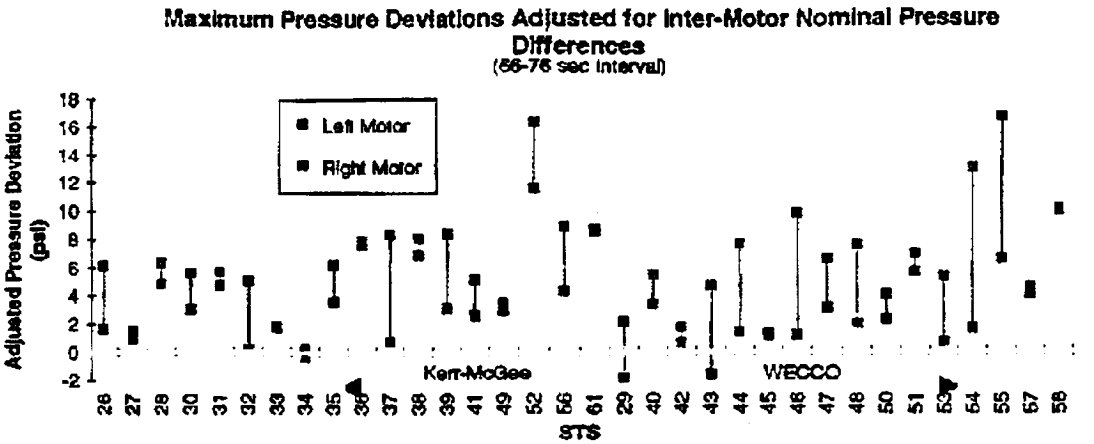


Figure 12. Nominal Intra-Motor Thrust Distribution Adjusted for Inter Motor Variation.

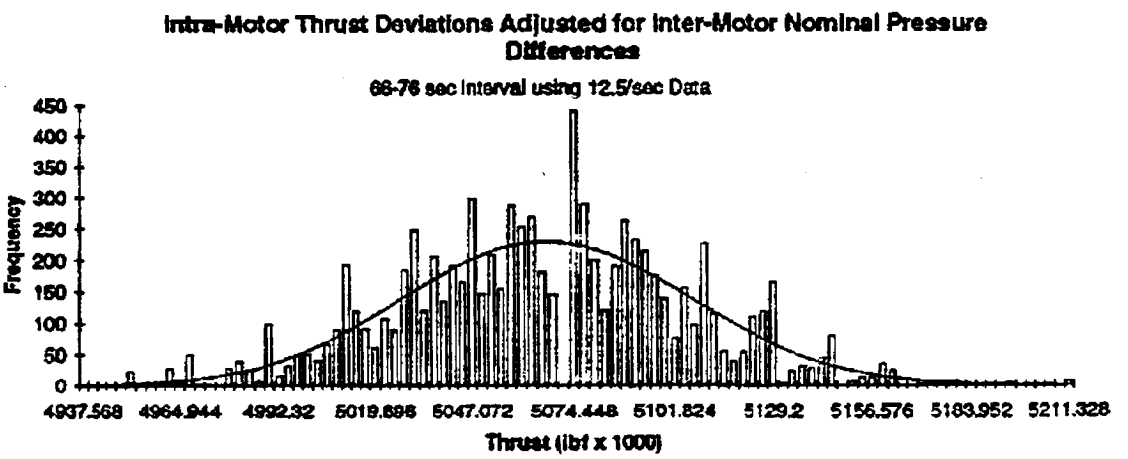
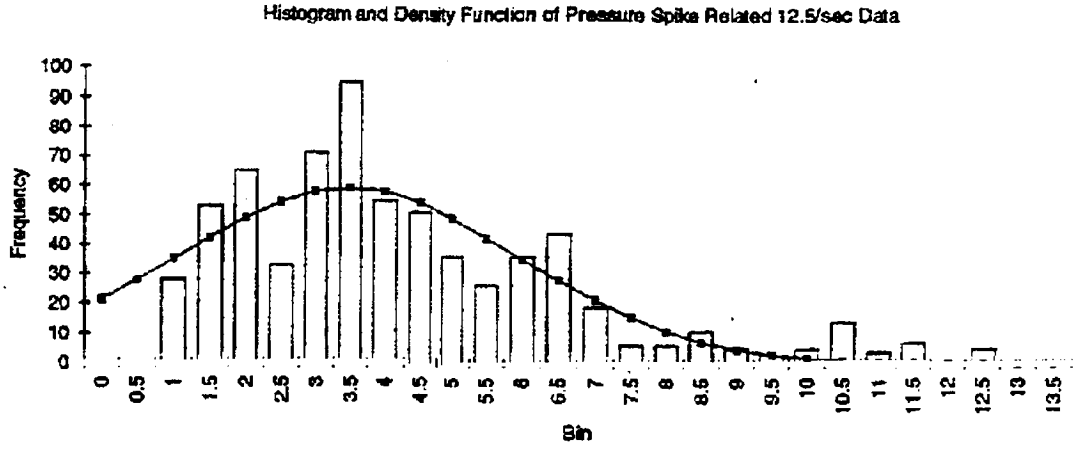


Figure 13. Pressure Spike Distribution After Adjusting for Inter- and Nominal Intra- Motor Variation.



Note that when inter- and nominal intra- motor variations are removed, the maximum pressure spike above the nominal pressure is 13.5 psi.

To ensure that the SRB thrust equation upper bound captured at least the variability in the pressure data a series of Monte Carlo simulations were performed. One set of simulations was based on a normal distribution using the mean and standard deviation of the "raw" pressure data. Since a normal distribution did not appear to fit the data particularly well, a second set of simulations was performed using the combined inter-motor, nominal intra-motor, and spike distributions described above. The results of these simulations, along with the other numerical results of this analysis, are summarized in Table 2.

Table 2. Summary of Numerical Results

Method of Calculation	Thrust Upper Bound	Corresponding Factor of Safety	Comments
Thrust Eqn, RSS. Example Data	5309	1.280	Benchmark - Defines ultimate equivalent thrust for all FOS calculations. Implicit assumption that high & low motor variations are fully correlated.
Thrust Eqn, Propagated. Example Data High & Low Correlated.	5310	1.280	Duplication of RSS results using propagation of uncertainties.
Thrust Eqn, RSS, Example Data High & Low NOT Correlated.	5238	1.297	Bulk of conservatism in RSS example is from tacit assumption that high & low are correlated.
Thrust Eqn, Propagated. Example Data High & Low NOT Correlated.	5240	1.297	
Thrust Eqn, Propagated, Example Data Block & Shape Correlated (0.75)	5325	1.276	Best guess at actual correlation of thrust equation terms except retains conservative assumption of high & low correlated.
Thrust Eqn, Propagated, Example Data All Terms Fully Correlated	5585	1.217	(Unreasonable) Worst Case Correlation
Thrust Eqn, RSS Solution, Example Data All Terms Fully Correlated	5583	1.217	(Unreasonable) Worst Case Correlation Further verification that propagation matches RSS for same assumptions.

Table 2. Summary of Numerical Results (continued)

Method of Calculation	Thrust Upper Bound	Corresponding Factor of Safety	Comments
Thrust Eqn. Propagated. Lognormal - all RSRM blips No Correlation (exc. high/low)	5277	1.288	Replace DFshape term in Thrust Equation with lognormal fit to all RSRM blips (Safie).
Thrust Eqn. Propagated. Lognormal - all RSRM blips w/out top 4 No Correlation (exc. high/low)	5277	1.288	Replace DFshape term in Thrust Equation with lognormal fit to all RSRM blips except top 4 (Safie).
Thrust Eqn. Propagated. Lognormal - all WECCO blips No Correlation (exc. high/low)	5286	1.285	Replace DFshape term in Thrust Equation with lognormal fit to all WECCO blips (Safie).
Thrust Eqn. Propagated. Lognormal - all WECCO blips w/out top 4 No Correlation (exc. high/low)	5279	1.287	Replace DFshape term in Thrust Equation with lognormal fit to all WECCO blips except top 4 (Safie).
Thrust Eqn. Propagated. Lognormal - WECCO blips + top 4 as separate population No Correlation (exc. high/low)	5284	1.286	Replace DFshape term in Thrust Equation with lognormal fit to WECCO blips & add top 4 as separate (normal) distribution w/ low probability (Safie).
12.5 Sample / Sec Data, Propagated, "Raw" data - normal distribution No Correlation (exc. high/low)	5215	1.303	Normal distribution fit to 12.5 sample / sec data in 66 - 76 second interval.
12.5 Sample / Sec Data, RSS, "Raw" data - normal distribution No Correlation (exc. high/low)	5214	1.303	Normal distribution fit to 12.5 sample / sec data in 66 - 76 second interval.
12.5 Sample / Sec Data, Propagated. SAIC separation of "Raw" data - normal inter- & intra- motor; lognormal spike No Correlation (exc. high/low)	5280	1.287	Separate 12.5 sample / sec data from 66 - 76 second interval into normal inter- and intra-motor distributions + lognormal spike distribution.
12.5 Sample / Sec Data, Propagated, SAIC separation of "Raw" data - normal inter- & intra- motor; lognormal spike Actual Right/Left Correlation Coefficients	**5251**	**1.294**	**SAIC's best estimate of actual Factor of Safety based on variation in observed 12.5 sample/sec data in 66 - 76 second interval. The thrust equation conservatively bounds this value.**

The RSS solution to the SRB thrust equation appears to provide a conservative upper bound on thrust relative to every reasonable alternative formulation examined, with the important exception of correlation among the terms of the equation. It is recommended that NASA identify the extent to which the terms in the thrust equation are correlated, and

incorporate a means for dealing with correlation when calculating maximum plausible thrust and factors of safety.

The thrust equation produces conservative upper bounds on thrust, and therefore reasonably conservative factors of safety, primarily because of the implicit assumption that the thrust variation in the high and low motors is fully correlated. Since the measured correlation coefficient between right and left motors is 0.63, the tacit assumption of 100% correlation is not excessively conservative.

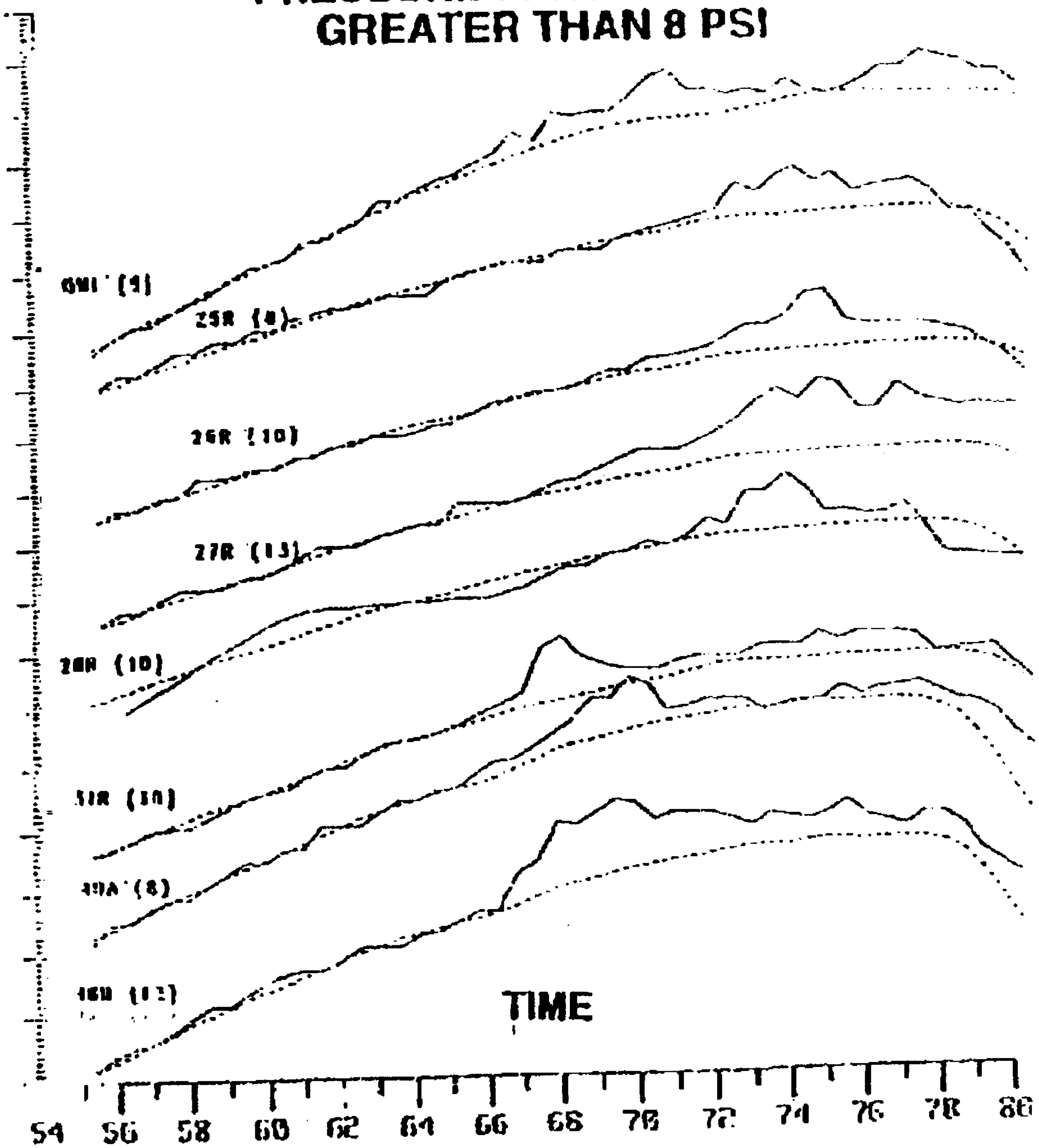
Appendix 6.
SRB Pressure Plots Used in Independent Statistical Analysis (excerpt from "Solid Rocket Booster Chamber Pressure Perturbation Review Committee Presentation to NASA," 14 January 1994)

Figure 15

RSRM FLIGHT MOTOR PRESSURE HISTORY BY AP VENDOR
(60 FLIGHT MOTORS AT A COMMON BURN RATE AND TEMP)

11

PRESSURE PERTURBATION GREATER THAN 8 PSI



Appendix 7.
Methodology for Determining Minimum Required External Tank Structural Safety Factor (excerpt form "External Tank Evaluation of RSRB Pressure Perturbation," 6 January 1994.

Key Design Criteria

	LWT
• S.F. General Loads	
- Ult	1.25 - 1.40 ← contract spec same as Vol X
- Yield	1.10
• Proof Test Basis	
- Life Factor	1.05 ← 101% to demo of mission lives
- FTR 2219	1.10
- Flight Ullage	Max Op.
• Stabilizing Pressure	
- S.F. Relieving	1.00
- P/L LO2 Fill and Drain	0.0 - 1.7 psig
- LH2 Fill and Drain	0.0 - 6.2
- TPS Enhancement (LH2)	21.6 psid

fracture toughness ratio

Combined Loads

K1(L well defined) + K2(L thermal) + K3(L pressure) + K4(L dynamic)
K1 = 1.25 for conditions when the term is additive to the algebraic sum
K2 = 1.40 for conditions when the term is additive to the algebraic sum, except that K2 = 1.25 for LH2 aft dome stability ← orig 2 SRBs attached
K3 = 1.25 for the ET main propulsion tanks when the term is additive to the algebraic sum
K4 = 1.40 for aerodynamic loads and dynamic transient loads.

} revised FOS for last 50 missions

LWT Variable Safety Factor

- Standard weight external tank was designed using a 1.40 Factor of Safety for general structure
- LWT design used a variable safety factor in the interest of saving weight for a previously qualified very similar structure
- A portion of any safety factor requirement can be allocated to load uncertainty; the remainder to many other uncertainties; eg material properties, tolerances, temperatures, analysis methods, etc.
- The portion of the factor-of-safety between 1.25 and 1.40 was considered appropriate to the load uncertainties
- Loads due to nominal thrust, pressure, and inertia were treated as well understood and used to define "static" or "well understood" load cases. Dynamic forces (other than nominal thrust/weight) and aero forces (other than nominal drag) were treated as not-well-understood
- Internal loads were calculated from the "limit" and "static" cases as:

$$F_{int} = 1.25\,(\text{static}) + 1.40\,(\text{Limit} - \text{Static})$$

- For flight times near SRB staging and thereafter an estimated mix of "well-understood" and "not-well-understood" loads was used per flight regime. The "mixed safety factor approach was supplanted with an appropriate fixed but reduced factor approach for these times of flight

Variable Safety Factor - History

- During the IVBC-3 analysis update, new Hi-Q load cases (thru M=1.8) were developed and we found that a 1.40 factor-of-safety could be imposed with no negative margins. Since this simplified both analysis and reporting, a 1.40 FS was used (Too complicated to consider wind induced loads, etc. in 1st 60 seconds - i.e. left aerodynamic regime as "not well defined" or FS 1.40)
- Just prior to "Return-To-Flight" the FRR Hi-Q indicator assessment analysis was extended to M = 2.2 - with results showing negative margins. Analyses showed 75% "well understood" and 25% "not-well-understood" loads at M = 2.2 as a conservative estimate. This resulted in a 1.29 FS requirement
- We interpreted this to apply also to pre-existing Mach 2.2 "BA" cases that had been previously analysed with a 1.26 SF (viz, BA302)

booster acceleration

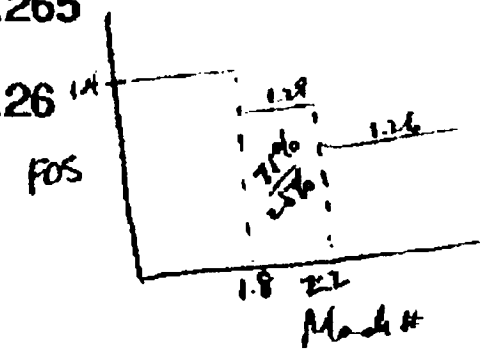
Heavy wt tank designed to ultimate load FOS 1.4

light wt - mixed FOS

MY NOTE: It is no guarantee we take advantage of conservatism in Hi-Q regime gotten from using FOS=1.40. Now, write some new concerns we would be better off with backing out the true failure prob. rather than just using FOS.

Required Factor-of-Safety History

		SWT	LWT	IVBC-3
Prelaunch		1.4	Mixed	Mixed
Liftoff		1.4	Mixed	1.4
High-Q	Mach ≤ 1.8	1.4	Mixed	1.4
	Mach > 1.8	N/A	N/A	1.29
BA	Mach ≤ 2.2	1.4	1.26	1.29
	Mach > 2.2	1.4	1.26	1.26
Pre-Sep		1.4	1.26	1.26
Post-Sep		1.4	1.265	1.265
OA		1.4	1.26	1.26
OE		1.4	1.26	1.26
AB	Time ≥ 128 & ≤ 260 Sec	1.4	1.265	1.265
AB	Time ≥ 260 Sec	1.4	1.26	1.26



- The yield factor-of safety is 1.1 for all regimes
- Factor-of-safety for relieving loads is 1.0
- Factors-of-Safety for tank pressures are 1.25 for LWT; 1.40 for SWT

LWT Variable Safety Factor

Percent "Well-understood"	Percent "Not -well-understood"	Safety Factor Required
100	0	1.250
95	5	1.26
90	10	1.265
85	15	1.27
75	25	1.29
50	50	1.325
25	75	1.363
10	90	1.385
0	100	1.40

External Tank Load Requirements

- Baseline (708 Cases)
  - Prelaunch - 94 cases
  - Liftoff - 353 cases
  - Maximum Dynamic Pressure (High-Q) - 206 cases
  - Maximum Acceleration with SRB's (BA) - 10 cases
  - Pre SRB Staging (PR) - 10 cases
  - Post SRB Staging (PO) - 9 cases
  - Maximum Acceleration with SSME's (OA) - 6 cases
  - Orbital End Burn (OE) - 6 cases
  - Aborts (AB) - 24 cases
- Flight Unique Data
  - 2 SRB thrust oscillation conditions for LO2 tank bottom and sidewall pressure assessment
  - 4 SRB thrust spike conditions for LO2 tank and intertank assessment

SAFETY OF THE THERMAL PROTECTION SYSTEM OF THE SPACE SHUTTLE ORBITER: QUANTITATIVE ANALYSIS AND ORGANIZATIONAL FACTORS

Phase 1:

RISK-BASED PRIORITY SCALE AND PRELIMINARY OBSERVATIONS

by

M. Elisabeth Paté-Cornell*
Department of Industrial Engineering and Engineering Management
Stanford University
and
Paul S. Fischbeck**
Department of Engineering and Public Policy
and Department of Decision Sciences
Carnegie-Mellon University

REPORT TO
THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Cooperative Research Agreement No. NCC 10-0001
between Stanford University and NASA (Kennedy Space Center)

* Associate Professor

** Assistant Professor, Commander USNR. Formerly: Graduate Research Assistant, Department of Industrial Engineering and Engineering Management, Stanford University.

C4

TABLE OF CONTENT

			Page
SUMMARY			6
Section 1:		INTRODUCTION	7
	1.1	Objectives of the overall project	9
	1.2	Scope of the work in Phase 1	13
	1.3	Gathering of information and technical points of contact	14
Section 2:		BACKGROUND INFORMATION	16
	2.1	System description	16
	2.2	Life cycle and maintenance operations	21
		2.2.1 Tile manufacturing and installation	21
		2.2.2 Flight profile loading	22
		2.2.3 Tile maintenance procedures	24
	2.3	Failure history: incident recording and data bases	26
		2.3.1 Failure history and incident recording	26
		2.3.2 Data bases	37
Section 3:		DESCRIPTION OF THE PRA MODEL FOR THE TILES	39
	3.1	Susceptibility and vulnerability	39
	3.2	Definition of min-zones	43
		3.2.1 Debris classification	44
		3.2.2 Burn-through classification	47
		3.2.3 Secondary tile loss classification	49
		3.2.4 Functional criticality classification	51
		3.2.5 Debonding due to factors other than debris impact	51
	3.3	PRA model: definition of variables	57
	3.4	Initiating event: initial debris impact on one tile only (D=1)	58
	3.5	Initiating event: initial debris impact on several tiles (D=d)	61

			Page
	3.6	Initiating events: debonding due to factors other than debris	63
	3.7	Additional information and data	64
Section 4:		ILLUSTRATION OF THE MODEL	72
Section 5:		EFFECTS OF ORGANIZATIONAL FACTORS ON TPS RELIABILITY: MAIN PRELIMINARY OBSERVATIONS	80
	5.1	Errors and risks	80
	5.2	Preliminary observations	82
		5.2.1 Time pressures	82
		5.2.2 Liability concerns and conflicts among contractors	83
		5.2.3 Turnover among tile technicians and low status of tile work	84
		5.2.4 Need for more random testing	85
		5.2.5 Contribution of the management of the ET and the SRBs to TPS reliability	86
Section 6:		CONCLUSIONS	87
Section 7:		REFERENCES	89
Section 8:		APPENDICES	
	8.1	Appendix 1: Organizational Extension of PRA Models And NASA Application (M. E. Paté-Cornell, PSA'89)	A-1
	8.2	Appendix 2: Data bases for tile performance	A-11

FIGURES

		Page
Figure 1:	The Space Shuttle Orbiter	17
Figure 2:	The thermal protection system (TPS) for OV 103 (Discovery) and OV 104 (Atlantis)	18
Figure 3:	The black tiles (all vehicles)	20
Figure 4:	The tile system	21
Figure 5:	Histogram of tile damage due to debris	31
Figure 6:	Accumulated major debris hits (lower surface) for flights STS-6 through STS-32R	33
Figure 7:	The tile system and bond problems	34
Figure 8:	Event diagram: failure of the TPS leading to LOV	41
Figure 9:	Event tree of LOV due to TPS failure	42
Figure 10:	Partition of the orbiter's surface into three types of debris zones (index: h)	45
Figure 11:	Partition of the orbiter's surface into three types of burn-through zones (index: k)	48
Figure 12:	Partition of the orbiter's surface into two types of secondary tile loss zones (index: l)	50
Figure 13:	Components and systems location	52
Figure 14:	Hydraulic system components and line locations	53
Figure 15:	Partition of the orbiter's surface into three types of zones of functional criticality (index: j)	54
Figure 16:	Four major debond problem types	56
Figure 17:	Tile workmanship errors	65
Figure 18:	Ascent debris trajectory simulation (side view)	67
Figure 19:	Ascent debris trajectory simulation (plan view)	68
Figure 20:	Thermal measurements of the orbiter's surface (bottom view)	69

		Page
Figure 21:	Measurements of temperatures and pressures on the orbiter's surface (bottom view)	70
Figure 22:	Re-entry thermal analysis of lost tile cavity	71
Figure 23:	Partition of the orbiter's surface into 38 main-zones (index: i)	73
Figure 24:	Relative risk of LOV due to debris-initiated TPS damage	78
Figure 25:	Relative risk of LOV due to debonding type TPS damage	79
Figure 26:	Relative risk of LOV due to both types of TPS damage	79

TABLES

		Page
Table 1:	Summary of orbiter flights and debris damage	30
Table 2:	Probabilities of debris hits in different areas shown in Figure 10	46
Table 3:	Probabilities of tile loss due to debris in different areas shown in Figure 10	47
Table 4:	Probabilities of burn-through due to tile loss in in areas shown in Figure 11	47
Table 5:	Probabilities of losing adjacent tiles due to initial tile loss in areas shown in Figure 12	49
Table 6:	Probability of LOV conditional on burn-through in functional criticality areas shown in Figure 15	51
Table 7:	Structure of the indices of the min-zones shown in Figure 22 and Table 8	72
Table 8:	Identification of min-zones and their contribution to the probability of LOV	74
Table 9:	Probabilities of Loss of Vehicle due to tile failure initiated (1) by debris damage and (2) debonding caused by factors other than debris, for each min-zone, and each tile in each min-zone	76
Table 10:	Risk-criticality factor for each tile in each min-zone	77

SUMMARY

This report describes the first phase of a study designed to improve the management and the safety of the black tiles of the Space Shuttle orbiter. This study is based on the coupling of a probabilistic risk assessment (PRA) model and relevant organizational factors. In this first-phase report, a first-order PRA model is developed and used to design a risk-based criticality scale combining the probabilities and the consequences of tile failures. This scale can then be used to set priorities for the maintenance and gradual replacement of the black tiles.

A risk-criticality index is assessed for each tile based on its contribution to the probability of loss of the vehicle. This index reflects the loads to which each tile is subjected (heat, vibrations, debris impacts etc.) and the dependencies among failures of adjacent tiles. It also includes the potential decrease of tile capacity caused by imperfect processing (e.g., a weak bond), and the criticality of subsystems exposed to extreme heat loads at re-entry in case of tile failure and burn-through. Using this model and some preliminary data, it is found that the (mean) probability of loss of an orbiter due to failure of the black tiles is in the order of 10^{-3} per flight, with about 15% of the tiles accounting for 80% of the risk. One of the report's key findings is that not all the most risk-critical tiles are in the hottest areas of the orbiter's surface; some are in zones of highest functional criticality (see Figure 23).

Management factors that can affect tile safety are identified as: (1) time pressures that increase the probability of cutting corners in processing; (2) liability concerns and conflicts among contractors, which affect the flow of information; (3) the low status of the tile work and the turnover among tile technicians, which may increase the work load and decrease its quality; (4) the need for more random testing to detect imperfect bonds and to monitor the evolution of the system over time; and (5) the handling of the external tank and the solid rocket boosters whose insulations constitute a major source of the debris that could hit the tiles at take-off.

Safety of the Thermal Protection System of the Space Shuttle Orbiter: Quantitative Analysis and Organizational Factors

Phase 1:

Risk-based priority scale and preliminary observations

Section 1:

INTRODUCTION

The National Aeronautics and Space Administration (NASA) manages many aspects of the Space Shuttle Orbiter program under tight resource constraints: time, money, human resources, personnel and management's attention, etc. The maintenance of the orbiter's Thermal Protection System (TPS) is an example of operations that must reckon with these limitations. The processing of the tiles between flights is labor intensive and time consuming and, because it is often on the critical path to the next launch, the work has to be done under sometimes severe time constraints. Although great attention is dedicated to the tile work, its quality is occasionally affected by this demanding schedule. The importance of the tiles varies according to their location on the orbiter's surface. Over some areas of the orbiter's surface, several tiles could be lost without causing major damage or risking the lives of the crew; in other areas the loss of a single tile could be catastrophic. This report shows that the contributions of different tiles to the overall probability of failure (defined here as "risk-criticality") vary widely according to their locations on the orbiter's surface. A large percentage of the probability of loss of vehicle (LOV) due to failure of the orbiter's TPS can be attributed to a small fraction of the tiles. Because there will always be resource constraints, *setting priorities* is a first critical step towards ensuring that the most risk-critical tiles receive maximum care and quality control so as to minimize the probability of failure.

The level of risk-criticality of a tile depends on several factors and not exclusively on the maximum heat load (temperature and duration) to which it is subjected. These factors include: (1) the heat loads, (2) the location of the tile with respect to possible trajectories of debris (e.g., pieces of insulation from the external tank (ET) and the solid rocket boosters (SRBs)), (3) the vibrations and aerodynamic forces, and (4) the criticality of the subsystems located directly under the aluminum skin of the orbiter. Failure of a single tile located directly over one of the most critical systems (such as the avionics, fuel cells, or hydraulic lines) is likely to cause a LOV even though these tiles are not exposed to the maximum heat loads. By contrast, severe tile damage next to the base of a wing has been survived in past missions. Therefore, the loads and consequence factors must be combined to estimate the probability of failure and to determine the risk-criticality of each tile.

A tile fails because the *loads* on it reach values that exceed its *capacity*. Understanding both factors, loads and capacities, is thus critical to the quantification of the risk associated with the TPS. The capacities vary considerably among individual tiles because of differences in installation conditions and procedures. For example, inspections have shown that several tiles have been installed with bonding on 10% only of the contact surface. In addition, the capacities of some tiles have decreased over time because of chemical reactions of the bond with some of the water proofing agents used on the orbiter. Similarly, the loads on the tiles are not uniform. In addition to expected loads of heat, vibrations, and aerodynamic forces, a tile may also be subjected to unexpected loads caused by debris impacts. The source of most of the debris is poorly-installed and maintained insulation on the ET and the SRBs. Therefore, both loads and capacities can be greatly affected by a variety of possible human errors.

Some of these errors can be traced back to weak organizational communications, misguided incentives, and resource constraints, which in turn, can be linked to the rules, the structures, and the culture of the organization (Paté-Cornell

and Bea, 1989; Paté-Cornell, 1990). Efficiency of the risk management process for the TPS requires an integrated approach (National Research Council, 1988.) Considering only organizational solutions or only technical solutions to minimize the risk of failure would be counterproductive and wasteful. Furthermore, each individual system cannot be evaluated and managed independently. The performance of the ET and SRBs affects the reliability of the tiles which, in turn, affects the performance of the subsystems that they protect from heat loads. Therefore, when setting priorities, the management teams for the ET and SRBs must account for the potential detrimental side effects of their procedures on the orbiter's TPS. By tracing back, even roughly, the location of the insulation on the ET and SRBs that could hit the most risk-critical spots on the orbiter's surface, it may be possible to identify the spots that should be given top priority.

1.1 Objectives of the overall project

The objective of this study is to provide recommendations to improve the tiles management at Kennedy Space Center (KSC), Florida, based on the development and extension of a Probabilistic Risk Analysis model (PRA) for the TPS of the Space Shuttle Orbiter with emphasis on the *black tiles.* The approach is to include in the analysis not only *technical aspects* that are captured by classical PRA (for example, resistance of the tiles to debris impact), but also the *process* of tile maintenance (for instance, when and how are the tiles tested) and the *organizational procedures and rules* that determine this process (see Appendix 1: Paté-Cornell, 1989.) The question is whether these organizational factors affect the reliability of the tiles, and if they do, to what extent. Linking the PRA inputs to some aspects of the process and the organization allows addressing the often-raised question that PRA, although it captures human errors, is of little help when considering more fundamental managerial and organizational problems. This model is designed to allow management to set priorities in the allocation of limited resources in a continuous effort to improve the reliability of the Space Shuttle. The method thus allows for a global approach to risk management, involving technical as well as organizational

improvements, while accounting for the uncertainties about the system's properties and human performance. In cases where the problem is sufficiently well defined, one can then assess (even if only coarsely) the corresponding increase of reliability.

Uncertainties about the performance of a complex system such as the TPS of the Space Shuttle can be at first described by its probability of failure (first-level uncertainties). When computing this probability, one faces uncertainties about the probabilities of the basic events including technical failures of individual components and human errors. These uncertainties can be described by placing probability distributions on the inputs, then computing the resulting uncertainty of the overall failure probability (second-level uncertainties). The role and importance of these second-level uncertainties depend on the intended use of the study. PRA can generally support two types of decisions: (1) whether or not a system is safe enough for operation on the basis of a chosen safety threshold or other acceptance criteria, and (2) (the main objective of this study) how to allocate scarce resources among different subsystems on the basis of risk-based priorities in order to achieve maximum overall safety. The depth of the supporting risk analysis must be adapted to the decision to be made.

In the first type of decision, where one is trying to decide if a system is safe enough, it is important to describe the result of the risk assessment not only by a point estimate of the failure probability but by a full distribution of this probability reflecting all the uncertainties of the input values. Second-order uncertainties, which are particularly critical for repeated operations, become important because they give the decision makers an indication of the accuracy of the analysis. A different launch alternative may be preferred if, for example, the mean probability of mission failure is less than one in a thousand but can take values as high as one in fifty. Note however that *the* overall failure probability per operation is the mean of that distribution.

In the second type of decision, where the objective is an optimal allocation of resources, the priority ranking has to be based on a single point estimate for the probability of failure. For optimality reasons, the mean of the distribution of the failure probability is the relevant characteristic. In this case, critical factors are, first, the relative values of the probabilities of mission failure associated with failure of each component, and second, the variations of these relative probabilities with additional units of resources (e.g., time). The combination of these two factors then allows giving priority to the components for which more resources will bring the greatest increase of safety.

In this study, we construct first a priority scale for the black tiles based on our current estimates of the means of the partial failure probabilities, i.e, the mean probability of LOV associated with the potential failure of each tile (first-order PRA). An analysis of the second-order uncertainties may change the priorities if they change the means of these partial failure probabilities. Across subsystems (e.g., tiles versus main engines), the uncertainty of the failure probabilities may vary widely because the failure modes involve a spectrum of basic events whose probabilities are known with different degrees of uncertainty. In this case, full analysis of uncertainties may well change the means themselves and the optimal resource allocation. Within a given subsystem, such as the tiles, the inputs of the analysis for the different elements (e.g., the initiating events) are generally of similar nature and the variations of uncertainties may be less important. Yet, uncertainties about extreme values of the heat loads clearly vary according to the location of a tile on the orbiter's surface. Furthermore, the probabilities of failure (and associated uncertainties) of the subsystems located directly under the skin given a loss of tile(s) and burn-through vary widely. Further study should therefore investigate the effect of second-order uncertainties to determine their impact on the resource allocation.

Our work on this problem is divided into two separate phases. The first phase, which is presented in this report, involves the development and illustration of

a first-order PRA model for the black tiles of the TPS based on a probabilistic analysis of different failure scenarios. In this analysis, we use mean probabilities to construct a risk-criticality estimate for each tile and to establish a scale of priorities for management purposes. Key features of this model are the *dependencies of failures* among adjacent tiles, and between failures of tiles in specific TPS zones and failures of the subsystems located in these zones under the orbiter's aluminum skin. The analysis thus relies on a *partitioning of the orbiter's surface* (1) among zones of temperature, debris, and aerodynamic loads, and (2) among critical system locations. For each tile, we compute a *risk-criticality* factor that represents its contribution to the overall risk of orbiter failure due to TPS failure accounting both for loads (*load-criticality*) and failure consequences at the location of the tile (*functional criticality.*)

The second phase of the work will involve refinement and implementation of the model, including (1) an analysis of (second-order) uncertainies about probabilities in order to determine if these uncertainties can affect management priorities, and (2) organizational extensions. The organizational extensions involve identification and evaluation of the mechanisms by which potential problems occur, are detected, and can be corrected. This second phase will thus involve a study of the maintenance process accounting for its ability to detect and correct past mistakes (weak tiles), ensure satisfactory quality control of the current work, and track the possibility of weakening of the TPS over time. The objective of Phase 2 will be to identify, with the help of experts, the organizational roots of technical and human problems and to make recommendations for possible improvements. The PRA model will be used to assess the relevance of these factors to the reliability of the black tiles and the effectiveness of proposed solutions.

In this study, the PRA model is not an end in itself, but a tool designed to assess specific management practices. The level of detail of the analysis is set with this goal in mind. One key limiting factor in this effort is the unavailability of precise

values for the probabilities of failure of the subsystems located under the orbiter's skin conditional on burn-through. Such data would be the natural results of a complete top-down PRA for the whole orbiter. Because NASA has chosen to do the analysis piecemeal and only for selected subsystems, these results have not been generated. Therefore, we use expert opinions instead of analytical results to assess globally these conditional failure probabilities.

1.2 Scope of the work in Phase 1:

As stated in the proposal, the objectives of this first phase are: (1) to understand the basic properties of the tiles, (2) to identify the main experts and establish working relationships with them, (3) to identify the main data bases and sources, (4) to design the Probabilistic Risk Assessment (PRA) model, and (5) to identify some of the relevant organizational features that affect the reliability of the Thermal Protection System (TPS) with emphasis on the black tiles and on the maintenance process. This first phase of the project was funded in part under SIORA (Stanford Space Systems Integration and Operations Research Applications), and in part as a separate research project (both under cooperative agreement NCC10-0001). Under the SIORA funding, we identified some fundamental issues involved in the linkage between the reliability of the black tiles and various features of the organizations that participate directly or indirectly in their maintenance (including, but not exclusively, NASA at the different space centers, Lockheed Corporation, and Rockwell International). The problem formulation was presented in a paper delivered at a major Probabilistic Safety Analysis conference (PSA'89) held in Pittsburgh, in 1989, in a session chaired by Mr. B. Buchbinder (NASA Headquarter, SRM&QA) on probabilistic safety assessment for space systems. This paper won the Best Paper Award of the American Nuclear Society for PSA'89. It is included in this report as Appendix 1.

This Phase 1 report is organized as follows:

1. Background information: functioning, maintenance, and failure history of the

tiles.

2. Description and illustration of the PRA model: inputs, preliminary results (means); sources of expertise and data.
3. Preliminary observations and (qualitative) coupling of organizational factors and the reliability model.

1.3 Gathering of information and technical points of contact

The data and the relevant information used in this study were gathered through meetings and informal interviews of tile specialists, tile personnel (technicians and inspectors), and management at Kennedy Space Center (NASA and Lockheed Corporation), Johnson Space Center (NASA), and in Southern California (Rockwell International in Downey). We conducted, in particular, extensive (although informal) interviews of tile technicians including both old-timers and newcomers. Several of them came from Rockwell and had participated in the initial tile installation work. They described to us procedures and problems and offered suggestions.

The probability estimates were obtained in two ways: frequencies of events from official or personal records (e.g., debris hits; frequency of tile damage), and subjective assessments (e.g., probability of failure of the subsystems under the orbiter skin if subjected to excessive heat loads due to a hole in the orbiter's skin). Note that:

1. The data used here for the illustration of the first-order PRA model are realistic but coarse estimates that can be refined in the implementation part of the second phase.
2. Second-order uncertainties about the probability estimates themselves have not been encoded at this stage. The probability figures that are used here represent implicitly the means of possible probability distributions of the probabilities of events. Assessment of these second-order probabilities or probability distributions for future frequencies of events (Garrick, 1988) will be

part of the implementation phase if it is judged necessary for the relevance of the results to management decisions.

For this study, the key technical points of contact were the following:

At KSC:

- David Weber (Lockheed)
- Frank Jones, Susan Black, Carol Demes, and Joy Huff (NASA)

At JSC (NASA):

- James A. Smith
- Robert Maraia
- Carlos Ortiz
- Raymond Gomez

In Southern California (Rockwell, Downey):

- B. J. Schell
- Frank Daniels
- Jack McClymonds

Section 2:
BACKGROUND INFORMATION

2.1 System description

The designers of the thermal protection system (TPS) for the space shuttle had to solve a series of complex problems due to the wide range of environments in which the orbiter has to operate. A single-component design could not meet all the necessary requirements of withstanding extreme temperatures and vibrations while remaining light weight and flexible and lasting for 100 missions. Instead, a complete, integrated system was developed relying on different components to solve different problems (Cooper and Holloway, 1981.)

In the highest-temperature areas, reinforced carbon carbon (RCC) is used. This material is extremely heat resistant and able to withstand temperatures up to 2800°F on a reusable basis and up to 3300°F for a single flight. The use of this material is limited to the leading edges of the wing and the nose cone. In areas of the orbiter where heating rates are lower, a flexible reusable surface insulation (FRSI) is used. This material is made of a silicon elastomeric coated Nomex felt, which is heat-treated to allow using it for 100 missions at temperatures up to 700°F. In areas where surface temperatures are above 700°F but below 1500°F, advanced flexible reusable insulation (AFRSI) is used. AFRSI is a "blanket" composition with one-inch stitch spacing. It consists of an outer layer of 27 mil silica "quartz" glass fabric and of an inner layer of glass fabric ("E" glass) which encompass a silica-glass felt material (microquartz, commonly called Q-felt). These materials have replaced most of the 5,000 thin white tiles on the upper surface of the orbiters, originally designated low temperature reusable surface insulation (LRSI). Their replacement has reduced the complexity of the TPS at the cost of a slight weight increase (see Figures 1 and 2.)

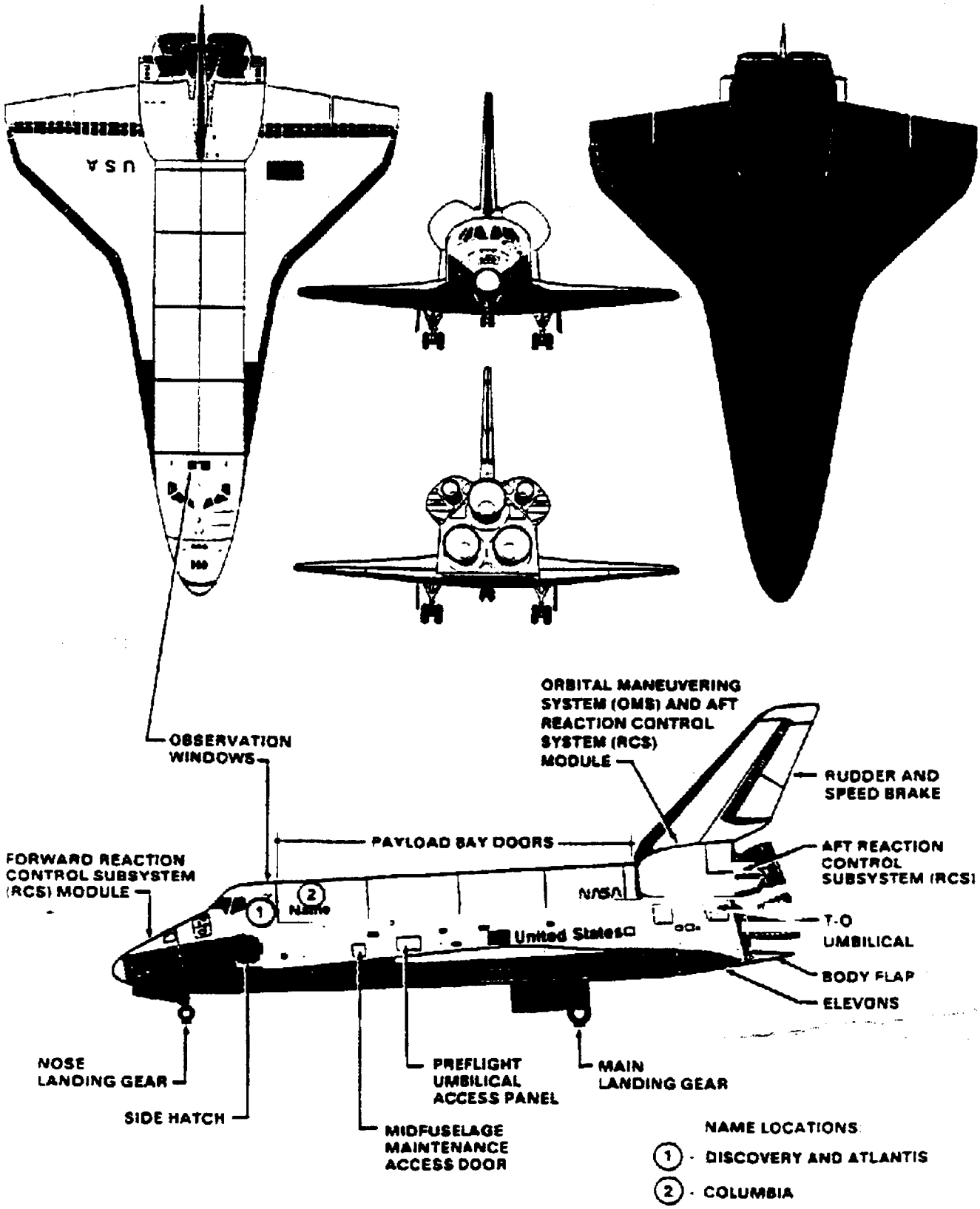


Figure 1: The space shuttle orbiter

Source: Shuttle Operational Data Book, JSC 08934, Vol. 4

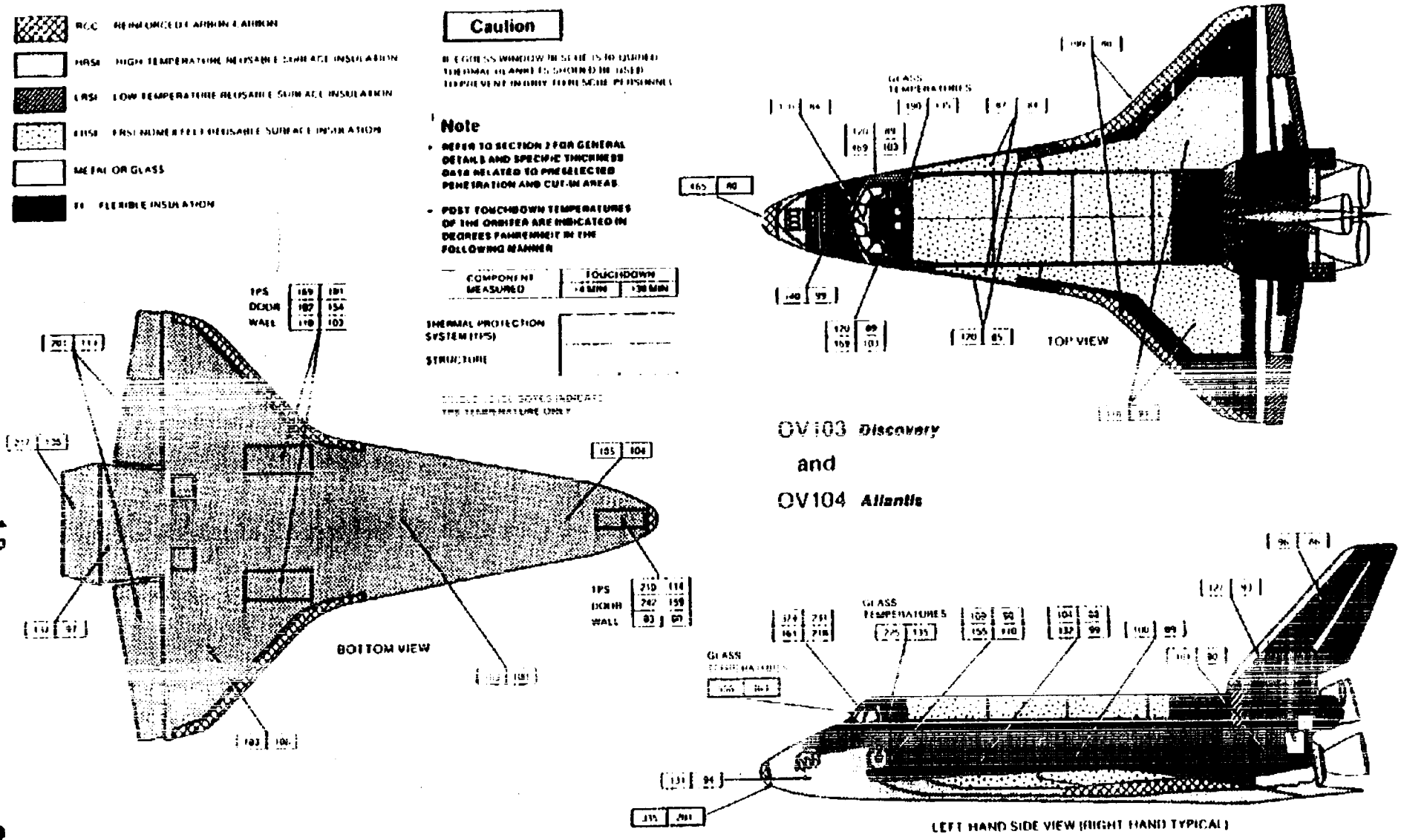


Figure 2: The thermal protection system (TPS) for OV 103 (Discovery) and OV 104 (Atlantis)

Source: Shuttle Operational Data Book, JSC 08934 Vol. 4

The tiles that are of primary interest in this report are designated *high temperature reusable surface insulation* (HRSI) (see Figure 3.) These tiles are coated with black reaction cured glass (RCG) and are certified for 100 missions up to a maximum surface temperature of 2300°F. Approximately 20,000 of these tiles are used to cover the bottom of the orbiter. Among them, approximately 17,000 have a density of 9 pounds per cubic foot (pcf). The remaining 3,000 tiles are of higher density (12 and 22 pcf). They are used in areas where higher strength is needed, primarily around doors and hatches, and where it is required by structural deflections. The 22 pcf tiles are capable of withstanding surface temperatures as high as 2700°F without shrinkage.

These tiles, being highly brittle, have a strain-to-failure performance that is considerably less than the aluminum skin of the orbiter. In addition, the tiles have a much lower coefficient of thermal expansion. Therefore, if they were bonded directly to the aluminum, thermal and mechanical expansion and contraction would cause the ceramic material to crack and fail. To protect the ceramic material, the sizes of the individual tiles were kept small (nominally 6 inches square). These numerous designed gaps allow for relative motion of the tiles as the aluminum skin expands and contracts and the substructure deforms under loading. However, this allowance is not sufficient to protect the integrity of the tiles. In order to further isolate the tiles from local forces, a strain isolation pad (SIP) is secured between the tiles and the skin. The SIP is a felt pad constructed of Nomex fibers and comes in three different thicknesses (0.09, 0.115, and 0.16 inch).

The tiles are bonded to the SIP and the SIP to the aluminum skin using a room temperature vulcanizing silicon rubber adhesive (RTV-560). In certain areas where the aluminum skin is particularly rough and disjointed, a screed or putty (RTV-577) is used to smooth the surface. In order for the SIP and tiles to vent during ascent and to protect the aluminum structure from gap heating, filler bar strips (RTV-560 coated heat-treated Nomex felt material) secured only to the aluminum

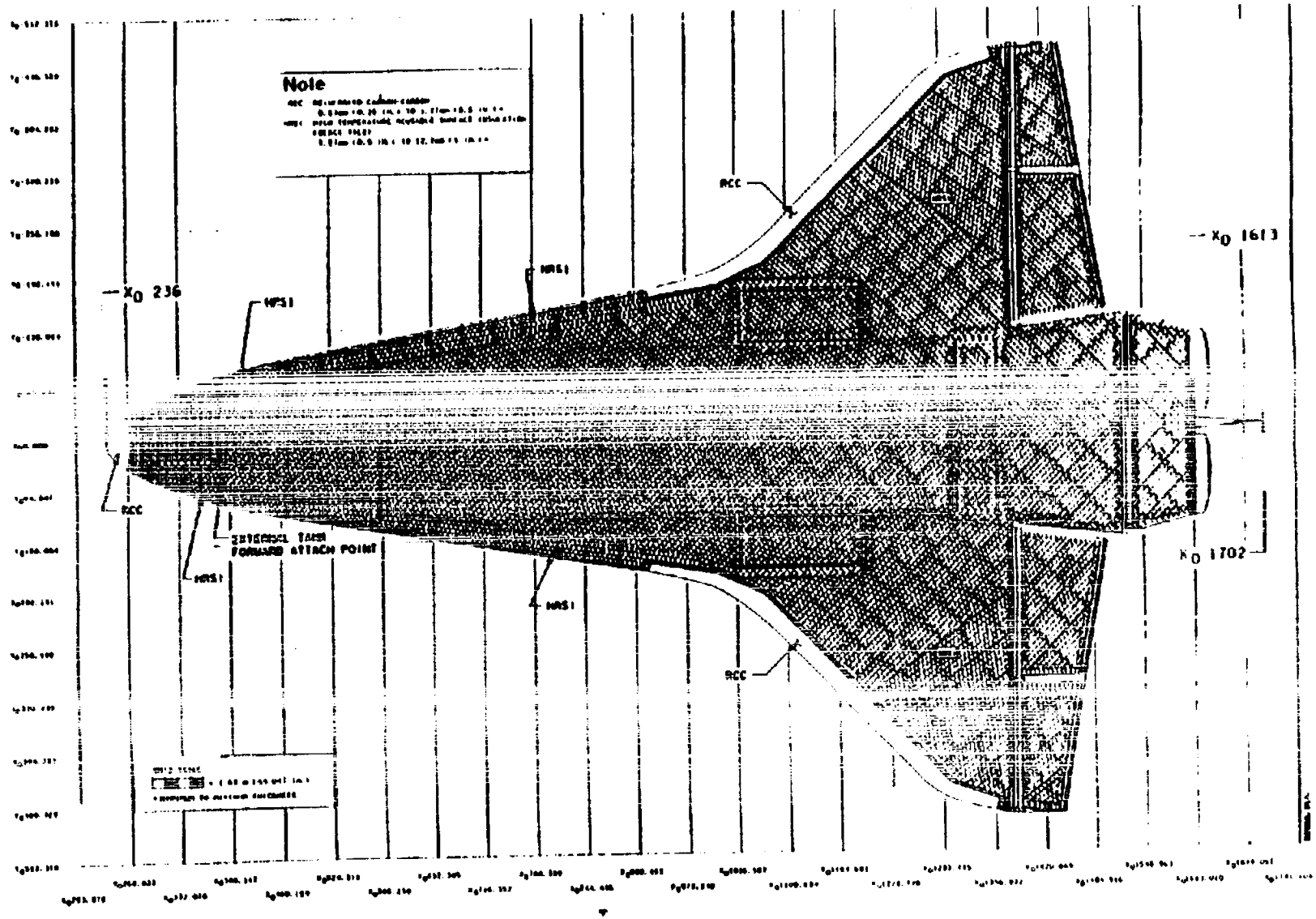


Figure 3: The black tiles (all vehicles)

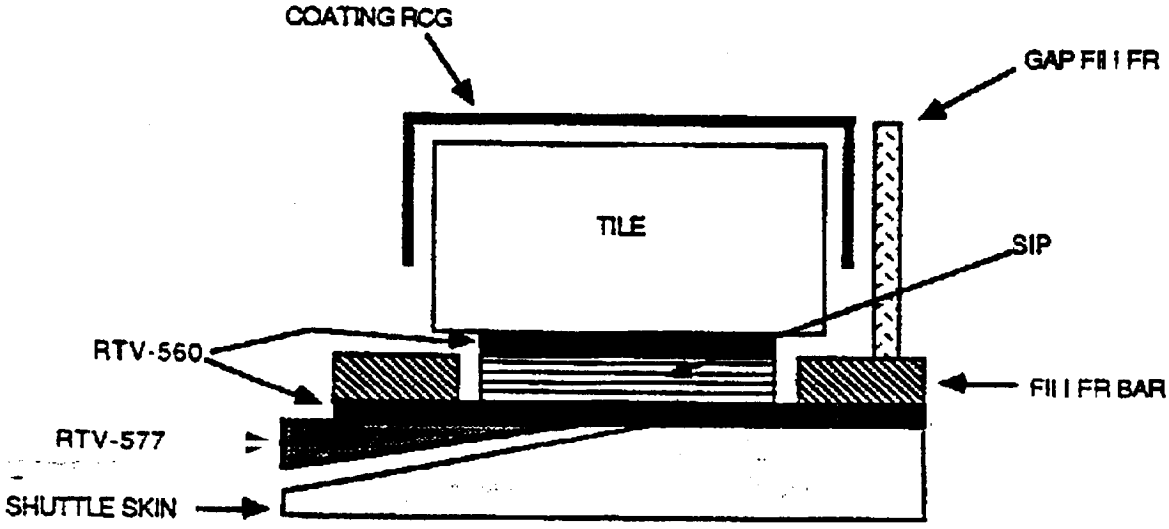
Source: Shuttle Operational Data Book, JSC 08934 Vol. 4

skin are placed around each piece of SIP. The porous tiles are allowed to vent since the RCG coating does not extend to the filler bar. Between tiles in the hotter areas (approximately 4,500 locations), gap fillers are used in addition to the filler bars to prevent gap heating damage during reentry. The gap fillers are secured in place with RTV. Figure 4 shows a typical black tile with all the related components.

2.2 Life cycle and maintenance operations

2.2.1 Tile manufacturing and installation

Because of the extreme environment in which the orbiter operates, the TPS must be made of only the purest materials. Contamination of the tiles during fabrication could lead to failure of the TPS well before meeting its 100 mission requirement. Raw material (amorphous silica fiber) has to be 99.7% pure (AW & ST, 1976).



Note: Thickness exaggerated for clarity; Screed (RTV-577) only where needed

Figure 4: The tile system

The fabrication process starts with a slurry of water and 1.5 micron diameter silica. The water is drained and binder added. This mixture is compressed into blocks slightly smaller than 1 cubic foot. After the binder sets up in 3 hours, the blocks are dried in a microwave oven. The sintering process which locks the fibers

together requires tight heat tolerances. The blocks are baked at 2,375°F for two hours. Next, they are cut into rough tiles (four to eight per block). Tile density and density gradient are verified using X-rays. Since each tile is different, the tiles are trimmed to specification using automated milling machines. A second quality check assures that the tiles are fit for coating. The coating is sprayed on and then glazed. A third quality check verifies the integrity of the coating. These tiles are then internally waterproofed with a silane material. During original construction, the tiles were next placed in arrays that matched their placement on the orbiter's surface. Each array consisted of approximately 35 tiles. The bottoms of the arrays were then shaved to match the shape of the orbiter. A fourth quality check verified the dimensions of randomly selected tiles from each array. All current replacement tiles are machined individually.

The original installation of the tiles at time of construction was done an array at a time. The SIP was first bonded to the tiles using RTV, while a lattice of filler bars were bonded to the orbiter. After these bonds had set, the entire array was bonded to the orbiter. Difficulty arose in aligning the tiles/SIP array with the grid of filler bars. If the tile/SIP array is partially resting on the filler bars instead of directly to the orbiter's skin, the strength of the TPS bond is greatly reduced. The arrays are held in place with 2-3 psi pressure while the RTV dries. Bonds are verified using a pull test on each tile. The strength of each test varies based on the location of the tile and the expected in-flight loading (2 to 13 psi). Once a tile has passed this initial pull test, it is unlikely that it will be checked again during its life cycle of 100 flights unless an anomaly is detected.

2.2.2 Flight profile loading

During a typical mission, the tiles are subjected to a wide range of loads and temperatures. These must be considered in order to determine the limitations and life cycle of the TPS. The description below summarizes a report by Cooper and Holloway (1981).

Ignition of the orbiter's main engines creates an oscillatory pressure wave that loads the tiles in the aft region of the orbiter. Though strong, this wave should dampen rapidly. In addition, acoustic pressure created by the engines can directly load the tiles and the aluminum skin. Any motion of the aluminum will, in turn, cause inertial pressure on the TPS. The amount of inertial pressure depends on the local response of the aluminum substructure, but noise levels up to 165 dB are attained during lift off. During ascent, the tiles experience a wide range of aerodynamic loads including: pressure gradients and shocks, buffet and gust loads, acoustic pressure loads caused by boundary layer noise, inertial pressure caused by substructure motion and deflection, and unsteady loads coming from vortex shedding from the connecting structure to the external tank. Almost every tile will experience loads of 160 dB during this phase of a mission.

Since the tiles are highly porous (90% void), it is during the ascent that any internal pressures must be vented in order to equalize with the external environment. Because of this, both the SIP and the tiles may experience varying degrees of internal pressure. Vent lag can cause tensile forces to build up. In addition, small residual tile stresses are caused by differences in the thermal expansion rates of the tiles and the coating. Also, any water that was absorbed will cause internal pressure as it expands and contracts with the temperature changes.

During re-entry, a second series of stresses are placed on the TPS including: substructure deformation, boundary layer acoustic noise, steady aerodynamic loads, unsteady aerodynamic loads caused by boundary layer separation and vortices, and loads from aerodynamic maneuvering. The *boundary layer transition* from laminar to turbulent flow always occurs, but the time of this transition (for the same entry trajectory) depends primarily on *vehicle roughness*. This roughness is divided into two types: discrete (one single large protuberance) or distributed (many small protuberances.) Early time of transition results in higher turbulent flow peak temperatures and higher total heat loads that depend on temperature and time of

exposure (Smith, 1989). Nearly one third of the tiles on the lower surface of the orbiter reach temperatures in excess of 1900°F and are subjected to problems of uneven thermal expansion.

The TPS has been rigorously tested and has withstood thousands of test cycles of limit load without failure. The system has then been certified for at least 100 flights. However, repeated exposure to the stresses and strains that accompany a space mission can affect the integrity of the individual components. The tiles can weaken, for example, above the densification boundary layer, the SIP can stretch as fibers pull out of the matrix, and the RTV can creep under very high loads. It is only through rigorous maintenance procedures and quality control verifications that the true life cycle of the TPS can be determined and that acceptable system safety can be achieved.

2.2.3 Tile maintenance procedure

The maintenance procedure is guided by the Rockwell specifications (Rockwell International, 1988, 1989). It involves (1) a sequence of tile-damage inspections and assessments after landing to decide which ones can be mended and which ones must be replaced; (2) tile replacement; (3) bond verification using pull tests; (4) step and gap measurement; (5) decision to install or not a gap filler.

The steps involved in the replacement of a tile are the following:

- First prefit
- Densification
- Second prefit
- Bonding of the SIP to the tile
- Cleaning of the cavity (inspection point)
- Priming of the cavity
- Mixing (and testing) of the RTV
- Application of the RTV to the tile/SIP system

° Bonding of the tile/SIP to the cavity

° Verification of the bond.

The verification of the bond at the end of this process involves a *pull test* of variable strength. One problem that has been reported is that this pull test may not allow detection of tiles that are only partially bonded because bonding to the adjacent gap fillers may provide sufficient strength to pass the test. Though these partial bonds pass the initial pull test, they tend to be more susceptible to deterioration over time and slumping.

Step and gap measurement is meant to ensure the smoothness of the orbiter's surface and avoid the excessive heat loads due to vehicle roughness. It is currently a time-consuming procedure involving 24 measurements per tile, done manually by insertion of plastic gauges to a certain depth in the space between tiles. The result of this inspection often leads to a decision to install standard gap fillers. Several problems have been reported in this part of the work, including inaccurate measurements due to misplacement of the plastic gauges. A laser system is currently being developed to automate step and gap measurement, making it both quicker and more reliable (Lockheed Research and Development Division, 1989; SIORA, 1990). Clearly, the corresponding reliability gain for the whole TPS depends on the initial contribution of wrong steps and gaps and orbiter's roughness to the probability of failure of the TPS.

Note that this maintenance procedure is mostly *maintenance on demand.* The only random testing that occurs is in select areas where a small number of tiles are pulled to determine if there has been any weakening of the original screed caused by initial and subsequent exposures to waterproofing materials. In the absence of a non-intrusive test of the bond, the fear is that the tests themselves may weaken the tile/SIP/RTV system.

2.3 Failure history: incident recording and data bases

2.3.1 Failure history and incident recording

A history of the tile problems can best be described by grouping the difficulties into three broad categories: (1) *design problems*, (2) *processing and maintenance induced problems*, and (3) *damage caused by external debris*. This information is summarized from data compiled by Carlos Ortiz at Johnson Space Center (JSC) in Houston, Texas. It should be remembered that to date, *only two black tiles have been lost prior to or during re-entry*: one due to RTV failure caused by chemical reaction with a waterproofing agent (Challenger, Flight 41-G) and one due to debris impact (Atlantis, Flight STS-27R). Even then, there was some remaining material in the tile cavity prior to entry. In both cases, there was neither catastrophic secondary tile damage, nor burn-through of the orbiter skin. This good fortune was due in part to the location of the missing tiles and the structure under the skin. Similar losses in different locations could have been far more costly. Nonetheless, the TPS has done very well and proven to be far more robust than anticipated.

With any complex system, the design process does not stop with the initial product. Improvements occur as the system is used and weaknesses are detected. The orbiter's TPS is no different. Revisions to the original design started before the first launch, and have continued ever since. These properly redesigned components have greatly increased the reliability and maintainability of the overall system. Deficiencies that have, as of yet, gone undetected will be solved in a similar fashion providing that they are uncovered prior to a major system failure.

Design

During the initial design of the TPS, each component (tile, SIP, and RTV) was certified individually; but it was not until they were combined during the construction of the first orbiter, Columbia, that a "weak link" in the bond between the tile and SIP was indentified. Tests of the tile/RTV/SIP/Koropon as a system revealed that the

combined tensile strength was weakest at the tile-to-SIP interface. This was caused by the RTV not impregnating enough the basic tile material to insure adequate attachment. The President of Rockwell Space Systems Group stated: " I think that it is a fair criticism that we didn't define the problems more clearly as far as the tile/strain isolation pad capabilities are concerned. We worked too hard on the quality of the material alone and waited too long for the thermal analysis." (AW&ST, 25 February 1980.) Because of this oversight, many of the already installed tiles had to be retested, pulled, *densified*, and replaced. To eliminate the "weak link", the tiles are densified by applying a mixture of Dupont's Ludox AS and silica slip to the underside --or inner mold line-- of the tile to an approximate thickness of 0.010 inches. The result of this procedure is to move the "weak link" up into the tile material itself. Since the minimum strength of the basic 9 pcf material is 13 psi, the majority of the tiles now satisfy the maximum induced-load requirements. Many of the installed tiles were known to have greater than the minimum 13psi strength and could be shown to have positive margins for flight loads. The tiles that could not be shown to meet flight loads with a positive margin were replaced with 22 pcf tiles whose minimum strength far exceeds the maximum flight loads. This additional work meant that the 30,000 tiles on Columbia required more than 50,000 tile installations before the first flight. Even so, not all the tiles were densified prior to the first launch, but were deemed acceptable based on proof load testing to 1.25 times the limit stress. For all the orbiters after Columbia, the tiles were densified during installation.

Even though the overall temperatures reached during re-entry were less than the maximum allowable, tiles in three areas were found by flight experience to be subjected to local thermal degradation and/or unacceptable thermal gradients resulting in a negative margin for the mid-fuselage structure. Three redesign solutions were used to resolve these area-related problems. Tiles inboard and forward of the main landing-gear doors (denoted as "location A" tiles) were knowingly made thinner than the initial thermal design thickness to minimize weight and to retain the aerodynamic mold line. The thin tiles were able to maintain the

structural temperature limits because the initial flights were flown from the Eastern Test Range at Kennedy Space Center, while the "thermal" design trajectory was based on launches from the Western Test Range, which put a greater heat load on the structure. However, extensive analyses, both thermal and stress, showed unacceptable negative structural margin due to thermal gradients. These negative margins were initially resolved by internal structural modifications and by installing internal heat sink material. Later, the "location A" tiles were replaced with slightly thicker tiles (approximately 1/10 inches thicker) which still provided an acceptable aerodynamic outer mold line based on flight data evaluation. Tiles between the nose cone and nose landing gear were receiving excessive heating, which caused tile slumping and subsurface flow. These tiles were eventually replaced with a much more durable RCC chin panel. A similar problem occurred with the elevon cove tiles. In this case, the size of the tiles was increased, thus reducing the number of troublesome gaps. All three modifications have proven successful.

Processing and maintenance.

The most critical TPS problems related to processing and maintenance have occurred with various waterproofing agents that have affected the strength of the RTV by reacting chemically with the bond. However, in addition, a significant set of other problems have arisen because of maintenance errors. Initial waterproofing was done with an external application of Scotchgard to the tile surfaces. This was not totally effective because the waterproofing degraded with exposure to rain and sunlight. On the second flight, tiles that had absorbed and trapped water, fractured when ice formed in orbit. This defined a need for an internal waterproofing agent. In addition, the Scotchguard was found to chemically attack the RTV-560. Fortunately, this was discovered immediately after an accidental overspray. The first internal waterproofing agent, HMDS, was found to react with the screed (RTV-577), slowly reverting it from solid to liquid. This interaction between waterproofing and screed was not immediate, and eventually led to the loss of a black tile. Fortunately, the other nearby tiles affected by the softened screed did not fail during reentry. A

second generation of waterproofing, DMES, has been developed and proven successful. However, the long-term, residual effects of the outdated HMDS are still causing concern.

Several chemical spills during tile installation have necessitated the removal and rebonding of nearly 1,000 tiles. These spills, involving an oxidizer on Columbia and hydraulic fluid on Challenger, demonstrate the sensitivity of the tiles and their bonds to their maintenance environment. Another incident involved the mislabeling of a container of the bonding agent. RTV-566 was labeled as RTV-560 which has a shorter drying time. The bonds were not allowed to cure for the appropriate time and thus were weaker than allowed. This discrepancy was caught during final pull testing. Finally, during a return flight from California to Florida on the back of a 747, the orbiter Columbia was flown through a rainstorm, damaging over 1,000 tiles of which 250 needed replacement.

Debris

Since the first flight, the orbiter has always been exposed to external debris damage. Table 1 summarizes the damage by listing total number of hits and major hits (greater than 1 inch). Simple statistical analysis demonstrates the great variation that has occurred (Total Hits: mean = 179, standard deviation = 157; Hits ≥1": mean = 51, standard deviation = 60). This variability is further highlighted in Figure 5, which shows histograms of the debris damage (for the upper graph, number of flights as a function of the total number of debris hits; for the lower graph, number of flights as a function of the number of hits greater than one inch). For the first flights (until STS-27R), the actual major source of debris was found to be from portions of SOFI insulation from the External Tank (ET). During STS-27R, the orbiter's TPS experienced significantly more debris damage than on any previous flight, including the loss of a large portion of one black tile (Orbiter TPS Damage Review Team, STS-27R, 1989). Based on the pattern of damage and the recovery of actual debris material lodged in the tiles, AFRSI, and gaps, it was possible to

Sequence	Designation	Orbiter	Date	Major Debris Hits > 1"	Total Debris Hits
1	1	Columbia	04/12/81	•	•
2	2	Columbia	11/12/81	•	•
3	3	Columbia	03/22/82	•	•
4	4	Columbia	06/27/82	•	•
5	5	Columbia	11/11/82	•	•
6	6	Challenger	04/04/83	36	120
7	7	Challenger	06/18/83	48	253
8	8	Challenger	08/30/83	7	56
9	41H	Columbia	11/28/83	14	58
10	41B	Challenger	02/03/84	34	63
11	41C	Challenger	04/06/84	8	36
12	41D	Discovery	08/30/84	30	111
13	41G	Challenger	10/05/84	36	154
14	51A	Discovery	11/08/84	20	87
15	51C	Discovery	01/24/85	28	81
16	51D	Discovery	04/12/85	46	152
17	51B	Challenger	04/29/85	63	140
18	51G	Discovery	06/17/85	144	315
19	51F	Challenger	07/29/85	226	553
20	51I	Discovery	08/27/85	33	141
21	51J	Atlantis	10/03/85	17	111
22	61A	Challenger	10/30/85	34	183
23	61B	Atlantis	11/26/85	55	257
24	61C	Columbia	01/12/86	39	193
25	51L	Challenger	01/28/86	•	•
26	26R	Discovery	09/29/88	55	411
27	27R	Columbia	12/02/88	250	707
28	29R	Discovery	03/11/89	23	132
29	30R	Atlantis	05/04/89	56	151
30	28R	Columbia	08/08/89	20	76
31	34R	Atlantis	10/18/89	18	53
32	33R	Discovery	11/22/89	21	118
33	32R	Columbia	01/09/90	15	120

Table 1: Summary of orbiter flights and debris damage

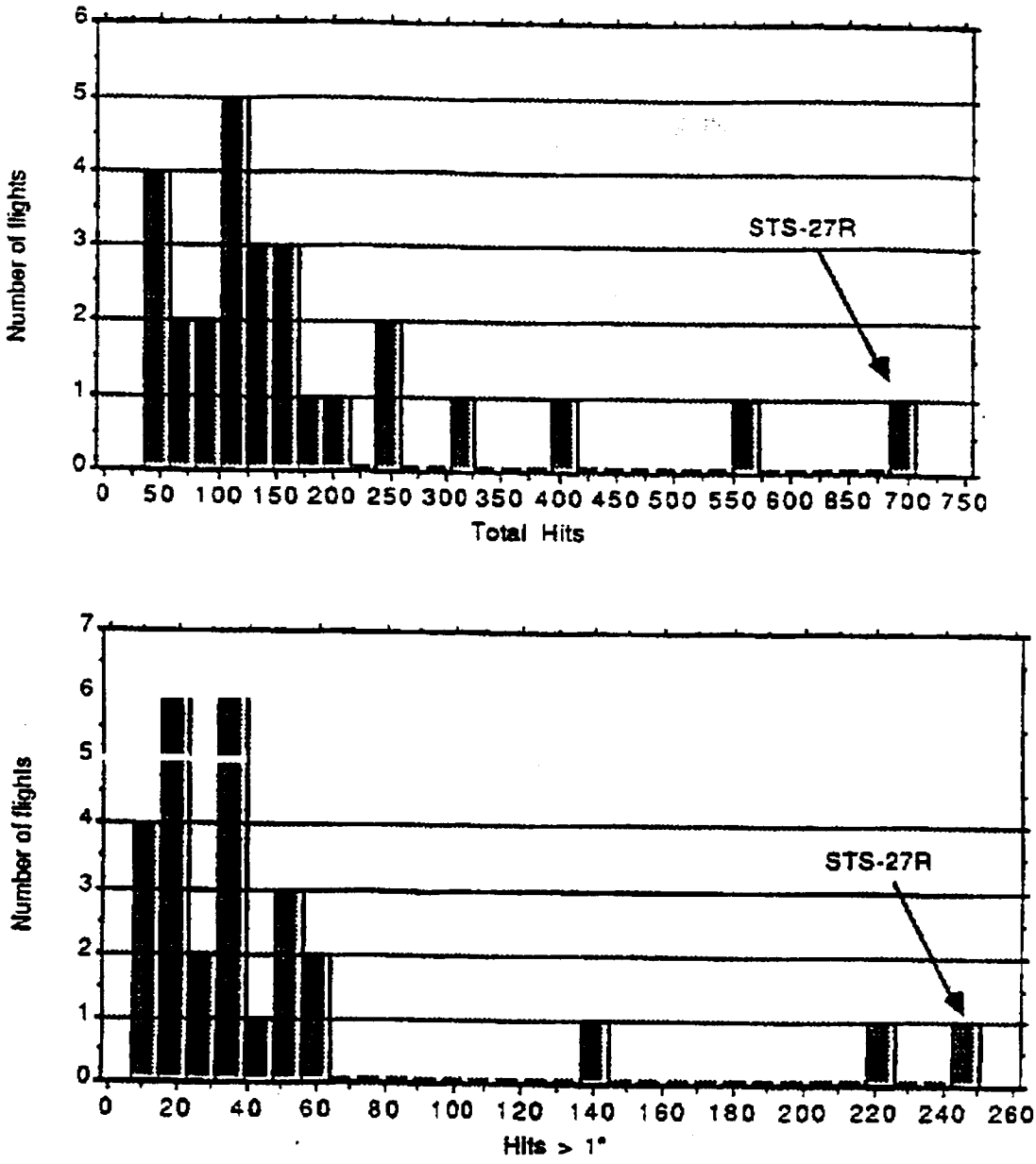


Figure 5: Histogram of tile damage due to debris.

Indicates the number of flights that experienced a specified amount of debris damage (i.e. four flights had 40-60 total hits, two different flights had 60-80 total hits, etc.) based on available data for the first 33 flights (missing: first five missions and STS-51L)

determine that much of the severe damage was caused by insulation from the cone area of the right SRB. Other damage, minor but more extensive than usual, was caused by the insulation of the ET. This was similar to the type of damage that had been experienced in previous flights. In addition, an in-depth analysis done at the time concluded that there was no obvious correlation between tile damage and launch conditions that might affect ice formation, which was considered earlier a possible source of tile impact damage (Orbiter TPS Damage Review Team, STS-27R, 1989).

Figure 6 displays on one orbiter surface a cumulative recording of all significant tile damage from all flights and all orbiters (through STS-32R.) The damage is obviously not uniformly distributed, and certain tiles are much more likely to be damaged than others. Computer models developed by Ray Gomez at JSC have been able to show how insulation from both the SRBs and the ET could cause such damage (see Figures 18 and 19 in Section 3.) The complexity of the problem does not currently allow for a direct and focused backtracking from a tile on the orbiter to a particular spot of insulation because the trajectory depends on many factors (e.g., the velocity of the orbiter and the angle of attack.) It may be possible, however, to determine roughly the initial location and the size of loose insulation necessary to inflict specific damage (location and severity) to the tiles.

Debonding of tiles due to factors other than debris impact

To date, as mentioned above, only one black tile has been lost due to factors other than debris impact (in that case, chemical reversion of the screed). There are several reasons for unsatisfactory bonds: 1) improper alignment during installation, 2) failure to comply with RTV drying limitations, 3) chemical reversion of the screed or RTV, and 4) possible weakening of various components in the TPS under repeated load cycles. An initial investigation of a small discrete set of tiles showed that a high proportion of the bonds that had passed the pull test were later found to be unsatisfactory (see Figure 7). Since then, however, this number has been found to

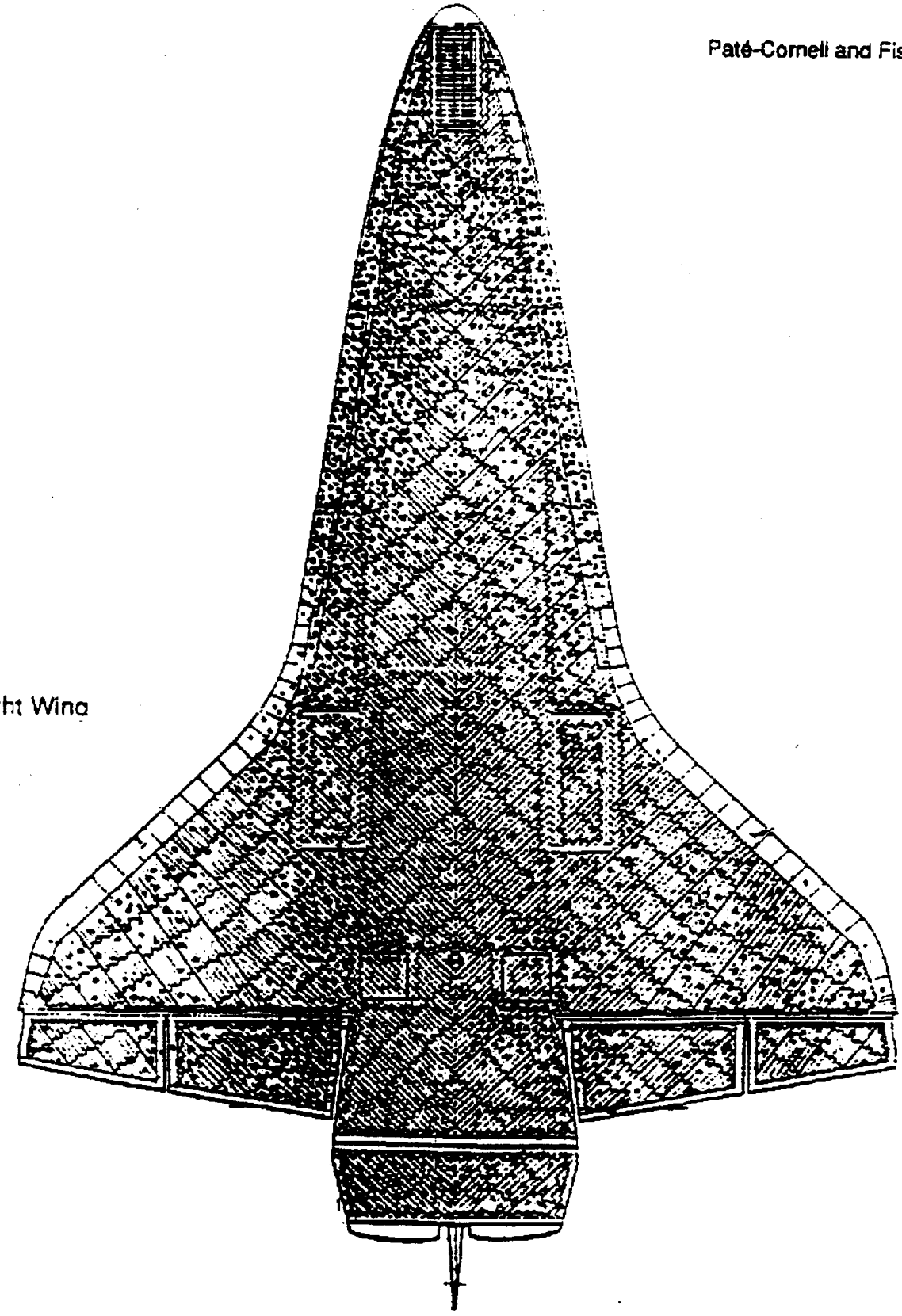
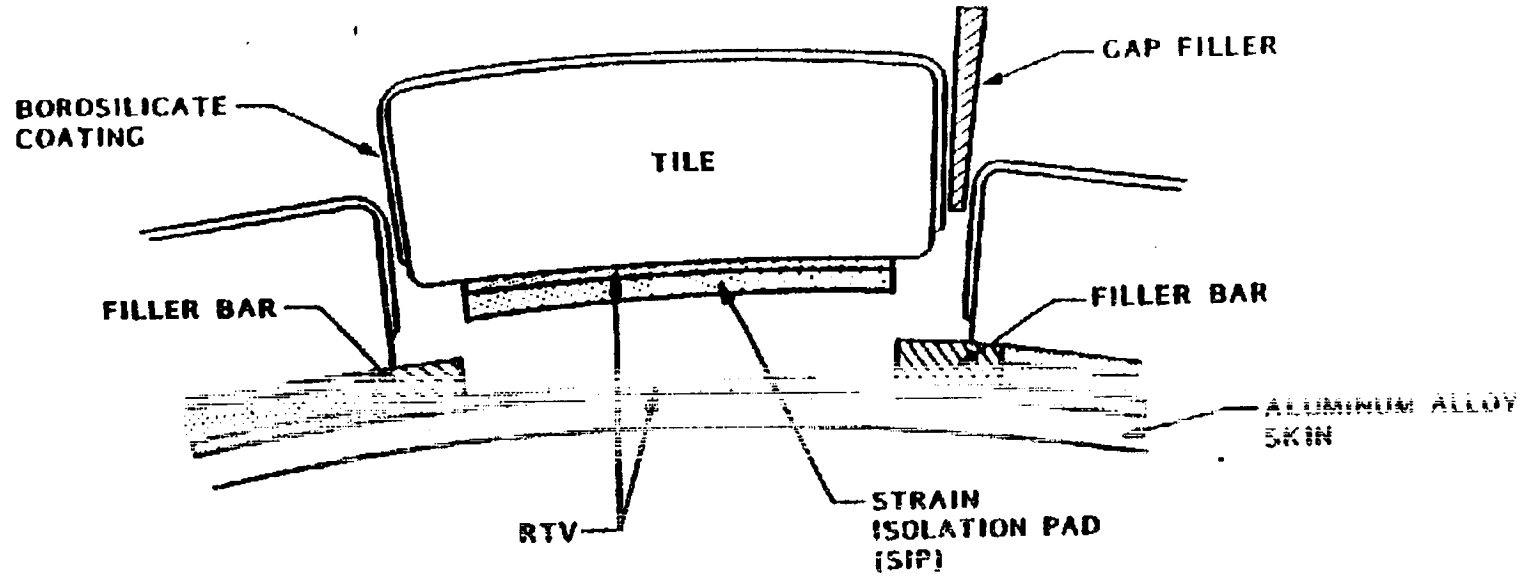


Figure 6: Accumulated major debris hits (lower surface)
for flights STS-6 through STS-32R

Source of data: J. McClymonds, Rockwell International

PROBLEM OVERVIEW



PROBABLE CAUSE OF BOND PROBLEMS

- POOR ADHESION BETWEEN SIP AND RTV
- POOR ADHESION BETWEEN RTV AND ORBITER SKIN
- PHYSICAL INTERFERENCE IN CAVITY; SIP RESTS ON EDGE OF FILLER BAR

CURRENT BOND CERTIFICATION METHOD IS A PULL TEST

- INADEQUATE: > 20% CERTIFIED BONDS LATER FOUND UNACCEPTABLE

Figure 7: The tile system and bond verification

Source: Lockheed Corporation (1989), R. Welling. Reproduced by permission

be much smaller. A recent and on-going evaluation of all 9,045 tiles using the 0.090 and 0.115 inch SIP has shown that of the 6,517 tiles evaluated to date, only 8 showed anomalous conditions (most of which, but not all, were subnominal bonds). So far, during normal maintenance and the replacement of debris-damaged tiles, 12 tiles have been found to have no bond between the SIP and the orbiter's skin. These tiles were only held in place by the gap filler's bond to adjacent tiles.

As mentioned earlier, the SIP is bonded to each tile using RTV while the filler bars are bonded to the skin. After all these bonds have firmed, a layer of RTV is placed on the skin in the hole defined by the filler bars. The tile/SIP combination is then held in place completing the installation. If the tile/SIP combination is not aligned correctly with the filler bars, the SIP may rest on the filler bars and never touch RTV or skin. Obviously, these tiles will have very poor bonds. In several cases the tiles were placed correctly between the filler bars, but directly over exposed sensor wires. These wires prevented complete contact between the SIP and the RTV and thus made for a weak bond. It should be noted that even with no primary bond between the SIP and the skin, tiles have still passed the pull tests (because of the gap filler bonds) and that, as of yet, no tile has been lost due to poor installation.

If the RTV is allowed to dry before the tile/SIP combination is placed on it, the bond will not develop to its full potential. This can happen when several tiles are been placed at one time, and a single batch of RTV is mixed for the several prepared sites. If the installersare not careful, the RTV may exceed its "pot life", i.e., the age beyond its safety margin, before the last tile is placed.

The chemical transformation of the RTV is very sensitive to temperature and humidity and must be monitored carefully during installation. In several cases, the curing time of the RTV has been reduced by the installers using water (or saliva). Such a procedure, which is explicitly forbidden, is not believed to affect the immediate strength of the bond, but may reduce its life. A similar class of problems

has occurred when the aluminum surface has not been properly prepared. In this case, the RTV bond may fail at the interface with the orbiter's skin.

The only black tile that has been lost due to debonding not caused by debris occurred when the first internal waterproofing agent, HMDS, reacted chemically with the screed causing it to soften and revert back to its more viscous form. The formula of the waterproofing agent has since been changed so that it will not affect the screed. This new waterproofing agent has completed 50 mission cycles on combined-environment testing, and no weakening of the TPS system was found. Yet, careful monitoring is required to ensure that no residual amounts of the old HMDS agent are causing a very slow reversal reaction and, eventually, loss of tiles. The current HMDS testing procedures involve removing two or three tiles after each flight to check the chemical composition of the screed. To date no additional problem has been found.

In the long term, repeated exposure to load cycles and environmental conditions of heat and humidity on the ground may weaken some of the TPS components and, eventually, cause tile failure. The most vulnerable tiles are those with no bond or very little bond (e.g., less than 10% of the surface) between the SIP and the orbiter's skin, and that are held primarily by the gapfiller's RTV bond to the adjacent tiles. RTV bonds, so far, have not shown visible signs of deterioration over time and load cycles. It is known, based on extensive testing, that the hundred-flight certification is justified for well-bonded tiles. What will happen in the future, however, is uncertain.

After some flights, several cases of slumping (sagging) tiles have been observed. These are easily identified visually since they break the smooth surface of the orbiters. According to David Weber at KSC, the most common cause of slumping is a weakening of the SIP's fibers due to repeated load cycles. Pre-densification testing showed that the part of the tile located right above its

interface with the SIP was the weakest part and was most likely to be affected by repeated load cycles. With densification, this weakest zone has moved, on one hand, further up into the tile, and on the other hand, down into the SIP itself. A problem in either location is difficult to detect if there is not overt visual clue. Yet, once again, to date no tile has been lost due to repeated load cycles.

2.3.2 Data bases:

Three data bases have been identified and described by Ellen Baker and Bonny Dunbar as part of their TPS Trend Analysis Survey (March, 1988). They are:

- **PRACA** (Problem Reporting and Corrective Action) which is managed by NASA. Tile problems constitute only a subset of these data. The information regarding the tiles can be accessed at KSC.
- **TIPS** (Tile Information Processing System) which is managed by Rockwell (Downey, California). The specialist is Ms. B. J. Schell, supervisor of the TPS Data Systems at Rockwell International, Downey, California. The information can be accessed at Downey, JSC, and KSC.
- **PCASS** (Program Compliance Assurance and Status System) which is part of a NASA (agency-wide) System Integrity Assurance Program Plan.

PRACA and TIPS are described in Appendix 2. The survey conducted in 1988 by Baker and Dunbar showed that a trend analysis was judged highly desirable:

1. To monitor the performance of the TPS in order to ensure conformance with design requirements
2. To ascertain long term effects of TPS-related procedures (repairs, etc.).
3. To enable engineering design changes to system failure.

The participants to the survey indicated that there was a need for a single user-friendly data base including all useful data and, in particular, results of trend analysis. They would want to have routine access to this data via a local PC or

terminal. As we show in section 4, the risk-criticality index that we have developed can be an important part of the record for trend analysis because it represents the relative contribution of each tile to the probability of LOV due to TPS failure. These probabilities can be updated on the basis of new information and the results can be encoded for all tiles that share similar characteristics.

Section 3:
DESCRIPTION OF THE PRA MODEL FOR THE TILES

3.1 Susceptibility and vulnerability

Our probabilistic risk assessment (PRA) model for the black tiles of the thermal protection system (TPS) of the space shuttle is based on two major factors: *susceptibility* of the tiles to damage and *vulnerability* of the shuttle once tile damage has occurred. The terms susceptibility and vulnerability have been standardized in the study of aircraft combat survivability; their use in the space shuttle context may facilitate the understanding of the problem.

Susceptibility of the tile system to damage is determined by the combination of *loads* on the tile and its *capacity* (strength) to withstand them. Failure occurs when the loads exceed the capacity. The problems can generally be divided into two categories: (1) tile loss caused by excessive external loads and (2) tile loss under regular loads caused by weaknesses in the tile system (debonding due to factors other than debris impact). A third possibility (a combination of the two) is the case where external loads not severe enough to cause the loss of a well-bonded tile, causes the loss of a weakened tile. In this study, this case is treated as a subset of the first category. Historically, the vast majority of excessive external loadings has been from *debris*, mostly from the external tank and the solid rocket boosters (defective insulation and ice). Also included in this category is space debris. Depending on the size and energy of the debris hitting the orbiter, several tiles can be damaged simultaneously. It is also conceivable that the reentry *temperature* may exceed the designed capabilities of the tiles, leading to tile failure or burn-through (for example, due to severe malfunction of the guidance system).

Capacity reduction caused by weaknesses of the tile system account for tile losses caused by long-term deterioration of the RTV, defective bonds not caught

during installation, and tile bonds weakened due to improper maintenance procedures, waterproofing, and spills. These weaknesses could affect a single tile (tile resting on its filler bar) or a group of tiles (use of a weak batch of RTV). Tile susceptibility can therefore be reduced by controlling the external debris, improving tile installation and maintenance procedures, and developing new tests (non-destructive pull tests and other types of tests) to ensure bond verification. Another approach to reducing the susceptibility of the tile system that will not be considered in this study would be to harden the tiles so that the impact of external debris would not cause any damage. Extensive use of RCC would be one such solution, but at the cost of a significant increase of weight and design complexity, as well as an enormous additional expense.

The vulnerability analysis starts with the premise that a tile has been lost for whatever reason, then proceeds to analyze the effects of this loss on the shuttle's performance and safe return. Of primary concern in this phase is the layout of the shuttle systems immediately below the shuttle's skin. A heating or burn-through of the skin could cause the loss of various hydraulic lines, computers, fuel tanks, or even a weakening of the structural integrity of the spacecraft. Also included in the vulnerability analysis is the effect of an initial loss on the surrounding tiles. When the TPS was developed, it was feared that one hole could lead to adjacent tiles peeling off because of reentry heating (the so-called zipper effect). This phenomenon has not occurred in the two instances where tiles have actually been lost. Yet, the loss of a tile clearly causes a local turbulence and exposes directly the side of the next tile/SIP/RTV system to high loads (forces and heat). The probability of loss of a secondary tile, although obviously not equal to one, is still higher than the probability of loss of the first tile in a patch. If not checked, the loss of subsequent tiles could lead to exposure of a much larger patch of the shuttle's skin. The vulnerability of the orbiter could be reduced by moving, hardening, or increasing the redundancy of various critical control systems. If the tile damage can be discovered prior to reentry, then, in some cases, the vulnerability of the shuttle could be reduced (either by

protecting the exposed patch or by rerouting, draining, or securing exposed lines and tanks.) In addition, by changing the reentry flight profile of the shuttle, it may be possible to reduce the temperature of some weak, vulnerable areas. The sequence of events that is studied in this analysis is shown in Figure 8.

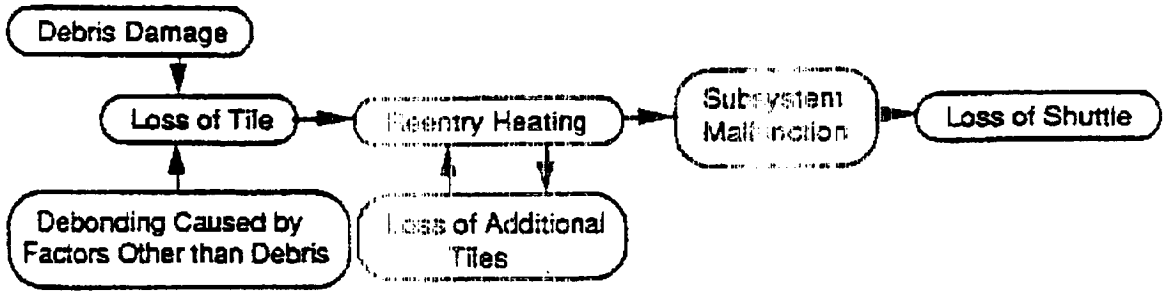
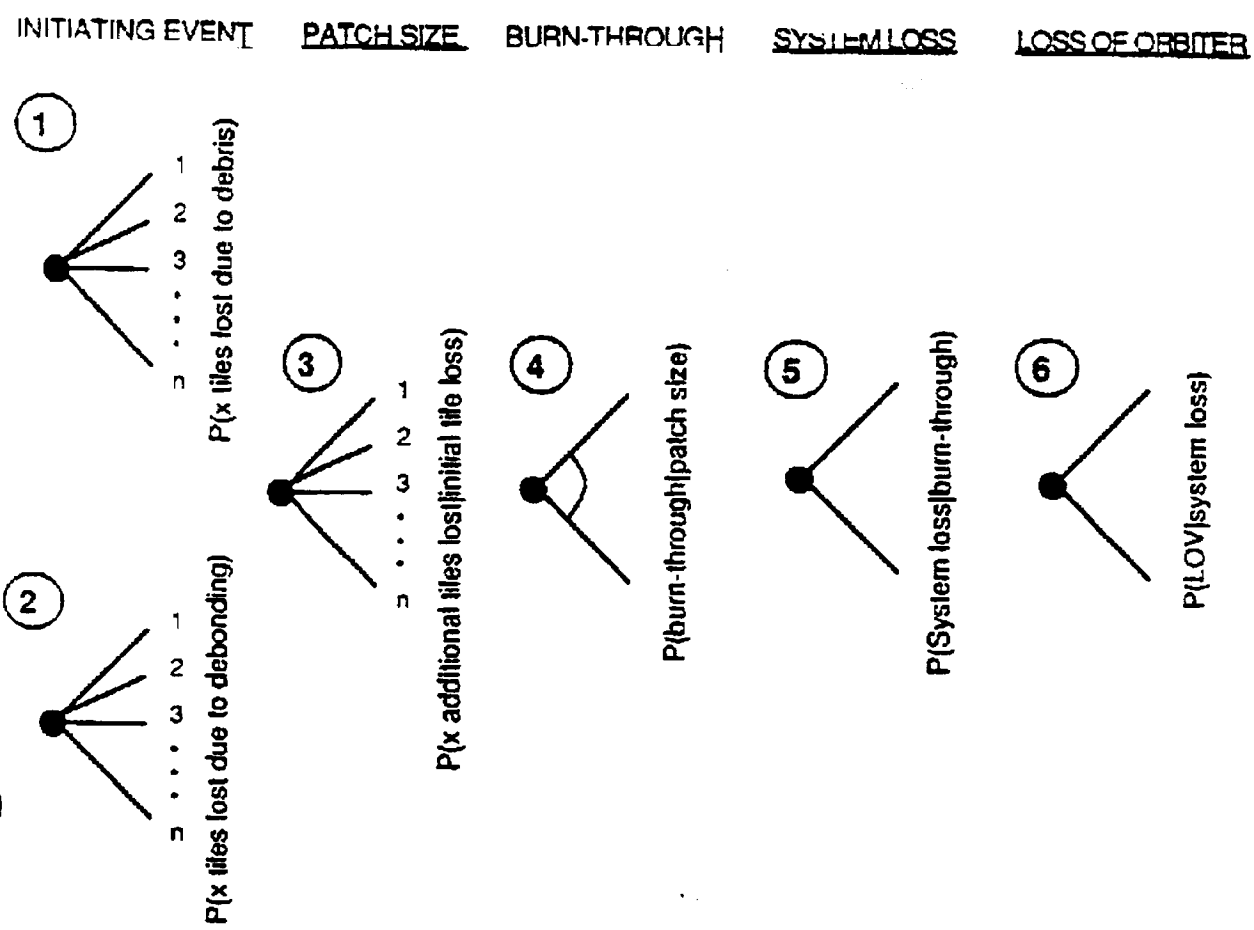


Figure 8: Event diagram: failure of the TPS leading to LOV

The structure of the probabilistic model used in the analysis (Figure 9) follows closely that of the elements presented in Figure 8. It includes: (1) *initiating events* (probability distributions for the number of tiles initially lost due to debris and to debonding caused by other factors), (2) *final patch size* (probability distribution of the number of adjacent tiles lost conditional on the loss of the first tile), (3) *burn-through* (probability of burn-through conditional on a failure patch of a given size), (4) *system loss* (probability of failure of systems under the skin conditional on a burn-through), and (5) *loss of orbiter* (probability of LOV, conditional on failure of subsystems due to burn-through.) The analysis is thus done using the usual mix of probabilities estimated through frequencies, and of subjective probabilities when needed (e.g., for the probabilities of failure of subsystems under the skin for which no formal PRA studies have been done). Bayesian formulas were used to compute the probabilities of different scenarios as described further in this section.

Note that, in this study, we did not account for excessive heat loads (above the design criteria) causing the burning of a tile due, for example, to tile design problems or to a malfunction of the guidance system and/or the control surfaces.



1. Discrete random variable: number of initial tiles lost due to debris
2. Discrete random variable: number of initial tiles lost due to debonding
3. Discrete random variable: number of additional tiles lost given initial tile damage
4. Continuous random variable: severity of burn-through given a patch size of missing tiles
5. Binary random variable: subsystem failure occurs given level of burn-through
6. Binary random variable: LOV occurs given loss of subsystems

Figure 9: Event tree of LOV due to TPS failure

Although this failure mode may contribute to the overall risk of failure of the orbiter's TPS, it was considered here that these initiating events now have a much lower probability than the loss of a tile due to debris damage and/or debonding caused by other factors.

We did not account for dependencies among the probabilities of failures of subsystems under the skin due to TPS failure; for example, two redundant elements of the hydraulic system could be crippled during the same flight by loss of tiles in two different locations. The probability of such simultaneous failures was considered to be too small. Finally, we did not account for dependencies among tile failures caused by the repetition of the same mistake (e.g., from the same technician) which becomes a common cause of failure (for example, addition of water to the RTV mix and treatment of several tiles). This concern will be part of the second phase of the study.

3.2 Definition of min-zones

Because of the factors described above, the black tile system cannot be treated as a uniform structure. Debris is more likely to hit some parts of the orbiter than others, different bonding materials are used in different areas, temperatures vary considerably over the surface, and critical subsystems are located only in a few areas. Therefore, for this analysis, the entire tile protection system is subdivided into smaller areas, called here *min-zones*, such that *all tiles of a specific min-zone have the same level of susceptibility and vulnerability*. Depending on the number of discriminating characteristics, the number of tiles in each min-zone could conceivably vary from a single tile to thousands. (An alternative approach would be to categorize each tile individually with regard to susceptibility and vulnerability, but since most adjoining tiles have identical characteristics, this level of detail is not needed.)

The definition of min-zones is critical to the analysis. The number of factors used to delineate the min-zones determines the complexity of the problem. As an initial cut, we define a min-zone by four factors: (1) susceptibility to debris impact, (2) potential for loss of additional tiles following the loss of the first one (depending on heat and aerodynamic loads), (3) potential for burn-through given one or more missing tiles (heat loads), and (4) criticality of underlying systems. For this study, it is assumed that the probability of debonding caused by factors other than debris impact is uniform over the orbiter's surface and does not require a separate partition of this surface. As mentioned above, it is also assumed that flight profiles will not expose the entire TPS to severe temperatures that would exceed their specifications.

3.2.1 Debris classification

In order to account for the fact that debris damage during ascent is not uniformly distributed across the underside of the orbiter, the black tiles are partitioned into three *debris areas* such that all tiles in a particular area have roughly the same probability of being initially damaged by external debris. The definition of these debris areas also accounts for the fact that some areas are more susceptible to being hit by large pieces of debris that will damage several adjacent tiles simultaneously.

To define the debris zones, we plotted all known debris damage from the first 33 flights on a single shuttle layout (see Figure 6.) These data came from J. W. McClymonds (1989) at Rockwell in Downey. Areas with similar damage intensity were grouped together into high, medium, and low debris damage areas (see Figure 10.) An estimated probability of tile damage due to debris per flight was determined by dividing the number of hits by the number of tiles in each area and by the number of flights. A similar plot and calculation was done for all damage to black tiles over one inch in size. (Historically about one fourth of the damage has been greater than one inch in size.) It should be noted that the only missing tile to date caused by debris is in one of the "high debris damage areas".

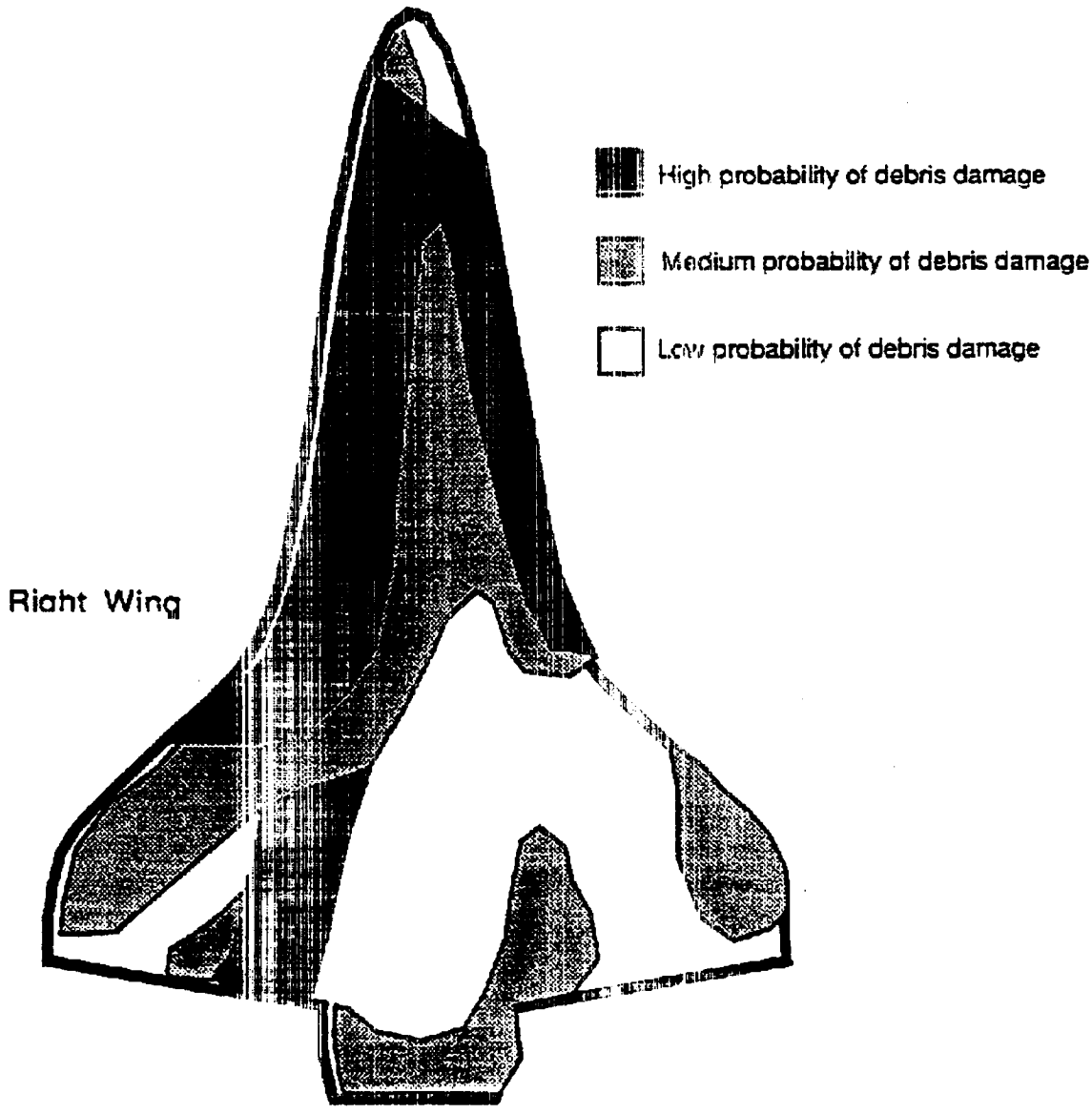


Figure 10: Partition of the orbiter's surface into three types of debris zones (index: h)

Based on this analysis, the probabilities of a specific tile receiving *any debris damage* were assessed as shown in Table 2. The probability of multiple tile damage was calculated using a typical six-inch by six-inch square tile and estimating the percentage area, within a 1/2 inch border, that would allow for other tiles to be hit simultaneously with sufficient energy to cause significant damage.

Debris Area	High	Medium	Low
P(Single tile hit)	10^{-2}	$3x10^{-3}$	$5x10^{-4}$
P(One of two tiles hit)*	$8x10^{-4}$	$2x10^{-4}$	$4x10^{-5}$
P(One of three tiles hit)	$7x10^{-5}$	$2x10^{-6}$	$3x10^{-6}$

*P(one of x tiles hit) = probability that a particular tile is in a group of x adjacent hit tiles

Table 2: Probabilities of debris hits in the different areas shown in Figure 10

Translating this information into the probability that a specific tile will be knocked off or so significantly damaged as to burn off during reentry is a more difficult task. It is logical to assume that the probability of this level of damage is the ratio of the number of destructive hits to the total number of hits in the past. Since one tile has been lost out of roughly two thousand significant debris hits, it is proposed, in this study, to use an initial estimate of 1 in 2,000 ($5x10^{-4}$) for the probability that large hits would destroy a tile's insulating capability in the high debris areas. Slightly smaller probabilities were used in the medium and low debris areas. The probabilities of tile loss due to debris hits for each tile in each area of Figure 10 have been further allocated as shown in Table 3. For example, the probability of a single tile loss in "high" debris area is the product of (1) the probability that the tile is hit by a debris, (2) the probability that the size of the hit is greater than 1" conditional on a hit and (3) the probability that the tile is knocked-off given a large debris hit.

Debris Area	High	Medium	Low
P(Single tile lost)	1.3 x 10^{-6}	10^{-7}	10^{-9}
P(One of two tiles lost)*	10^{-7}	10^{-8}	0
P(One of three tiles lost)	10^{-8}	10^{-9}	0

*P(one of x tiles lost) = probability that a particular tile is in a group of x adjacent lost tiles

Table 3: Probabilities of tile loss due to debris in the different areas shown in Fig. 10

3.2.2 Burn-through classification

In a similar fashion the tiles are partitioned into three *burn-through areas* (see Figure 11.) The probability of a burn-through is dependent on two factor: the temperature that the surface reaches during reentry (and for how long), and the ability of the unprotected aluminum skin to dissipate the heat build up. The denser and stronger the structure under the skin, the greater the capacity to resist burn-through. In both cases where tiles have been lost, burn-through has not occurred in part for this reason. The larger the patch of missing tiles, the greater the likelihood of burn-through. The probabilities shown in Table 4 were estimated from information provided by Robert Maria of NASA Johnson Space Center in Houston. Once again, these are only coarse estimates.

Burn-through Area	High	Medium	Low
P(Single tile lost)	0.2	0.1	0.001
P(One of two tiles lost)*	0.7	0.25	0.01
P(One of three tiles lost)	0.95	0.7	0.1

*P(one of x tiles lost) = probability that a particular tile is in a group of x adjacent lost tiles

Table 4: Probabilities of burn-through due to tile loss in areas shown in Fig. 11

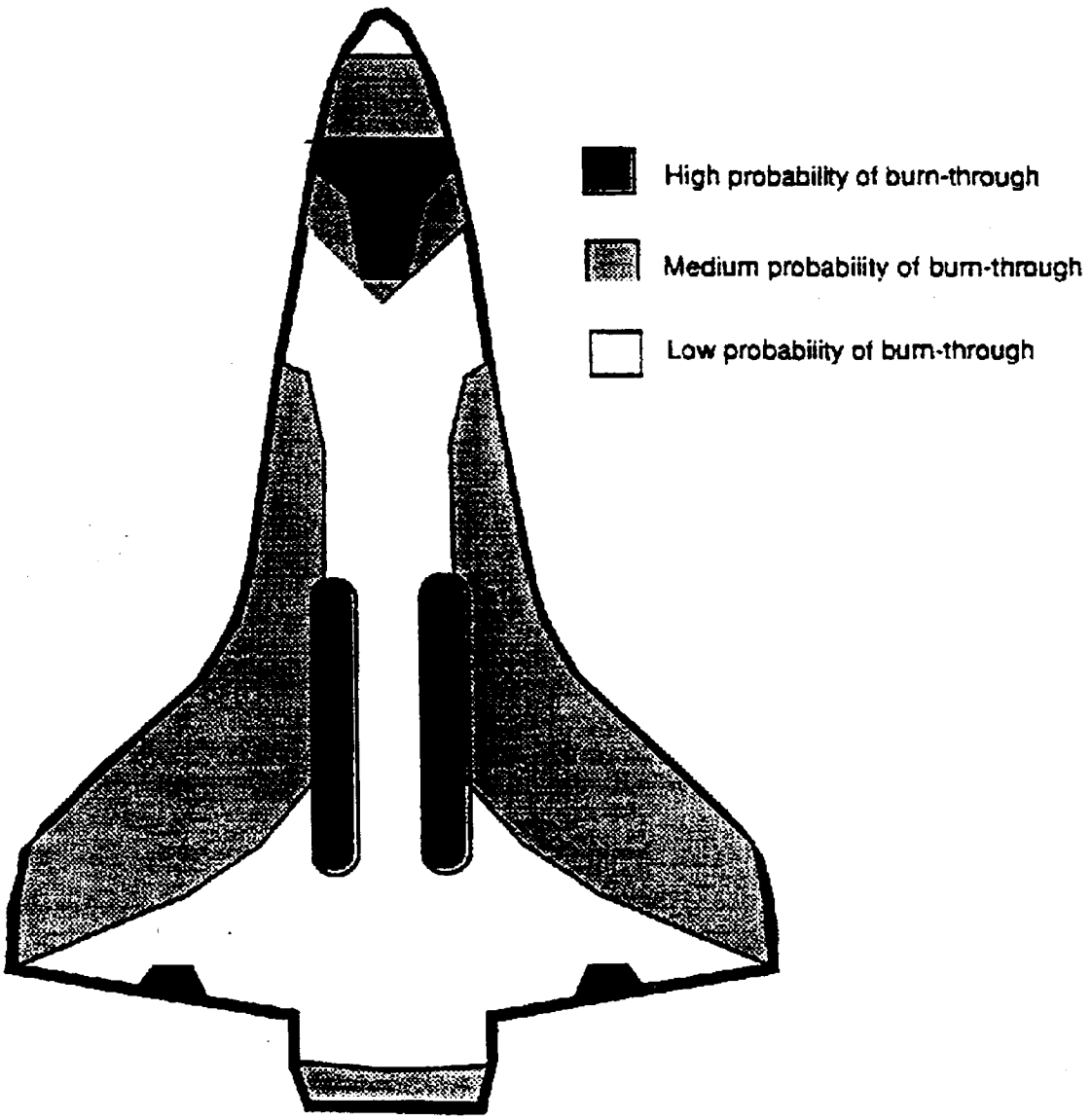


Figure 11: Partition of the orbiter's surface into three types of burn-through zones (index: k)

Note that the two areas just in board of the main landing gear have been notated as being in the high burn-through area. This is not, strictly speaking, a burn-through problem. The structure in those areas is extremely sensitive to temperature differences and would fail even without a burn-through. However, because of their sensitivity to temperature, these two areas were grouped in the high burn-through category.

3.2.3 Secondary tile loss classification

In order to account for the potential of a single tile causing the loss of adjacent tiles, the orbiter is divided into two *secondary tile loss areas* (see Figure 12.) The probability of additional tile loss depends on the aerodynamic forces and on the magnitude and duration of the increased reentry temperatures that occur around a missing tile due to the disruption of the laminar flow. This increase of temperature also depends on the ability of the skin to dissipate the heat build-up. The RTV bond will fail above 500°F. Because of this, the secondary tile loss areas are related to the temperature areas used in the burn-through analysis above. In this study, the two secondary tile loss areas will be defined by the probability of adjacent tile loss shown in Table 5. These values were estimated from information provided by Robert Maria from NASA in JSC.

Zone 1 (high loads):	P(Additional tile lost | One tile lost) = 10^{-2}
Zone 2 (low loads):	P(Additional tile lost | One tile lost) = 10^{-3}

Table 5: Probabilities of losing adjacent tiles due to initial tile loss in areas shown in Figure 12

A *failure patch* is defined as a group of lost tiles that started from one initiating event (initial tile loss) and has reached its maximum size. The size of a failure patch depends on the number of tiles initially damaged and on the subsequent vulnerability of the adjacent tiles.

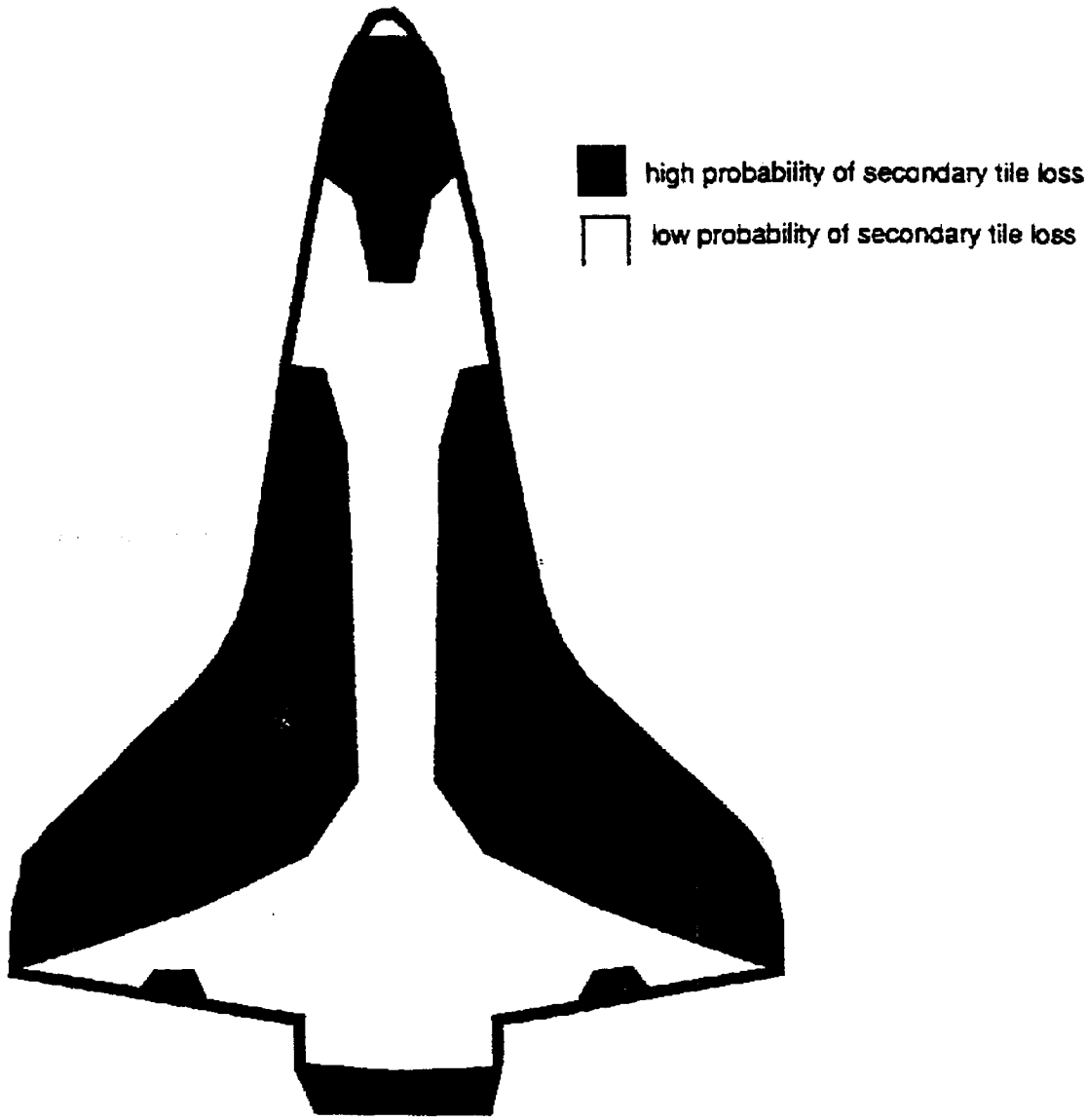


Figure 12: Partition of the orbiter's surface into two types of secondary tile loss zones (index: i)

3.2.4 Functional criticality classification

The varying criticality of the subsystems of the orbiter located under the aluminum skin is handled by partitioning the tiles into three *functional criticality areas.* Once a burn-through has occurred, various systems would be exposed to extreme heat and would fail. If those systems were essential for flight, their failure could lead to the loss of the orbiter. By examining the location of critical systems (electrical, hydraulic, fuel, etc. as shown in Figures 13 and 14), three areas were identified (Figure 15). The following probabilities were estimated by assuming that a burn-through would cause an area of four square feet around the hole to be exposed to hot gases.

Area of high functional criticality:	P(Loss of orbiter | Burn-through) = 0.8
Area of medium functional criticality:	P(Loss of orbiter | Burn-through) = 0.2
Area of low functional criticality:	P(Loss of orbiter | Burn-through) = 0.05

Table 6: Probabilities of LOV conditional on burn-through in functional criticality areas shown in Figure 15

3.2.5 Debonding caused by factors other than debris impact

In this model, it is assumed that the probability of debonding caused by factors other than debris impact is the same for all tiles. In reality, the location of screed, thin SIP, and gap filler as well as the age of RTV, and the temperature and pressure zones would affect the probability of debonding. Short of conducting considerable additional research, this simplification should be adequate. Again, the probabilities used for illustration are only coarse estimates that are intended to provide an idea of the relative magnitude of the debonding problem to the debris problem. Another relationship not considered directly in this analysis is the effect of weak bonding on the susceptibility of a tile to debris impact. A weakened tile is much more likely to be dislodged by a medium-sized debris hit. For the purposes of this

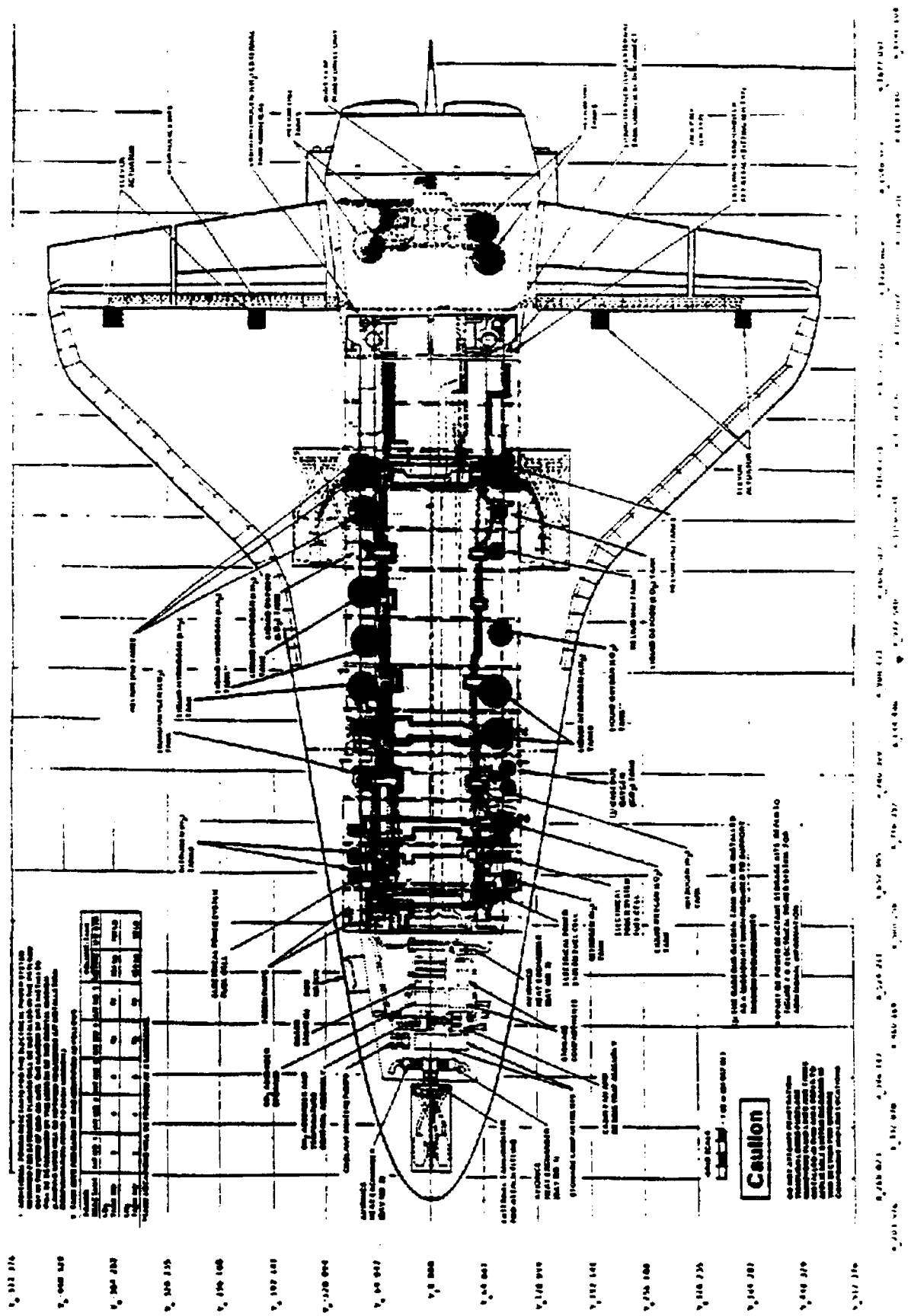


Figure 13: Component and systems location

Source: Shuttle Operational Data Book, JSC 08934 Vol. 1

Figure 14: Hydraulic system components and line locations

Source: Shuttle Operational Data Book, JSC 08934 Vol 4

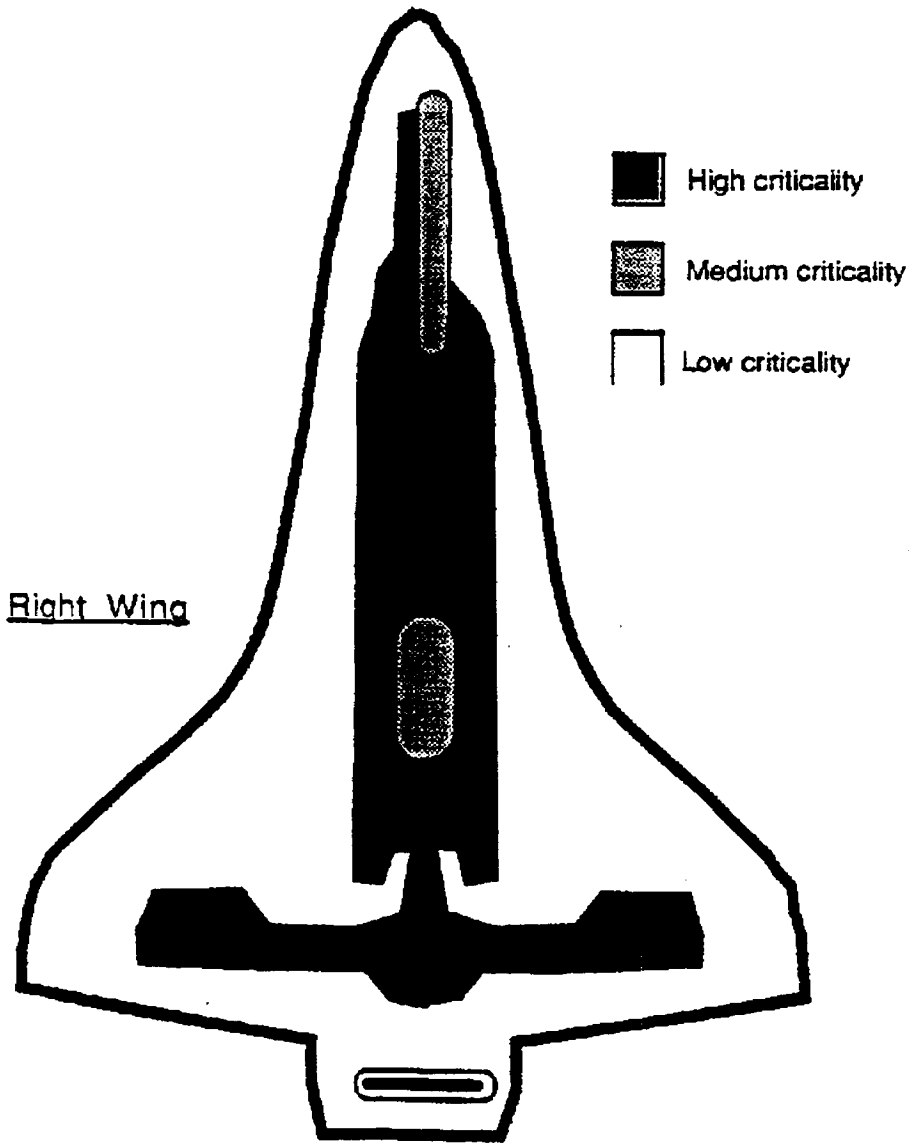


Figure 15: Partition of the orbiter's surface into three types of zones of functional criticality (index: j)

model, with its uniform distribution of debonding, this factor is included in the debris analysis.

Of the approximately 130,000 black tiles that have been installed at various times on all the orbiters, 18 have been found during maintenance to have no bond other than through the gap filler. A complete analysis of tile capacity, as revealed by the maintenance observations, will be part of the second phase of this work. We assumed, for the moment, that about half of the unbonded tiles that are held in place by the gap fillers have been detected by now, either because of visible slumping or because they have been replaced for other reasons such as debris damage (about 25% so far have been replaced.) Those with no bond that have not been detected so far are those that have not yet shown visible signs of weakness and have not needed replacement.

David Weber from KSC estimated that a tile with this weak a bond would have a probability of failure of one in a hundred (10^{-2}) per flight, making the probability of debonding of this kind, for any tile, to be approximately 9.0×10^{-7} per flight. Estimating the probabilities for the other types of debonding (excluding those caused by debris impact) is more subjective. We used a previous Lockheed study of bond verification (see Figure 16) and confirmed the results during discussions with David Weber. This study gives relative values of the probabilities of different debonding modes. Following these results, we assumed that chemical reversion of the screed and weakening due to repeated exposure to load cycles are less likely to cause debonding, and we used a probability of failure of 2×10^{-7} per tile and per flight. As a further simplification, these two probabilities (weakening due to repeated exposure to load cycles and insufficient bonding) are assumed to be independent and can thus be added. In actuality, poorly bonded tiles or tiles resting on soft screed are likely to be much more susceptible to this kind of weakening. Using these values, the probability of losing at least one of the tiles due to debonding caused by other factors than debris impact, on any flight, would be a little more than 0.02, which

FOUR MAJOR DEBOND PROBLEM TYPES

DEBOND TYPE	FREQUENCY-OF-OCCURRENCE FACTOR (1-10)	RISK FACTOR (1-10)	PRIORITY	SAMPLE PREPARED
GAP BETWEEN SIP AND RTV				
• DRIED RTV	9	10	1	X
• SIP RESTS ON EDGE OF FILLER BAR	4	10		X
GAP BETWEEN RTV AND KOROPON/AI SKIN				
• SURFACE PREPARATION	8-9	5	2	X
"FUZZ BOND" - PARTIAL PENETRATION OF RTV INTO SIP	7	3	3	
• RTV CURE RATE				X
• MISMATCH OF SIP AND FILLER BAR				X
RTV CHEMICALLY REVERTS	3	8	4	

Figure 16: Four major debond problem types

Source: R. Welling, Lockheed Corporation (1989) Reproduced by permission

then implies that over 35 flights, the probability of losing at least one tile on one of the flights is a little less than 1 50. This appears reasonable based on historical events and the one missing tile.

3.3 PRA model: definition of variables

Throughout the rest of the analysis, the areas defined in the previous section are indexed as follow:

- **i:** Index of min-zones
- **h:** Index of debris areas
- **j:** Index of functional criticality areas
- **k:** Index of burn-through areas
- **l:** Index of secondary tile loss areas

Note that a double subscript (e.g., ji) represents parameter j (criticality in this case) of min-zone i and that the term "debonding" refers to "debonding due to factors other than debris impact"

- **n:** Total number of black tiles on the orbiter
- **n_i:** Number of tiles in min-zone i.
- **N:** Total number of min-zones
- **N_i:** Number of failure patches in min-zone i.
- **q:** Index for the failure patches in any min-zone
- **M:** Final number of tiles in any failure patch
- **m:** Index for the number of tiles in a failure patch
- **Ft:** Initiating failure of a tile
- **Fa|Ft:** Failure of any adjacent tile given initiating failure
- **D:** Number of adjacent tiles in initial debris area
- **S:** Number of adjacent tiles in initial debonding area
- **L:** Loss of vehicle (LOV)
- **P(X):** Probability of event X
- **P(X|Y):** Probability of event X conditional on event Y
- **P(X,Y):** Joint probability of event X and event Y
- **EV(Z):** Expected value of random variable Z

This analysis follows closely the structure of variables described in Figure 9. Two types of initiating events are considered: those caused by debonding, and those caused by debris impact. A third category, failure of the tile itself due to heat loads,

may be added later.) It is assumed that the two types of initiating events are probabilistically independent. Since each min-zone has its own set of characteristics, they are treated as separate entities. Tiles in each specific min-zone have the same probability of being initially damaged and of causing a larger failure patch, burn-through, damage to a critical system, and the loss of the vehicle. Because of these assumptions, the analysis determines first the probability of losing the vehicle for each type of initiating event and each min-zone. The overall failure probability is the sum of the failure probabilities for all zones and initiating events. Debris impacts are considered first.

3.4 Initiating event: initial debris impact on one tile only (D=1)

To determine the probability that a specific tile in min-zone i starts a patch due to debris impact, it is also necessary to consider the size of the initial damage. We consider first the case where a single tile is initially damaged. Throughout section 3.4, it should be remembered that the probability of initial tile failure in min-zone i, $P_i(Ft)$, should be read as $P_i(Ft|D=1)$. Next sections consider $P_i(Ft|D=2)$ and $P_i(Ft|D=3)$. These additional levels of initial damage (two and three tiles simultaneously) are combined later.

Once the first tile in min-zone i is lost due to debris, there is the potential for adjacent tiles to also fail. The probability that the final patch size reaches M depends on the secondary loss index of the min-zone (l_i) and is given by the following geometric distribution (which means that M-1 additional tiles fail and no adjacent tile afterwards:)

$$P_i(M \mid Ft) = P_{li}(Fa|Ft)^{M-1} \times [1-P_{li}(Fa|Ft)] \qquad (1)$$

Note that M must be at least equal to 1. This equation assumes that the probability that adjacent tiles debond does not change as the patch grows.

In each min-zone, there is the possibility of several patches starting. The probability that the number of patches reaches N_i in min-zone i is:

$$P_i(N_i) = \frac{n_i!}{N_i!\,(n_i-N_i)!} P_i(Ft)^{N_i} \times [1-P_i(Ft)]^{n_i-N_i} \qquad (2)$$

This formulation assumes that the initial tile failures are independent, and that there will be no overlapping of patches because the probability of an initiating event (Ft) is small compared to the number of tiles in each min-zone (n_i). The product $EV(N_i) \times EV(M)$ which equals the total number of tiles lost in each min-zone is considered negligible compared to n_i. Also, N_i (number of patches) and M (size of patches) are considered independent random variables. Based on these assumptions, the expected number of patches is approximately:

$$EV(N_i) = n_i \times P_i(Ft) \qquad (3)$$

and the size of each patch is given by the mean of the distribution of M:

$$EV(M) = 1 / [1-P_i(Fail|Ft)] \qquad (4)$$

Given this result, it is now possible to calculate the probability that the orbiter will fail due to debris that impact one tile only. Remembering that j is the index of the criticality areas and k is the index of the burn-through areas, we define the probabilities of orbiter failure due to a patch of size M, in min-zone i, initiated by debris impact (D=1) as follows:

$$P_i(L|\,M=1) = p_{jki,1}$$

$$P_i(L|\,M=2) = p_{jki,2}$$

...

$$P_i(L|\,M=m) = p_{jki,m} \qquad (5)$$

It must be remembered that any given min-zone could have several patches in it, and each patch could be of a different size. To calculate the probability of orbiter loss due to specific number of patches (N_i) in min-zone i, the following definition is necessary. Let p'_i be the probability that an arbitrary patch in min-zone i causes a failure.

$$p'_i = \sum_{m=1}^{\infty} p_{jki,\,m} \times P\,(\text{patch size} = m) \qquad (6)$$

$$p'_i = \sum_{m=1}^{\infty} p_{jki,\,m} \times P_{ji}\,(Fa|Ft)^{m-1} \times [1-P_{ji}(Fa|Ft)] \qquad (7)$$

Therefore, q being the number of patches in a given min-zone, the failure probability for a specific number of patches in a min-zone is:

$$P_i(L|\, N_i=q) = p'_i \times q \qquad (8)$$

Once again, this assumes that the probabilities are small and that the patches will not interfere with each other (they are assumed to be separate and independent). These assumptions are valid providing that each min-zone has a sufficiently large number of tiles and that the size of the patches is relatively small.

Based on Equation (8), the probability of orbiter failure given all patches that occur in min-zone i becomes:

$$\begin{aligned} P(L|\text{min-zone i}) &= \sum_{q=0}^{\infty} P_i(L|N_i=q) \times P_i(N_i=q) \\ &= \sum_{q=0}^{\infty} p'_i \times q \times P_i(N_i=q) \\ &= p'_i \times EV(N_i) \\ &= p'_i \times n_i \times P_i(Ft) \end{aligned} \qquad (9)$$

This result represents only the cases of debris impact causing the initial failure of a single tile. A more complete rewriting of Equation 9 highlights this fact:

$$P(L|\text{min-zone } i, D=1) = a'_i(D=1) \times n_i \times P_i(Ft|D=1) \qquad (10)$$

3.5 Initiating event: initial debris impact on several tiles (D=d)

In order to expand this model to include the possibility that the initial debris impact damages more than one tile, it is necessary to modify some of the above equations. It is assumed that if a large enough piece of debris hits the orbiter, several adjacent tiles may be knocked loose at once. Each of these missing tiles may in turn cause their adjacent tiles to fail and a specific number of additional tiles can fail in multiple ways. Therefore, additional summations are required in order to account for the increased number of exposed tiles. This compounded problem requires that Equation (1) be rewritten to account for this potentially larger patch growth rate. If the initial damage involves two tiles, the probability that the final patch reaches size M is:

$$P_i(M|Ft, D=2) = (M-1) \times P_{ii}(Fa|Ft)^{M-2} \times \left[1 - P_{ii}(Fa|Ft)\right]^2 \qquad (11)$$

If three tiles are damaged initially:

$$P_i(M|Ft, D=3) = \left[\sum_{k=1}^{M-1} k\right] \times P_{ii}(Fa|Ft)^{M-3} \times \left[1 - P_{ii}(Fa|Ft)\right]^3 \qquad (12)$$

If four tiles are damaged initially:

$$P_i(M|Ft, D=4) = \left[\sum_{k=1}^{M-4} \sum_{i=1}^{k} i\right] \times P_{ii}(Fa|Ft)^{M-4} \times \left[1 - P_{ii}(Fa|Ft)\right]^4 \qquad (13)$$

This set of equations can be extended to include greater initial damage; historical evidence, however, supports limiting the analysis to this level. It must be remembered that the value M of the final patch size must always be at least equal to the size of the initial damage area, D. Equation (2) in its most general form is written:

$$P_i(N_i|D=d) = \frac{N_i!}{n_i!\,(N_i-n_i)!} P_i(Ft|D=d)^{Ni} \times [1-P_i(Ft|D=d)]^{ni-Ni} \qquad (14)$$

and Equation (3) becomes:

$$EV(N_i) \approx n_i \times P_i(Ft|D=d) \qquad (15)$$

Equations (5) and (6) do not change except for the indexing of the summation since their results depend only on the final patch size and the functional criticality index. Equation (7) would change as Equations (11) to (13) are integrated to account for the various debris damage areas. The final probability for each initial damage area and min-zone is computed using a variant of Equation 10:

$$P(L|\text{min-zone } i, D=d) = p'_i(D=d) \times n_i \times P_i(Ft|D=d) \qquad (16)$$

Because all the initial damage probabilities are very small, it is possible to approximate the probability of debris causing loss of an orbiter for all damage areas in a particular min-zone by:

$$P(L|\text{min-zone } i, \text{debris}) = \sum_{d=1}^{\text{Max } d} P(L|\text{min-zone } i, D=d) \qquad (17)$$

Once this probability is determined, the probability of orbiter failure for all min-zones due to debris impact is simply the sum of the probabilities of failure for all min-zones since all min-zones and initiating events are assumed to be independent:

$$P(L|debris) = \sum_{i=1}^{N} P(L|min\text{-}zone\ i, debris) \qquad (18)$$

3.6 Initiating event: debonding caused by factors other than debris impact

The same procedure and basic formulas are used to determine the probability of orbiter failure due to debonding caused by factors other than debris impact. Again, the probability of orbiter failure due to failure of the TPS is computed from the probability of tiles spontaneously debonding in groups of various sizes in each min-zone. The problem is slightly easier since it is assumed that the likelihood of such debonding is uniform across all tiles. The probability of secondary tile failure $P_i(Fa|Ft)$ is the same as for the debris problem. The probability of orbiter failure based on all patches in min-zone i that started from a damage area of initial size s is given by:

$$P(L|min\text{-}zone\ i, S=s) = p'_i(S=s) \times n_i \times P_i(Ft|S=s) \qquad (19)$$

The other equations follow accordingly. The total probability of shuttle failure for damage initiated by debonding caused by factors other than debris impact is:

$$P(L|debonding) = \sum_{i=1}^{N} P(L|min\text{-}zone\ i, debonding) \qquad (20)$$

Finally, assuming independence of initiating events (debris and debonding due to other causes), the overall probability of shuttle failure per flight due to tile damage is:

$$P(L|tile\ problem) = P(L|debonding) + P(L|debris) \qquad (21)$$

3.7 Additional information and data

A PRA model like the one described above needs to be constantly updated to reflect information that may have existed before but had not been uncovered at the time of this initial study, and information from new experience including recent inspections, tests, evaluations, studies, and in-flight performance data. In this implementation phase, more refined data may thus be used and additional information available at NASA can be introduced in the analysis. One important part of the problem at that stage will be to capture the evolution of the failure probability of the orbiter. Clearly, *the system is not in a steady state*. On one hand, the quality of the maintenance work appears to improve (Figure 17). Initial defects of the installation work that resulted in a decrease of the tile capacity are progressively being discovered and corrected during successive maintenance operations. Existing problems, such as the impact of chunks of insulation from the ET and the SRBs or the elevon-cove design problem, are resolved as they are discovered. On the other hand, the possibility of long-term deterioration of the TPS clearly increases the probability of tile failure (even if slowly) and the rate of deterioration is a major unknown. Of specific concern are: the possibility of degradation of the bond over time, of slow chemical reaction due to water proofing agent, and of weakening of the SIP/tile system under exposure to repeated load cycles. Additional data regarding the initial test results used in the certification procedure from JSC and from the manufacturers of the tiles, the SIPs, and the bond are needed to update the model. Therefore, this updating should be based not only on statistical data on tile performance during each flight, but also on basic information about the components of the TPS.

A complete analysis of the distribution of tile capacities will require additional data from maintenance operations including:

- The numbers of tiles replaced so far on each orbiter;
- A statistical distribution of the percentage of the surface of the tile/SIP system that was found to be actually bonded to the orbiter's skin;

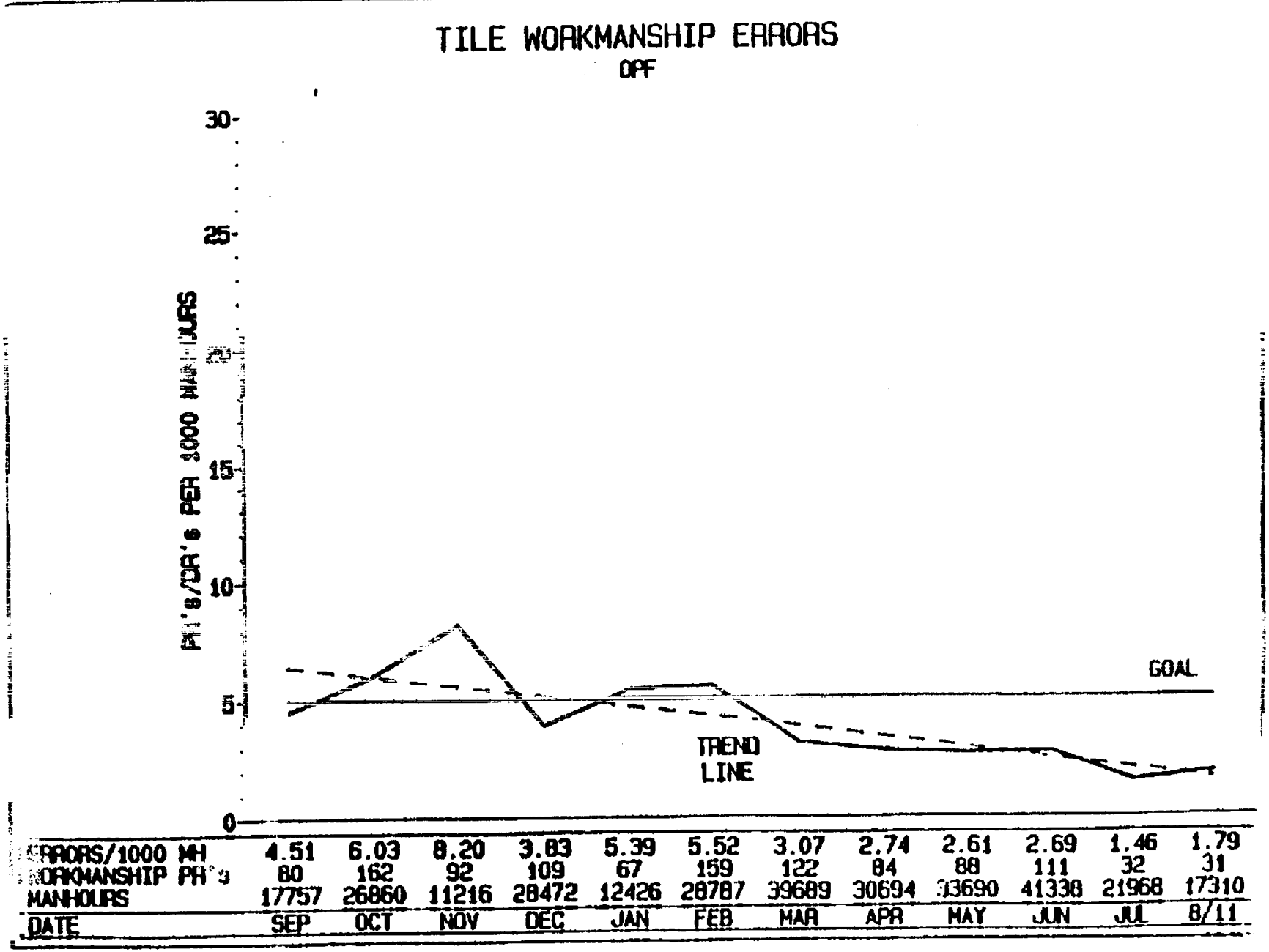


Figure 17: Tile workmanship errors

Source: D. Weber, Lockheed Corporation (1989)

- Estimates of the probability of failure of a tile of given capacity (e.g., 10% bonded) under different kinds of load (e.g., debris hit >1").

A more refined partition of the orbiter's surface can be obtained using data such as:

- Effect of excessive step and gap on the heat load in different locations;
- Possibility of partial failure of the guidance system or control surfaces at re-entry and corresponding increase in the heat load;
- Trajectories of debris from the ET and the SRBs. Computer simulations done at JSC (see Figures 18 and 19) could give better information about the vulnerability of the orbiter's TPS, in particular in the most risk-critical areas;
- Measurements of temperatures and aerodynamic forces on the surface of the orbiter (see Figures 20 and 21);
- Effect of tile loss on the orbiter's surface temperature in the cavity (Figure 22).

The analysis itself can be refined in several ways. A major unknown is the performance of the subsystems under the orbiter's skin once they are exposed to excessive heat loads due to TPS failure. The only alternative, short of a systematic PRA of these individual systems, is to use subjective estimates. Finally, it seems that the availability of a kit for in-orbit repair of the tiles might provide a significant reliability gain. An assessment of its effectiveness will be included in Phase 2 of this study.

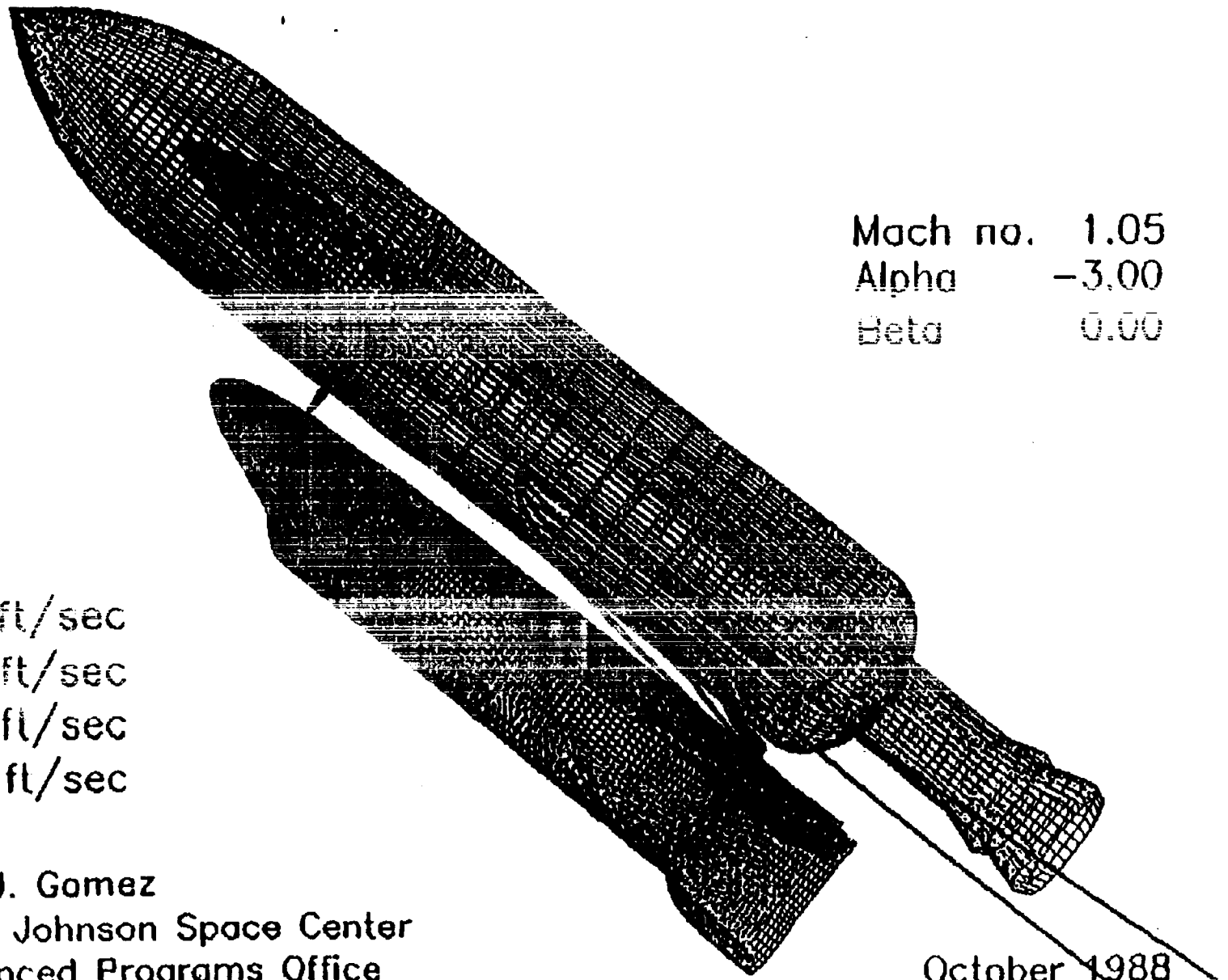
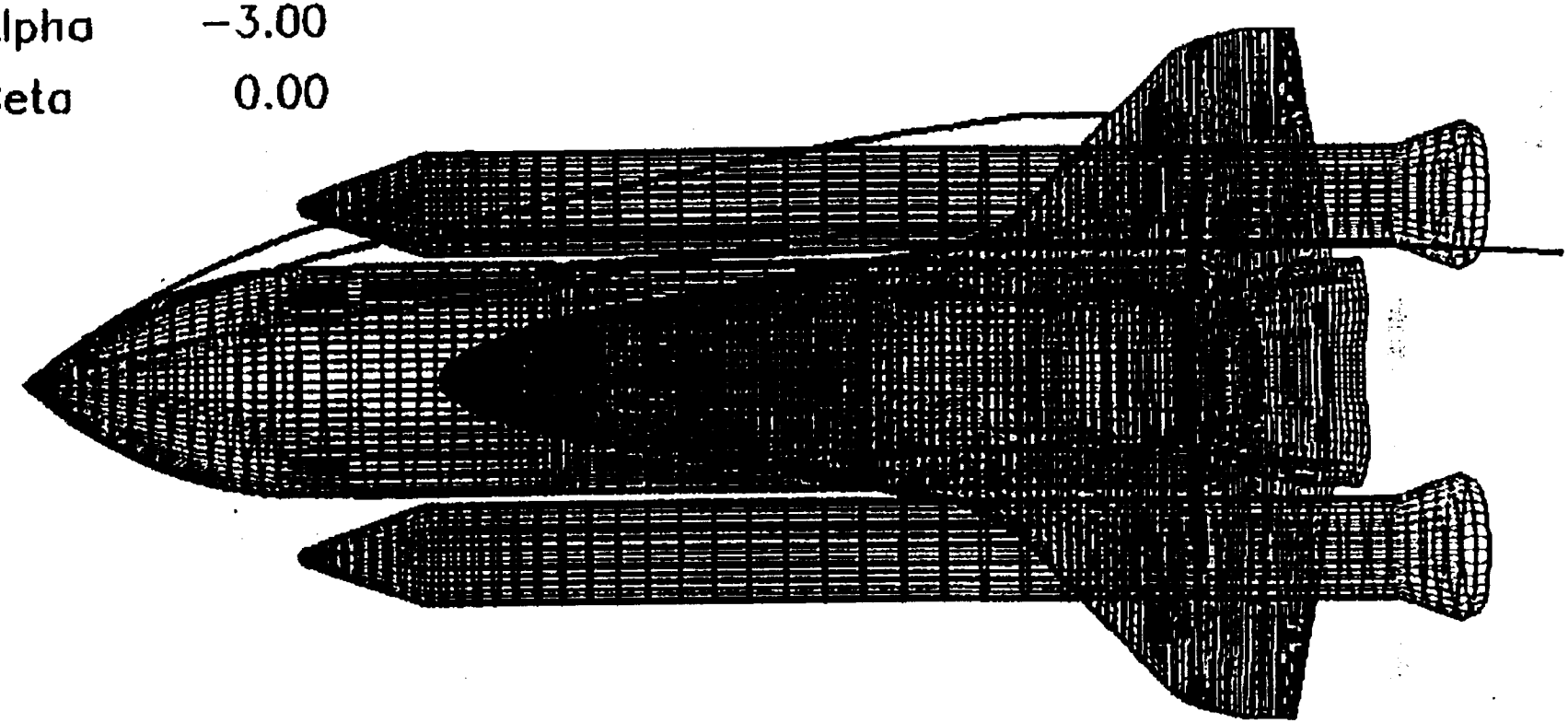


Figure 18: Ascent debris trajectory simulation (side view)

Source: R. Gomez, NASA JSC (1988)

Ascent Debris Trajectory Simulation



Ray J. Gomez
NASA Johnson Space Center
Advanced Programs Office

October 1988

Figure 19: Ascent debris trajectory simulation (plan view)

Source: R. Gomez, NASA JSC (1988)

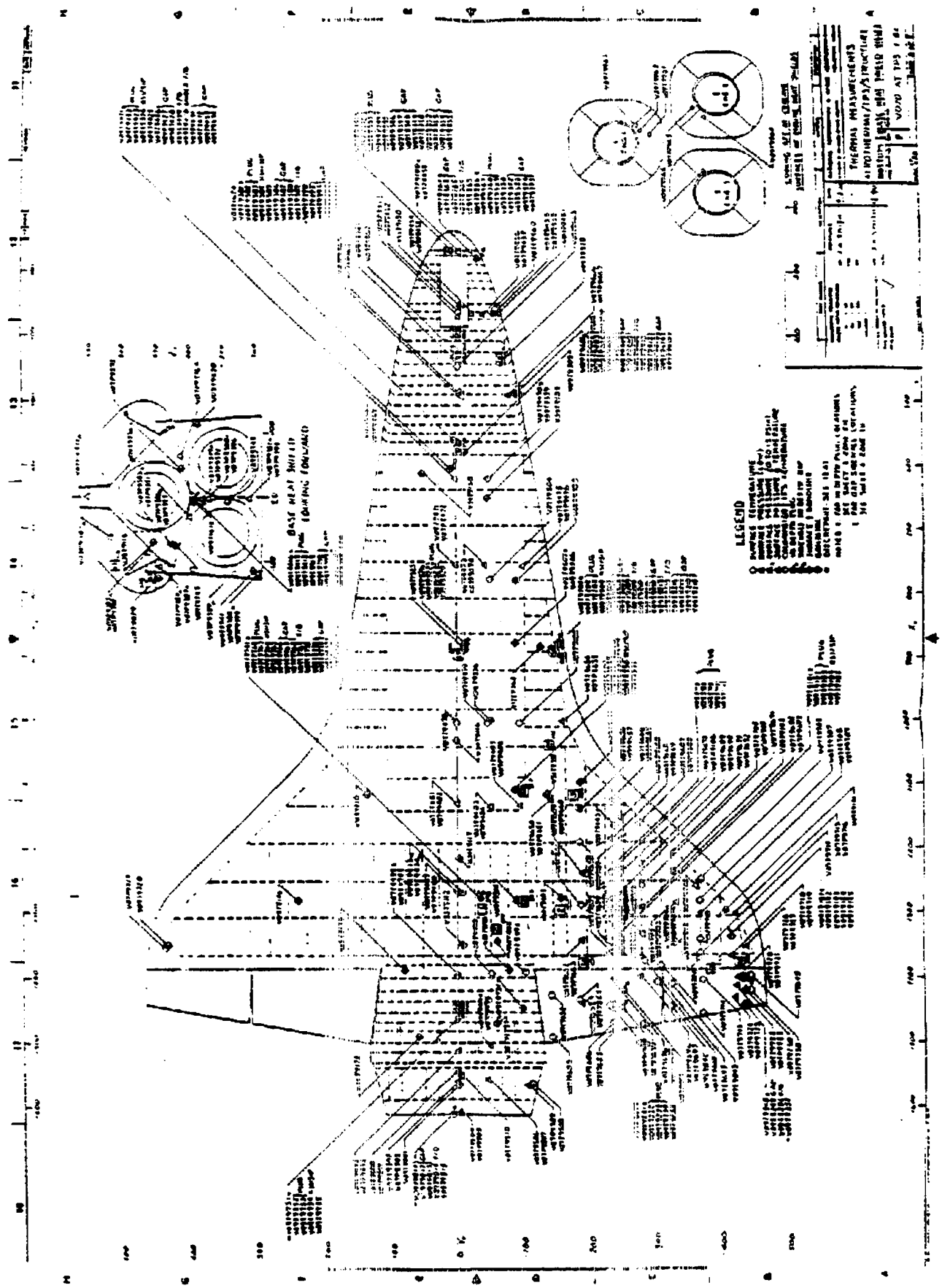


Figure 20: Thermal measurements (bottom view)
Source: Structural & Aerodynamic Pressure Measurement Locations JSC 17889

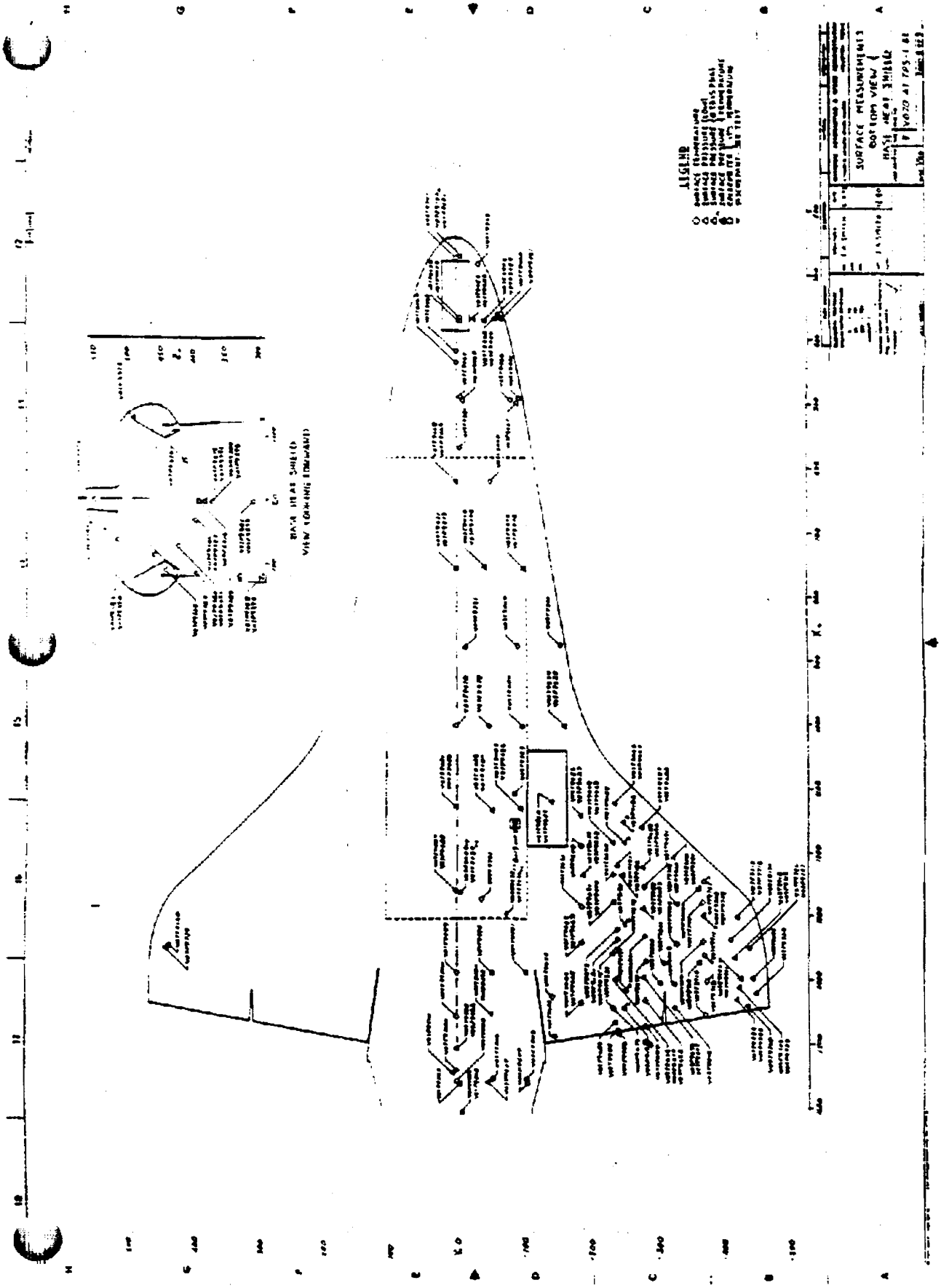


Figure 21. Surface measurements (bottom view)
Source: Structural & Aerodynamic Pressure Measurement Locations JSC 17889

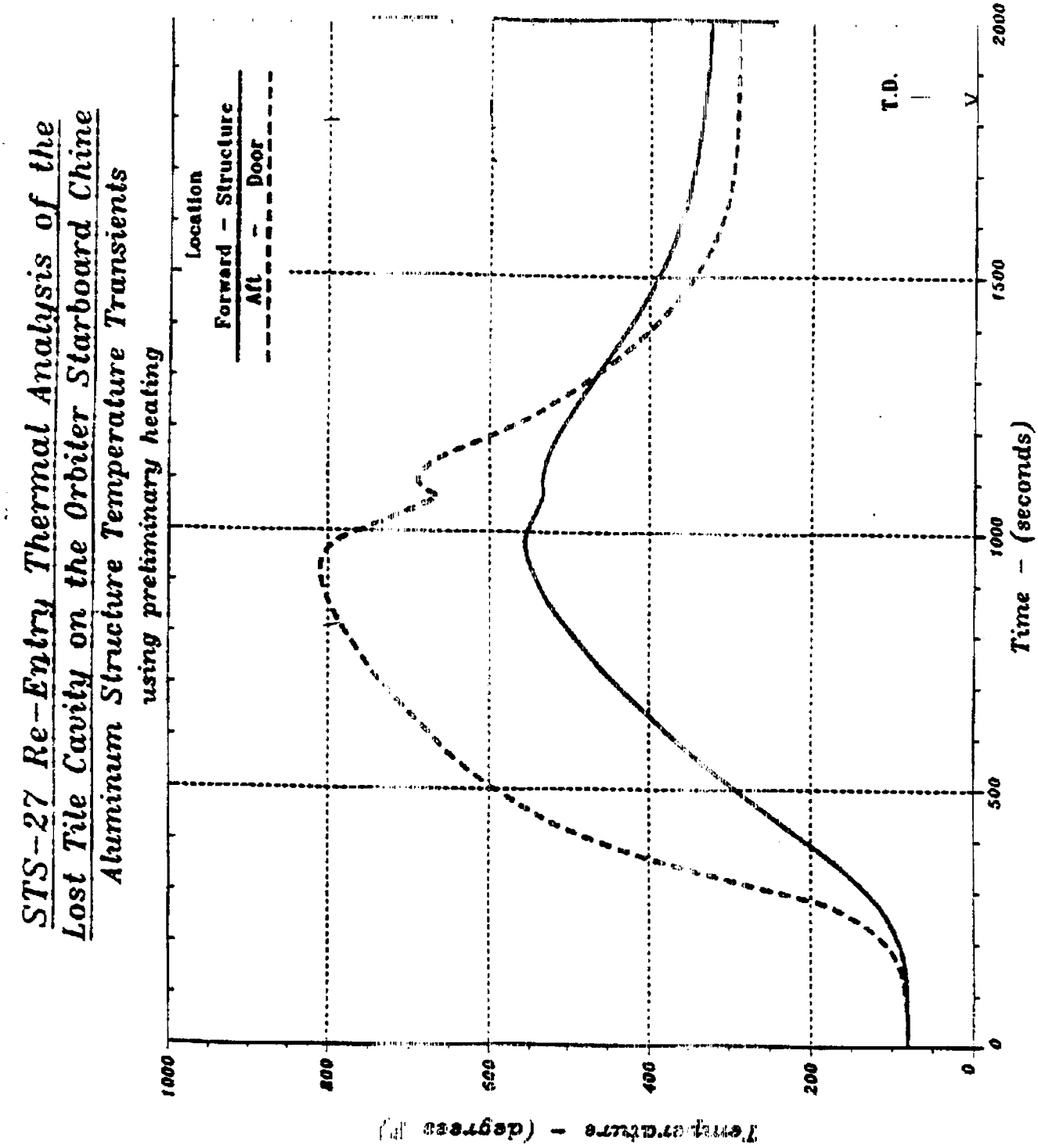


Figure 22: Re-entry thermal analysis of lost tile cavity

Source: R. Maria, NASA JSC (1988)

Section 4:
ILLUSTRATION OF THE MODEL

The illustration of the model presented here is based on coarse numbers whose relative values are more significant than their absolute values. By overlaying the functional criticality, burn-through, debris damage, and secondary tile loss areas, 33 min-zones were established. Of these, 21 are unique zones (i.e., that have different sets of indices). Several zones with the same combinations of indices appear on different locations on the orbiter. Figure 23 shows the final layout of the min-zones and the numerical results of the model. Each zone is assigned an identification number. The lower numbers are generally assigned to more critical areas. Each zone is also identified by an index number whose digits relate to the four area types shown in Table 7:

1st digit:	Burn-through areas (1 high, 2 medium, 3 low, probabilities)
2nd digit:	Functional criticality areas (1 high, 2 medium, 3 low, criticality)
3rd digit:	Debris damage areas (1 high, 2 medium, 3 low, probabilities)
4th digit:	Secondary tile loss areas (1 high, 2 low, probability)

Table 7: Structure of the indices of the min-zones shown in Figure 22 and Table 8.

Table 8 lists the min-zones, and shows the number of tiles in each zone and the probability of failure of the orbiter attributable to this zone. This value was determined by calculating this probability for both initiating events and then summing to obtain the results. The boundaries of the min-zones have been simplified: the number of tiles in each area is only an approximation and is not based on an actual count. The location description is only intended to provide a rough placement of the

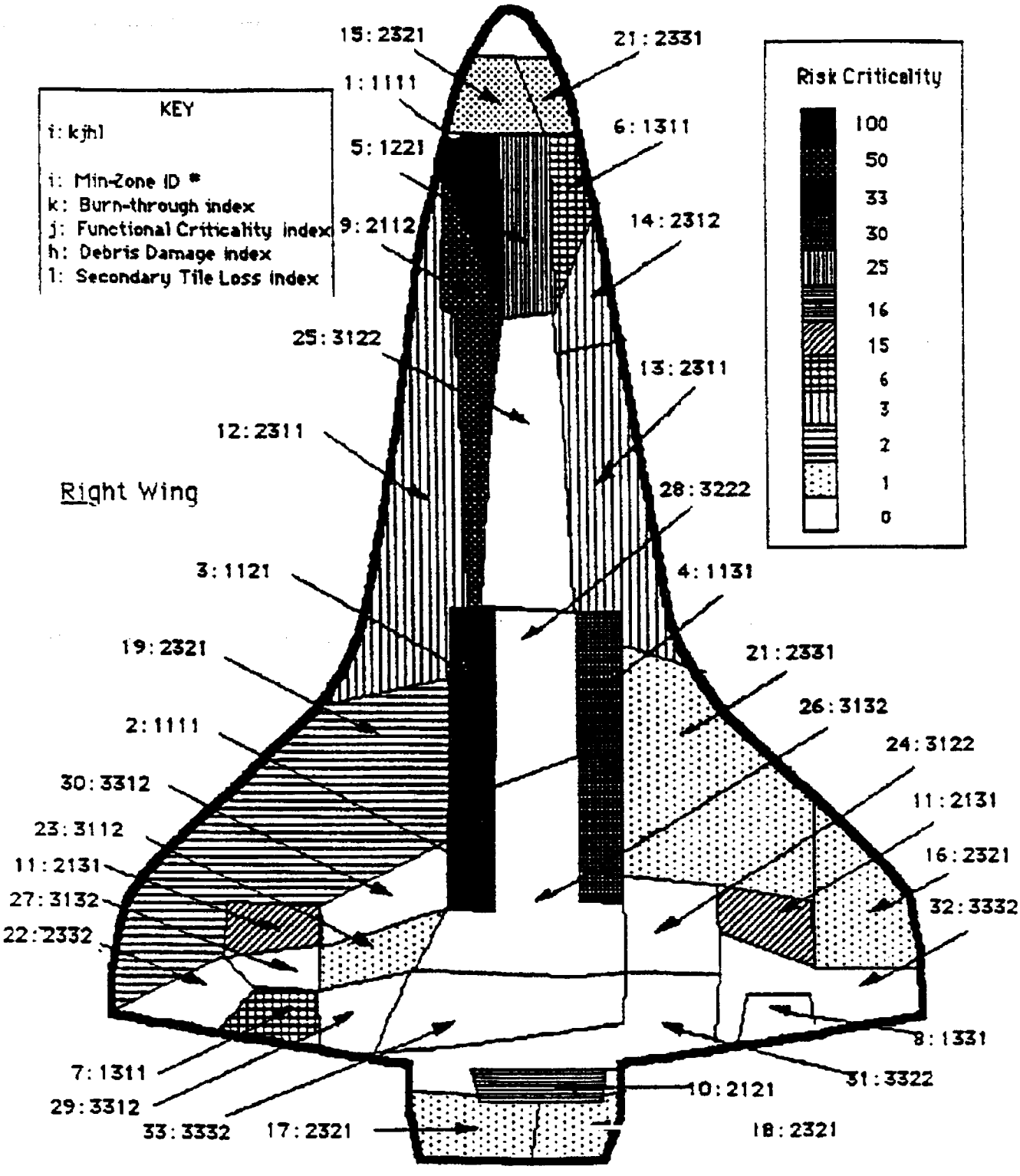


Figure 23: Partition of the orbiter's surface into 33 min-zones (index: i)

ID #	Index	Location	# Tiles	P(LOV) 10^{-4} Debris	Debond	Total
1	1111	Right side, under crew	156	0.87	0.36	1.23
2	1111	Right side, near main ldg gear (aft)	156	0.87	0.36	1.23
3	1121	Right side, near main ldg gear (fwd)	676	0.13	1.62	1.75
4	1131	Left side, near main ldg gear	780	0.00	1.87	1.87
5	1211	Centerline, under crew	364	0.51	0.22	0.73
6	1311	Left side, under crew	312	0.11	0.04	0.15
7	1311	Center of right elevon	104	0.04	0.01	0.05
8	1331	Center of left elevon	104	0.00	0.00	0.00
9	2112	Right side, fwd mid edge	624	1.73	0.75	2.48
10	2121	Center of body flap	208	0.02	0.24	0.26
11	2131	Left wing, center	468	0.00	0.56	0.56
12	2311	Right side, mid edge	1664	0.30	0.13	0.43
13	2311	Left side, mid edge	1196	0.21	0.08	0.29
14	2312	Left side, fwd mid edge	572	0.10	0.04	0.14
15	2321	Right side, nose	277	0.01	0.02	0.03
16	2321	Left wing, center	832	0.01	0.06	0.07
17	2321	Right side, body flap	104	0.00	0.01	0.01
18	2321	Left side, body flap	104	0.00	0.01	0.01
19	2321	Right wing	2132	0.18	0.16	0.34
20	2331	Left side, nose	312	0.00	0.02	0.02
21	2331	Left wing, fwd	1768	0.00	0.13	0.13
22	2332	Right elevon, outboard	312	0.00	0.02	0.02
23	3112	Right wing, center	364	0.01	0.01	0.02
24	3122	Left wing, center	468	0.00	0.01	0.01
25	3122	Center, payload bay fwd	1664	0.00	0.02	0.02
26	3132	Center, payload bay aft	1976	0.00	0.02	0.02
27	3132	Right wing, center	468	0.00	0.01	0.01
28	3222	Center, payload bay, mid	520	0.00	0.00	0.00
29	3312	Right elevon, in board	312	0.00	0.00	0.00
30	3312	Right wing, center	416	0.00	0.00	0.00
31	3322	Left elevon in / center body flap	728	0.00	0.00	0.00
32	3332	Left elevon, outboard	572	0.00	0.00	0.00
33	3332	Center, aft	1040	0.00	0.00	0.00
			Totals	5.09	6.79	11.88

Table 8. Identification of the min-zones and their contribution to the probability of LOV

min-zone. No attempt has been made to use orbiter notations. The final numerical results of the model are presented in the right-hand column as multiples of 10^{-4}. The probability values are mostly in the order of 10^{-4}. Again, it is important to remember that the importance of the numbers is not their magnitude, but their relative values when compared to each other. According to our coarse numerical analysis, the total probability of losing the orbiter on any given mission, due to TPS failure, is in the order of 10^{-3}. It is interesting to note that approximately 40% of this probability is attributable to debris-related problems and that 60% comes from problems of debonding caused by other factors. By scanning the columns, it appears that a few min-zones contain most of the risk.

Using a risk-per-tile measure, the min-zones can be ordered according to their criticality with respect to the two types of initiating events, and to the total probability of failure. The results are shown in Tables 9 and 10. Table 9 displays the contribution of each min-zone and of each tile to the probability of LOV separated into debris and debonding due to other factors. Table 10 shows the contribution of each tile and each min-zone to the overall probability of LOV. In this table, we show for each tile, *a risk-criticality factor* that is proportional to the relative contribution of this tile to the overall failure probability, accounting not only for the loads applied to this tile but also for the consequences should it fail. This risk-criticality factor is the point of reference that will be used in the second phase of the study to set priorities among different management measures designed to improve tile reliability.

A slightly different graphic representation of this table is displayed in Figures 24, 25, and 26. It is possible from our results to identify *the most sensitive min-zones* by ranking them by order of individual tile criticality. One can then plot the marginal increase of the failure probability for each added min-zone, the slope of each segment representing the (decreasing) contribution of each tile to the failure probability. Each black dot represents the addition of the next most critical min-zone. The greater the horizontal spacing between the dots, the larger the number of tiles in

Debris			Debonding		
ID#	P(LOV)/zone 0.00E-4	P(LOV)/tile 0.00E-8	ID#	P(LOV)/zone 0.00E-4	P(LOV)/tile 0.00E-8
1	0.870	55.770	4	1.870	24.000
2	0.870	55.770	3	1.620	24.000
9	1.230	27.720	1	0.360	23.100
5	0.610	14.010	2	0.360	23.100
6	0.[illegible]10	3.365	9	0.750	12.000
7	0.[illegible]40	3.365	11	0.560	12.000
3	0.[illegible]80	1.923	10	0.240	11.500
12	0.[illegible]00	1.785	5	0.218	5.990
13	0.[illegible]10	1.781	6	0.045	1.440
14	0.[illegible]00	1.748	7	0.015	1.440
10	0.[illegible]20	0.961	15	0.023	0.829
19	0.[illegible]35	0.867	12	0.130	0.781
23	0.[illegible]0	0.274	16	0.065	0.781
17	0.[illegible]02	0.192	21	0.133	0.752
18	0.[illegible]02	0.192	14	0.043	0.752
15	0.[illegible]03	0.108	20	0.023	0.737
16	0.[illegible]08	0.096	22	0.023	0.737
4	0.[illegible]00	0.000	19	0.156	0.673
8	0.[illegible]00	0.000	17	0.007	0.673
11	0.[illegible]00	0.000	18	0.007	0.669
20	0.[illegible]00	0.000	13	0.080	0.137
21	0.[illegible]00	0.000	23	0.005	0.128
22	0.[illegible]00	0.000	24	0.006	0.128
24	0.[illegible]00	0.000	27	0.006	0.121
25	0.[illegible]00	0.000	26	0.024	0.114
26	0.[illegible]00	0.000	25	0.019	0.038
27	0.[illegible]00	0.000	28	0.002	0.000
28	0.[illegible]00	0.000	8	0.000	0.000
29	0.[illegible]00	0.000	29	0.000	0.000
30	0.[illegible]00	0.000	30	0.000	0.000
31	0.[illegible]00	0.000	31	0.000	0.000
32	0.[illegible]00	0.000	32	0.000	0.000
33	0.[illegible]00	0.000	33	0.000	0.000

Table 9: Probabilities of Loss of Vehicle due to tile failure initiated (1) by debris damage and (2) debonding caused by factors other than debris, for each min-zone, and each tile in each min-zone

ID #	P(LOV)/zone 0.00E-4	P(LOV)/tile 0.00E-8	Risk Criticality 0-100 scale	Number of Tiles	Location
1	1.2300	78.800	100	156	rt under crew
2	1.2300	78.800	100	156	rt main gear aft
9	2.4800	39.700	50	624	rt fwd mid edge
3	1.7500	25.900	33	676	rt main gear
4	1.8700	24.000	30	780	lt main gear
5	0.7280	20.000	25	364	center crew
10	0.2600	12.500	16	208	body flap cen
11	0.5600	12.000	15	468	lt/rt wng cen out
6	0.1500	4.810	6	312	lt crew
7	0.0500	4.810	6	104	rt elevon cen
12	0.4270	2.570	3	1664	rt side mid edge
14	0.1430	2.500	3	572	lt fwd mid edge
13	0.2930	2.450	3	1196	lt middle
19	0.3410	1.600	2	2132	rt wing
15	0.0260	0.938	1	277	rt nose
16	0.0730	0.877	1	832	lt wing outboard
17	0.0090	0.865	1	104	body flap rt
18	0.0090	0.865	1	104	body flap lt
21	0.1330	0.752	1	1768	lt wing forward
20	0.0230	0.737	1	312	lt nose
22	0.0230	0.737	1	312	rt elevon out
23	0.0150	0.412	1	364	rt wing center in
24	0.0060	0.128	<1	468	lt wing center in
27	0.0060	0.128	<1	468	rt wing cen out
26	0.0240	0.121	<1	1976	center bay aft
25	0.0190	0.114	<1	1664	center upper bay
28	0.0020	0.038	<1	520	center mid bay
8	0.0000	0.000	<1	104	lt elevon center
29	0.0000	0.000	<1	312	rt elevon in
30	0.0000	0.000	<1	416	rt wing cen
31	0.0000	0.000	<1	728	lt elev/body flap
32	0.0000	0.000	<1	572	lt elevon out
33	0.0000	0.000	<1	1040	center aft

Table 10: Risk-criticality factor for each tile in each min-zone

C-5

the zone. Several small min-zones contain a large part of the risk (those with the steepest slope), whereas several very large min-zones carry only a small part of the risk (those with zero slope). Figure 23 shows the contribution of increasing percentages of the tiles to the risk for debris-initiated damage. Note that, for failures initiated by debris, *80% of the risk is due to only 8% of the tiles.* For debonding problems that are not caused by debris, the contribution of increasing percentages of tiles are shown in Figure 24: *80% of the risk is due to 13% of the tiles.* Finally, the overall result is shown in Figure 25: for the total risk, including both initiating events, *80% of the risk can be attributed to 14% of the tiles.* It is important to remember that the same tiles do not necessarily appear in the same order in each graph. Clearly, some zones pose a much higher risk for one type of initiating event than for the other. For example, min-zone 4 located near the left main gear has not historically experienced significant debris damage and is not on the obvious trajectory of tractable debris; so, the probability of LOV due to TPS *debris* damage in that zone is basically zero. There are, however, some critical components that are temperature sensitive under the skin in that area; so, the risk of LOV due to *debonding* is non negligible (1.07×10^{-4}).

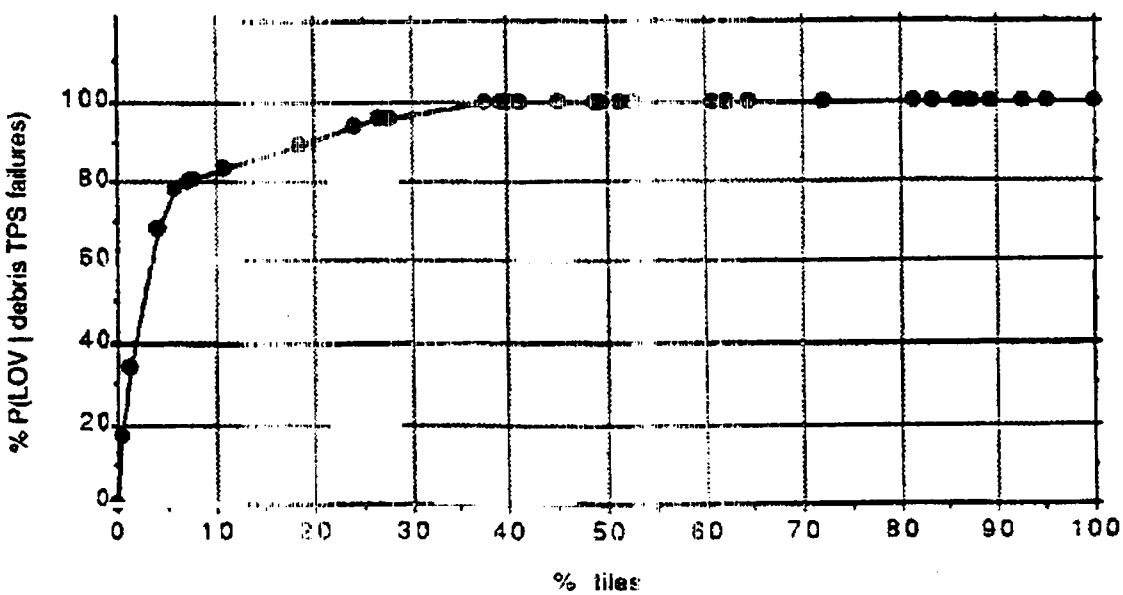


Figure 24: Relative risk of LOV due to debris-initiated TPS damage

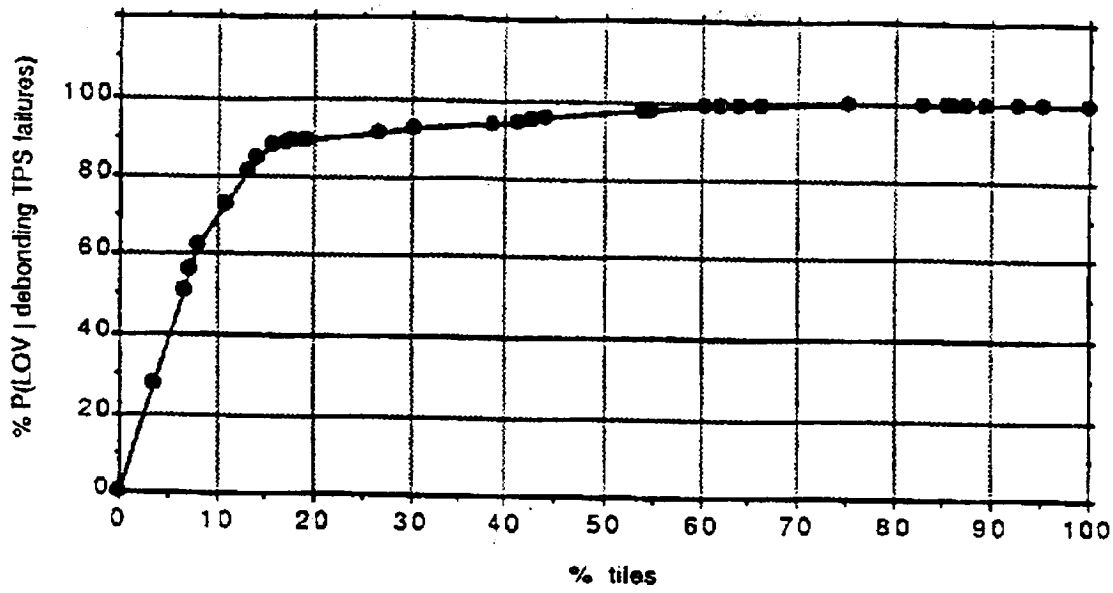


Figure 25: Relative risk of LOV due to debonding-type TPS damage

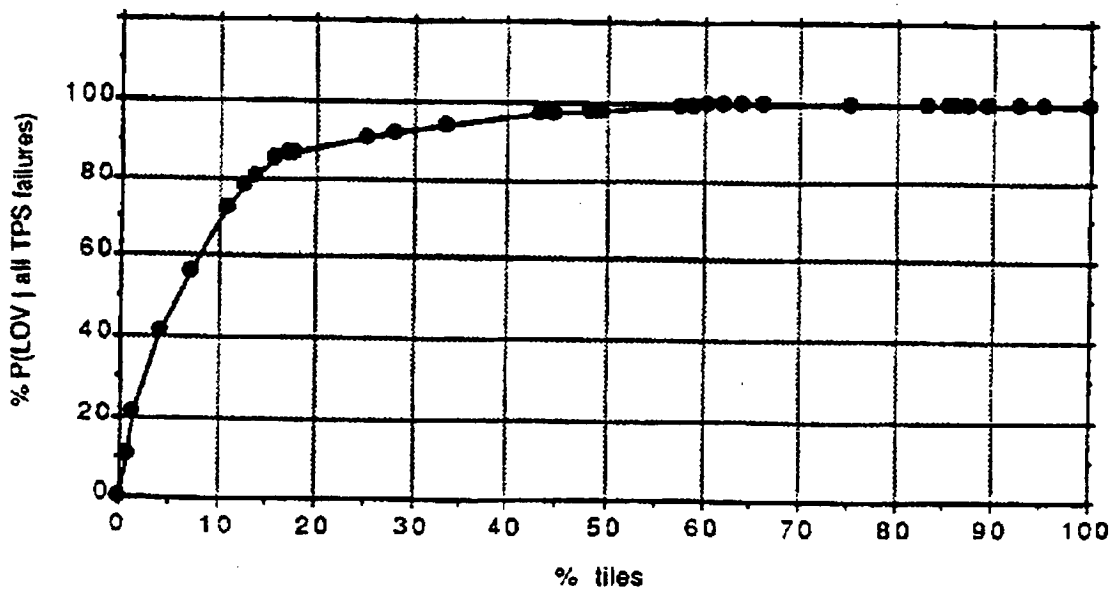


Figure 26: Relative risk of LOV due to both types of TPS damage

Section 5:
EFFECTS OF ORGANIZATIONAL FACTORS ON TPS RELIABILITY: MAIN PRELIMINARY OBSERVATIONS

5.1 Errors and risk

Well-bonded tiles are very unlikely to debond even under moderate debris loads. Given the temperature gradients measured inside the tiles during flights, it has been determined that the tiles absorb most of the heat within a fraction of their thickness and that they are very unlikely to burn, even considering a wide range of re-entry scenarios. If the tiles are to fail, it is likely to be because they have been weakened and/or hit by debris. The problem is that one does not know which ones are weak. Human errors (past and present) are at the source of at least three of the fundamental causes of tile failure: (1) decrease of tile capacity because of undetected partial or weakened bonding, (2) increase in the heat loads due to roughness of the orbiter's surface (caused, for example, by protruding gap fillers), and (3) poorly-installed and maintained insulation on the SRB's and ET that flakes off during ascent, damaging the TPS. These human errors are often the consequences of the way the organizations (NASA and its contractors) operate.

In the second phase of this work, we will explore to what extent *organizational procedures* (for instance, those that induce time pressure and turnover of the personnel) are at the root of these incidents. Rules that apply uniformly across tiles of widely variable risk-criticality, and rules that do not account for the possibility of system weakening over time may become major contributors to the overall risk. Furthermore, the scope of the research cannot be strictly limited to the TPS. Procedures and management decisions regarding the maintenance of the insulation of the ET and the SRBs also affect the reliability of the tiles since they are a

source of debris. Finally, in the long term, weakening of the tile system due to repeated load cycles, exposure to environmental conditions on the ground, or chemical reversion, may become a dominant factor of the failure risk. The problem of deterioration over time may not be (and is not likely to be) of immediate concern for well-bonded tiles, but may become a critical factor for those tiles whose capacities have been reduced by defective installation and maintenance. Therefore, in the second phase, we will examine closely the procedures of the organization, using our PRA model to see how the relative contributions of each of these factors affect flight safety.

In addition, the *structure of the organization* and its peripherals (NASA, plus Lockheed, Rockwell etc.) and the rules that determine the relations among these organizations (for example, in setting contracts, pay scales, and incentives, as well as schedule and budget constraints,) may also affect flight safety to the extent that they determine the occurrence and severity of human errors and their probabilities of detection. Some organizational improvements (which may have been recommended before and ignored for various reasons) may have only a minor effect on the reliability of the orbiter; others may be essential soon. Our analytical model will be used to determine which of these factors actually affect the probability of failure of the tiles (and consequently, of the orbiter) and by how much. Finally, the *culture of the organization* may also play a role. As we describe below, the low status of the tile work may induce low morale among some tile technicians. Furthermore, the behaviors of other workers towards the tile technicians may be a significant source of additional work load and time pressure.

Errors (most of which can be traced back to these organizational factors) can be classified using a taxonomy which has been designed to guide the choice of management improvements (Paté-Cornell, 1990.) Errors are categorized into two groups: *gross errors* (uncontroversial mistakes, for example, an unbonded tile) and *errors of judgment under uncertainty* (for instance, the decision to live with a

problem that seems minor --but may not be so-- until the next flight in order to decrease the work load.) Gross errors generally call for improvements of the hiring and training procedures, inspection and quality control, and information flow; errors of judgment generally require modification of incentives and rewards, improvement in the treatment and communication of uncertainties, and adaptation of the resource constraints.

5.2 Preliminary observations

In this preliminary phase, we identified the following factors as possibly affecting the efficiency of tile risk management: (1) time pressures, (2) liability concerns and conflicts among contractors, (3) turnover among tile technicians and low status of tile work, (4) need for more random testing, and (5) contribution of the management of the ET and the SRBs to TPS reliability problems. The study of these factors will be the object of the Phase 2 of this work. The foundation of this analysis will be *the risk-criticality of each tile* so that limited resources --for example, the limited number of *tile inspectors*-- can be directed first where the probability and the consequences of tile failure could be most severe.

5.2.1 Time pressures

Tile maintenance is often on the critical path to the next flight, specially after missions where tile damage has been extensive. People who find themselves under time pressures sometimes cut corners. For example, it was found in January 1989, that a tile technician had added water to the RTV mix in order to make it cure faster. Adding water at that stage (or spitting in the RTV) may decrease the long-term reliability of the bond: the catalytic reaction, which occurs during the curing, may reverse earlier and thus increases the probability of debonding under different types of loads. Time pressure is also probably the cause of more frequent errors, such as the misalignment of the tile/SIP system with the filler bar, so that only a fraction of the surface of the SIP is in contact with the orbiter's surface. Time pressures may be unavoidable, but some organizational improvements may attenuate their effects,

first, by reducing them whenever possible and second, by increasing tile quality control in the most risk-critical zones.

The time pressure under which the tile personnel operates can be reduced in several ways. First, automation of step and gap measurement (using laser devices and automatic data recording systems currently under development) may result not only in a significant reduction of the processing time, but also in a decrease of the roughness of the orbiter's surface. Second, simplifying the paper work for the tile technicians would allow them to spend more time working on the tiles and less time shuffling papers (an apparent source of frustration). Third, it seems desirable to avoid over monitoring. For example, imposing daily targets (as opposed to weekly ones) for the number of tiles to be processed may decrease the variability and the flexibility needed for optimal performance and system reliability. Fourth, time pressure may be alleviated by reducing the access time to data bases and information that is necessary for prompt maintenance decisions. The maintenance at KSC is done by Lockheed, while some of the relevant data bases are controlled by Rockwell. NASA may want to improve the transfer of information from one to the other and/or within these two organizations.

5.2.2 Liability concerns and conflicts among contractors

Relatively harmonious relations have been instituted among the people who work on the tiles. They share a common concern for the safety of the system despite obvious sources of conflicts. Rockwell and Lockheed are in a competitive situation which does not always provide incentives to make the other's work easier. Among other factors, the liabilities of the main contractors are such that they occasionally have incentives to withhold technical information (for legal and contractual reasons) that may be useful (if not essential) for the performance of the other. These decisions may be justified given the ways the contracts have been set. There are ways of writing and handling contracts that improve incentives for cooperation and encourage the sharing of relevant technical information. This implies that contracts

that affect the same subsystems (e.g., the tiles) and are signed with different firms cannot be managed independently. The positive side of this competition among contractors is that there are no incentives for complacency and strong motivations to detect and correct errors made by the other. There are, however, strong incentives to hide those made by one's own company.

5.2.3 Turnover among tile technicians and low status of tile work

The turnover among the tile maintenance personnel is high. Because tile technicians are classified in the low-pay category of material (fiberglass) technicians (a practice that NASA apparently inherited from the DoD), many of them leave their tile maintenance jobs shortly after completing the training program and obtaining certification. Organization experts generally believe that high turnover is incompatible with learning (individual and organizational) and optimal performance. Therefore, this turnover might affect TPS safety due to inferior quality work by less experienced people. Protruding gap fillers, for example, are caused by poor quality installation and are a probable cause of early boundary layer transition (Smith, 1989.) This condition may not, in itself, threaten flight safety unless it is coupled with other factors. It does decrease the overall TPS reliability and may be an adverse result of high turnover and the corresponding lack of experience of the work force. On the other hand, according to some of the technicians, the old-timers may not be as respectful of "the book" as the newcomers. Assessment of the net result of inexperience and complacency requires a study of the coupling between time on the job and occurrences of errors.

The low-paying job factor may have other indirect, negative effects on the reliability of the tiles. Because of the low consideration that other categories of technicians seem to have for tile work when doing other types of technical work on the orbiter (e.g., mechanical, or electrical) other workers do not pay sufficient attention to the integrity of the tiles. They damage tiles frequently (if not seriously) thus adding considerably to the tile maintenance work. Therefore, the low status of

the tile workers, grounded in the pay scale, may have several detrimental effects: (1) a waste of money in training tile technicians that leave the job as quickly as possible, (2) low morale for some of them, which is seldom conducive to high-quality work, and (3) the "no respect" syndrome on the part of other technicians who carelessly damage tiles. The result is an increase of time pressure for a system that is already "the long pole" a large part of the time. In the end, these factors may encourage detrimental corner-cutting in tile processing.

5.2.4 Need for more random testing:

The original tile work and subsequent maintenance work has not always been perfect. Some of the tiles have been only partially bonded and, in a few instances, not glued at all. For example, in November 1999, it was found in that one tile on orbiter Columbia had been holding for several flights by the friction of (or perhaps some RTV adherent to) the gap fillers. The fact that this tile held and did not cause an accident was called "a miracle" by the personnel who discovered the problem. How "miraculous" can be determined using the risk assessment model. (In fact, according to our estimate, the probability of debonding is 10^{-2} per flight for such a tile, making the probability of debonding in five flights in the order of 5%.) Because of these hidden weaknesses, it may be desirable to do more random, non-destructive pull tests of the black tiles between flights, focusing on the most risk-critical areas of the orbiter's surface in order to detect and replace the tiles that are far below the expected capacity.

In addition to the possibility that previous work may not have been perfect, the possibility of long-term deterioration of the room-temperature vulcanized (RTV) bond should be acknowledged and taken into account in maintenance procedures. This calls (1) for additional random testing to monitor the possible chemical degradation of the RTV after repeated heat-load cycles, and (2) for the development and implementation of non-destructive and, if possible, non-pull testing of the tiles' bond, to be applied in priority to the most risk-critical tiles.

5.2.5 Contribution of the management of the ET and the SRBs to TPS reliability:

A significant fraction of the risk of TPS failure is due to debris, in particular, pieces of insulation from the external tank and the nose cone of the solid rocket boosters. In addition, tiles are much more likely to debond under the shock of chunks of debris when they are already loose or less than completely bonded. By backtracking the computer-simulated trajectories of pieces of debris from the most risk-critical parts of the orbiter surface back to the corresponding parts of the surface of the ET and the SRBs, it may be possible to identify which parts of the surface of the ET and the SRBs should be given special attention in the treatment of the insulation. Additional testing should, therefore, be performed for tiles located in zones that are most likely to be hit by SRB and ET insulation debris.

For each of these organizational factors, the analytical procedure is to identify the decisions that they affect, the errors that they can cause, the frequency with which they occur, the nature and the severity of the resulting errors as a function of the severity of the conditions, and their effect on the probability of failure of the system using our PRA model. The efficiency of possible management improvements can then be roughly assessed so that efforts are concentrated where they can provide the greatest benefits. This assessment will be the objective of the second phase of this study.

Section 6:
CONCLUSIONS

The results of our model's illustration suggest that the probability of loss of an orbiter due to failure of the black tiles is in the order of 10^{-3} with about 15% of the tiles accounting for about 80% of the risk. If one accepts the rough NASA estimates that the probability of losing an orbiter is in the order of 10^{-2} per flight (Broad, 1989) and that a significant part of it is attributable to the main engines, then the proportion of the risk attributable to the TPS (about 10%) is not alarming, but certainly cannot to be dismissed. (Our probabilities are coarse numbers that can be refined in the second phase of the work, but they are probably in the ball park.) A critical issue is: how will these probabilities evolve in the years to come? On one hand, the quality of the tile work and the detection mechanisms for defective tiles are expected to improve. On the other hand, exposure to repeated load cycles and environmental conditions or chemical reaction may deteriorate the system's peformance capacity unless closely managed.

One of our key findings is that the most risk-critical tiles are not all in the hottest areas of the orbiter's surface. We introduced, in this study, the notion of risk-criticality and the computation of a *risk-criticality index* to account for the loads to which the tiles are subjected and the consequences of their failures given their location with respect to other critical subsystems which they protect (functional criticality). This index can serve as a guide to set management priorities, for example, for the gradual replacement of the tiles, focusing first where tile failure could be most damaging.

Well-designed, manufactured, bonded, and maintained tiles are extremely unlikely to fail. A large fraction of the risk seems to be attributable to tiles that are

only partially bonded, or to those that are not bonded at all and are held in place by the gap fillers. Management assumes unnecessary risk by denying that errors have occurred and will occur again and that, consequently, the capacity of the TPS is reduced. To assume that all work is perfect leads to a potentially gross underestimation of the risk, rendering the maintenance procedures based on this assumption of perfection suboptimal. What the actual magnitude of this part of the risk is and which organizational improvements can bring the greatest risk-reduction benefits will be studied further in the second phase of this study. This part will involve a systematic analysis of the maintenance process to identify the different types of errors (past and present), their rates of occurrences, their probabilities of detection and correction, and their severity levels (i.e., by how much they decrease the system's capacity in each case). Relating these errors to the organizational factors described in the previous section will allow us to identify management improvements, their costs, and their expected positive effects on the TPS performance.

After the completion of the first of two phases of research, our preliminary conclusions are that it is desirable: (1) to expand the current concept of criticality for the tiles (to include functional criticality, as well as the heat loads in a risk-criticality measure), (2) to adapt the inspection and maintenance procedures to focus in priority on the most risk-critical tiles, and (3) to modify the existing data bases to include the risk-criticality factor for each tile.

Section 7:

REFERENCES

Aviation Week and Space Technology. Shuttle Orbiter To Use Silica Insulation. January 26, 1976.

Aviation Week and Space Technology. Orbiter Protective Tiles Assume Structural Role. February 25, 1980.

Baker, E. and B. Dunbar. Thermal Protection System (TPS) . Trend Analysis Survey. NASA Lyndon B. Johnson Space Center. Flight Crew Operations Directorate, March 2, 1988.

Broad, W. J. NASA Now Admits It's Worried About Disasters. San Francisco Chronicle, April 10 1989.

Cooper, P. A. and P. F. Holloway. The Shuttle Tile Story. Astronautics and Aeronautics. January 1981, pp. 24-34.

Garrick, B. J. Quantitative Risk Assessment and the Space Program. Risk Analysis Seminar Series, Department of Industrial Engineering, Stanford, California, March, 1988.

Lockheed Research and Development Division Tile Bond Verification Shuttle Inspection System (Rebecca Welling et al.) Palo Alto California, March, 1989.

Lockheed Space Operations Company. Orbiter Thermal Protection System Review. Part II. Presentation by David Weber, Kennedy Space Center, November 7, 1989.

McClymonds, J. W. Records of Debris Impact and Tile Damage. Rockwell International, Downey, California, 1989.

National Research Council. Post-Challenger Evaluation of Space Shuttle Risk Assessment and Management. (Slay Committee Report) National Academy Press, Washington D.C. 1988.

Orbiter TPS Damage Review Team, STS-27R, OV-104. Summary Report, Vol. 1, Feb. 1989.

Paté-Cornell, M. E. Organizational Extension of PRA models and NASA Application. Proceedings of PSA'89 (ANS Conference on Probabilistic Safety Assessment), Pittsburgh, Pennsylvania, April, 1989.

Paté-Cornell, M. E. and F. G. Bea. Organizational Aspects of Engineering Systems Reliability and Application to Offshore Platforms. Research Report No. 89-1, Department of Industrial Engineering and Engineering Management, Stanford University, Stanford, California, April, 1989.

Paté-Cornell, M. E. Organizational Aspects of Engineering System Safety: the Case of Offshore Platforms. Science, Vol. 250, November 30, 1990, pp. 1210-1217.

Presidential Commission on the Space Shuttle Challenger Accident. Washington D.C. June, 1986.

Rockwell International, Shuttle System Integration. Debris Damage Assessment Summary, Downey, California, 1989.

Rockwell International, Thermal Protection System. Standard Maintenance Procedures Specification. Downey, California, September, 1989.

Rockwell International, Thermal Protection System Reusable Surface Insulation (RSI) Maintenance. Specification. Downey, California, September, 1988.

SIORA. Final Report for the SIORA Program--Shuttle Tile Automation Project, Stanford University, April, 1990.

Shuttle Operational Data Book. Vol. 4, Orbiter Landing Emergency Rescue. Data Part 1, NASA, Lyndon B. Johnson Space Center, Houston, Texas, January, 1988.

Smith, J. A. STS-3, Structural and Aerodynamic Pressure and Aerothermodynamics and Thermal Protection System Measurement Locations. NASA, Lyndon B. Johnson Space Center, January, 1982.

Smith, J. A. STS-28R Early Boundary Layer Transition. Engineering Directorate, Johnson Space Center, Houston, Texas, December 1989.

Section 8:

APPENDICES

Appendix 1

Organizational Extensions of PRA models and NASA Application

Nuclear

GPU Nuclear Corporation
One Upper Pond Road
Parsippany, New Jersey 07054
201-316-7000
TELEX 136-482
Writer's Direct Dial Number:

May 18, 1990

Prof. Elizabeth Paté-Cornell
Department of Industrial Engineering
Stanford University
Stanford, CA 94305

Dear Professor Paté-Cornell:

On behalf of the American Nuclear Society Nuclear Reactor Safety Division, I am pleased to inform you that your paper, "Organizational Extension of PRA Models and NASA Application" (which was presented at the PSA '89 Conference in Pittsburgh, Pennsylvania), has been selected for a Best Paper Award. This award was determined on the basis of an evaluation by the Technical Program Committee members for the PSA '89 Conference.

As I mentioned to you on the phone, arrangements are being made to recognize you at the NRSD Annual Luncheon on Wednesday, June 13, 1990 in Nashville, Tennessee (in conjunction with the ANS annual meeting). At that time you will be presented with a certificate. The luncheon will begin at 11:30 a.m., you will be seated at the head table, and your luncheon ticket will be complimentary.

Congratulations again on receiving a Best Paper Award.

Yours truly,

Donald N. Grace

Donald N. Grace
Chairman, Honors & Awards Committee, NRSD

cc: Dr. Raymond DiSalvo

Proceedings of PSA '89
Pittsburgh, Pennsylvania
April 1989

Best Paper Award
American Nuclear Society
Nuclear Reactor Safety Division
PSA '89

ORGANIZATIONAL EXTENSION OF PRA MODELS AND NASA APPLICATION

Elisabeth Paté-Cornell
Department of Industrial Engineering
and Engineering Management
Stanford University
(415) 723-3823

ABSTRACT

This paper describes a probabilistic method which extends classical PRA to include some characteristics of the organization that processes or manages an engineering system. A taxonomy of errors is presented and their organizational roots examined. An assembly model is proposed for the analysis of the resulting spectrum of capacities of the system. The management of the Thermal Protection System of the Space Shuttle is used as an illustration. The model allows assessment of the benefits of organizational improvements of the orbiter's processing.

PROCESS ANALYSIS IN RELIABILITY MODELS

The quantitative analysis of the reliability of an engineering system such as a nuclear power plant or the space shuttle allows identification of its different failure modes and computation of their probabilities. Therefore, it permits a decision maker to choose technical solutions that maximize an objective function (including reliability) under resource constraints. This means, for instance, the choice of design characteristics that minimize the probability of failure during the lifetime of the system under constraints of costs, time, and performance.

Technical modifications, however, represent only one class of risk management strategies. When a system's failure is studied *a posteriori*, it is often pointed out that what resulted in a technical failure was actually rooted in a structural or functional failure of the organization. This was the case, for example, of the accident of the space shuttle Challenger where a number of organizational factors contributed to NASA's decision to launch under unacceptable temperature conditions.[1] These organizational factors include, for example, geographic dispersion (thus, sometimes poor communications), time constraints, and pressures of public relations. Modifications and improvements of the organization itself may address some of the reliability problems at a more fundamental level than strengthening the engineering design alone.[2] Such modifications include, for example, improving communications, setting effective warning systems, and ensuring consistency of standards across the organization.[3]

The object of this paper is to discuss a quantitative approach to analysis of the effects of organizational factors on system reliability. The principle is to compute the probability of occurrence of the basic events in greater depth than it is generally done in classical PRA by linking this probability to the industrial process itself.[4] The method involves explicit assessment of the effect of managerial procedures on the probability of technical failures and, therefore, allows an extension of the value of information of conventional PRA. By assessing explicitly the reliability benefits of organizational improvements along with technical ones, the results allow setting priorities among safety measures that go beyond technical modifications alone.

The National Aeronautics and Space Administration (NASA) presents some organizational features that influence its mode of operations and thus the reliability of its space systems. NASA is a high-visibility organization, uncertain about its future funding and, therefore, dependent on public relations. It is also fragmented in two ways: geographically among space centers, and operationally among space programs. In the early 1960's, NASA decided against probabilistic risk analysis, thus avoiding the issue of "how safe is safe enough" in what is generally recognized as a high-risk operation. Yet, following the Challenger accident in January 1986 and faced with a long list of potential corrections, NASA is beginning to complement its qualitative methods of identification of the failure modes by quantifying probabilities and dependencies as recommended by the Rogers Commission.[5] A current objective is clearly to increase the effectiveness of the organization and the efficiency of resource allocation by setting priorities among the technical solutions to existing problems. Yet, as the Rogers Commission pointed out,[1] it is clear that some of NASA's reliability problems cannot be resolved by design modifications alone because their roots are organizational. The fragmentation of the organization, the apparent buffering between engineers and managers and the divergence of their risk perceptions,[1] difficulties of learning given the scarcity of usable trend records, all these factors have contributed to the vulnerability of space systems operations. These effects, however, vary among the different subsystems according to their physical and functional characteristics and to the features of the managing organizations.

The Thermal Protection System (TPS) of the space shuttle provides an example of the coupling between technical and organizational problems. It is a complex system that is designed, manufactured, processed, and maintained by several organizations. It is made of black and white tiles (about 24,000 on the orbiter Discovery), reinforced carbon-carbon in the hottest zones, thermal blankets in colder zones, and flexible insulation. The tiles themselves are attached by a gap-filler (RTV) to a flexible pad designed to

absorb the bending of the orbiter's surface. The pads are bonded to the aluminum skin (itself covered with a primer) by the same RTV. The TPS can fail in three ways: debonding, burn-through, and damage by impacts. It is subjected to a set of external loads, some of them mostly predictable (like vibrations and heat under normal operating conditions), some of them more random like debris. Important features of the PRA model for the tiles are the potential failure dependencies from tile to tile, and the coupling between failure of the TPS and failure of the subsystems located directly under the aluminum skin of the orbiter.

The management of the TPS presents many characteristics that are typical of the linkage between organizations and reliability. It involves several organizations and contractors in different places (including Rockwell, Lockheed, and NASA, at Kennedy Space Center and at Johnson Space Center) and procedures that were mostly developed for the initial shuttle construction and not for a long term maintenance program. The TPS inspection and maintenance procedures are extremely labor intensive and time consuming, and are often on the critical path to the next launch. The training, dedication, and motivation of the personnel involved in this process is critical to the reliability of the system. The current procedure relies mostly on maintenance on demand. Although destructive pull tests are performed for a small sample of tiles, in most places, the problems posed by the aging of the bonding are not addressed directly. The recording of operations involves a mass of paper documents. Furthermore, the procedure involves some prioritization among the TPS elements based on qualitative judgments, but systematic priorities based on a quantitative assessment of the risk of failure due to tiles' location with respect to other critical systems.

A new method to automatize the inspection of the tiles is currently being implemented.[7] An important aspect of this method is that it greatly simplifies the current tasks of observing, communicating, storing, and retrieving information concerning the current state of the tiles and their past performance. It should, therefore, increase the reliability of the inspection and maintenance operations. By accelerating the process, automation may also, in many instances, take the tiles off the critical path to the next launch. The gain in shuttle reliability between manual inspection and automation is a function (1) of the initial contribution of the TPS to the overall failure risk and (2) of the gains made in TPS reliability. One specific issue that can be addressed by the extension of PRA described here is the benefit of accounting for the relative criticality of the tiles in different locations on the orbiter's surface in the management of the TPS. This may result in increasing maintenance efforts in key areas such as the surface covering the hydraulic command system, but also, perhaps, special monitoring of the installation operations for these most critical areas. Another issue that can be addressed by extension of PRA as described here is the relative importance of the management of the TPS itself and of the management of other systems that are sources of debris (e.g., the external tank insulation) in the overall reliability of the thermal protection function.

INTEGRATION MODEL

Probabilistic risk analysis (PRA) for engineering systems allows identification of their weakest parts through quantification of the probabilities of the different failure modes (see, for example, Henley and Kumamoto).[8] Extension of the PRA model permits more explicit consideration of major organizational characteristics[9] (structure, procedures, and culture[10]) that affect the reliability of operations, specially in situations of distributed decision making.[11] The method extends the scope of PRA through a Bayesian analysis of the sequence of tasks to be performed in the process of design, manufacturing, inspection, maintenance, and operations, and the computation of the probabilities of technical as well as organizational failures that can affect the system's reliability. The reasoning involves analysis and extension of errors to include not only the classical operators errors but also errors that are due to the procedures and structure of the organization. An essential distinction is made here between gross errors and errors of judgment because remedial actions to address these two types of problems may be of different nature.[12]

The first phase is an analysis of the process[13] (e.g., engineering, maintenance, and operation) in order to identify what constitutes "normal performance" and potential problems with their probabilities or base rates per time unit or per operation, which depend, among other factors, on the organization's culture and incentive structure. Given that a basic error occurs, the next phase is an analysis of the organizational procedures and incentive system to determine the probability that it is observed, recognized, communicated, and corrected in time (i.e., before it causes a system failure). The results of these two phases is a computation of the probabilities of the different system's states corresponding to possible types of structural defects and, therefore, to different levels of system's capacity. The third phase is a probabilistic risk analysis of the physical system that allows computation of the overall failure probability (1) under normal circumstances, and (2) given potential weaknesses of the different elements and increase of their failure probabilities. These three models (process, organization, and PRA for different levels of system's capacity) are integrated using an event tree (or an influence diagram) to compute the overall failure probability and the relative contribution of different scenarios (e.g., occurrence and correction of a given problem). Figure 1 provides a schematic illustration of the structure of this integration model.

PRA FOR THE THERMAL PROTECTION SYSTEM OF THE SPACE SHUTTLE: MODEL STRUCTURE

A PRA model currently under study for the TPS of the space shuttle relies on a partition of the surface along several dimensions: (1) the external loads (mainly heat and debris) to which the orbiter can be subjected and that vary according to the location on the orbiter's surface and (2) the criticality of the different subsystems located immediately under the aluminum skin. In order to allow recommendations regarding the management of the relevant subsystems, the model is divided into two parts: the first part is a study of debonding and burn-through due to weaknesses of the bond, heat loads, vibrations, etc.; the second part is a separate study of the impact of debris, their sources, and their effects on the TPS reliability. In this paper, the scope of the PRA model is limited to the tiles located on the underneath surface of the orbiter.

First part: debonding and burn-through (excluding the effect of debris)

Figure 2 provides a schematic illustration of the partition of the orbiter's underneath surface for the first part of the analysis (there is no attempt at this stage to locate realistically the different zones according to temperature and criticality). A minimal zone (or min. zone) is an element of the final partition of the surface. Each min. zone of index i is thus characterized by a heat index (k(i)) and a criticality index (j(i)).

The basic notations are the following:

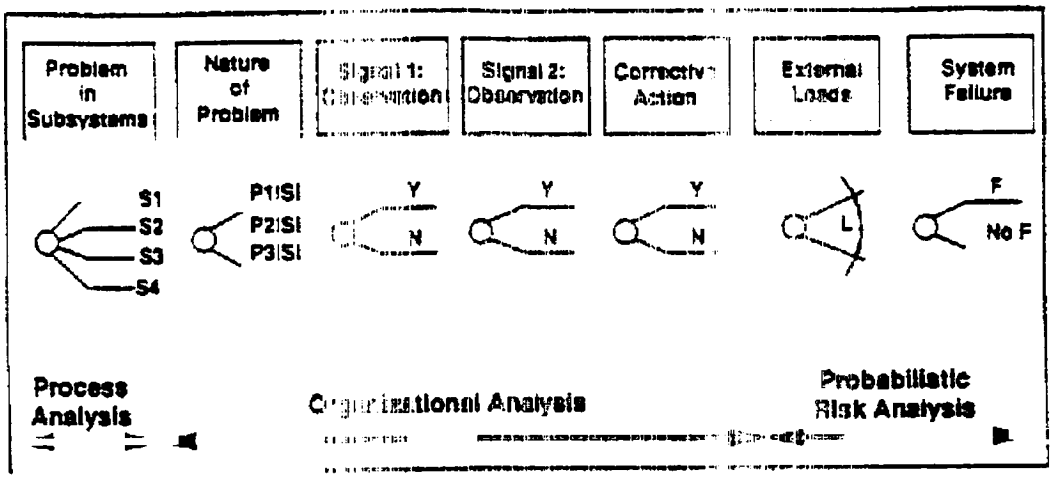


Figure 1: Structure of the general risk reliability model including organizational features and error detection

F(t): Failure of the orbiter: loss of vehicle and crew (LOV/C) at launch primarily caused by failure of the TPS

n: Total number of tiles on the orbiter

j: Index of criticality area (ex: criticality of the min. zones covering the hydraulic system)

k: Index of temperature area

i: Index of min. zones (j, k) => j(i), k(i)

N_i: Number of failure patches in min. zone i.

n_i: Number of tiles in min. zone i.

F1: Failure of the "first tile" (initiating failure) in a failure patch

F'|F1: Failure of any adjacent tile given initiating failure

Initiation of a failure patch:

It is assumed in this phase of the analysis that any failure patch (of size one or more) develops by the loss of a first tile (F1: initiating failure for the patch), followed or not by the failure of adjacent tiles (F'|F1). The probability of losing the first tile in a patch depends on the failure mode (debonding or burn-through):

$$p_i(F1) = p(F1, \text{debonding}) + p_{bth}(F1, \text{burn-through})$$

The probability of debonding is assumed to be independent of i (the location on the orbiter) whereas the second term (burn-through) depends on the temperature component of the min.zone descriptor k(i).

Development of a failure patch of size M given that it starts in min zone i:

$$p_i(M \mid F1) = p_{adj}(F' \mid F1)^{M-1} \times [1-p_{adj}(F' \mid F1)]$$

This probability depends on the temperature of the min. zone (index k(i)).

Development of N_i patches in min. zone i:

$$p(N_i) = p(F1)^{N_i} \times [1-p_{adj}(F1)]^{n_i - N_i}$$

This equation assumes that the development of different patches are independent events and that there is no overlap of patches, i.e., that the product $EV(N_i) \times EV(M)$ is negligible.

$EV(N_i) = n_i \times p_{ini}(F1)$ (= expected value of the number of patches in min. zone i)

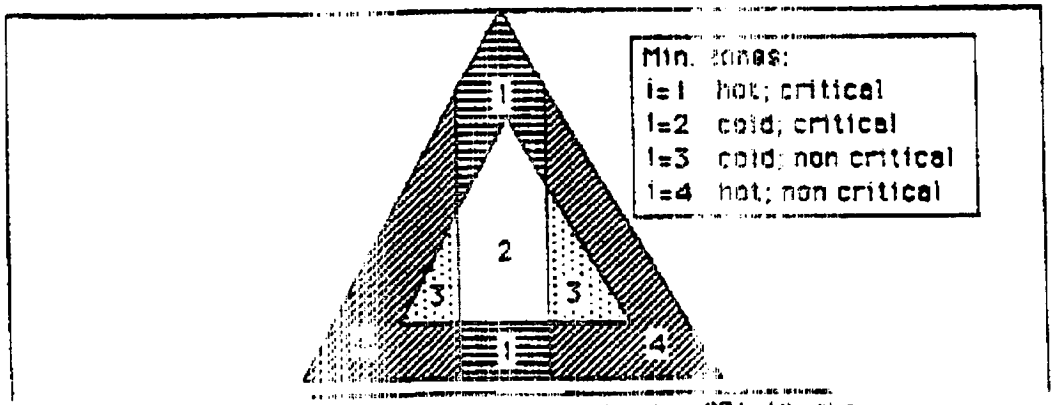


Figure 2: Double partition of the crater's surface for a NRA of the tiles

$EV(M) = 1 / [1-p_{s,m}(F' \mid F1)]$ (= expected value of the size of a patch conditional on its start)

Failure of the orbiter due to a patch of size M:

As part of the data, one needs the probability of failure of the orbiter due to the development of a failure patch of a given size in a zone of given criticality. These data may be obtained through an analysis of the reliability of the systems located under the orbiter surface and their contribution to the overall reliability of the orbiter. These probabilities can be used to define criticality itself. p(F) thus depends on j(i), the criticality index of min. zone i.

$p_j(F \mid M=1) = p_{j,1}$
$p_j(F \mid M=2) = p_{j,2}$
$p_j(F \mid M=m) = p_{j,m}$

Failure of the orbiter due N patches of random size:

A failure of the orbiter due to TPS failure in min. zone i occurs if any (one or more) of the patches of min. zone i causes failure. Given that failure probabilities p(F1) and p(F') are assumed to be small, one can write:

$$p(F \mid N_i=q) = q \times p'_i$$

where p'_i is the probability that an arbitrary patch in zone i causes failure.

$$= \sum_{m=1 \text{ to } \infty} p_{s(i),m} \times p(\text{size } m)$$

$$p'_i = \sum_{m=1 \text{ to } \infty} p_{s(i),m} \times p_{s(i)}(F' \mid F1)^{m-1} \times [1-p_{s(i)}(F' \mid F1)]$$

Infinity is used as a convenient approximation of upper bounds when the probability of large values of the random variable is sufficiently small.

Probability of orbiter failure due to TPS failure in zone i:

p(F for all patches in min. zone i)

$$= \sum_{q=1 \text{ to } \infty} p(F \mid N_i = q) \times p(N_i = q)$$

$$= \sum_{q=1 \text{ to } \infty} p'_i \times q \times p(N_i = q)$$

$$= p'_i \times EV(N)$$

$$= p'_i \times n_i \times p_{s(i)}(F1)$$

Failure of the orbiter for all the min. zones:

$$p(F) = \sum_{i=1 \text{ to } 4} p'_i \times n_i \times p_{s(i)}(F1)$$

Effect of external events

The probability of failure is the sum over all values of the external load X (e.g., maximum temperature if it turns out to be critical) of the probability density function for X multiplied by the probability of failure of the orbiter conditional on X.

$$p(F) = \int_x f_x(x) \; p(F \mid x) \; dx$$

In the complete analysis of the external events, it is necessary to take into account the different phases of the flight in order to obtain a distribution over time of loss of first tile and a measure of the dependence on time of the loss of subsequent tiles after loss of the first one.

Second phase: risk of failure due to debris

The analysis begins with the study of the sources of debris (e.g., insulation of the external tank, other parts of the STS, external objects) in order to obtain the probability of different scenarios characterized by the nature and the size of debris, the impact's location on the orbiter's surface, and the time of impact during the flight. This analysis leads to a description of the initial tile damage (including probability of a hit for tiles in different zones, distribution of number of tiles initially hit conditional on debris impact, severity of the damage conditional on impact). In this second part, the start of a failure patch is characterized by the possibility of multiple initial failures with different levels of severity. The study of further development of failure patches conditional on initiating failure(s) and consequent effect on the orbiter is similar to the analysis performed in the first part. The main difference is that the analysis of the effects of debris involves different levels of damage severity.

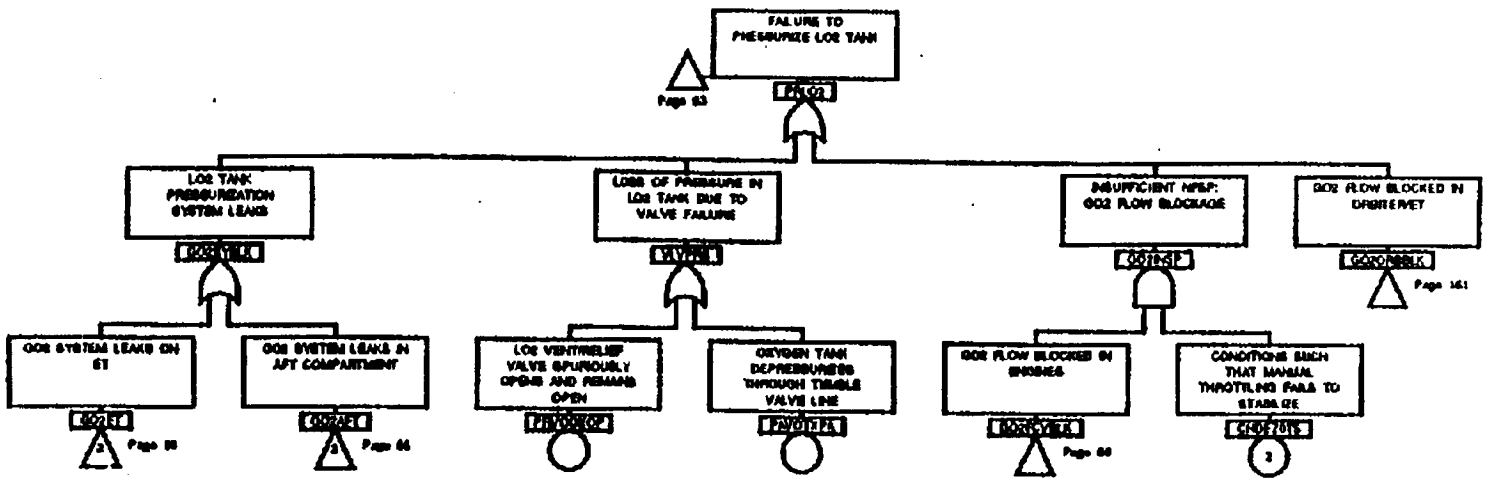
MANAGEMENT OF THE TILES AND POTENTIAL ERRORS

TPS management and reliability

The quality of the process of design, manufacturing, installation, inspection, and maintenance of the tiles affects the probability of initial and subsequent failures through burn-through or debonding (p(F1) and p(F'|F1) in the previous model). The quality of the management of other systems such as the external tank that are potential sources of debris affects the probability and the severity of damage due to debris impact in different locations of the orbiter. Given its structure, the model described above can be used to assess the gains of improvements in the management of the tiles and in the processing of the orbiter through the assessment of the changes in p(F1), p(F'), and similar variables for the case of debris impact.

For example, current maintenance of the tiles depends on the expected heat loads (with emphasis on zones such as the leading edges of wheel doors) the procedure is independent of the criticality of the systems located directly under the aluminum skin. Prioritization in the TPS processing as well as the processing of adjacent sources of debris may be designed to decrease further the probability of initiating tile failures in the most critical zones. The results can then be measured by computation of the overall risk by the previous model using new values of initiating failures. Another example of improvement that can be assessed through the model is the development and the use of non destructive testing of the RTV. The probabilities of failure p(F1) and p(F') in the first part of the model increase over time with the number of flights of the orbiter. Non destructive testing can indicate deterioration of the bonding and allow timely replacement.

In addition to conscious decisions such as ignoring the aging phenomenon or uniform inspection of the tiles, errors can occur at every step of the manufacturing of the different elements of the TPS (for example, a bad batch of RTV), of the inspection and maintenance process (e.g., wrong measurement of step and gap),



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 64	1/05/88

In cases where there is no controversy about value judgments involved in top level decisions (considering, for example, that the opinions of Congress must prevail) the question is to ensure that relevant information is available to the top management when fundamental decisions are made, and that the organizational and individual's risk attitudes eventually reflect that of this top level. The objective is to design an incentive structure and/or a feedback mechanism that ensures this adequacy. This implies the use of appropriate information that is readily available, the acquisition of additional information when it has a net positive value given the organization's preference system, and a decision making process that leads to consistency in risk attitudes. The quality of the leadership clearly plays an essential part in the clarity and the consistency of standards across the organization.

SOME ORGANIZATIONAL PROBLEMS THAT AFFECT SYSTEM RELIABILITY

From this analysis of errors one can identify two broad categories of organizational problems that relate to the failure probability of a system because they affect the probability of process errors: *information* problems and *incentive* problems with the possibility of combination of both.

Information problems

Information problems may occur within an organization or across organizations managing the same system. They may be the following:

* Sequential engineering and lack of feedback. The engineering process may be designed in a linear manner without feedback loops to check that the design corresponds to the needs, or that resources at allocated properly for optimal reliability. For example, there may not exist any mechanism to check the shadow price of the constraints set by management, i.e., what would be the gains (e.g., in reliability) associated to different levels of relaxation of the constraints (e.g., of schedule).

* Access to relevant information. The organization's problem is to identify and communicate signals that are relevant and reliable. Organizational filters may be such that some important signals end up missing while irrelevant ones overload and confuse the system. First, the individual must be able to identify what to look for and to obtain this information in time. Communications may fail for a variety of reasons. Appropriate communication channels may simply not exist, or existing channels may not work due to accidents, or impractical procedures, or deliberate retention of information. Also, the signal may be ignored because of previous false alerts (the cry-wolf effect).

* Communication of uncertainties. The information may also be distorted. For example, the organization may not be equipped (in its procedures, its culture, etc.) to communicate properly imperfect information and uncertainty. Therefore, qualifiers ("Go but...") may be dropped in the process.

Incentive problems

Incentive problems may affect the system's performance throughout the process and include the following:

* Incentives towards optimism. In organizations whose final goal is to produce a positive product (as opposed to detecting faults) and where the risks of visible failures are sufficiently low, incentives at each level may lead to the suppression of bad news and, therefore, a bias towards optimism. This is true, in particular, when the information is incomplete and in situations of uncertainty (as described above).

* Pressures on the critical path. The technical groups whose task is on the critical path to production or operation may find themselves under pressure to cut corner. This pressure increases with the difference of total time (objective function) between them and the next critical task.

* Difficulties of learning in a high-visibility situation. It may be difficult for an organization subjected to public scrutiny to assess its own performance and learn from its mistakes. In situations of success, there may be a tendency to overlook signals of potential problems whereas in situations of difficulties, the organization may be overwhelmed by signals of problems if it does not have clear procedures to assess their relative severities and to set priorities among remedial actions. Furthermore, organizational learning and in particular change of rules may be difficult when it can be interpreted as admitting that previous procedures were inadequate.

RETURN TO THE PRA MODEL

Assembly model

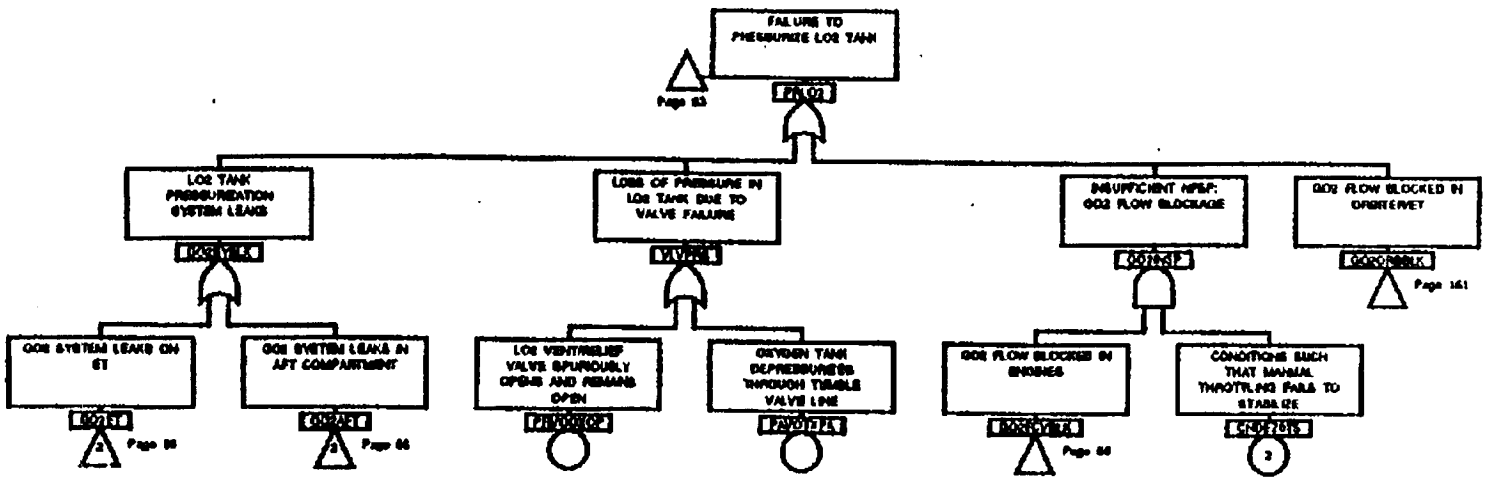
The probability of failure p(F1) and of subsequent failures p(F'|F1) can be linked to the occurrence of errors of different types (e.g., a fraction of the surface only was covered with RTV) and, furthermore, to combinations of errors (e.g., insufficient quantity of bonding or inappropriate step to next tile due to mis-measurement). For each type of error, the question is to know what is its level of severity, the number of tiles that it can affect, and their location with respect to the criticality partition of the orbiter surface. In addition, it may be important to consider whether it is a gross error or an error of judgment that may be less easily identified and corrected. An error having occurred, the inspection process can be analyzed as a sequence of filters: at each step the error may be identified or missed. Finally, given that an error has occurred and been identified, it may or may not be corrected.

This analysis is described by the influence diagram shown in Figure 4. The result is a distribution for the probability of initiating failure p(F1) given possible combinations of errors and their levels of severity and the distribution of the number of tiles affected. This distribution of values of p(F1) is then entered in the previous model to obtain a spectrum of failure probabilities (LOV/C) due to failure of the TPS. The model can then be used to assess the effects of organizational improvements designed to increase the reliability of the TPS.

Examples of organizational improvements of TPS management and their analysis through the model

* Improvement in learning. Possible measures include trend analysis and feedback mechanisms. Their effect, in the model, is to decrease the probability of occurrence of errors in the first place. Also, improvement of the testing (such as the testing of RTV for aging effects) whose effect is to decrease the probability of failure itself.

* A better allocation of resources according to the criticality of the tile location can be analyzed by the model through the



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 64	1/05/88

ase of the probability of initiating failure in the most critical

* Better procedures for the inspection of tiles and the storage trieval of information increase the probability of observation ir conditional on occurrence and increase the probability of ection conditional on observation.

CLUSION

The extensions of classical PRA presented in this paper ease considerably the value of information of such studies se it allows setting priorities among a larger number of ial improvements. An analysis of the engineering process focusing attention and resources (time in particular) on the st critical tasks. Organizational aspects of engineering reliability of interest to researchers in organizations' behavior.[14] The lative method outlined here allows inclusion of this body of dge in the decision making process by assessing the relative ortance of these organizational effects through their contribu- to the overall system reliability.

OWLEDGEMENT

This work was funded by NSF grant SES-8709810 and by grant NCC 10-0001. The author thanks Dr M. Wiskerchen P. Fischbeck for their help in this study.

FERENCES

1. PRESIDENTIAL COMMISSION ON THE SPACE SHUTTLE CHALLENGER ACCIDENT Report of the Presidential Commission on the Space Shuttle Challenger Accident. Washington, D.C.(1986).

2. LEWIN, A. Y. and J. W. MINTON. Determining Organizational Effectiveness: Another Look, and an Agenda for Research. Management Science, Vol. 32, No. 5, pp. 514-538. May, 1986.

3. PATE-CORNELL, M.E. and J. P. SEAWELL. Engineering Reliability: The Organizational Link. Proceedings of the 5th ASCE Specialty Conference on Probabilistic Methods in Civil Engineering, Blacksburg, VA, May, 1988.

4. PATE-CORNELL, M.E. Organizational Factors in Reliability Models, Proceedings of the 1988 Meeting of the Society For Risk Analysis, Washington D. C., November, 1988.

5. NATIONAL RESEARCH COUNCIL, Committee on Shuttle Criticality Review and Hazard Analysis Audit, Post Challenger Evaluation of Space Shuttle Risk Assessment and Management, National Academy Press, January, 1988.

6. FEYNMAN, R. P. Personal Observations on Reliability of Shuttle, Appendix F to the Presidential Commission Report on the Space Shuttle Challenger Accident, 1986.

7. WISKERCHEN, M. J. and C. MOLLAKARIMI. Training Simulation Environment for Space Shuttle Processing, AIAA Flight Simulation Technology Conference, September 1988.

8. HENLEY, E.J. and H. KUMAMOTO. Reliability Engineering and Risk Assessment, Prentice Hall Inc., Englewood Cliffs, NJ. 1981.

9. MARCH, J. G. and H. A. SIMON. Organizations, John Wiley & Sons, New York, 1958.

10. WEICK, K.E. Organizational Culture as a Sources of High Reliability, California Management Review, Winter, 1987.

11. FISCHOFF, B. and S. JOHNSON. The Possibility of Distributed Decision Making, Workshop on Political-Military Decision Making, The Hoover Institution, Stanford University, 1986.

12. PATE-CORNELL, M. E. and R. BEA, Organizational Aspects of Engineering System Reliability and Application to Offshore Platforms, Department of Industrial Engineering and Engineering Management, Stanford University, 1989.

13. MILLER, S.M. and D. M. STRONG, A Model for Evaluating the Performance of Operational Level Information Handling Activities, Proceedings of the Seventh International Conference on Information Systems, San Diego, CA. Dec. 1986.

14. KAHNEMAN, D., P. SLOVIC, and A. TVERSKY. Judgment under Uncertainty: Heuristics and Biases, Cambridge University Press, Cambridge, U.K., 1982.

15. LA PORTE, T.R., High Reliability Organization Project, University of California Berkeley, 1988.

Appendix 2:

Data Bases for Tile Performance

PRACA

(PROBLEM REPORTING AND CORRECTIVE ACTION)

NASA
Lyndon B. Johnson Space Center
FLIGHT CREW OPERATIONS DIRECTORATE

SUBJECT: THERMAL PROTECTION SYSTEM
TREND ANALYSIS SURVEY

NAME: CB/E. BAKER
CB/B. DUNBAR

DATE: MARCH 2, 1988

PRACA DEFINITION

NSTS 08126C; JUNE 1987; REV. C

5.1 NASA PROGRAM OFFICE IS RESPONSIBLE FOR:

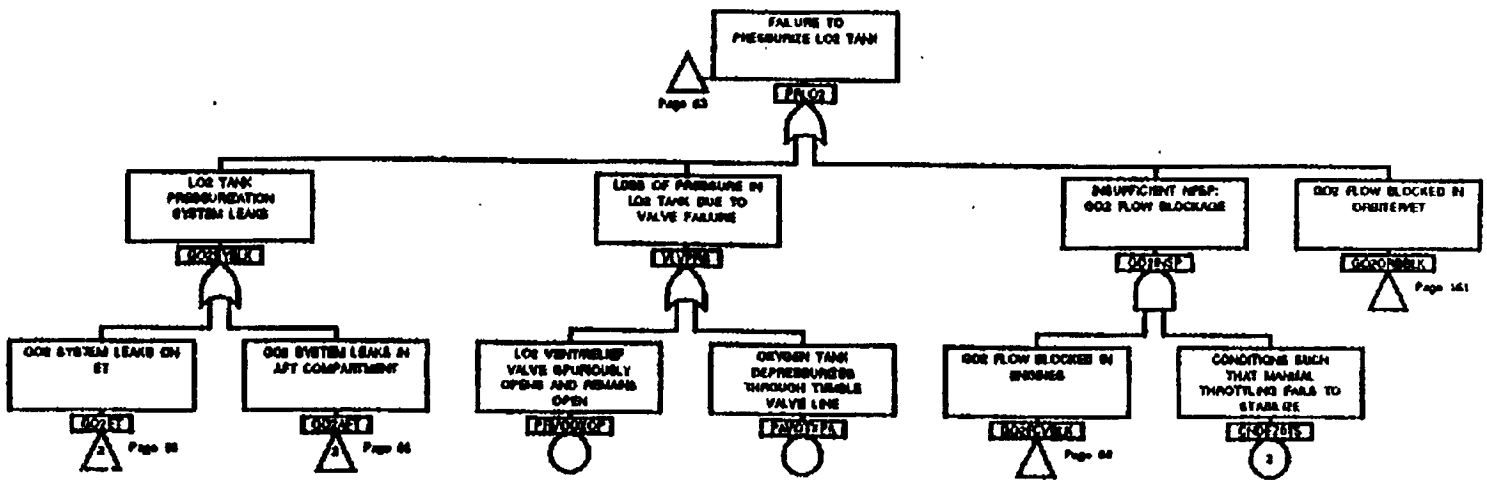
C. PROVIDING NECESSARY RESOURCES TO SUPPORT THE PRACA SYSTEM, INCLUDING THE PRACA DATA SYSTEM, COMMUNICATION SERVICES, AND COMPATIBLE HARDWARE AND SOFTWARE.

E. ASSURING THAT THE DEVELOPMENT OF A PRACA DATA SYSTEM WILL PROVIDE INFORMATION IN A FORMAT WHICH WILL BE SUPPORTIVE OF A TRENDING SYSTEM TO BE USED BY ALL ELEMENTS AS SPECIFIED IN TBD.

5.2 JSC & MSFC ELEMENT PROJECT OFFICES ARE RESPONSIBLE FOR:

B. ASSURING THAT ALL REPORTABLE PROBLEMS, INCLUDING IN-FLIGHT ANOMALIES, ARE IMMEDIATELY REPORTED INTO THE NSTS PRACA DATA SYSTEM.

D. ASSURING THAT THE INFORMATION WITHIN THE PRACA SYSTEM IS IN A FORMAT WHICH IS COMPATIBLE WITH AND SUPPORTS TRENDING ANALYSIS.



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 64	1/05/88

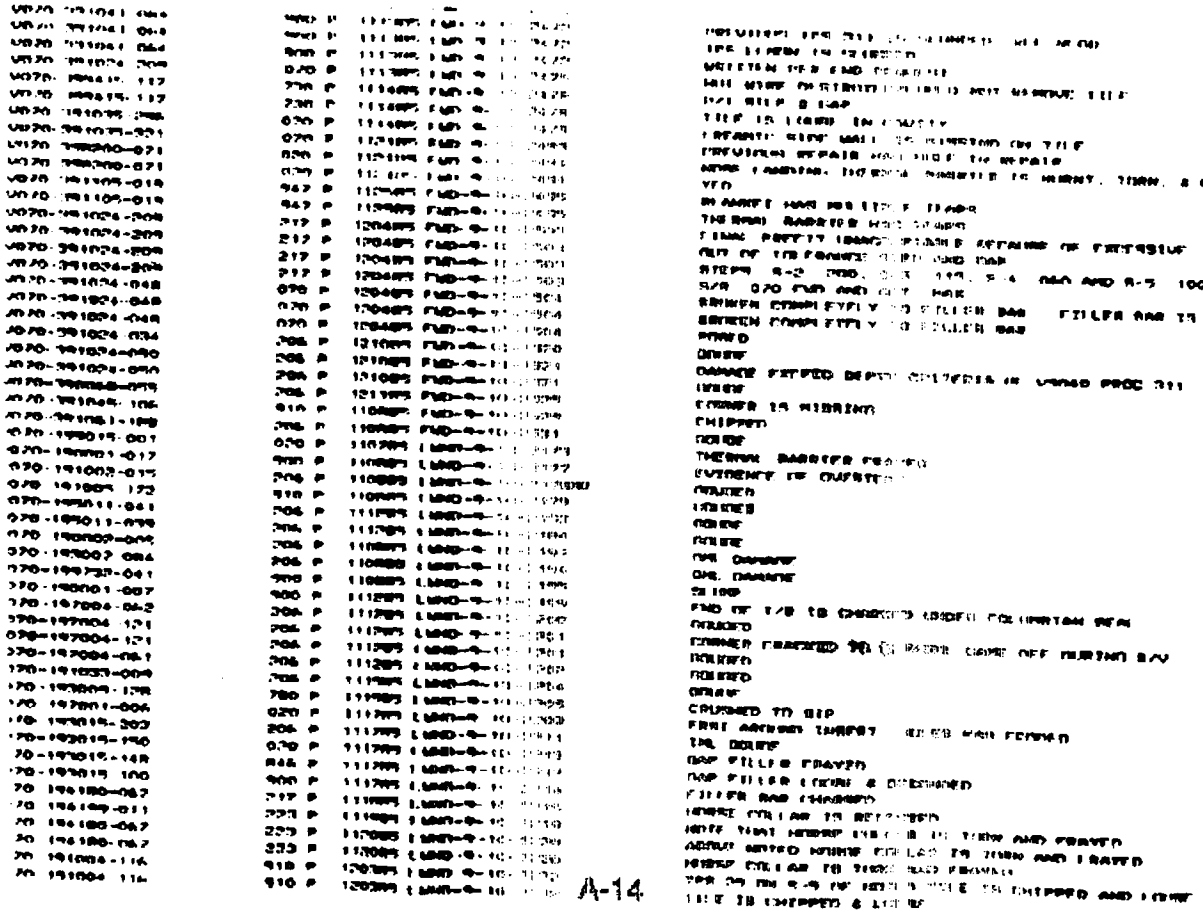
USE PRACA

ACCESS /DATA / TRENDING

- TERMINALS AVAILABLE AT NASA CENTERS
- DATA BASE COVERS ALL TPS ELEMENTS
- SOME DATA IS SUSPECT
  - INCOMPLETE
  - SUBJECTIVE

- SKILL IS REQUIRED TO ASK THE RIGHT QUESTION THE RIGHT WAY SO AS TO GET THE INFORMATION YOU WANT IN A USEFUL FORM
  - IF NOT QUERIED PROPERLY MAY MISS DATA
  - MAY GET MORE INFORMATION THAN YOU WANT

- DATA RETRIEVAL MAY BE A MANUAL TASK
- USERS HAVE PRIMARILY BEEN QE, [illegible]ABILITY, LOGISTICS
- LIMITED USE / INPUT BY SUBSYSTEM EXPERTS
- NO FORMAL TRENDING
- VERY LIMITED GRAPHICS CAPABILITY



TIPS

(TILE INFORMATION PROCESSING SYSTEM)

NASA
Lyndon B. Johnson Space Center
FLIGHT CREW
OPERATIONS
DIRECTORATE

SUBJECT:
THERMAL PROTECTION SYSTEM
TREND ANALYSIS SURVEY

NAME:
CB/E. BAKER
CB/B. DUNBAR
DATE:
MARCH 2, 1988

DATA BASE

INCLUDES: VEHICLE CONFIGURATION (TPS RELEVANT)
- TILE AND SIP, FIB, SCREED, PVT, BV
- DESIGN GAP FILLERS (NEW)
- F/B ANOMALIES (NEW)
- S/G ON ORIGINAL BUILD PLUS ON OCCASION
- ENGINEERING DATA / REQUIREMENTS FOR LAST FLOW OF TILE

PR'S RESULTING IN TILE OR FIB REMOVAL, MR, SHAVED

DOESN'T INCLUDE: TCS, THERMAL BARRIERS

MANY TPS REPAIRS

CAN SORT BY: MULTIPLE FIELDS

INCLUDES INFORMATION BACK TO STS-4

AT THE END OF A FLOW, FLIGHT DAMAGE RECORDS ARE REMOVED FROM ACTIVE DATA BASE

ACTIVE DATA BASE FOR TILE REMOVAL GOES BACK THREE FLIGHTS

EARLIER DATA CAN BE ACCESSED ON REQUEST

TIPS

DATA FORMATS

1. TILE CHARACTERISTICS
2. ENGINEERING REQUIREMENTS
3. TILE LOCATION
4. PART NUMBER REVISIONS
5. CARRIER PLATES
6. INSTALLATION DATA (REMOVAL CODES)
7. BOND VERIFICATION (BV)
8. PULSE VELOCITY TEST/SONIC DATA
9. SCREED/HEATSINK
10. TILE STEP/GAP CORNER STEP
11. TILE SIP/FOOTPRINT DATA

MALFUNCTION CODES

1. IDENTIFICATION REQUIREMENT
2. FLIGHT DAMAGE (BROKEN, CHIPPED, CRACKED, GOUGE)
3. ENGINEERING EVALUATION
4. ENGINEERING CHANGE (MCR, EO, SAR)
5. CHARRED/DAMAGED FILLER BAR
6. ACCESS
7. BOND VERIFICATION FAILURE
8. GROUND DAMAGE (BROKEN, CHIPPED, CRACKED, GOUGE)
9. LOST IN FLIGHT

TIPS

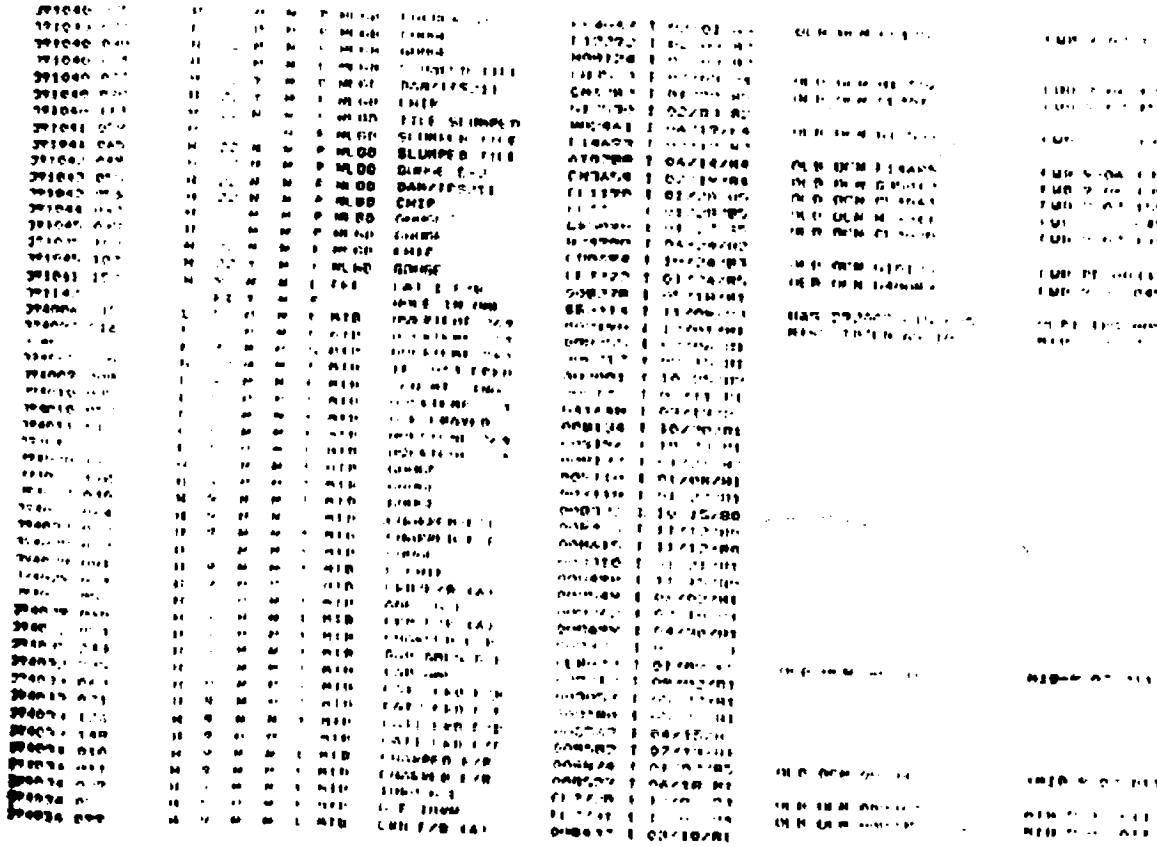
MALFUNCTION CODES CONT'D

A. ENVIRONMENTAL DAMAGE (WIND, HAIL, LIGHTNING, RAIN)
B. REMOVED IN ERROR
C. HEAT DAMAGE (MELT)
D. SIP DAMAGE/PROBLEMS
E. STEP AND GAP OUT OF TOLERANCE (OUT OF TOLERANCE)
F. TILE EROSION (THRUSTERS)
G. FLUID CONTAMINATION (SPILLS OR LEAKS)
H. LOOSE TILE
I. TRANSFER SCRAP (FERRY FLIGHT INSTALLATION ONLY)
J. LOST DURING FERRY FLIGHT
K. TRANSFER DAMAGE FROM PALMDALE)
L. MISCELLANEOUS
M. N/A APPLICABLE TRANSFER FROM PALMDALE
N. NOT BUILT TO DRAWING
O. SONIC FAILURE
P. MISLOCATED BOND
Q. TRANSFER DAMAGE (FROM KSC)
R. RTV PROBLEMS
S. SILTS RELATED
T. SCREED PROBLEMS
U. TILE "A" MOD
V. CANNIBALIZATION
W. IMPROPER PROCESSING
X. GAP FILLER

TIPS

ACCESS / DATA / TRENDING

- TERMINALS AVAILABLE AT DOWNEY, KSC, JSC
- DATA ENTERED BY VERY KNOWLEDGEABLE TPS OPERATORS
- DATA BASE NOT "CONTROLLED"
- WIDESPREAD USE BY TPS COMMUNITY
- NO FORMAL TRENDING
- GRAPHICS CAPABILITY IS AVAILABLE



PCASS

(PROGRAM COMPLIANCE ASSURANCE AND STATUS SYSTEM)

NASA
Lyndon B. Johnson Space Center
FLIGHT CREW
OPERATIONS
DIRECTORATE

SUBJECT:
THERMAL PROTECTION SYSTEM
TREND ANALYSIS SURVEY

NAME:
CB/E. BAKER
CB/B. DUNBAR
DATE:
MARCH 2, 1988

SYSTEM INTEGRITY ASSURANCE PROGRAM PLAN

NSTS 07700, VOL XI

APRIL 8, 1987

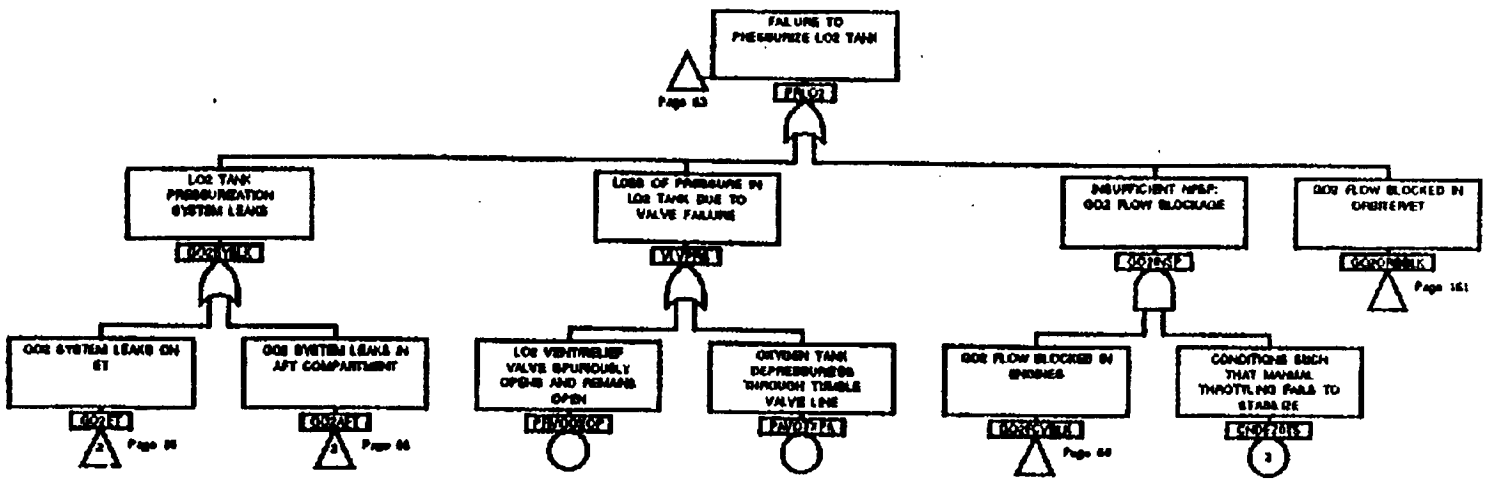
1.6 PROGRAM DESCRIPTION. THE SIAP ENCOMPASSES THOSE ACTIVITIES/FUNCTIONS REQUIRED TO PROVIDE COMPREHENSIVE CONFIGURATION AND MAINTENANCE PROGRAMS, CLOSED LOOP ACCOUNTING, TREND ANALYSIS AND MANAGEMENT INFORMATION.

1.7.1 THE DEPUTY DIRECTOR, NSTS PROGRAM IS RESPONSIBLE FOR MANAGING THE SIAP...

THE NSTS ENGINEERING INTEGRATION OFFICE IS THE OFFICE OF PRIMARY RESPONSIBILITY...

1.7.2 THE NSTS ELEMENT PROJECT MANAGERS ARE RESPONSIBLE FOR IMPLEMENTATION OF ELEMENT PROJECT ACTIVITIES IN SUPPORT OF THE SIAP. THIS INCLUDES BUT IS NOT LIMITED TO THE FOLLOWING:

G. DEVELOP AND CONDUCT RELIABILITY, PERFORMANCE, AND SUPPORTABILITY TREND ANALYSIS FOR FLIGHT AND CRITICAL GROUND SYSTEMS.



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 64	1/05/88

SPACE SHUTTLE MAIN PROPULSION PRESSURIZATION SYSTEM PROBABILISTIC RISK ASSESSMENT, FINAL REPORT

Job Order 72-709

PREPARED BY

G. N. Henning, Project Engineer
Advanced Programs and Space Station
Engineering Department

LEMSCO APPROVAL

H. E. Smith, Project Manager
Engineering and Science Program Office

K. R. Frohme, Manager
Propulsion and Power Department

M. M. Miller, Director
Engineering Support Branch

NASA APPROVAL

J. D. Norris
Technical Monitor

C. A. Vaughan, Chief
Propulsion and Power Division

H. O. Pohl, Director
Engineering

R. W. Moorehead, Manager
NSTS Engineering Integration Office

Prepared By

Lockheed Engineering and Management Services Company

For

Propulsion and Power Division

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
LYNDON B. JOHNSON SPACE CENTER
HOUSTON, TEXAS

February 1988

LEMSCO-24122

ABSTRACT

During the post-Challenger investigation the National Research Council Shuttle Criticality Review and Hazard Analysis Audit Committee expressed concern that the approximately 1,300 safety-critical failure points were not prioritized based on probability of occurrence. They suggested that an integrated systems assessment be devised which would provide for failure probability quantification. The National Space Transportation System Program Office subsequently initiated a pilot project employing the probabilistic risk assessment (PRA) methodology to evaluate its usefulness and also to identify any areas of concern not previously established.

This report describes the PRA performed on the Shuttle Main Propulsion Pressurization System, which is an assembly of many components contained within three of the four vehicle elements (the Orbiter, the External Tank, and the main engine) and which crosses the element interfaces. The PRA was performed by Lockheed Engineering and Management Services Company in conjunction with the Lockheed Missiles and Space Company Research and Development Division. The report includes a discussion of the scope of the analysis, a description of the team organization, a description of the PRA methodology and its application in this study, and a summary of lessons learned. A matrix is also provided to map the information in this report to the information in the analysis report (LMSC-F2230402, January 1988), which is provided as an attachment.

CONTENTS

Section		Page
1.	BACKGROUND	1-1
2.	SCOPE OF ANALYSIS	2-1
3.	TEAM ORGANIZATION	3-1
4.	PRA METHODOLOGY	4-1
	4.1 SYSTEM DEFINITION	4-1
	4.2 FAULT TREE	4-1
	4.3 FAILURE RATE DATA BASE DEVELOPMENT	4-6
	4.4 PRA SOFTWARE	4-6
	4.5 SUMMARY OF PRA METHODOLOGY	4-6
5.	LESSONS LEARNED	5-1
	5.1 MPPS PROBLEM AREAS	5-1
	5.2 USEFULNESS OF PRA FOR NASA	5-1
	5.3 RISK HIERARCHY	5-1
	5.4 KNOWLEDGE CAPTURE	5-2
	5.5 COMPLEXITY OF THE PRA METHODOLOGY	5-2
	5.6 THE FAILURE RATE DATA BASE	5-2
	5.7 SOFTWARE CONSIDERATIONS	5-3
	5.8 PRA AS A MANAGEMENT TOOL	5-3
6.	REFERENCE MATRIX	6-1

ATTACHMENT 1

VOLUME I. SECTIONS 1 - 7

VOLUME II. APPENDICES A - 7

VOLUME III. APPENDICES E - K

FIGURES

Figure		Page
3-1	Team organizational responsibilities	3-3
4-1	Space Shuttle Main Propulsion System Pressurization System PRA flow	4-2
4-2	Top-level fault tree	4-3
4-3	Fault tree architecture	4-4

ACRONYMS

CIL	critical items list
DOD	Department of Defense
ET	external tank
FMEA	failure modes and effects analysis
GSE	ground support equipment
HA	hazard analysis
LEMSCO	Lockheed Engineering and Management Services Company
LHS/TEMAC	Latin Hypercube Simulation/Top Event Matrix Analysis Code
LLNL	Lawrence Livermore National Laboratories
LMSC	Lockheed Missiles and Space Company
LRU	line replaceable unit
MIL-SPEC	military specification
MPPS	Main Propulsion Pressurization System
NASA	National Aeronautics and Space Administration
NSTS	National Space Transportation System
OMS	Orbital Maneuvering System
OPF	Orbiter Processing Facility
PC	personal computer
PRA	probabilistic risk assessment
PRACA	Problem Reporting and Corrective Action
R&DD	Research and Development Division
SAIC	Science Applications International Company
SSME	Space Shuttle Main Engine
STS	Space Transportation System
SR&QA	Safety, Reliability, and Quality Assurance

1. BACKGROUND

During the post-Challenger investigation the National Research Council Shuttle Criticality Review and Hazard Analysis Audit Committee expressed concern that the approximately 1,300 safety-critical failure points were not prioritized based on probability of occurrence. They suggested that an integrated systems assessment be devised which would provide for failure probability quantification. The committee further recommended that the assessment be closely coupled with the existing failure modes and effects analysis/critical items list (FMEA/CIL) activity to assure coverage of the truly safety-critical items in the Space Transportation System (STS).

The National Space Transportation System (NSTS) Program Office initiated a pilot project employing the probabilistic risk assessment (PRA) methodology to evaluate its usefulness and also identify any areas of concern not previously established. This methodology has been used successfully by the nuclear industry in analyzing, quantifying, and prioritizing the risks presented by nuclear power plants.

This report describes the PRA performed on the Shuttle Main Propulsion Pressurization System (MPPS). The MPPS is an assembly of many components which is contained within three of the four vehicle elements (the Orbiter, the External Tank (ET), and the main engine) and which crosses the element interfaces. The PRA was performed by Lockheed Engineering and Management Services Company (LEMSCO) in conjunction with the Lockheed Missiles and Space Company (LMSC) Research and Development Division (R&DD).

A summary of the conclusions found herein is as follows:

a. The PRA methodology and the NSTS FMEA/CIL techniques complement each other, and together provide an enhanced approach to risk management.

b. The PRA methodology is adaptable to NASA space systems and is usable throughout the NASA organizational environment.

c. The PRA methodology can be learned and applied, using the currently available tools, by any integrated aerospace organization, and does not require extensive training.

This report consists of a discussion of the scope of the analysis, section 2. This discussion is followed in section 3 by a description of the PRA team organization, including the skill mix and experience of the team personnel. Section 4 describes the PRA methodology and its application in the study of the MPPS. The lessons which were learned from the study are contained in section 5. Section 6 provides a matrix to map the information outlined in this report to the detailed information contained in the LMSC R&DD analysis report (LMSC-F2230402, January 1988), which is provided as an attachment.

2. SCOPE OF ANALYSIS

The MPPS which NASA requested be analyzed using PRA methodology is comprised of those elements which furnish the pressurant gas at the necessary conditions for proper and safe operation of the entire Main Propulsion System, from the beginning of ground operations to successful return of the Orbiter to earth. A complete analysis would have required consideration of the entire Main Propulsion System which includes the ET, the Orbiter, the Space Shuttle Main Engine (SSME), and the ground support equipment (GSE). Such a task was a far greater effort than was required to meet NASA's objectives of demonstrating the usefulness of the PRA methodology for manned space applications in a reasonable time and at a reasonable cost.

The MPPS system, which was defined with NASA's concurrence, can best be described as a collection of functions which cross many system boundaries rather than as a well-defined system in itself. The following functions are considered:

a. Supply of pressurant gas to the ET to prevent its collapse from external pressure, and to provide sufficient positive pressure to prevent cavitation of the SSME pumps.

b. Supply of purge gases and gases to inert the system, minimizing the explosion hazard.

c. Supply of pressurant gas to actuate engine valves as a backup to a malfunctioning hydraulic system.

d. Supply of gas as a primary source of actuation pressure for various system valves.

The analysis considered those elements and components of the Orbiter, the ET, the SSME, and the GSE which either affect the pressurization functions or are affected by the pressurization functions. The scope of the analysis led to partial inclusion of the Electrical Power Distribution and Control System, the Electronic Instrumentation and Control System, and the Hydraulic Power System, as well as operational considerations. The scope of work chosen for

the analysis, while abbreviated from what would be considered in a complete system approach, provided extremely useful results and demonstrated the effectiveness of the PRA methodology.

3. TEAM ORGANIZATION

The team organization is shown in figure 3-1. The task was administered by the NSTS Program Office with technical management assigned to the Propulsion and Power Division of the Engineering Directorate. LEMSCO provided program management, performed engineering and organizational support, and provided the liaison with other related NASA organizations. LMSC R&QA performed the PRA analysis and delivered an analysis report (LMSC-F2230402, January 1988) which is included as attachment 1. The engineering and analysis teams consisted of personnel having a broad mix of PRA and spacecraft systems engineering expertise, including new college graduates, journeyman-level engineers with PRA and system engineering experience, senior project engineers, and managers. These teams possessed little or no experience with propulsion systems. They were assisted by consultants who contributed an understanding of the system's operation and an understanding of NASA's needs across the communities of engineering; safety, reliability, and quality assurance (SR&QA); program management; and PRA peer disciplines. Support for the site-licensed PRA CAFTA software was provided by the vendor, Science Applications International Company (SAIC).

A subsequent independent peer review of the PRA was accomplished by Lawrence Livermore National Laboratories (LLNL) under the sponsorship of the NSTS Program Office. This review was supported by the LMSC analysis team, and the LLNL review results and team responses are included in attachment 1.

The team mix brought these various specialty areas to the project; however, the systems engineering specialists originally had no knowledge of PRA methodology, nor did the PRA specialists have any knowledge of manned spacecraft systems. LEMSCO personnel and the consultants provided the understanding of engineering, operations, and NASA's SR&QA techniques and policy. LMSC provided the necessary expertise in PRA analysis techniques. Meetings and working sessions between the groups provided the necessary cross-fertilization across disciplines. This interdisciplinary exchange required by the process made it evident that PRA would be especially useful on a new project as an integrated activity during the design, development, and test

phases rather than as a separate appraisal after vehicle development is mature.

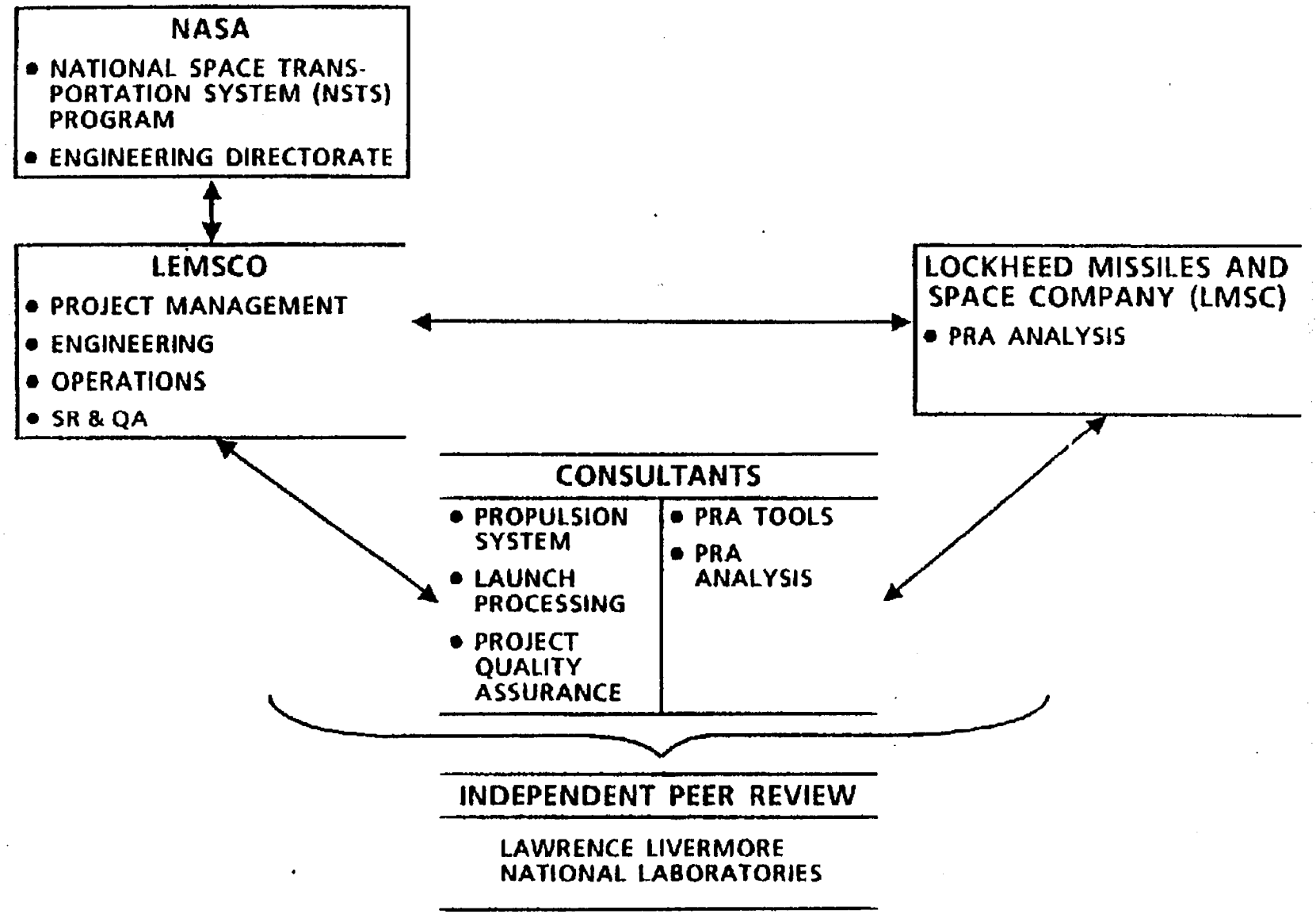


Figure 3-1.- Team organizational responsibilities.

4. PRA METHODOLOGY

Figure 4-1 is a graphical summary of the process flow used to perform the MPPS PRA. The figure depicts the following process elements: a system definition, failure rate data base development, and PRA software tools. Figures 4-2 and 4-3 are provided for discussion of fault trees contained in section 4.2.

4.1 SYSTEM DEFINITION

The most important step in a PRA project is system definition. This is accomplished by an engineering review of all system and component documents, drawings, and schematics to provide a clear understanding of the system requirements and operation. This allows the creation of a system definition and the establishment of boundaries defining what will be included in the scope of the study. This was difficult because the MPPS crossed many Shuttle element boundaries and mission-operational regimes.

4.2 FAULT TREE

The end product of this analysis is a fault tree whose top level is shown in figure 4-2. The fault tree in itself does not reflect the system reliability or likelihood of failure. PRA assumes that components fail; hence, it is necessary to characterize all malfunctions as failures at the component or functional level. The fault tree is constructed in a logical manner to depict the relationships between failures. This requires generation of failure modes as had previously been done by the NSTS program using the FMEA technique. These previously generated FMEA's and hazard analyses (HA's) were used to complement and validate the current fault tree analysis. It is then necessary to determine whether failures of one or more components or functions at any level will propagate into the top level event, which is loss of life or vehicle. This is illustrated in figure 4-3. The fault tree progresses from the top event through the definition of mission phases, categories of failures, and definition of contributing functions. The bottom level represents failures or groups of failures which contribute to system-level failures. The fault tree simply provides a mapping of all failure

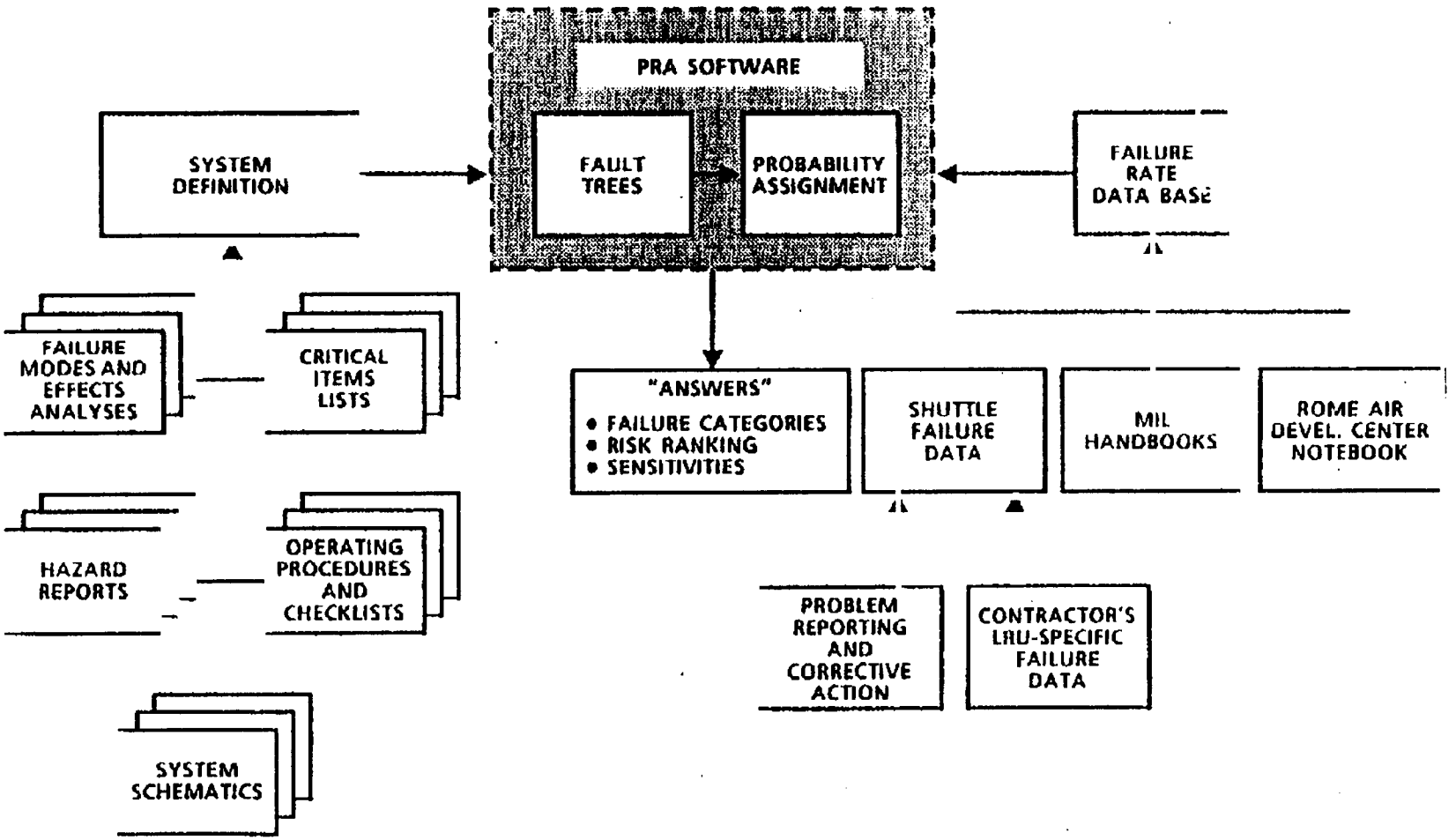


Figure 4-1.- Space Shuttle Main Propulsion System Pressurization System PRA flow.

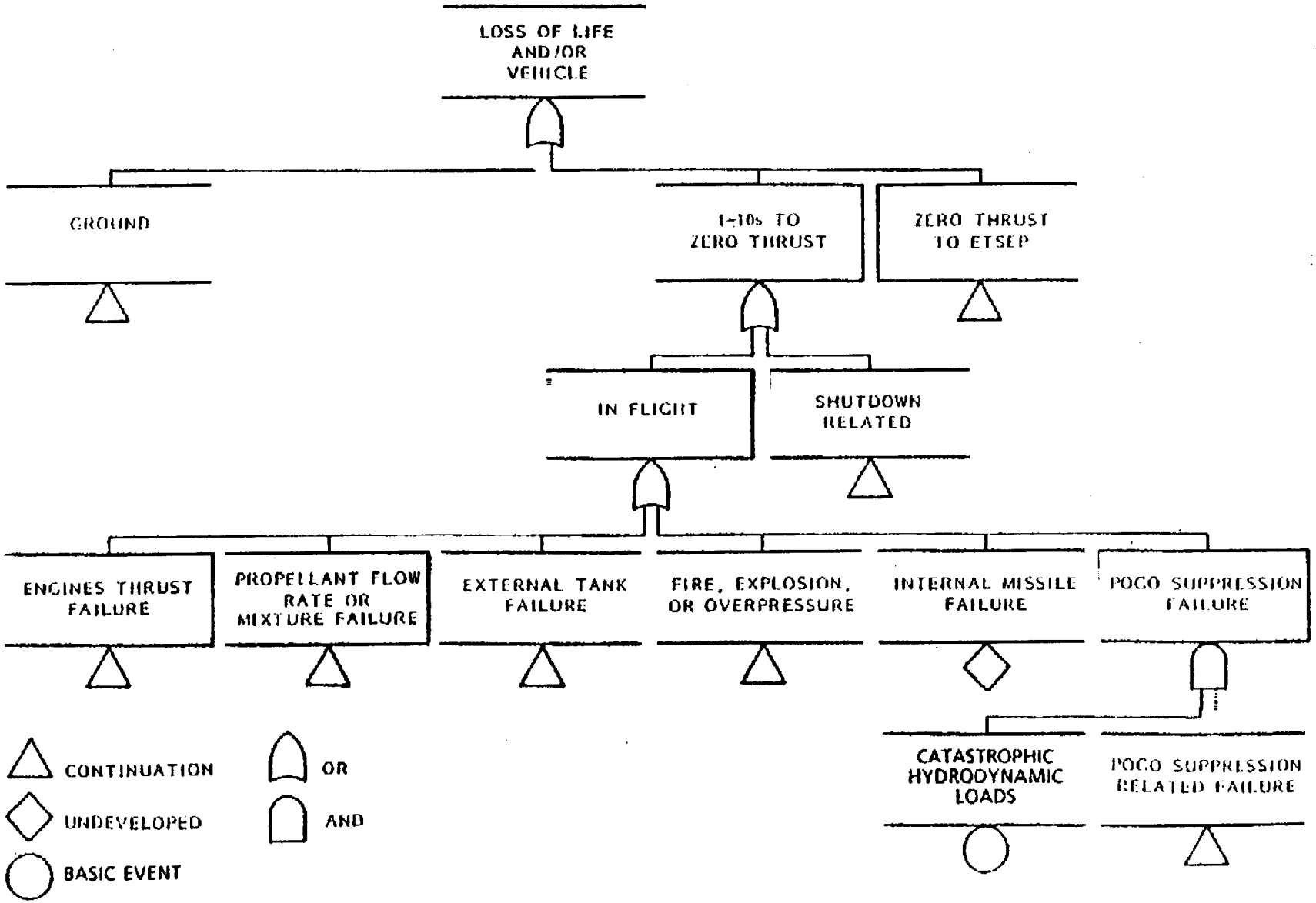


Figure 4-2.- Top-level fault tree.

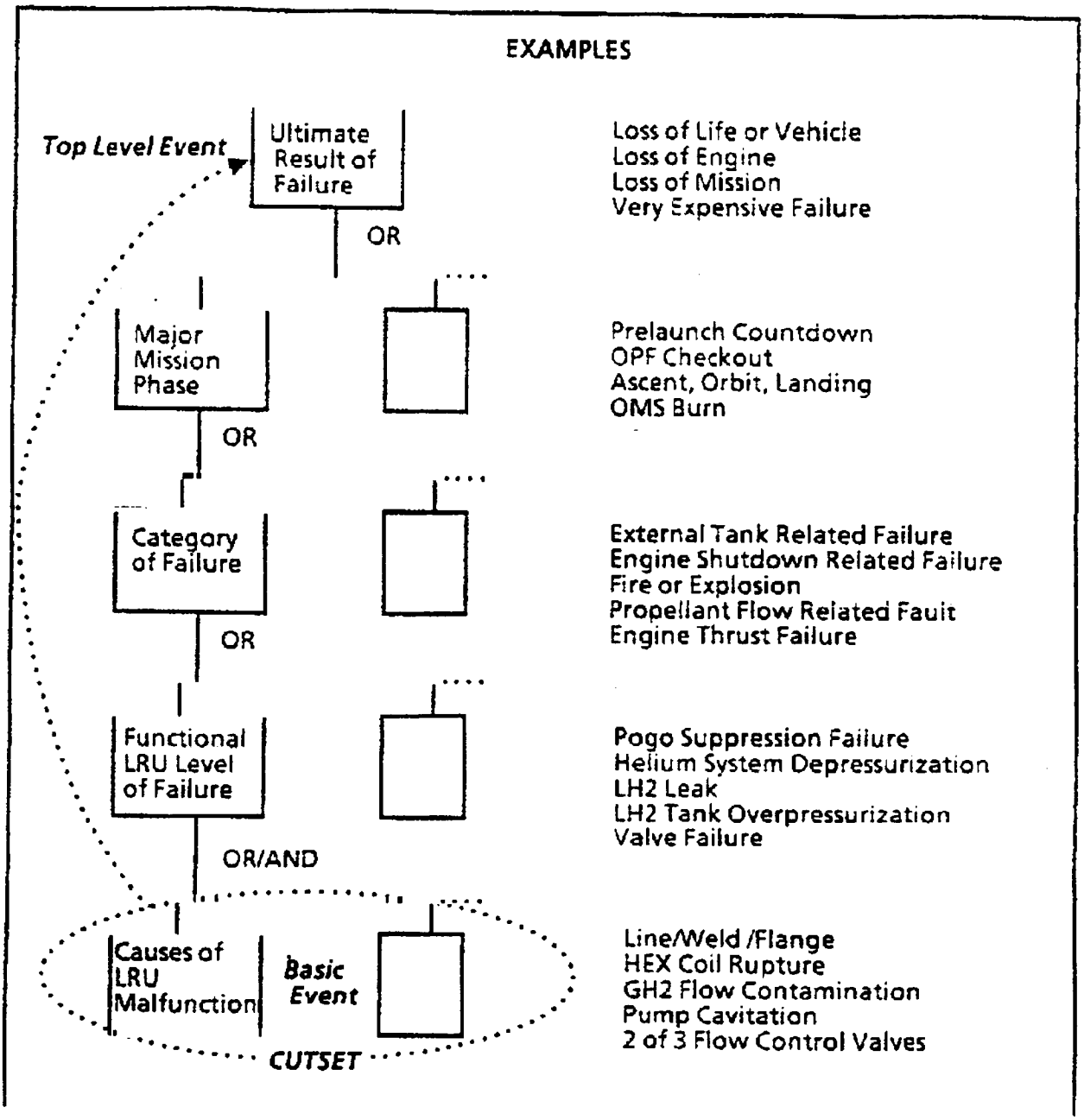


Figure 4-3.- Fault tree architecture.

events which can progress to a top event. The analysis is iterative, as the PRA analyst modifies the engineering fault tree model to improve computational efficiency while preserving engineering clarity.

The fault tree does not reflect the degree of system usefulness. In the original application of PRA, response to failure results in a safe shutdown. In manned space operations, safe shutdown of critical components or functions is not acceptable, and it is necessary to continue the mission using redundant systems which have not failed or default to operational workarounds, or to continue operations during a safe abort.

At the top of the fault tree in figure 4-2 is the top-level event - loss of life and/or vehicle, which would result from a failure in some component of the MPPS which propagated to the top level event. The system was analyzed in three phases of mission operation: (1) prelaunch, (2) powered flight, and (3) ET separation. Each phase has an operating environment so distinctive that the three phases were identified as the second level of the tree. Each phase then forms its own unique tree, and the software treats each separately. The next level of the tree provides categories of failures which can cause the top-level event to occur. Examples of these are ET-related failures and catastrophic failure due to fire and overpressure. Finally, the malfunctions which may, by themselves or in combination with others, cause the loss of function were identified and placed in the fault tree as <u>basic</u> or <u>bottom level</u> events.

The fault tree indicates those events which were not analyzed, as well as those that were. The diamond symbol under the event "catastrophic failure due to internal missile generation" indicates that this event was not analyzed. The triangle symbol indicates continuation of the tree event in more detail. The complete fault tree is quite detailed and fills approximately 150 pages similar to figure 4-2.

4.3 FAILURE RATE DATA BASE DEVELOPMENT

In reference to figure 4-1, it was necessary to obtain failure rate data on the various components in order to get some type of relative ranking of the failures. NASA sources such as Problem Reporting and Corrective Action (PRACA) and other NASA data sources were inadequate, either because of the small number of samples or because service life and operation cycles were not available. The PRA team extracted, from Department of Defense (DOD) sources such as military handbooks and Rome Air Development Center notebooks, generic failure rate data on similar components in an operating environment very close to that experienced on Shuttle flights. These data proved to be more acceptable than was originally anticipated.

4.4 PRA SOFTWARE

In reference to figure 4-1, the software, CAFTA, was provided under license from SAIC. This software greatly simplifies the PRA analysis process. It is used in developing and updating the fault trees, can be used to manage the failure rate data base, can quantify and prioritize the various failures, and can be used in sensitivity analyses where the effect of component reliability on the probability of a top-level event occurring can be evaluated.

The software, which was run on an IBM PC-AT, was easy to use and understand. Training times were short for PRA team members who had no previous exposure to PRA. The load imposed by the MPPS analysis taxed the limits of the addressable memory of the machine and indicates that more complex systems will require something larger than a personal computer (PC).

4.5 SUMMARY OF PRA METHODOLOGY

The PRA methodology accomplishes what is intended. It provides an accurate representation of failure scenarios, pinpoints weak areas in system design, flags those areas requiring more attention, and prioritizes the various categories of failures.

Its weaknesses are as follows:

a. It cannot test for model completeness.

b. Its quantitative results are limited by the quality of input data.

c. The analysis may be simplistic in its representation of the system-level behavior.

Fortunately, these weaknesses can be minimized or eliminated by use of the FMEA and HA techniques; thus PRA and FMEA, when used together, complement each other.

5. LESSONS LEARNED

As a result of the MPPS pilot project experience, eight major lessons were learned. These lessons are discussed in sections 5-1 through 5-8.

5.1 MPPS PROBLEM AREAS

No new problem areas were identified by the PRA study. This is not surprising, since the Shuttle is a mature engineering system that has undergone years of development and study. This observation lends additional confidence to the FMEA/CIL process.

The study identified the single largest category of catastrophic failures to be those associated with leakage of pressurized mechanical system components which results in explosion or compartment overpressurization. This single failure category contributes over 84 percent of the MPPS risk. The addition of functional redundancy will not, in general, reduce overall risk. Additional piping and components containing propellants or pressurants increase, rather than decrease, the catastrophic risk sources, with the resulting failure probability growing at a polynomial rate. It would appear more beneficial to emphasize controlling the direct sources of risk through ground maintenance and early leak detection.

5.2 USEFULNESS OF PRA FOR NASA

The PRA has the ability to quantify risk. The FMEA methodology does not. Not only does the FMEA process ignore quantification in general, but it (by definition) cannot consider "multiple failure modes." In principle, such analyses could be performed, but the question would always remain whether all reasonable combinations had been considered. The heart of a PRA study is its "top down" methodology, in which the system is dissected and quantified free from designer-level prejudice.

5.3 RISK HIERARCHY

The PRA analysis yielded an effective ranking of the risks relative to loss of life and/or vehicle due to MPPS failure. Sensitivity computations served

to verify the internal consistency of the fault tree. The PRA methodology points toward an objective resolution of the conflicts of traditional engineering analysis. If the results of the PRA study are disputed, it is necessary to identify and resolve the flaws, either in the fault tree or in the assigned failure rate data. The bottom line is that the study provided an explicit quantification of the risks inherent to the MPPS.

5.4 KNOWLEDGE CAPTURE

Two major products of the PRA analysis were the fault tree and the associated MPPS system description. In retrospect, it is evident that both of these products serve a purpose beyond their immediate intent, in that they provide a vehicle for knowledge transfer. To be precise, the system description was generated because there was no comparable document in the NASA literature. It organized information available in many sources into a comprehensive system description. The fault tree, originally developed to support the quantification critical to the PRA procedure, also served to reinforce the system description. These products capture corporate knowledge far beyond their obvious intent.

5.5 COMPLEXITY OF THE PRA METHODOLOGY

Contrary to expectations, the PRA methodology proved to be easily understood by the technical staff. There are subtleties that require specialized knowledge, but the project staff had no trouble in absorbing the general technique. This is especially noteworthy when one considers the diverse composition of the engineering and analysis teams. In actual fact, it was found that the PRA analysis process provided a common forum which encouraged inputs from the various engineering and SR&QA disciplines. The PRA process demands of its practitioners a commitment to excellence, and all members of the team responded to the challenge.

5.6 THE FAILURE RATE DATA BASE

The study illustrated the inadequacy of the extant NASA data base for failure rate data. In general, the problem is easily described; the current data reflects failures, but without quantification as to time, cycle, cause, or

detail. On the other hand, the MIL-SPEC generic data bases proved quite adequate to the quantification of the MPPS fault tree. This indicates that effective analyses can be performed in the absence of Shuttle-specific data, though the latter is clearly preferred.

5.7 SOFTWARE CONSIDERATIONS

The computer software was crucial to the success of the MPPS analysis. In particular, the CAFTA fault tree analysis program allowed easy development and manipulation of the fault tree. The Latin Hypercube Simulation/Top Event Matrix Analysis Code (LHS/TEMAC) sensitivity codes allowed the PRA team to perform computations that were far beyond the capability of hands-on calculation. On the minus side, the magnitude of the MPPS project taxed the CAFTA program to its limits. It is clear that software support is necessary, and that studies larger than the MPPS will require expansions of computer capability (more memory and better program integration).

5.8 PRA AS A MANAGEMENT TOOL

The immediate results of the MPPS PRA study provide a convenient tool for management, in that the resulting risk hierarchy aids in the allocation of sometimes scarce engineering resources. Furthermore, the fault tree and its associated quantification are extremely flexible in practical application. For example, once the basic fault tree and risk data base are in place, it is easy enough to reflect changes in the MPPS system, simply by editing the tree or data base. The products of the analysis serve as a flexible and visible model of the MPPS system.

6. REFERENCE MATRIX

The attached matrix has been provided as a cross-reference guide between this report and LMSC document LMSC-F2230402, which is included as attachment 1.

The purpose of this matrix is to provide the reader with a convenient guide to obtain detailed information relative to specific sections of this report.

TABLE 6-1.- REFERENCE MATRIX*

Subject	Section	LMSC-F2230402	
		Volume	Section
Background	1.0	1	1.0 1.1 1.2 2.0 2.4 Table 1-1 Table 2-4
Scope of analysis	2.0	1	2.2 2.3 2.6 2.6.1 2.6.2 Table 2-3 Table 2-5 Table 2-6 Section 5
		2	Appendix D.1
Team organization	3.0	3	Appendix K
Methodology and limitations	4.0		
System definition	4.1	1	Figure 3-1 Figure 3-4 Section 5
		3	Appendix E

*Matrix is concluded on next page.

TABLE 6-1.- REFERENCE MATRIX (Concluded)

Subject	Section	LMSC-F223040Z	
		Volume	Section
Fault tree	4.2	1	1.2 2.3 3.1 3.1.2 2.5 3.0 3.1.1 Figure 3-2 Figure 3-3 6.1 6.1.1
		2	Appendix D
Failure rate data	4.3	1	1.0 2.2.2 2.3 3.2.1 3.2.2 3.3.3 Table 3-1
		2	Appendix C
PRA software	4.4	1	3.3.1 3.3.2 4.5
		3	Appendix I
Summary of PRA methodology	4.5	1	1.0 2.0

National Aeronautics and
Space Administration

Lyndon B. Johnson Space Center
Houston, Texas 77058

JSC-22851

SPACE SHUTTLE MAIN PROPULSION PRESSURIZATION SYSTEM PROBABILISTIC RISK ASSESSMENT, FINAL REPORT

Job Order 72-709

ATTACHMENT 1

VOLUME I

Prepared By

Lockheed Engineering and Management Services Company
Houston, Texas

Contract NAS 9-17900

For

PROPULSION AND POWER DIVISION

February 1988

LEMSCO-24122

PROBABILISTIC RISK ASSESSMENT OF THE SPACE SHUTTLE MAIN PROPULSION PRESSURIZATION SYSTEM

VOLUME I
SECTIONS 1-7

January 1988

Research and Development Division
LOCKHEED MISSILES & SPACE COMPANY, INC.
3251 Hanover Street
Palo Alto, California 94304

VOLUME I

CONTENTS

SECTION

ACKNOWLEDGEMENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

1.0 INTRODUCTION

- 1.1 Use of PRA
- 1.2 Comparison of PRA with Other Methodologies
- 1.3 Organization of the Report

2.0 EXECUTIVE SUMMARY

- 2.1 Significant Findings
  - 2.1.1 Risk Contributors
- 2.2 Recommendations
  - 2.2.1 Prevention of Explosion and Overpressurization Scenarios
  - 2.2.2 Failure Rate Data Base Development
  - 2.2.3 Improvement of Documentation System
- 2.3 Study Limitations
- 2.4 Comparison of MPPS PRA to Earlier Studies and Tests
- 2.5 Summary of Analytical Approach
- 2.6 Scope of Analysis
  - 2.6.1 Basis for Inclusion of Events
  - 2.6.2 Specific Scope Boundaries

3.0 METHODOLOGY

- 3.1 Model Development
  - 3.1.1 Fault Tree Organization
  - 3.1.2 Example of Model Development
- 3.2 Database Development
  - 3.2.1 Component Failure Rates
  - 3.2.2 Basis for Exposure Times
- 3.3 Probabilistic Computations
  - 3.3.1 CAFTA Code
  - 3.3.2 Importance Measures
  - 3.3.3 Synthetic Sampling Statistics

4.0 QUANTITATIVE EVALUATION

- 4.1 System and Component Failure Rates
- 4.2 Human Error
- 4.3 Failure Probability Calculations
- 4.4 Sensitivity Analysis
- 4.5 Importance Calculation of Dominant Events
  - 4.5.1 Results of Fussell-Vesely Importance Ranking
  - 4.5.2 Results of Structural Importance Ranking

5.0 SYSTEMS DESCRIPTION

5.1 LH2 and LO2 Propellant Flow Functions

5.1.1 Propellant Flow Path
5.1.2 Propellant Pressure Boundary
5.1.3 Control of Major Mechanical Component
5.1.4 External Tank Pressurization

5.1.4.1 LO2 Tank
5.1.4.2 LH2 Tank

5.2 Support Systems

5.2.1 Pneumatic System
5.2.2 Hydraulic System

5.3 Pressure Control

5.3.1 Pressure Sensing
5.3.2 Pressure Relief

5.4 Pogo Suppression
5.5 Electrical Instrumentation and Control (EI&C) Functions

5.5.1 Avionics System Features and Interfaces
5.5.2 Propellant Flow Rate/Mixture Control
5.5.3 Engine Isolation on Demand (Shutdown)
5.5.4 External Tank Separation

5.6 Main Engine Shutdown

5.6.1 Failure to Shutdown a Single Engine
5.6.2 Two Engine Shutdowns

5.7 Ground Operations (MPS)
5.8 Mission Accomodation of In-Flight Failures

6.0 RISK ASSESSMENT

6.1 Launch and Prelaunch Time Sequence
6.1.1 Basis for Division of Time Intervals
6.1.2 Consequence Data
6.2 Summary of Risk Computations

7.0 REFERENCES

VOLUME II

CONTENTS

APPENDICES

A TERMINOLOGY

B MNEMONICS, EXPLANATIONS, AND LOCATIONS OF BASIC EVENTS

C FAILURE PROBABILITY DATA BASE

D DETAILED MISSION FAILURE FAULT TREE

D.1 Ground Accident Events

D.2 Flight and Ignition Sequence Accidents

D.2.1 Shutdown-Related Failures
D.2.2 Inflight Failures

D.2.2.1 Failure to Provide Sufficient Thrust
D.2.2.2 External Tank Related Failures
D.2.2.3 Catastrophic Failure Due to Fire or Explosion
D.2.2.4 Catastrophic Failure Due to Internal Missile Generation
D.2.2.5 POGO Suppression Failure

D.3 Accidents Occurring During Separation of ET and Orbiter

D.4 Major Components Appearing in More Than One Fault Tree Branch

VOLUME III

CONTENTS

APPENDICES

E DETAILS AND OUTLINE DRAWINGS FOR MAJOR SYSTEM COMPONENTS

- E.1 ET Components
- E.2 Orbiter Components
- E.3 SSME Components
- E.4 Helium Pneumatic System Components

F GROUND OPERATIONS DATA

- F.1 Flight Scrub Safeguards
- F.2 Human Error Probabilities

G FIRE AND EXPLOSIONS CAUSED BY LEAKAGE AND CONTAMINATION

- G.1 Component Leakage or Rupture
- G.2 Contamination or Plugging Induced Explosions

H FAULT TREE CONSISTENCY EVALUATION

I CAFTA CODE OUTPUT FILES

J TOP EVENT MATRIX ANALYSIS CODE (TEMAC) OUTPUT FILES

K INDEPENDENT REVIEW COMMENTS

VOLUME I

LIST OF TABLES

1-1	A Comparison Between Fault Tree Analysis and Current Safety Analysis Techniques
2-1	MPPS Performance Summary
2-2	Recommendations Based on Probabilistic Risk Assessment
2-3	Sources of Risk Excluded From PRA Investigation
2-4	Summary of Previous SSMP Risk-Related Studies
2-5	Summary of PRA Scope
2-6	Summary of Risk Sources Excluded from MPS PRA
3-1	Summary of Failure Rate Data Sources
3-2	Summary of Minimum Success Parameters and Criteria
4-1	Sensitivity Analysis Summary
4-2a	Summary of Highest Ranking Basic Event Importance Values Using Fussell-Vesely Measures
4-2b	Summary of Highest Ranking Basic Event Importance Values Using Structural Measures
5-1	Salient Differences and Points of Asymmetry Between LO2 and LH2 Propellant Systems
6-1a	Event Tree Quantification Using Fault Tree Cutsets for Explosion, Overpressurization and Other Non-Recoverable Events
6-1b	Event Tree Quantification Using Fault Tree Cutsets for Recoverable Events
6-2	Definition of Consequence Categories and Specific Consequences
6-3	Consequence Data Summary
6-4a	Aggregate Probabilities and Risk (Loss of Human Life)
6-4b	Aggregate Probabilities and Risk (Loss of Hardware)

VOLUME II

LIST OF TABLES

A-1	Acronyms and Initialisms
A-2	Nomenclature
A-3	Glossary of Aerospace Terms
A-4	Glossary of Statistics and Probability Terms
B-1	Basic Event Mnemonics
B-2	Explanation and Location (Page in Fault Tree) of Basic Events
C-1	Basis for Hardware Failure Rates
C-2	Human Failure Rate Data Summary
C-3	Major Assumptions Regarding Human Error Probability Data
C-4	Basis for Initiating Events, Undeveloped Events, and Conditional Probabilities
C-5	Time-Phased Input Probability Data
C-6	Summary Data for Propellant Leakage and Rupture Terms
C-7	Summary Data for Helium Leakage and Rupture Terms

VOLUME III

LIST OF TABLES

F-1 Ground Rules, Definitions and Assumptions Regarding Consequence Determination

F-2 MPS Propellant System Load Operations

F-3 Summary of Ground Operator Actions Which Could Result in a Catastrophic Accident

G-1 Impact of Leaks and Ruptures During Launch

H-1a Cross Reference Between the SSME FMEA (Ref. 9) and the MPPS Fault Tree

H-1b Index of SSME FMEA (Ref. 9) Items Not Cross-Referenced to the MPPS Fault Tree

H-2a Cross Reference Between the Orbiter FMEA (Ref. 18 and 30) and the MPPS Fault Tree

H-2b Index of Orbiter FMEA (Ref. 18 and 30) Items Not Cross-Referenced to the MPPS Fault Tree

H-3a Cross Reference Between the External Tank Hazard Catalog (Ref. 10) and the MPPS Fault Tree

H-3b Index of External Tank Hazard Catalog (Ref. 10) Items Not Cross-Referenced to the MPPS Fault Tree

H-4a Cross Reference Between the SSME Detail Design Hazard Analysis (Ref. 11) and the MPPS Fault Tree

H-4b Index of SSME Detail Design Hazard Analysis (Ref. 11) Hazards Not Cross-Referenced to the MPPS Fault Tree

H-5a Cross Reference Between the Lightweight External Tank (Propulsion/Mechanical Subsystem) FMEA (Ref. 8) Items and the MPPS Fault Tree

H-5b Index of Lightweight External Tank (Propulsion/Mechanical Subsystem) FMEA (Ref. 8) Items Not Cross-Referenced to the MPPS Fault Tree

H-5c Cross Reference Between the Lightweight External Tank (Propulsion/Mechanical Subsystem Part Level) FMEA (Ref. 8) Items and the MPPS Fault Tree

H-5d Index of Lightweight External Tank (Propulsion/Mechanical Subsystem Part Level) FMEA (Ref. 8) Items Not Cross-Referenced to the MPPS Fault Tree

H-5e Cross Reference Between the Lightweight External Tank (Electrical Subsystem) FMEA (Ref. 8) Items and the MPPS Fault Tree

H-5f Index of Lightweight External Tank (Electrical Subsystem) FMEA (Ref. 8) Items Not Cross-Referenced to the MPPS Fault Tree

H-5g Cross Reference Between the Lightweight External Tank (Electrical Subsystem Part Level) FMEA (Ref. 8) Items and the MPPS Fault Tree

H-5h Index of Lightweight External Tank (Electrical Subsystem Part Level) FMEA (Ref. 8) Items Not Cross-Referenced to the MPPS Fault Tree

H-5i Cross Reference Between the Lightweight External Tank (Aerodynamically Sensitive Items) FMEA (Ref. 8) and the MPPS Fault Tree

I-1 CAFTA Code Capabilities and Limitations (Ref. 28)

I-2 Cutsets

I-3 Importance Measures

I-4 Structural Importance

J-1 TEMAC Output File: Exponential Distribution (Using Table C-5 Failure Data)

J-2 TEMAC Output File: Exponential Distribution with Ignition Source Probability Set to Zero (Using Table C-5 Failure Data)

J-3 TEMAC Output File: Exponential Distribution with Lognormal Distribution for Weld and Seal Failures (Using Table C-5 Failure Data)

K-1 Response to Lawrence Livermore National Laboratory Review Comments

VOLUME I

LIST OF FIGURES

2-1 Time-Phased Risk Profile

2-2 Top Level Fault Tree

3-1 Main Propulsion Pressurization System PRA Flow

3-2 Fault Tree Symbology and Terminology

3-3 Fault Tree

3-4 LH2/LO2 Valve Schematic

5-1a LO2 Propellant Delivery System (During Fill Operations)

5-1b LO2 Propellant Delivery System (During Flight)

5-2a LH2 Propellant Delivery System (During Fill Operations)

5-2b LH2 Propellant Delivery System (During Flight)

5-3a LO2 Tank Pressurization Schematic

5-3b LH2 Tank Pressurization Schematic

5-4 Simplified Helium System Schematic

5-5 Pogo Suppression System Schematic

5-6 Simplified Functional Block Diagram of MPPS Electrical Control System

5-7 SSME Controller Simplified Redundency Diagram

6-1a Mission Time Sequence Event Tree (Explosion, Overpressurization, and Non-Recoverable Events)

6-1b Mission Time Sequence Event Tree (Recoverable Events-Functional Failures)

VOLUME II

LIST OF FIGURES

D-1 Fault Tree Symbology and Terminology

D-2 MPPS Expanded Fault Tree

ACKNOLEDGEMENTS

This probabilistic risk assessment was performed by Lockheed Corporation. The main effort was conducted at Lockheed Missiles and Space Company (LMSC), Palo Alto Research and Development Division, and at Lockheed Engineering and Management Services Company (LEMSCO), Houston, Texas. The study was jointly directed by Mr. H. Ed Smith (LEMSCO), Program Manager and Dr. Joan K. Plastiras (LMSC), Analysis Manager.

Responsible engineers and technical support personnel are as follows:

Analysis	Dr. J. K. Plastiras	(LMSC)
	A. V. Rubin	(LMSC)
	S. Patterson	(LMSC)
Systems Engineering	G. Henning	(LEMSCO)
	G. Brown	(LEMSCO)
	D. Feuerstein	(LEMSCO)
	T. Hall	(LEMSCO)
	M. Landeck	(LEMSCO)
Computer Utilization	Dr. D.Hackler	(LEMSCO)
	J. E. Cabaniss	(LMSC)
	D. N. Quintal	(LMSC)
	L. Scharp	(LMSC)
Quality Assurance	R. Robbins	(LEMSCO)

Special thanks go to consultants and technical contributors, Mr. Hagaii Cohen, Mr. Mark Dezendorf, Mr. Guy Thibodaux, Dr. Ron Iman, Dr. Howard Lambert, and Dr. Lee Stewart. Lockheed also appreciates the independent review conducted by Garth Cummings, Jim Wells and Gary Johnson of Lawrence Livermore National Laboratory.

ABSTRACT

A number of safety studies, failure modes and effects analysis (FMEA's) and hazards analysis have been performed for the space shuttle main propulsion pressurization system (MPPS). The method of analysis in each of these evaluations has been deterministic: one in which a source of hazard is identified, the impact is determined and appropriate control measures are applied. These studies are exhaustive and comprehensive in identifying the credible modes and mechanisms of individual component failures and in assessing the impact of these failures on the system. The studies, however, do not account for the effects of multiple failures occuring simultaneously, nor do they quantify the likelihood of such failures. This study attempts to quantify the likelihood of a catastrophic accident by utilizing Probabilistic Risk Assessment (PRA) techniques. The results of this study identify that the major contributors to catastrophic failure of the MPPS are associated with hardware leakage and rupture which result in explosion or aft compartment overpressurization. Breach of pressure boundary is the direct result of random seal/weld/joint leakage and loss of component structural integrity.

Section 1

INTRODUCTION

In January 1987, the National Research Council Risk Oversight Panel recommended that NASA perform a Probabilistic Risk Assessment (PRA) of several Space Shuttle systems. In response to the recommendation, the NASA National Space Transportation System Program Office requested that Lockheed Engineering and Management Services Co. (LEMSCO) perform a PRA on the Shuttle Main Propulsion Pressurization System (MPPS). The intent of this effort was to determine if any areas of concern not previously identified by the FMEA/HA were uncovered and to evaluate the usefulness of PRA methodology. This effort parallels a similar task currently being peformed by McDonell Douglas on the Auxiliary Power Unit (APU) which supports hydraulic power generation for the Shuttle Main Engine and the Flight Control System.

Under the direction of LEMSCO, Lockheed Missiles & Space Company's (LMSC) R&D Division was commissioned to perform a comprehensive evaluation of risk posed by the MPPS during flight and preflight phases. Periodic meetings were held between NASA and LEMSCO/LMSC to further define the scope of analysis and to discuss specific risk issues of interest within the MPPS.

The principal purpose of this study is to quantify in probabilistic terms the risk which the Space Shuttle's MPPS poses to human life and property. PRA is the analysis technique used for this purpose. A description of the historical use of PRA as an analytical tool and a definition of MPPS boundaries considered within the scope of analysis are provided in the following paragraphs.

1.1 USE OF PRA

PRA is a method of quantifying the probabilities of potential accidents and their consequences. PRA employs fault tree analysis (FTA) to develop and evaluate a system model as well as to analyze consequences and their associated risks. PRA has been used as a technique to formally address these risks at nuclear power plants since the Reactor Safety Study, WASH-1400, was performed in 1975. Prior to WASH-1400, the Boeing Corporation applied PRA to an evaluation of the Minuteman missile. The aerospace industry initially viewed PRA as too expensive and subsequently replaced it with non-probabilistic (i.e. deterministic) methods such as Failure Modes and Effects Analyses (FMEAs) and hazards analyses (HAs). These were the tools NASA had used to date in their analyses of the risk posed by Space Shuttle systems.

Since WASH-1400, PRA has been applied to many other industries such as chemical, petrochemical and defense, but not to the same extent as in the nuclear industry. Consequently, the methods of analysis and the computer codes used to solve the numerical computations for this study were adopted from the nuclear industry where the PRA technique is most mature.

PRA is recognized in the nuclear industry as the best available tool for quantifying the frequency and severity of serious accidents. PRA provides information to support a concerted effort to identify corrective (or preventive) actions with the greatest potential to reduce overall risk. Nonetheless, PRA is not a stand-alone analysis for the evaluation of risk; a well-executed PRA is based on FMEAs, hazard analyses, and other standard design activities.

Since data are often incomplete, PRA does have certain limitations which may be summarized as follows:

- o PRA may not identify all events that could start or direct the course of an accident. In addition, there is no test of model completeness (i.e. important accident scenarios could be unintentionally omitted by the analysist).
- o Sufficient and reliable data may not be available to model and quantify the behaviors of system and accident processes.
- o The fault tree analysis tool utilized in PRA may be simplistic in its representation of system level behavior.

These limitations do not, however, diminish the need for a probability-based assessment of risk. PRA is a systematic approach to evaluating risk given the information and understanding available at the time that the analysis is performed. In effect, PRA is an attempt to determine: What can go wrong? How likely is it to happen? If it happens, what are the consequences?

1.2 COMPARISON OF PRA WITH OTHER METHODOLOGIES

Qualitative techniques such as FMEA have been widely used in the aerospace industry as a means to identify and control sources of risk. The FMEA is essentially a bottoms-up approach; each component or subcomponent is analyzed for its failure modes, causes of its failure and the effects of its failure on the system to which it belongs. For example, in the case of the O-rings in the Challenger accident, the effects of a leak were correctly identified as resulting in "high-temperature gas flow burn-through and case burst; catastrophic failure of SRM (solid rocket motor); mission loss; vehicle loss and personnel loss". Nevertheless, in the case of Challenger, a decision was made to launch despite the existence of this and hundreds of other identified single point failures.

FMEAs and other hazards analyses are also limited in that they consider occurrence of only one failure at a time. The logical connection between events and systems is not apparent from the FMEA documentation. In many situations, subtle interactions between various systems or between man and machine are missed in the consideration of individual component failures in the FMEA approach. (See Table 1-1 for a comparison of the advantages and disadvantages of FMEAs and FTAs.) Combinations of events that can lead to failure may have a greater probability of occurrence than single failures; yet the FMEA is not designed to address combinations of failure.

By contrast, the FTA is a top-down approach: a top level event is first identified, such as "failure of the MPPS which results in loss of life and/or vehicle". Then the possible failure combinations causing this event are developed. For each event, contributory events or chains of events are successively developed, until arriving at the basic events, which are usually single component failures or human errors. By this method a downward branching fault tree is formed. Figure 2-2 consists of the top branches of the fault tree generated for this report. Using Boolean "and" "or" logic, the total probabilities of various failures are calculated and their relative contributions to the total risk are assessed. Refer to Figure 3-2 for definitions of symbols.

1.3 ORGANIZATION OF THE REPORT

This report is divided into a main report (Volume I) and Appendices A through K which are contained in Volumes II and III. This report is divided

into a main report (Volume I) and Appendices A through K which are contained in Volumes II and III. Volume I contains the methods by which the analysis was performed, the data sources used for probabilistic quantification , and descriptions of the systems and events included in the reliability model.

The executive summary, Section 2.0, discusses the major conclusions and recommendations resulting from this PRA. Methodology and computational techniques are presented in Section 3.0. Quantitative evaluation of reliability is performed in Section 4. A brief description of in-scope systems and hardware is presented in Section 5. Risk and consequence analysis is summarized in Section 6.

Appendices contain all the supporting documentation and computation for the technical evaluation. A brief description of the Appendices is provided below:

Appendix A: A description of abbreviations, acronymns, initialisms and terms used throughout the report.

Appendix B: A description of fault tree basic events and the shortened descriptors (mnemonics), along with a cross reference of pages where each basic event appears in the tree.

Appendix C: Tabulated failure rates, exposure times and other supporting data used to calculate basic event probabilities.

Appendix D: Detailed fault tree showing all branches expanded. A description of each of the branches along with rationale for the fault tree structure is provided.

Appendix E: Details and outline drawings for major system components. These drawings supplement system descriptions.

Appendix F: A discussion of fire and explosion caused by leakage and contamination. General discussion to illustrate mechanisms by which leakage and contamination can cause catastrophic failures.

Appendix G: Ground operations and tasks which are required during ground fill and flight preparation.

Appendix H: Fault tree consistency evaluation to cross index FMEA sequences with appropriate portions of the PRA model. This index is a comprehensive review of all FMEA's which are related to the main propulsion system.

Appendix I: CAFTA code files used to analyze and quantify risk are attached to a brief synopsis of the program's capabilities.

Appendix J: Codes used to test statistical sensitivity using Latin Hypercube techniques and TEMAC software.

Appendix K: Comments resulting from Lawrence Livermore National Laboratory's independent review of this report are addressed and the impact of the comments on the report are discussed.

Each of the tables and figures in the Appendices are supplemented by accompanying text and descriptions of their use within the main report.

TABLE 1-1
A COMPARISON BETWEEN FAULT TREE ANALYSIS AND CURRENT SAFETY ANALYSIS TECHNIQUES

	FAULT TREE ANALYSIS	CURRENT METHOD (FMEA/HAZARDS ANALYSIS)
ADVANTAGES	• DEDUCTIVE • ACCOMODATES FAILURE COMBINATIONS/INTERACTIONS • PRIORITIZES THE PROBABILISTIC IMPORTANCE FAILURES • SYSTEM ORIENTED	• EASILY UNDERSTOOD (INDUCTIVE) • SYSTEMATIC • COMPONENT ORIENTED
DISADVANTAGES	• UNIQUE PERSONNEL TALENTS • TIME INTENSIVE	• ROUTINE APPLICATION MISSES SUBTLETIES • MAY OMIT - HUMAN ERRORS - SECONDARY FAILURE EFFECTS - COMMON CAUSE FAILURES • TRADITIONALLY LIMITED TO SINGLE FAILURES • OBSCURES DEPENDENCIES

Section 2

EXECUTIVE SUMMARY

In post-Challenger discussions with Congressional Committees and the National Research Council Risk Management Oversight panel, criticism was levied against NASA because of the inability to prioritize the 1300+ single point failures. In the absence of a ranking it was difficult to determine where special effort was needed in failure evaluation, in design improvement, in management review of problems, and in flight readiness reviews. The belief was that the management system was overwhelmed by the quantity of critical hardware items that were on the Critical Items List and that insufficient attention was paid to the items that required it.

Congressional staff members from Congressman Markey's committee who have oversight responsibilities in the nuclear industry, and specifically over the nuclear power supplies for NASA's Galileo and Ulysses missions, felt very strongly that the addition of PRA to the existing Failure Mode Effects Analysis/Hazard Analysis (FMEA/HA) methods was exceedingly important. They indicated that the PRA approach had matured to the extent that it could handle very small failure rate data bases, such as that maintained by NASA. NASA responded with arguments that the FMEA/HA had illuminated all significant failure modes satisfactorily and that no failure rate data base was available.

A compromise position to evaluate PRA application to two pilot systems, MPPS and Auxiliary Power Unit (APU), was suggested. The plan was to do a PRA on these two sub-systems to:

1. Identify areas of concern not previously identified by the FMEA/HA process.

2. Evaluate the usefulness of the PRA methodolgy.

The plan was put into effect and has resulted in the Lockheed PRA effort on the MPPS. With regard to item #1 above, no new failures or combinations of failures were identified by the PRA process. This result is not unexpected if one considers that the MPPS is a mature system, has flown repeatedly after a thorough design, development, test, and evaluation and has passed through a thorough qualification and certification program - all of which effectively detect design, manufacturing, and inspection weaknesses. In addition, the FMEA on the MPPS elements is equally mature, as it has been scrutinized by numerous contractors and issued twice.

The selection of the MPPS was perhaps not the best for illustrative purposes, since it contains numerous single failure points (SFPs). The dominant risk contributors, therefore, are associated with the individual SFP's, rather than with the combinations of failures which the PRA highlights so effectively.

With respect to item #2 above, the usefulness of using PRA on a shuttle sub-system is effectively demonstrated. The fault tree itself provides managers with a logical, top-down perspective of the entire system during all mission phases. The quantification of the various events on the tree, based on the best generic failure rate data available (in the absence of shuttle-specific failure rate data), combined with a Monte Carlo treatment of uncertainty, yield a

probability range for the loss of life and/or vehicle due to failures originating in the MPPS. The PRA process serves as an excellent cross-check against the FMEA's, building upon the knowledge of component failure modes, causes and system effects. The determination of a ranked listing of failure contributors provides guidance to NASA management as to where attention must be focused to reduce risk. This ranking is seen as a useful tool in a variety of areas involving the following program decisions:

a) Design
b) Failure analysis
c) Selections of improvement changes
d) Design review decisions by management
e) Readiness reviews
f) Waivers
g) Spares provisioning plans
h) Material review board
i) Procurement controls
j) Inspection planning
k) Establishment of critical process controls
l) Designing test programs
m) Execution of cost benefit analysis

Some specific benefits of PRA which result from the Lockheed application of PRA to the MPPS include:

1. General failure categories in the top branch of the fault tree are highlighted, thereby providing better system insights to NASA management.

2. Inter-system dependencies and interactions such as this are typically omitted from NASA FMEAs. An example is the hydraulic system which is out of scope. The PRA quantifies the extent to which the pneumatic system is challenged by a failure in the hydraulic system.

3. The fault tree graphically displays the limits of the analysis; for example, contamination and ice plugging are not treated quantitatively (because of a lack of data), but do appear on the fault tree to highlight areas of future investigations.

4. The fault tree treats combinations of failures such as a two-out-of-four criterion for the hydrogen and oxygen depletion sensors and a two-out-of-three criterion for the flow control valves. Common cause or mode failures such as these are treated incompletely or not at all in NASA FMEAs.

5. The fault tree incorporates mission phasing by considering the multiple consequences of failures for various mission phases; for example, incorporation of different engine requirements for intact abort scenarios allows for an assessment of system reliability over the entire mission. In contrast, the NASA FMEAs typically provide only the worst case effect of a component failure on the system rather than a more realistic assessment of consequence sensitive to system modes and configurations.

6. The fault tree offers a terse presentation of the paths which lead to the top event catastrophy "loss of life and/or vehicle due to failures in the MPPS". The only sequences which appear are those which lead to failure, and these are contained in slightly more than 150 pages. In contrast, the NSAS FMEAs contain many more pages, as they include items which do not either by themselves, or in combination, lead to loss of life and/or vehicle.

In conclusion, PRA, coupled with sensitivity analyses, provides a ranking system with which to assess NASA systems throughout their life. It is important to apply PRA early in system life, when changes can be effected at minimal cost. It is also important to develop a failure rate data base on program hardware to enhance the realism and credibility of the PRA.

It is therefore recommended that PRAs be utilized at the beginning of new NASA programs, and that selected high energy systems on space shuttle, where catastrophic failures can be generated, be considered for a retro-active application of PRA.

2.1 SIGNIFICANT FINDINGS

Table 2-1 shows a compositional breakdown of events leading to loss of life and/or vehicle. The events have been grouped into the following general categories:

1. Explosion/compartment over-pressurization,
2. Valve-related failures,
3. Turbopump failures,
4. Loss of Pogo suppression system,
5. Loss of propellant system screens, and
6. Miscellaneous.

These classifications were based on the top level fault tree model for the MPPS presented in Figure 2-2. Details regarding the development of lower branches in the tree are provided in Section 3.

2.1.1 Risk Contributors

1. Catastrophic Explosions and Overpressurization Events

The single largest category of catastrophic failures is that associated with the random breach of mechanical system pressure boundary. This includes release of material through either the propellant piping/components or the helium (He) pneumatic system. At the individual component level the failures in the High Pressure Oxidizer Turbopump (HPOT) heat exchangers and turbopumps are major contributors. Collectively, however, the numerous other weld joints, seals, fittings and mechanical connections (through which gross leakage could occur) are the most significant factor.

The mechanism for these catastrophic failures varies depending on the type of material released. For helium system depressurization, the primary effect is compartment overpressurization. Helium is an inert gas incapable of ignition. The impact of gross leakage or component rupture on the Space Transportation System (STS) is, therefore, mainly one of structural damage to the orbiter (if vent panels in the aft compartment cannot compensate for the overpressurization).

The accident consequence of breaching the propellant system piping and components is immediate explosion. Most of these leaks occur within the orbiter aft compartment resulting in either an immediate explosion or overpressurization of the compartment. Immediate explosion would be the result of cryogenic fluid contacting elevated temperature sources. Overpressurization is the primary accident consequence when immediate ignition sources are not present in the vicinity of leakage (e.g. gaseous oxygen pressurization line). That is, gradual or rapid depressurization leads to structural damage of the aft compartment if pressure relief is not achieved.

2. Valve Related Functional Failures

The most important valve-related failures are those which constitute single point failures. Functionally redundant valves which operate independently of each other (through separate control signals, power supplies, pneumatic supply etc.) contribute minimally to overall risk.

The bleed valve and anti-flood valves contribute significantly to the top event occurrence within this category of failures. In the helium system, flow regulators comprise the most important functional failures. Other system valves such as external tank pressurization flow control valves and External Tank (ET)/orbiter disconnect valve failure are minor contributors to risk.

3. Turbopump

Turbopump failures associated with the MPPS are primarily caused by leakage through mechanical seals.

4. Loss of Pogo Suppression System

The valves, piping, and accumulators which comprise the POGO suppression system account for less than one percent of the total failure probability. Failure to regulate low frequency oscillations is assumed to cause structural damage to the STS and/or loss of life.

5. Loss of Propellant System Screens

Break-apart or tearing of propellant screens (located downstream of engine pre-valves) is assumed to cause pump binding. Fragments of the screen will destroy the turbopump on impact. The likelihood of these single point failures collectively amount to less than one half of one percent of the total failure probability.

6. Miscellaneous

Remaining events contribute negligibly to overall risk. This category consists primarily of spurious actuation of control circuits and other in-scope portions of the electrical instrumentation and controls.

2.2 RECOMMENDATIONS

The key to minimizing the likelihood of catastrophic accidents is controlling ignitable leaks and sources of compartment overpressurization. Breach of pressure boundary, whether the result of random failure or human error, are expected to account for more than four fifths of the total risk. In comparison, failures strictly related to the functional performance of the engine (i.e., safe engine shutdown capability) constitute a small fraction of a percent of all events leading to catastrophic accidents.

These percentages represent preliminary findings based on issues addressed as part of the scope of this analysis. Other risk sources associated with the MPPS were not included in the analysis and require further investigation. A partial list of risk sources not addressed or probabilistically quantified in this study is contained in Section 2.6.

Addition of functional redundancy will not, in general, significantly reduce overall risk because additional piping and components containing propellant, hydraulic oil or high pressure helium will contribute more sources of fire and explosion. It is therefore recommended that efforts be directed towards controlling direct sources of explosion or those leakage and rupture events which lead to an explosion. Table 2-2 contains recommendations based on the PRA. Additional areas requiring further investigation are itemized in Table 2-3.

2.2.1 Prevention of Explosion and Overpressurization Scenarios

Explosion and overpressurization events were quantified based on generic data for component ruptures, seal failures and other leakage terms. The data is based on reported failures for environments and applications similar to that of the STS. However, leakage on the STS may have a lower frequency of occurrence than that reported in the data book due to the increased level of inspection of hardware. Similarly, early detection of the leak may preclude catastrophic explosions under certain scenarios. A brief discussion is provided below.

Inspections Between Flights

A comprehensive investigation of the accuracy and consistency of nondestructive testing (NDT) is recommended. The investigation should include 1) a review of human reliability in performing the tests and detecting potential flaws and 2) a statistical assessment of the accuracy of the test performed in actually detecting potential flaws.

The test types presently being utilized between flights involve:

- Ultrasonic extensiometer
- Ultrasonic leak
- Optical leak
- Laser interferometry
- Differential radiometry
- Holographic leak
- Resistivity monitoring
- Halogen leak
- Flow leak
- Mass spectroscopy
- Thermal leak

- Torquing
- Leak fluid
- Pressure decay
- Isotope thermometry
- Isotope tracers
- Borescoping
- Exoelectron emission
- Positron annihilation
- Electric current injection
- Eddie current
- Continuity checking
- X-ray radiography
- Polarometry
- Hygrometer
- Optical Pyrometry

Other specialized flow detection methods may also be included.

Leak Detection

Sophisticated detection of potential thermal shock conditions or early leak sensing prior to SRB ignition is critical to accident prevention. Following SRB ignition, efforts should be focused on in-flight leakage and high pressure turbopump cavitation prevention. In the PRA, high pressure turbopump cavitation is assumed to result in pump explosion.

Pump cavitation detection must be responsive to the relatively short time between transient initiation and pump explosion. Currently existing parametric sensing such as pump suction pressure drop, excess vibration of the pump body, pressure fluctuations throughout the propellant system and ullage pressure may represent only a small number of detection schemes.

2.2.2 Failure Rate Data Base Development

The computed top event probability depends on basic event failure rates. Failure rate information for the STS hardware was found to be fragmentary and incomplete. This required that generic data be used to supplement STS specific failure data.

It is strongly recommended that a failure data collection system be established to facilitate future PRA and re-design activities. The main components of this consolidated data base should include (as a minimum) the following information:

- Hardware name/description (e.g. unique identifier)
- Hardware type (i.e., pneumatically actuated hydraulic valve, turbopump, etc.)
- Failure history (i.e., time of failure, number of test hours/cycles, time between failures, repair time)
- Each test must be described in sufficient detail so that its significance for the estimation of the probability of failure under operational conditions can be determined

- o Reason for any testing that is not part of the preplanned test program
- o Failure mode description/root cause evaluation
- o Hardware duty cycle and operating modes

Any STS failure rate data which can be compiled can be used to update earlier estimates of performance based on generic data. It is important to note, however, that the observed failures may constitute a statistically small sample for analytical purposes. Caution should be taken to establish the confidence interval when few failures are recorded or when few operating hours without failure have been observed. Also, test data must be treated differently from actual operating data.

The manpower required to implement this failure rate data base will be dependent on initial setup efforts. Most of the cost will be incurred during data base development and installation. Once in place, reporting and record updating should average 2-4 hours per failure incident plus periodic updates to record the operating log time for those components which have not experienced a failure. Such updates primarily involve data transcription and require significantly less than one hour of effort per component. Data transfer option from contractor maintenance or maintainability data bases should be investigated.

2.2.3 Improvement of Documentation System

It was the concensus among persons contributing to this study that NASA's documentation system (for technical analyses, drawings and reports regarding the MPPS and other systems) requires substantial improvement. This is particularly important in the following areas:

- o Centralization of Technical Data: Collection of the appropriate documents/drawings to perform this study was time intensive. The necessary documentation had to be obtained from a variety of NASA organizations and subcontractors. No central coordination of such documents was found.
- o Document Control: A number of factual inconsistencies were identified in and between the various documents utilized in this study. The proper control of governing documents is essential to the accuracy of the PRA results.
- o Quality of Documents: In a number of instances, particularly those relating to ground operation, the reproduction quality was extremely poor. Better copies were often unavailable or non-existent within NASA's documentation system.

Future PRA and other safety studies can be more effectively and efficiently performed with the improved availability and quality of technical documents.

2.3 STUDY LIMITATIONS

The fault tree model represents failures which, in themselves, or in combination with other events, result in occurrence of the top event. Initially, the fault tree top event is calculated based on point (single value) estimates for basic event probabilities. The probabilities are based on the point estimate of a statistically significant sample of recorded failures. Each population of failed components has an associated distribution. This information is lost, however, when only the point estimate is used.

Several methods are available to incorporate uncertainties about basic event probabilities into a calculation of the top event probability. This can be accomplished by Synthetic sampling, a variant of which is used in this analysis. A less sophisticated but simpler alternate method used to determine top event variance is by evaluating sensitivity. Sensitivity is tested by varying specific basic event probabilities while maintaining others constant. In this manner, a range of top event probabilities can be generated, thus bracketing "worst" and "best" case conditions. Information regarding Synthetic sampling and other sensitivity techniques is provided in Section 3.

The generic failure data is based on field experience with a population of well-maintained components and systems assumed to be in the useful midlife performance range. The degraded reliability of parts due to wear-out, limited life, or fatigue is not a part of the analysis because aerospace parts are assumed to be properly inspected, tested, and maintained prior to launch. Furthermore, the failure data from which the probabilities were derived are based on experience with aerospace missile and satellite components. Information regarding equipment duty cycle, modes of operation and environmental stresses provides at most a "best estimate" of expected hardware performance on the STS. Much of the uncertainty arises due to the translation of "per-hour" failure rate data (much of which is expressed in failures per millions hours of operation) into a "per demand" or cyclic failure rate. This is a particularly difficult problem in the derivation of failure probability values for equipment required to operate in different modes during the various launch phases.

Latent failures are considered out of scope. Although latent failure rates are generally insignificant compared with post launch failure rates, the cumulative latent period for the total of all components under evaluation will add to overall risk. In addition, ice plugging and contamination are excluded from the PRA as out of scope because data were unavailable.

2.4 COMPARISON OF MPPS PRA TO EARLIER STUDIES AND TESTS

The value of a PRA depends heavily on the understanding of accident sequences, and their subsequent quantification. A review of previous analytical evaluations was crucial to both model development and quantification. A brief description of some of the documents examined during the course of this study is included below.

A number of previous safety and functional studies have been performed by NASA contractors to assess the potential risks associated with the MPPS. A few of these studies used in this PRA are provided in Table 2-4. These studies provide only a deterministic or qualitative assessment of potential risks. No probabilities have been assigned to the postulated accident sequences.

The MPPS FMEAs (Refs. 8, 9, 18 and 30), were the most important guides to understanding component failure modes, causes and system effects. This information was also valuable in identifying certain failures which may be induced by human errors in the man-machine interfaces. The FMEA's are particularly useful to PRA in that they can be used to verify the accident sequences generated in the risk model.

A comprehensive review of FMEA single point failures was performed to ensure that the safety-related FMEA items were properly included in the risk model; the resulting consistency check is documented in Appendix H. A description and cross index between the FMEA single point failures and fault tree basic events are provided to facilitate this cross check. More discussion on details regarding the risk model are provided in Section 4.

2.5 SUMMARY OF ANALYTICAL APPROACH

The analysis is based on a deductive logic procedure called fault-tree analysis. A fault tree is a graphical representation of all conceivable accident sequences which can lead to a system level catastrophy. The fault tree model consists of hardware failure, human error and environmental contributors to the system level catastrophy.

In risk analysis, the top event is typically a system-level accident such as "loss of life and/or vehicle". The undesirable top event is successively reduced to a combination of lesser failures represented in the lower branches. The lowest events depicted in a fault tree are represented by rectangles, circles, and diamonds. The diamond is used to indicate an event which could be further reduced but which is not, to simplify the depicted fault tree structure. The individual failures which are not further reduced (basic events) are represented by circles. The rectangle is used to indicate an intermediate event to be further reduced to basic events. The triangle is used to indicate a continuation of the fault tree. Figure 3-2 contains a depiction of fault tree symbols and terminology.

Boolean algebra is used to depict the relationships amongst the failures. The "and" gate indicates the events necessary to produce the next higher event in the tree. The "or" gate indicates all events such that any one of which is sufficient to produce the next higher event.

In addition to the calculation of top-event probabilities, cutsets are generated. A cutset is a collection of basic events sufficient to cause the occurence of the top event. A minimal cutset has the property that no proper subset of it is also a cutset. The collection of minimal cutsets provides qualitative information about the vulnerability of the system. In the absence of failure data it can be said that the vulnerability of a system increases as the cutset size decreases and the cutset number increases.

The dominant cutsets identified in the FTA are then used to quantify event tree branches. An event tree is a success/failure model defining the possible outcome or consequence states based on sequential or time dependent conditions. This defines the time-phased risk as well as recovery factors (such as abort scenarios) which cannot be easily depicted on a single fault tree model. Details regarding FTA and event tree development are provided in Sections 4 and 6.

2.6 SCOPE OF ANALYSIS

The scope of this PRA includes the MPPS and major portions of associated support systems. The MPPS consists of the ET, aspects of the Space Shuttle Main Engine (SSME), and those components of the Orbiter which connect the ET to the SSME and provide the necessary services for proper MPPS Functioning.

Ground operations commencing at eight hours prior to launch were examined for impact on the launch but not quantified in the analysis. Table 2-3 contains some of the major risks not included in this PRA.

2.6.1 Basis for Inclusion of Events

The MPPS is an integral part of the Main Propulsion System (MPS). It is not, however, a separate and distinct system with strictly defined boundaries and interfaces. Reference to a "system" is merely a convention which recognizes a requirement within the MPS for gaseous pressurants. Thus, the MPPS is defined herein for the specific purpose of performing a PRA. The "system" is comprised of various MPS pressure-related functions with interfaces included for analytical completeness. The study participants recognize that there may be differing definitions of the MPPS, based on historical boundaries and/or contractor responsibilities.

The scope of the MPPS for the purpose of this PRA was based on various analytical, as well as engineering considerations. As a general rule, an element is in scope if its failure directly fails an element of the MPPS or if it is directly failed by an MPPS element. Out of scope elements include component failures outside the MPPS which lead directly to loss of life and/or vehicle and for which subsequent failure of the MPPS is irrelevant. The interconnection of piping and control systems necessitates that subsystems which interface directly with gaseous pressurants be included within scope for this PRA. Interactions between systems and spatial dependency of major components can cause failures in the MPPS which ultimately lead to loss of life and/or STS vehicle. A general itemization of hardware and human activities considered in-scope and out-of-scope is provided in Tables 2-5 and 2-6, respectively.

2.6.2 Specific Scope Boundaries

A number of scenarios involving interfaces with the MPPS must be examined for analytical completeness. Evaluation of failures occurring strictly within the MPPS and affecting only the MPPS hardware address only a small fraction of total risk contributions to the STS.

The general categories of items considered within analytical scope may be summarized as follows:

1. Events affecting MPPS pressurization functions. This category includes all failures which lead to loss of pre-pressurization and re-pressurization functions. Additionally, this category includes any and all events which create insufficient ullage pressure conditions in the external propellant tanks.

2. All portions of the closed process loop containing the MPPS. Interconnections with main engines, orbiter piping and external propellant tanks create a single pressure boundary and flow loop. Loss of pressure boundary or flow through the closed loop necessarily affects MPPS function.

3. Hardware and human actions which directly support MPPS hardware or in-scope hardware defined by 2). This category includes local electrical control signals, pneumatic (helium) system lines and components, and hydraulic lines directly supporting main engine valve hydraulic actuation. Excluded from this category are all controller/general purpose computer failures and all hydraulic supply and servo control failures (including hydraulic control of yaw and pitch functions).

4. Elements contained clearly within the MPPS boundaries. These include flow control valves, HPOT heat exchangers, heat exchanger bypass flow orifices and gaseous oxygen (GO2) and gaseous hydrogen (GH2) pressurization lines and components.

5. Events that challenge the MPPS, requiring a response. For example, MECO requires closures of the prevalves which are in scope. The duty cycle, process conditions and environmental stresses greatly affect the ability of the MPPS to perform its pressurization functions. By evaluating the impact these factors have on the MPPS, one can establish the number of valve actuations, pressure transients or flow restrictions that the MPPS hardware will experience. Those influences are, for the most part, external to the MPPS.

6. Events which define MPPS success criteria. These are primarily functional failures in the main engine which establish whether the MPPS can function under specified conditions. For example, loss of more than two engines, aside from failing to provide proper thrust, may also result in insufficient ullage pressure.

7. Crew or ground control actions which cause or mitigate MPPS failures or failure of hardware defined by 2), 3), and 4). These are exclusively errors of omission or failures to respond when required. Errors of commission which induce a failure are not within the scope of analysis.

8. Miscellaneous hardware included for analytical completeness and to account for symmetry between subsystems. Issues of symmetry arise frequently when comparing the liquid oxygen (LO2) and liquid hydrogen (LH2) propellant systems. The HPOT preburner has an internal heat exchanger which provices a pressurization function within the MPPS. The HPOT preburner, therefore, is in-scope. The High Pressure Fuel Turbopump (HPFT) has no analogous heat exchanger on its preburner, but the HPFT preburner is included within scope for analytical completeness.

TABLE 2-1

MPPS PERFORMANCE SUMMARY

Failure Category	Description of Events	% of Total	Expected Probability of Occurrence (per launch)
Explosion and compartment overpressurization	Explosions or flow diversion due to leakage or rupture of propellant system pressure boundary (including pressurization lines)	39.30%	9.55E-04
	Compartment overpressurization events or loss of pneumatic system due to helium system leakage	44.86%	1.09E-03
	subtotal	**84.16%**	**2.05E-03**
Valve related failures	Bleed valve/anti-flood valve	3.10%	7.54E-05
	Pneumatic system flow regulation	4.44%	1.08E-04
	Disconnect valve, Prevalves	1.84%	4.46E-05
	subtotal	**9.38%**	**2.28E-04**
Loss of filter	Filter rupture or break-apart	0.84%	2.04E-05
Pogo suppression	Pogo suppression system related fatalities/damage	1.56%	3.80E-05
Shutdown and separation failures	Separation related failures	0.81%	1.98E-05
	Shutdown related failures	0.66%	1.60E-05
	subtotal	**3.88%**	**9.42E-05**
Turbopump failures	Turbopump seizure	0.05%	1.15E-06
	Heat Exchanger failures	0.04%	8.79E-07
	Catastrophic turbopump seal failure	0.02%	4.82E-07
	subtotal	**0.10%**	**2.51E-06**
ALL OTHER FAILURES		**2.48%**	**6.03E-05**
	TOTAL	**100.00%**	**2.43E-03**

Table 2-2

Recommendations Based on the Probabilistic Risk Assessment

Risk Source	Recommended Action
Leakage through Seals in Components and Piping	Seal leakage-related failure rates are two orders of magnitude higher than welded connection failure rates. An evaluation of whether welds can be used in lieu of flanged connections (involving O-ring or other seals) should be performed. The trade-off of this modification in that one sacrifices serviceability when connections between components and piping are welded together.
Release of Ignitable Materials into Aft Compartment	Evaluate the addition of an in-flight leak detection system in the aft compartment. The leak detection system can be used as a shutdown parameter input to the engine controller.
Depressurization of Helium Pneumatic System in Aft Compartment	Evaluate the adequacy of the aft compartment vents in relieving overpressurization conditions. Of specific concern are scenarios in which high pressure helium supply system pressure boundary is breached.
Bleed valve/antiflood valve failures	Evaluate options to ensure that these valves assume their proper position during flight. Increased functional testing prior to launch preparation and cryogen detection in bleed line may prevent overpressurization explosion event during engine start, although it is recognized that excessive functional testing may actually degrade reliability.
Pneumatic System Pressure regulator failure	Evaluate options to automatically isolate the regulator from the downstream system upon a high pressure detection via an overboard vent.
All other failures	No action recommended as the failure rates are sufficiently low to contribute negligibly to overall risk.

TABLE 2-3

SOURCES OF RISK EXCLUDED FROM PRA INVESTIGATION

GENERAL

- External events (specifically natural phenomena such as lightening and strong winds).
- Propellant hydrodynamic transients.
- Structural failure of ET under dynamic loadings.
- Spatial interactions between structural components.
- Latent flaws and common cause failures introduced during repair and refurbishment.
- Common cause failures of sensors which occur during flight due to power supplies, control systems and other hardware interactions
- Piping and tubing failure mechanisms.
- End-of-Life, wear-out and fatigue characteristics of major mechanical components.
- Valve sequencing failures.

SPECIFIC

- Turbine blades on high pressure pumps should be examined for potential redesigns to prevent missile generation.
- Yaw and pitch control subsystem's ability to compensate for loss of a single engine.
- Detailed evaluation of controller and engine interface unit internal architecture.
- Thermal shock in piping downstream of SSME prevalves.

TABLE 2-4

Summary of Previous SSMP Risk-Related Studies

Type of Study	Reference (Section 7)	Information Contained in Study
Element Interface Functional Analysis (EIFA)	7	◇ Qualitative analysis of systems and their interfaces. ◇ Examines effects of failure in one system on other related systems. ◇ Also identifies non-redundant failure points and assigns criticality levels (1-3) to items.
FMEA	8 External Tank 9 SSME & Critical Items List 18, 30 Orbiter	◇ Qualitative analysis of failure modes and effects.
Hazard Analysis	10 External Tank 11 SSME design - operational flights 12 LO2 Control System 13 LH2 Control System	◇ Summary of applicable hazards, precautions and remedie in a system. Identifies hazards, controlled and eliminated. Evaluates systems and responses on a deterministic (qualitative) level. ◇ Utilizes limited qualitative fault tree modelling.
Maintenance Study	14 Reusable Rocket Engine 15 SSME Combustion Chamber	◇ Summary of SSME and other liquid rocket motor failure ◇ Recommends controls for reducing failures

TABLE 2-5
SUMMARY OF PRA SCOPE

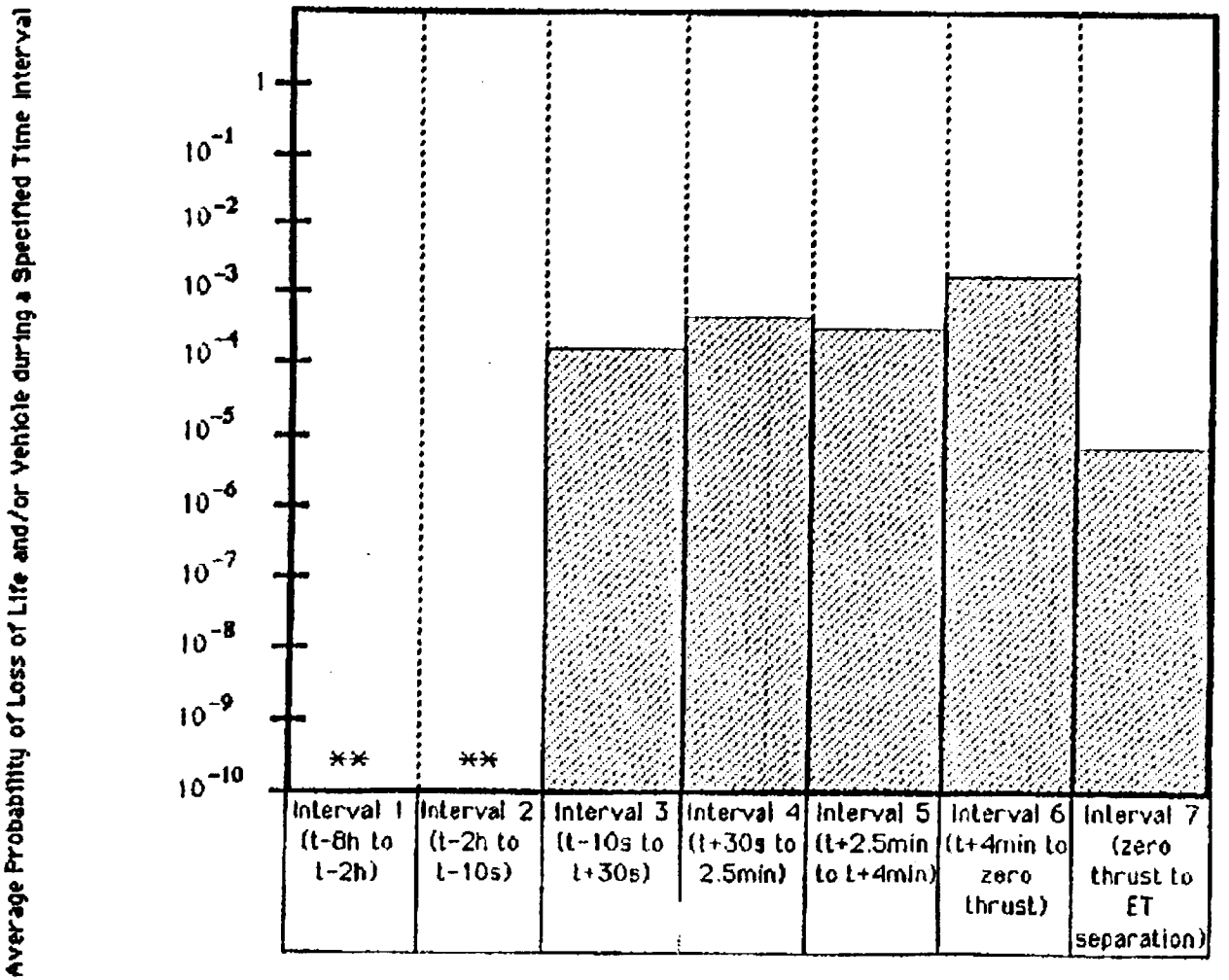
Time Interval:	T-8 hours to MECO/ET separation or intact abort initiation
Risk Sources:	• Hardware Failures • Human Errors
Consequence Categories:	• Loss of Human Life • Loss of Vehicle
Hardware Included:	• Piping, tubing, valves, pumps and other components forming the MPS pressure boundary inside the orbiter and SSME compartments, External Tank and Orbiter Umbilicals. • Support systems - pneumatic subsystem - hydraulic subsystem (select functions) - local control circuitry and ssme controllers (select • ET separation pyrotechnics • MPPS dedicated instrumentation and sensors • Ground support equipment associated with LH2 and LO2 fill and He pre-pressurization operations operations.

TABLE 2-6

SUMMARY OF RISK SOURCES EXCLUDED FROM MPS PRA

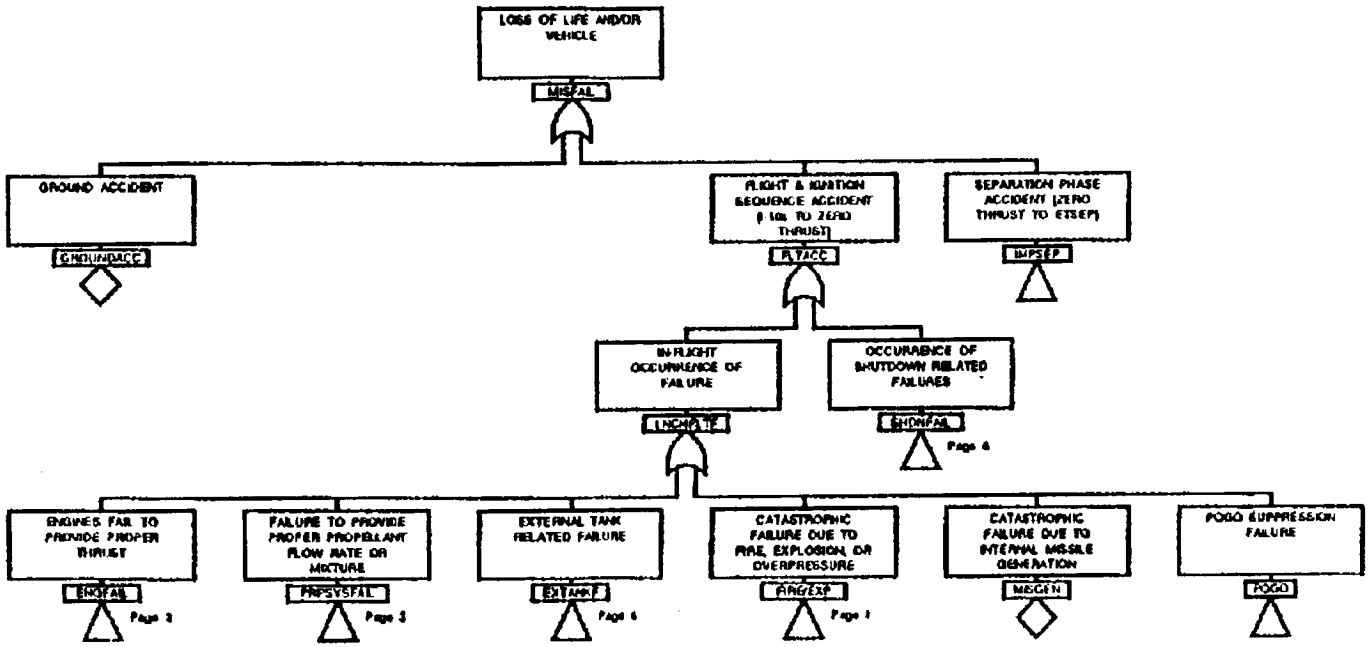
- Solid Rocket Booster (SRB) System and any SRB interfaces to the External Tank
- Structural failures (except for failures of MPS propellant, pneumatic and lines).
- Events external to the STS (natural or other)
- Latent design inadequacy, workmanship, installation or servicing defects introduced prior to T-8 hours
- Sabotage and security violations
- Primary failures outside the MPS which induce secondary failures in MPS
- General Purpose Computer, Main Engine Controller, Engine Interface Unit and Cockpit Display Control Failures
- Software and firmware induced failures
- Electrical power supply and distribution
- Cabling, wiring or connector-related failures.
- Wear-out (e.g., end-of-life failures)
- Delayed accidents (i. e., after orbiter/ET separation) resulting from a failure occuring during the time interval T-8 hours to ET separation.
- Thrust vector adjustment-related failures (e.g. gimbaling, throttle-up, thruster collision, yaw/pitch actuators)
- Cryogenic leakage spraying on adjacent components causing temperature decrease below safe operating limits.

Figure 2-1
Time-Phased Risk Profile
(per launch) *

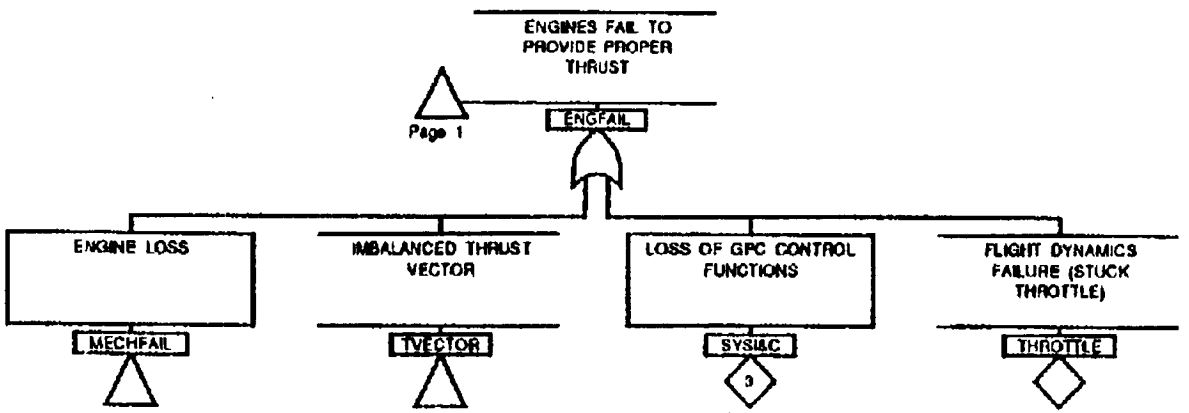


* Based on event tree results in Tables 6-1a and 6-1b.

** Ground accident. Outside scope of analysis.



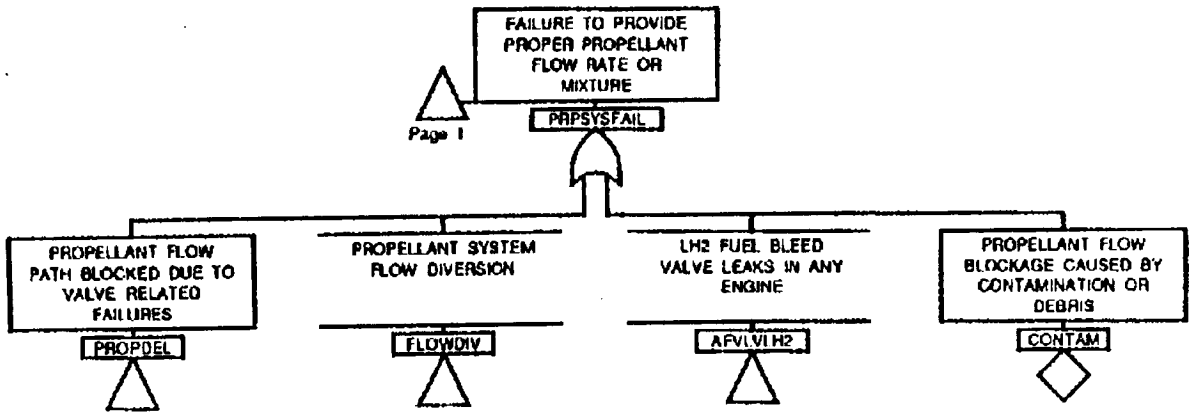
TITLE	
Figure 2-2: Top Level Fault Tree	
DRAWING NUMBER	DATE
Page 1	1/05/88



TITLE

Figure 2-2
Top Level Fault Tree

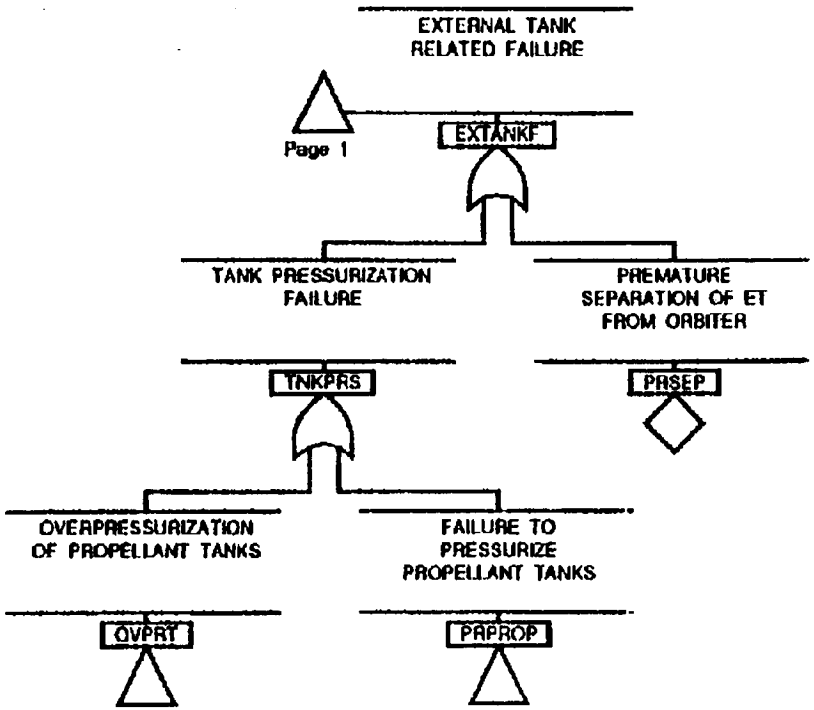
DRAWING NUMBER	DATE
Page 2	9/04/87



TITLE

Figure 2-2
Top Level Fault Tree

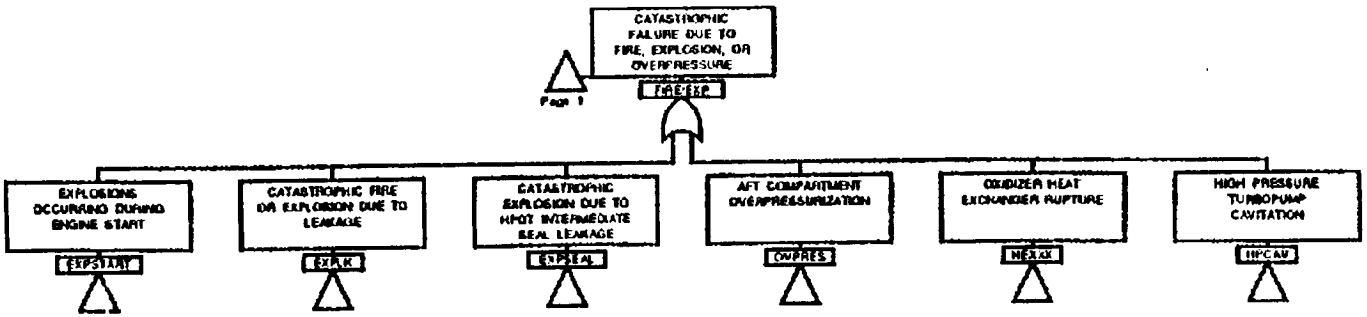
DRAWING NUMBER	DATE
Page 3	9/04/87



TITLE

Figure 2-2: Top Level Fault Tree

DRAWING NUMBER	DATE
Page 4	1/05/88



TITLE

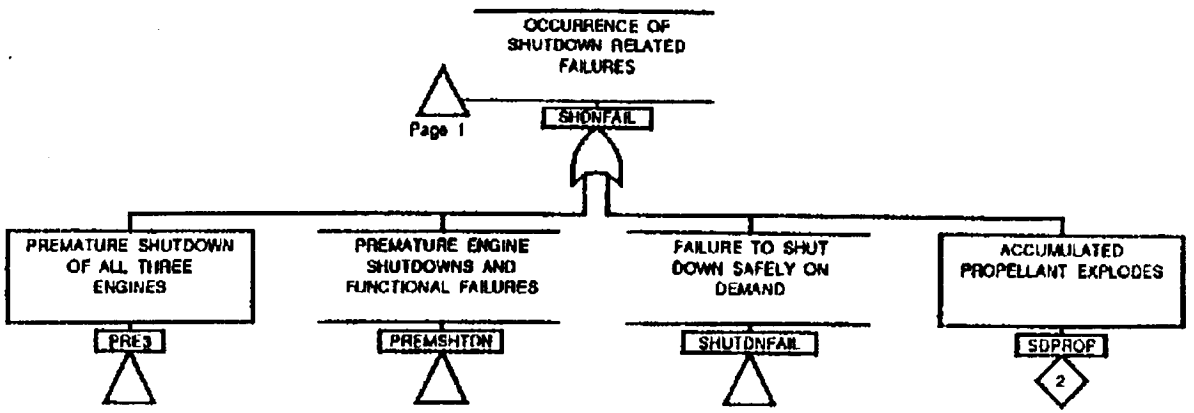
Figure 2-2
Top Level Fault Tree

DRAWING NUMBER

Page 5

DATE

9/04/87



TITLE

Figure 2-2
Top Level Fault Tree

DRAWING NUMBER	DATE
Page 6	9/04/87

Section 3

METHODOLOGY

PRAs rely on both FTA and event tree analysis (ETA) to quantify risk. FTA is used to establish the logical relationship between a system level failure and all conceivable combinations of component level failures which cause it. ETA relates each adverse outcome possibility with the time sequence of systems or subsystems failures which cause it.

The fault-tree model, is structured from a knowledge of system operation and previous FMEA's/hazards studies (Table 2-4). Data is derived from various failure rate or probability data bases (Table 3-1). These are the input values for the fault-tree model.

The fault-tree model can then be used to generate a "top event" (e.g., loss of life and/or vehicle) probability. Because the input data is generic (i.e., not specifically based on STS hardware failure history), an evaluation of FTA model and failure rate date sensitivity is needed. Sensitivity analysis involves perturbing the input data to determine its effect on the top event. Sensitivity analysis can be performed by altering the fault-tree model to test different assumptions. Sensitivity analyses may involve modifications, such as the deletion/addition of fault-tree branches, changing gate logic, and changing the success criteria. The recomputed top events provide some insight of the sensitivity of the model to the parametric or structural changes. In addition, one can vary the value of a specific failure rate input. In this manner, one can begin to bracket the top event probability range. Subtleties associated with sensitivity calculations are discussed in more detail in Section 4.

The results of FTA are then used in the final ETA computations, where consequences are factored in based on the time of accident, the probability of loss of life (respectively, loss of vehicle). If, for example, the accident occurs when the STS is still on the launch pad, hardware losses will be greater than once the STS has cleared the launch facility. The time-phased aspect of consequences and ETA in general are provided in Section 6.

These activities and results are presented in Figure 3-1.

3.1 MODEL DEVELOPMENT

A fault tree model is based on Boolean mathematics. That is, logical operators consisting primarily of and, or, not, and combination gates are used to represent the parts from lower order events and the top event. A description of Boolean logic symbology and terminology is provided in Figure 3-2. This standard convention is used for all FTA in this report.

A brief description of fault tree organization and an example of the method in which major MPPS components were accounted for in the FTA are provided below.

3.1.1 Fault Tree Organization

A fault tree model (Figure 3-3) was developed from the review of various design drawings and systems evaluations. Piping schematics were first analyzed to provide a basic understanding of the main process flow of the LH2 and LO2 propellant lines. Major components including pumps, valves and other active devices which are required to deliver the propellant to the main engine burners, and their actuators/controllers are depicted in Figure 3-4. Components providing a secondary function and systems supporting the MPPS are not depicted in Figure 3-4, but include the hydraulic, pneumatic and electrical controls. The complete fault tree, along with descriptions of its basic events, is included in Appendix C.

In general, the fault tree model was structured in three parts: ground, launch and MECO/ET separation failures. These three time sequences represent the actual time of occurrence of the top event. Failures occurring during the pre-flight phase included human errors; for example, fire/explosion at the launch site could be the result of human error during maintenance, repair or flight preparation activities. Human error on the ground prior to launch can also manifest itself as a latent failure during the actual flight; i.e., improper execution of prelaunch tasks can cause or allow an undetected problem to contribute to the manifestation of a catastrophic failure during the first few minutes of the launch. In contrast with the ground operation failures, flight failures consist primarily of hardware problems, because there is such limited opportunity for inflight human error.

To ensure that all previously identified single point failures have been included in the fault tree, a cross reference check with FMEA's and HA's is performed. That is, every criticality 1 event in the FMEA/HA is cross indexed to a specific basic event or gate. In some cases an FMEA item may appear in multiple branches of a tree. For details regarding this consistency evaluation, refer to Appendix H.

NOTE: Figure 3-3 is an edited version of the fault tree, provided for convenience. Branches which do not add significantly to understanding the model are not provided. For example, all redundant branches associated with the center and right engines are not included, as left engine is typical. The page numbers are identical with those in Figure D-2, the expanded fault tree. Figure D-2 should be consulted for transfer gates on pages not provided.

3.1.2. Example of Model Development

Structuring a fault tree from engineering diagrams is not, however, a straight forward process. Hardware failure modes, failure rate data, and time-phased operation greatly affect the manner in which the component is treated within the fault tree. To illustrate this point, a simplified LH2/LO2 pump valve schematic was developed (Figure 3-4). The component and major piping lines represent the main process flow and pressurization functions associated with the LH2 and LO2 propellant subsystems.

There are many subtleties regarding the various operating modes and functional requirements of the hardware. However, the schematic does provide a starting point and a basic description of those components most strongly affecting system operation.

Component failures may appear on different branches of the fault tree depending on their impact on STS. This is evident by examining the cross reference notes shown in Figure 3-4. Each note (i.e., identification number appearing next to the component) corresponds to a basic event or basic events in the fault tree model. The failure mode and time of failure are clearly very important factors in determining in which branches of the tree each component belongs. More discussion regarding fault tree organization is contained in Appendix D.

3.2 DATABASE DEVELOPMENT

3.2.1 Component Failure Rates

Component failure rates are based on widely used generic sources. Rome Air Development Center (RADC) documents provide most of the data used in this analysis. A summary of RADC and other failure rate documents is provided in Table 3-1. Whenever available, however, shuttle specific data is utilized to establish failure rates.

Electronic component failure rates are primarily based on MIL-HDBK-217E with the failure mode allocation determined by IEEE Standard 500. That is, the base failure rate is calculated for the parameters and quality factors as outlined in MIL-HDBK-217E. In a case when only selected component failure modes lead to catastrophic system failures, the overall failure rate is adjusted according to the failure mode allocation determined by IEEE Standard 500.

3.2.2 Basis for Exposure Times

The probability values used for each of the basic events depends on both the failure rate and on the exposure time. Assuming that the component reliability deceases exponentially in time, the probability of failure is calculated via the expression below:

$$P = 1 - \exp(-\lambda \tau)$$

Equation 3-1

Where $\lambda\tau$ is the product of failure rate (λ) and the exposure time (τ).

Many components are required to function on a "per-demand" basis. Examples of components required on demand consist primarily of valve openings/closings, pyrotechnic firings or human actions associated with operation. "Failure on demand" means that at a discrete time, certain components must perform a one-time action. "Per-demand" may alternatively be expressed as "per cycle".

In the case of a component required to operate on demand, total failure probability is the product of the failure rate per demand and the number of demands.

The expression in Equation 3-1 may be used to estimate per demand failures by setting the exposure time for that basic event equal to the entire time prior to the occurrence of the on-demand requirements. For example, the prevalves and the engine hydraulic valves isolate engines in redline condition on demand. The need to shut down a particular engine may occur at any time prior to MECO. Therefore, the cumulative exposure time is the time between start of ignition sequence to MECO or approximately 8.1 minutes. Note that this estimate may fail to be conservative if the "on-demand" requirements of the data base components are less than those of the MFPS components.

The time-phased nature of the fault tree requires that for some component failures (e.g. those which could occur at any time to contribute to the top event) separate exposure times must be established for each time segment. Break-up of other time phases not shown in the fault tree is required for the purpose of consequence analysis. Details regarding the partitioning of time intervals are provided in Section 7. A tabulation of the time-phased probabilities is contained in Appendix C.

3.3 PROBABILISTIC COMPUTATIONS

3.3.1 CAFTA Code

All fault tree computations are performed using the CAFTA code. CAFTA is a microcomputer-based program which performs fault tree analysis on a system or group of systems. The program includes a fault tree editor for building and updating fault tree models, and a reliability data base for storing all basic events used in the models. A brief description of the code capabilities and limitations is provided in Appendix I.

CAFTA relies on FTAP algorithms to generate the minimal cutsets. The complexity of the fault-tree model prohibits the generation of all possible minimal cut sets. Therefore, a truncation limit (10-8) is defined to eliminate consideration of very low probability sequences.

CAFTA truncates low probability sequences in a bottom-top manner at each level of fault tree intermediate events. Intermediate events above the cut-off threshold remain for inclusion in cutset reduction. The sum of minimal cutset probabilities conservatively approximates the top event probability.

It was judged that cutsets with probabilities below 10-8 are negligible contributors to top event occurrence and can be eliminated from consideration, as the probability of the top event is on the order of 2.5 x 10-3.

3.3.2 Importance Measures

Importance, in the probabilistic sense, refers to the significance which a basic event (or minimal cutset) has towards the outcome of a top event. Consider the importance of a lowest level event (i.e., basic event) to the top event. Basic event "i" (BEi) will appear in at least one sequence or cut set

which leads to the top event. Most likely, however, a basic event will appear in many cut sets as defined by the tree branches. The Boolean sum of the probability of all such sequences determines the probability of the top event.

Six different importance measures are calculated by CAFTA's cut set editor: these are Fussell-Vesely, Birnbaum, Risk Achievement Worth, Risk Reduction Worth, Criticality, and Structural Importance. Each of these different importance measures provides different information. For this PRA, only the Fussell-Vesely and Structural Measures of Importance are used, so only these are defined.

Fussell-Vesely Importance

The collection of cut sets Kj where BEi is contained in Kj is used to compute the importance of BEi. The ratio of the probability of all sequences in which a given basic event occurs to the total top event probability determines the importance of the basic event.

The Fussell-Vesely measure of basic event importance is effectively a weighting function with numerical value between 0 and 1. The Fussell-Vesely measure, $I_{FV}(BE_i)$, is defined by the following ratio:

$$I_{FV}(BE_i) = \frac{\text{Probability of The Boolean union of minimal cut sets } BE_i}{\text{Top Event Probability.}}$$

Equation 3-2a

If a basic event is contained in each minimal cut sets (also called min cut set) then its importance value is unity. Stated in other terms, the Fussell-Vesely is the conditional probability that a min cut set containing the basic event occurs given the occurrence of the Top Event. The Fussell-Vesely importance is therefore computed as:

$$I_{FV}(BE_i) = \frac{\text{Sum of min cut set probabilities containing } BE_i}{\text{Sum of all min cut set probabilities.}}$$

Equation 3-2b

Equation 3-2a represents a universally applicable Fussell-Vesely relationship between a specific basic event and the top event. This relationship is useful in expressing how much attention should be given to each basic event within the fault tree. Note that the importance of BEi as defined by Equation 3-2a will vary with the choice of different top events. A weakness of the Fussell-Vesely measure of importance is that it depends on failure data which may be uncertain (as in this study).

Structural Importance

A second measure of importance utilizes qualitative ranking. This measure is often called the structural importance because computation of the importance value is dependent upon the structure of the fault tree rather than upon probabilities assigned to basic events. This measure is therefore useful in establishing a first order ranking of significant basic events, when there is either scarcity of failure data or much uncertainty.

Structural Importance is defined as the fractional number of system states that are critical for a component. A critical system state for a component is defined as a system state such that the system makes a transition from the unfailed to failed state when a component fails, or more generally the top event occurs when a basic event occurs. This can be computationally approximated by the expression below:

$$I_S = \text{Sum of the probabilities of all cut sets given } P(BE_i) = 1.0 \text{ and } P(\overline{BE_i}) = 0.5 \; - \; \text{Sum of the probabilities of all cut sets given } P(BE_i) = 0.0 \text{ and } P(\overline{BE_i}) = 0.5$$

Equation 3-3

Where $P(\overline{BE_i}) = 0.5$ signifies that all basic events except for BE_i are assigned a probability of 0.5.

Structural importance measures are most useful in fault tree structures in which minimal cutsets are comprised of doubletons (i.e. two basic events) or higher order cutsets. Minimal cutsets in which only singletons exist necessarily have a computed value of zero by structural measure. Furthermore, minimal cutsets consisting primarily of singletons combined with other events which appear in only or a few cutsets, have computed values at or near zero. It is, therefore, very important to understand the cutset conditions and composition which exist prior to computing the structural importance value.

It is important to realize, however, that structural importance is not computed entirely independent of probabilities assigned basic events. CAFTA uses a truncation value to eliminate cutsets with probability below a specified limit. The structural importance measure is calculated only for those basic events which appear in cutsets above the truncation value. Structural importance can provide a useful tool for ranking. The reader is cautioned, however to exercise careful judgement when analyzing importance of basic events which appear in cutsets at or near truncation value.

Each relationship provides valuable information regarding the significance of hardware and human actions in precluding a major accident. Prioritization based on the ranking scheme is a useful tool for possible upgrades, modifications and procedural changes.

A summary of the highest ranking basic events and their respective importance values is provided in Section 6 and in Appendix I

More discussion on the application of this measure is provided in Section 4.

3.3.3 Synthetic Sampling Statistics

The unavailability of STS-specific failure rate data can be addressed mathematically through a synthetic sampling method discussed below.

The variable of interest in this study is the top event (e.g. loss of life and or vehicle). The top event (TE) is a function of basic events BEi, BE2...BEk. The function is complicated and represents the sum total of all cut sets above the specified cut set truncation limit. The question to be investigated is: How does TE vary when the BE's vary according to their individual probability distributions? Related questions are: What is the expected value of TE? What is the 90th percentile of TE? etc.

By sampling repeatedly from the individual probability distributions of the BE's and evaluating TE for each sample, a probability distribution for TE is produced. This PRA will utilize the Top Event Matrix Analysis Code (TEMAC) for the statistical computations needed to generate the TE distribution.

TABLE 3-1

Summary of Failure Rate Data Sources

DOCUMENT (Ref #)	DATA CONTAINED
Nonelectronic (Mechanical) Parts Failure Rates, LMSC/D520737, Revision C, Nov. 26, 1986, prepared by J. T. Yee (1)	◇ Compiled from various sources: RADC, Hughes Aircraft Co., TRW, LMSC internal documents. ◇ Strictly mechanical components. ◇ Provides failure rate (per hour)point estimates; includes environment/application, but no breakdown of failure modes.
Nonelectronic Parts Reliability Data, NPRD-3, RADC, Fall 1985, prepared by Michael J. Ross. (2)	◇ Data from Rome Air Development Center for non-electronic parts. ◇ Provides failure rate (per hour) point estimates, also 60% upper single sided, 20% lower and 80% upper intervals from chi squared distribution. ◇ Includes breakdown by environment; failure mode distribution given separately.
RADC Nonelectronic Reliability Notebook, RADC-TR-85-194, Interim Report, Oct. 1985, Hughes Aircraft Company. (3)	◇ Provides failure rate (per hour) estimates with 80% upper and lower bounds from exponential and Weibull distributions. ◇ Includes breakdown by environment, not by failure mode.
Nonelectronic Reliability Notebook, RADC-TR-75-22, AD/A005-657, RADC, Jan. 1985. (4)	◇ Same as above, except uses 90% confidence limit.
IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations, IEEE STD 500-1977, June 30,1977. (5)	◇ Provides failure rates per hour and/or per cycle; gives high, low, maximum, and recommended values for 90% confidence interval from chi squared distribution; gives breakdown by failure mode.
Reliability Prediction of Electronic Equipment, MIL-HDBK-217E, 15 Jan 1986. (19)	◇ Provides equations and parameters for calculation of failure rates based on environment, quality, packaging, etc. ◇ Data from RADC.
Handbook of Piece Part Failure Rates, Martin Marietta Corp., Denver Division, GIDEP 031-1273. (27)	◇ Point estimate failure rates for mechanical piece parts.
Handbook of Human Reliability Analysis with Emphasis on Nuclear Plant Applications, NUREG/CR-1278, SAND 80-0200, August 1983.	◇ Human reliability data. ◇ Human error probability shaping factors.

TABLE 3-2

SUMMARY OF MINIMUM SUCCESS PARAMETERS AND CRITERIA

Component or System	Success Parameter/Criteria
SSME System	Two of three engines are available and fully functional for the first 5.8 minutes of the flight. Thereafter at least one engine is availabe to press to MECO and abort. No credit is given for the existence of a shutdown inhibit preventing shutdown of a second engine under many redline conditions. This conservative modelling assumption is used because we cannot assess the performance of a redline engine.
SSME	All major components (e.g. LPFT, LPOT, HPFT, HPOT, OPOV, FPOV, MFV, MOV) are fully functional in order for an engine to be considered available.
ET Separation	Complete separation of the ET from the orbiter on demand considered a success. Partial, premature, or delayed separation are all considered to be failures.
Tank Pressurization	Tank integrity is maintained during flight conditions by maintaining proper ullage pressure. Failure to maintain prescribed pressure results in structural damage to tanks and/or main engine pump cavitation.
Pressure Boundary Integrity	Pressure boundary failure of a high pressure system is considered an immediate catastrophic failure. An ignition source must be present to cause such a failure in a low pressure system. Any break of propellant system, hydraulic system or pneumatic system piping in conjunction with an ignition constitutes a loss of vehicle.

FIGURE 3-1 MAIN PROPULSION PRESSURIZATION SYSTEM PRA FLOW

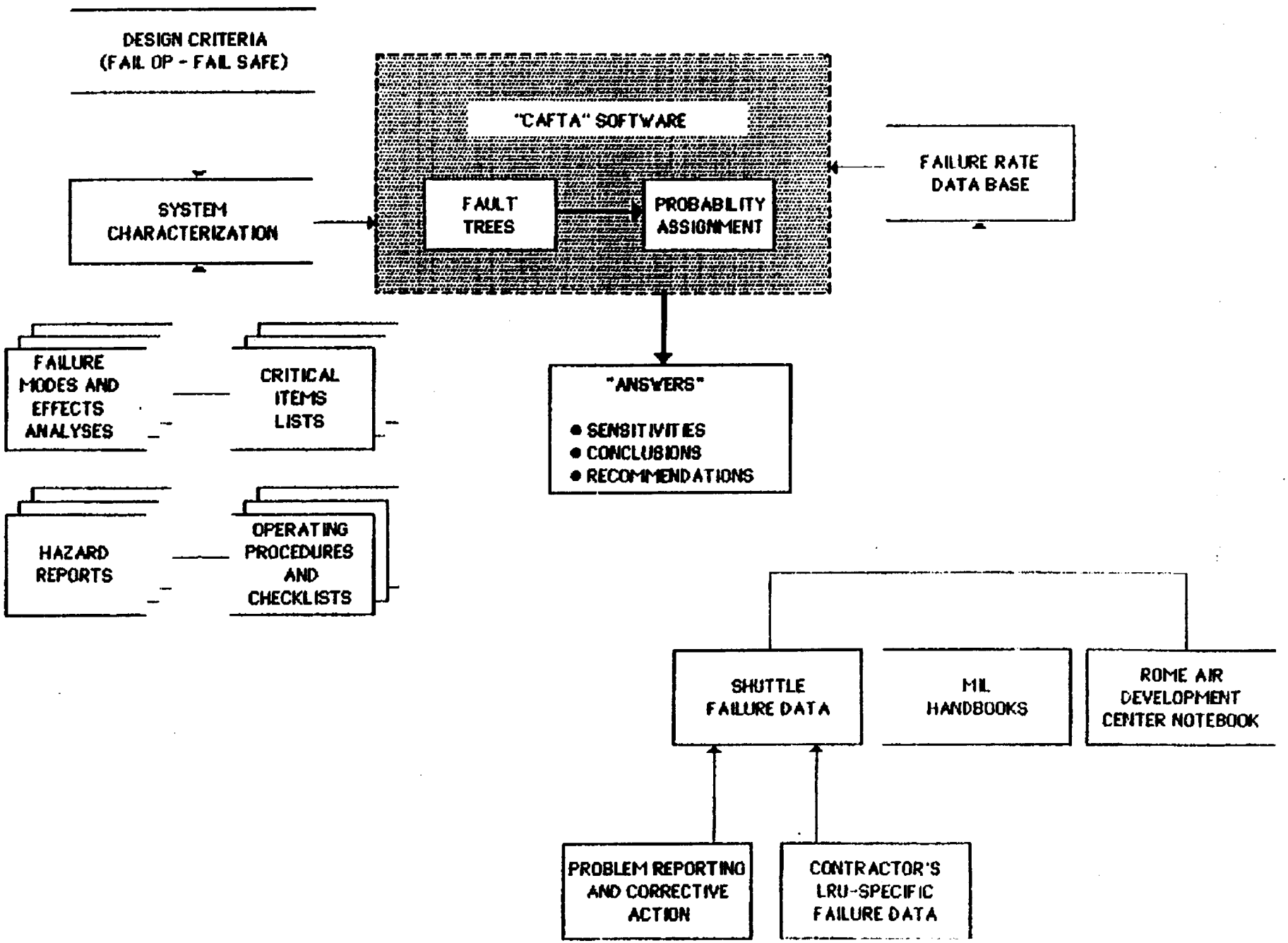
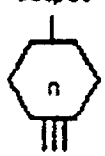
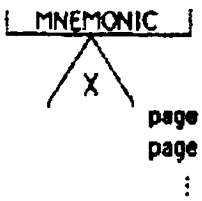
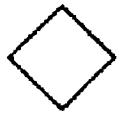
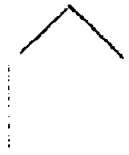
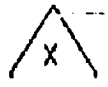


FIGURE 3-2
Fault Tree Symbology and Terminology

SYMBOL	NAME	DESCRIPTION
output  inputs	"AND" gate	All inputs must occur in order for the output to occur.
output  inputs	"OR" gate	Any input must occur in order for the output to occur.
output  input	"NOT" gate	Negated input causes the output to occur. In probabilistic terms, the output is the complement of the input or 1-P(input).
output  n inputs	"Combination" gate	At least "n" of total inputs must occur in order for the output to occur.
 MNEMONIC X page YY page ZZ ⋮	"Transfer" In gate *	A transferred branch of the tree appearing in "x" different locations as identified by page number(s) shown; if no page number is shown, that denotes a suppressed portion of the tree, which is presented in Appendix D.

* *Appears beneath mnemonic descriptor.*

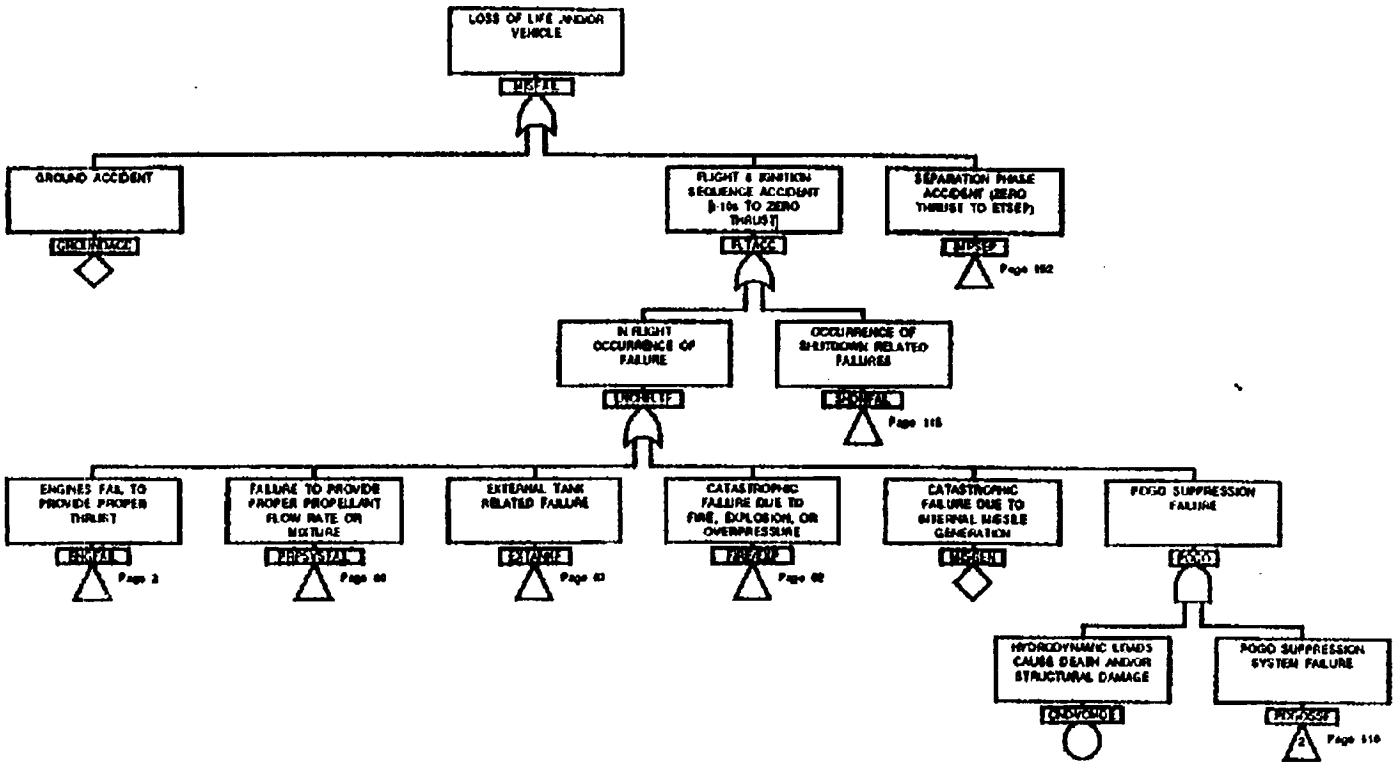
Figure 3-2
Fault Tree Symbology and Terminology

SYMBOL	NAME	DESCRIPTION
	Basic event *	Lowest element in the fault tree. The basic event represents the limit of resolution of the fault tree.
	Undeveloped event*	Self explanatory; used to represent events considered outside the scope of analysis. Further definition or quantification may be required at a future date.
	House Event	Used as a toggle device (e.g., value of event is set to "0" or "1") to isolate branches of the fault tree as necessary. This is primarily used for time phase aspects of fault tree development.
| 12345678 |	Mnemonic Descriptor	Encoded information regarding event type, name, and failure mode. See Appendix B for details regarding Basic Event Mnemonics.
GATE DESCRIPTION	Event or gate descriptor	A brief description of logical outcome of any event or gate.
GATE DESCRIPTION  X page YY page ZZ	"Transfer" out gate	A transfer of a gate to other branches of the tree. "X" denotes the number of locations to which the gate was transferred.

* *Appears beneath mnemonic descriptor.*

Figure 3-2
Fault Tree Symbology and Terminology

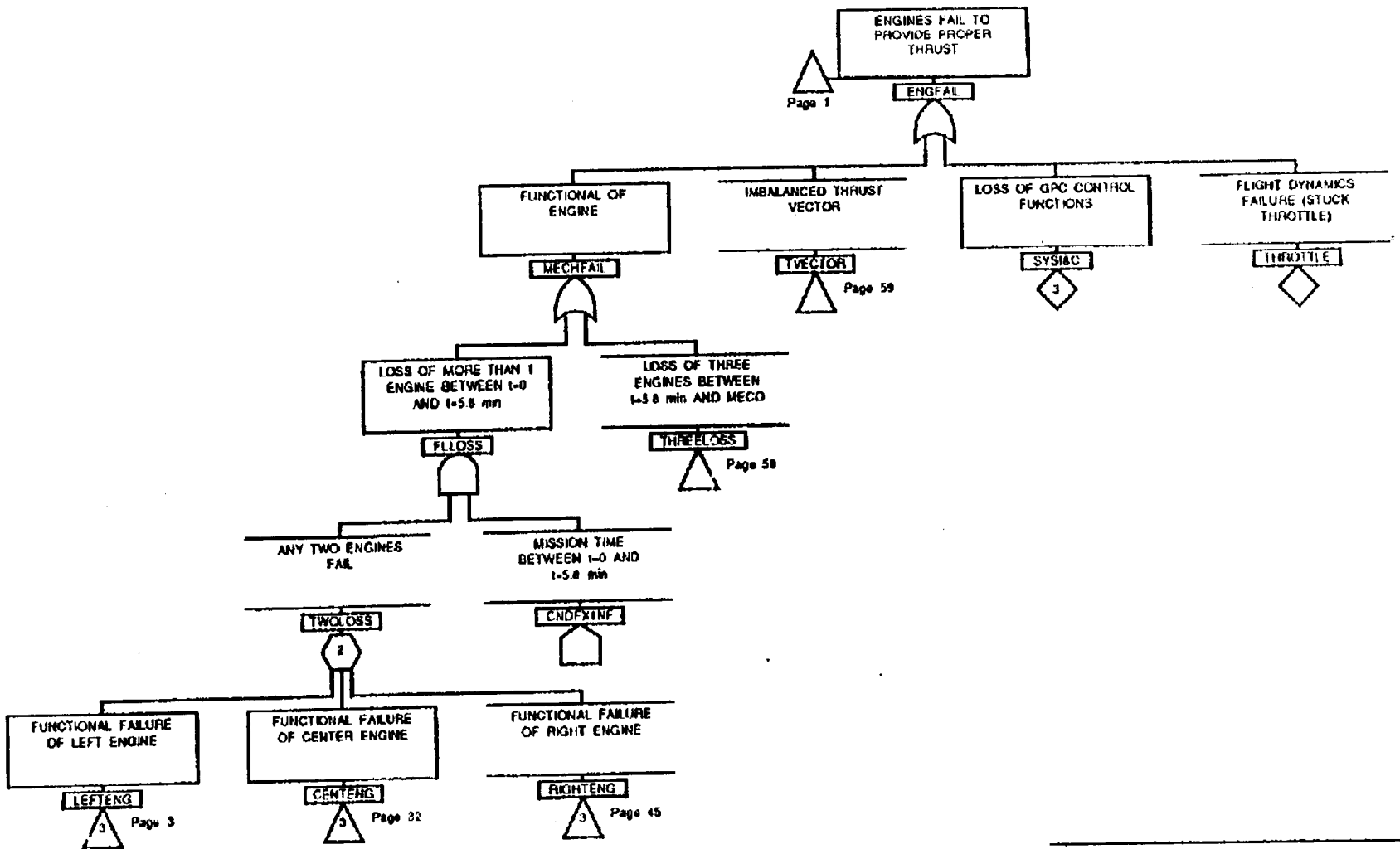
TERM	DESCRIPTION
Basic Event:	The lowest order event developed in the fault tree logic model. In most cases this corresponds to a component failure, human error, or an environmental condition. Basic events are the inputs to the logic model.
Intermediate Event or Gate:	A logical outcome resulting from a single or combination of basic event or lower order event occurring at any level in the fault tree.
Top Event:	The logical outcome of a fault tree model. The top event in this analysis is the catastrophic loss of human life and/or STS vehicle and facilities.
Cut Set:	A combination of basic events which leads to the top event.
Minimal Cut Set:	A cut set with no proper subset which is itself a cut set.
Event Sequence:	The success and failure paths defined by critical time intervals, ET separation and mission abort landings.
Consequence:	The outcome of an event tree sequence measured in terms of success, or loss probabilities. Consequences will be measured both in terms of loss of life and/or vehicle.



TITLE

Figure 3-3: MPPS FAULT TREE

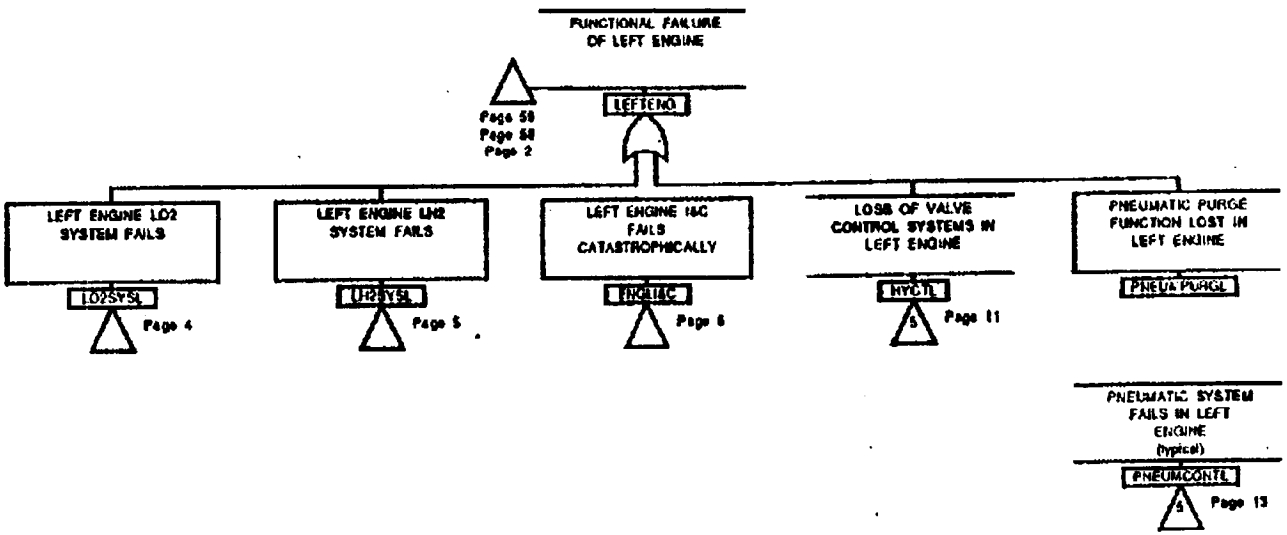
DRAWING NUMBER	DATE
Page 1	1/05/88



TITLE

Figure 3-3: MPPS FAULT TREE

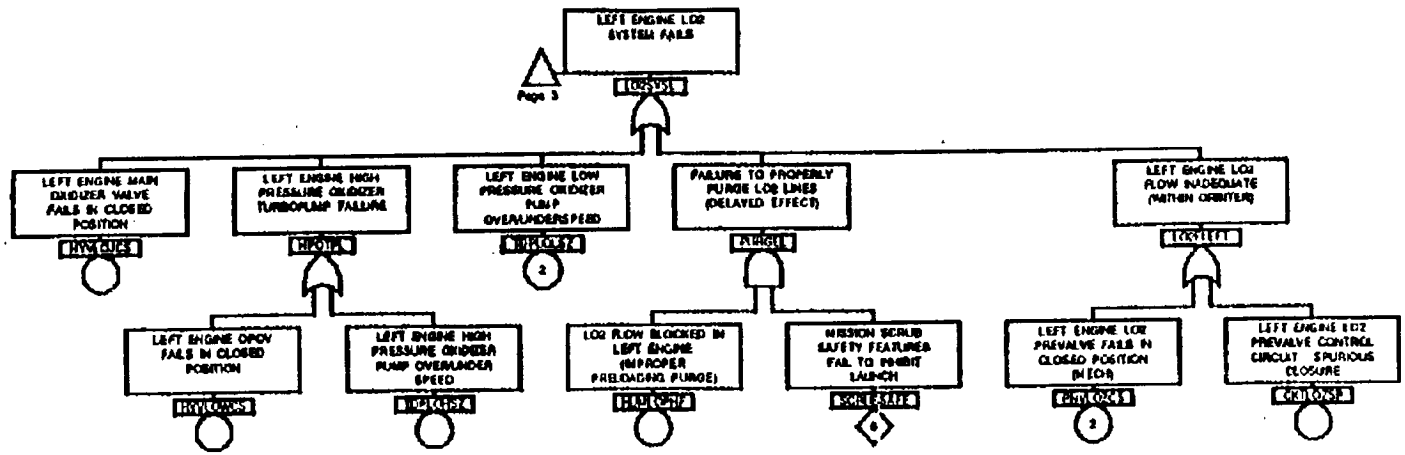
DRAWING NUMBER	DATE
Page 2	9/04/87



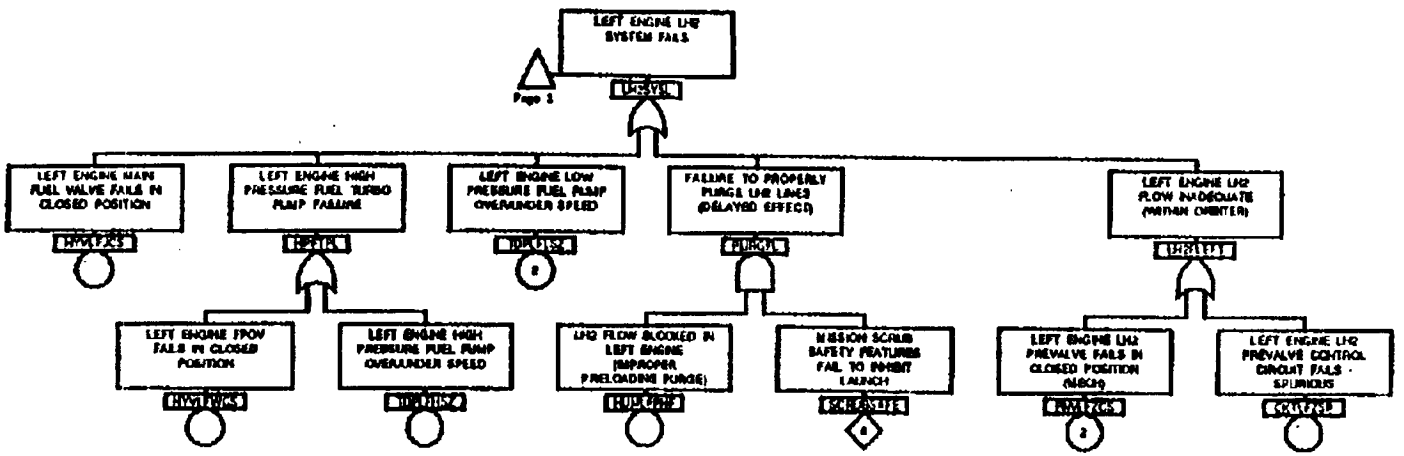
TITLE

Figure 3-3: MPPS FAULT TREE

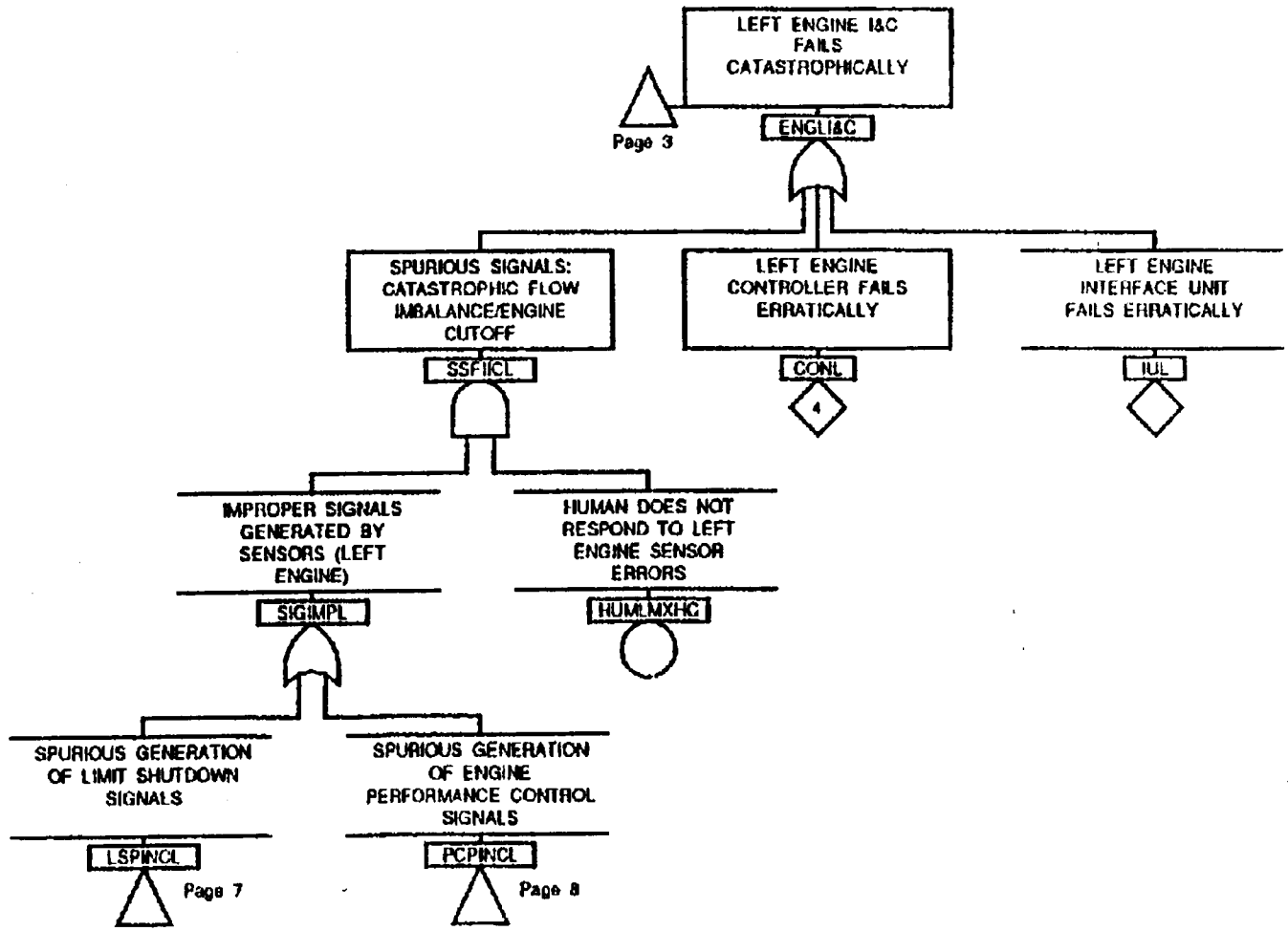
DRAWING NUMBER	DATE
Page 3	9/04/87



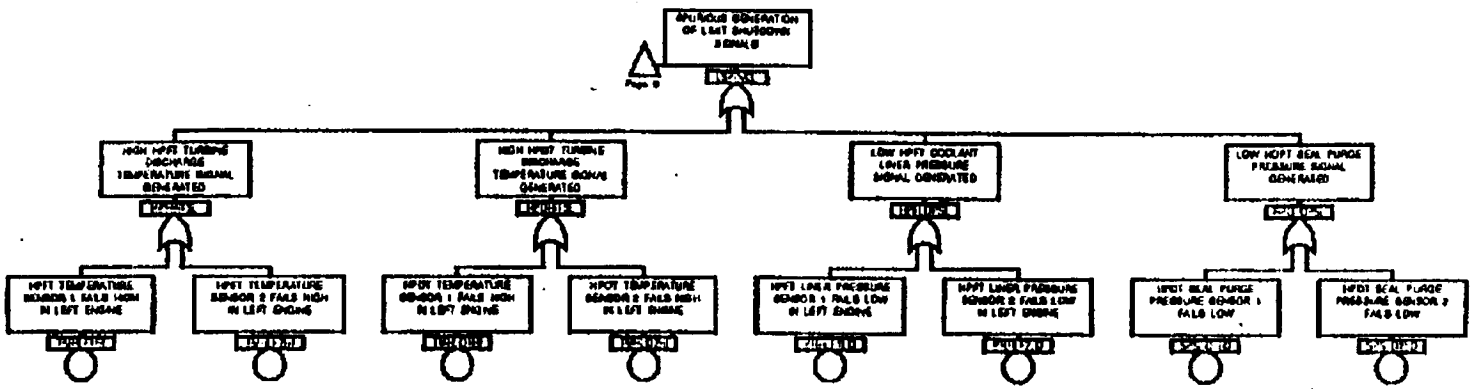
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 4	9/04/87



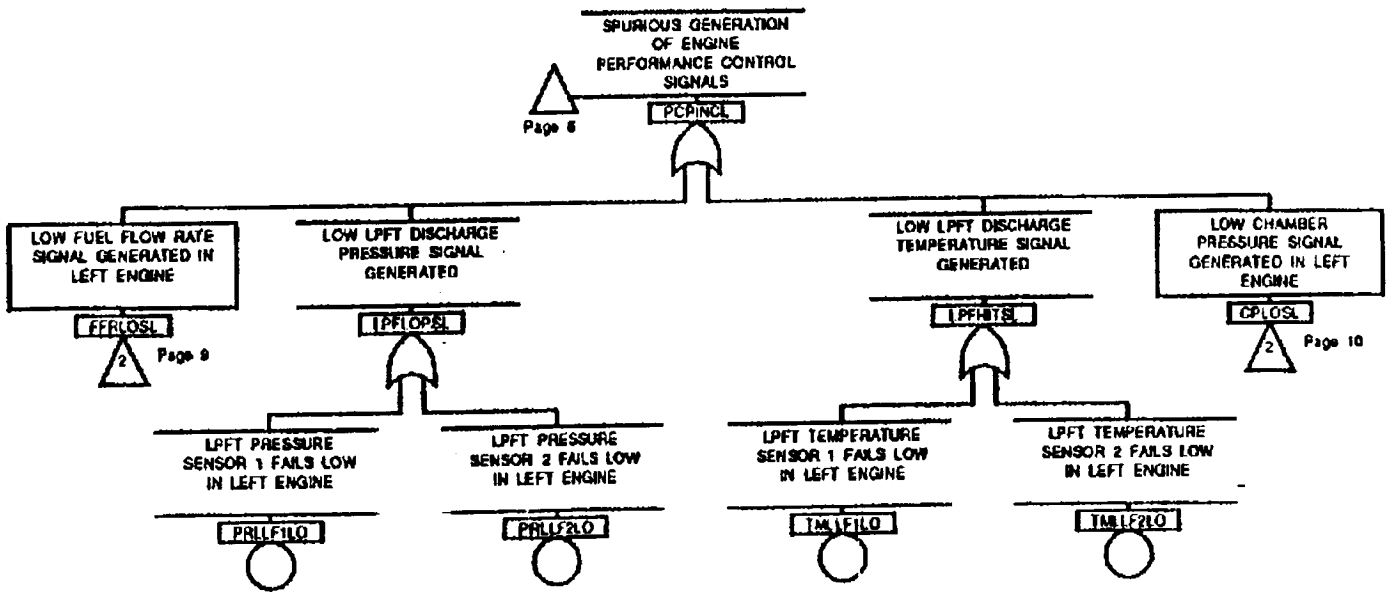
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER Page 5	DATE 9/04/87



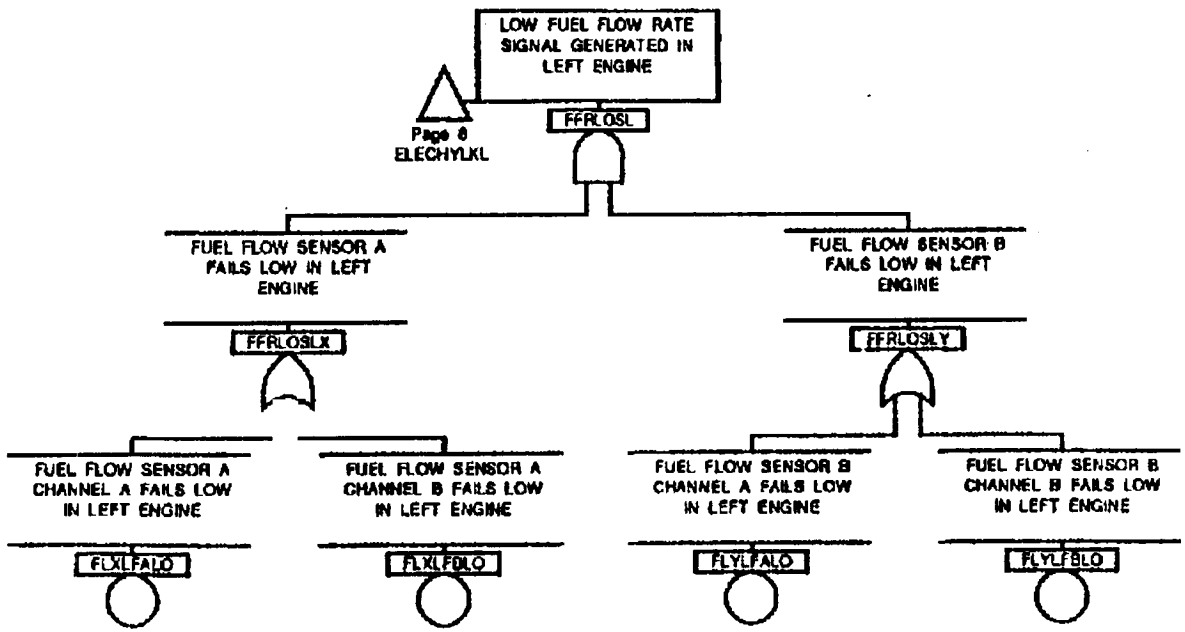
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 6	9/04/87



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER Page 7	DATE 9/04/87



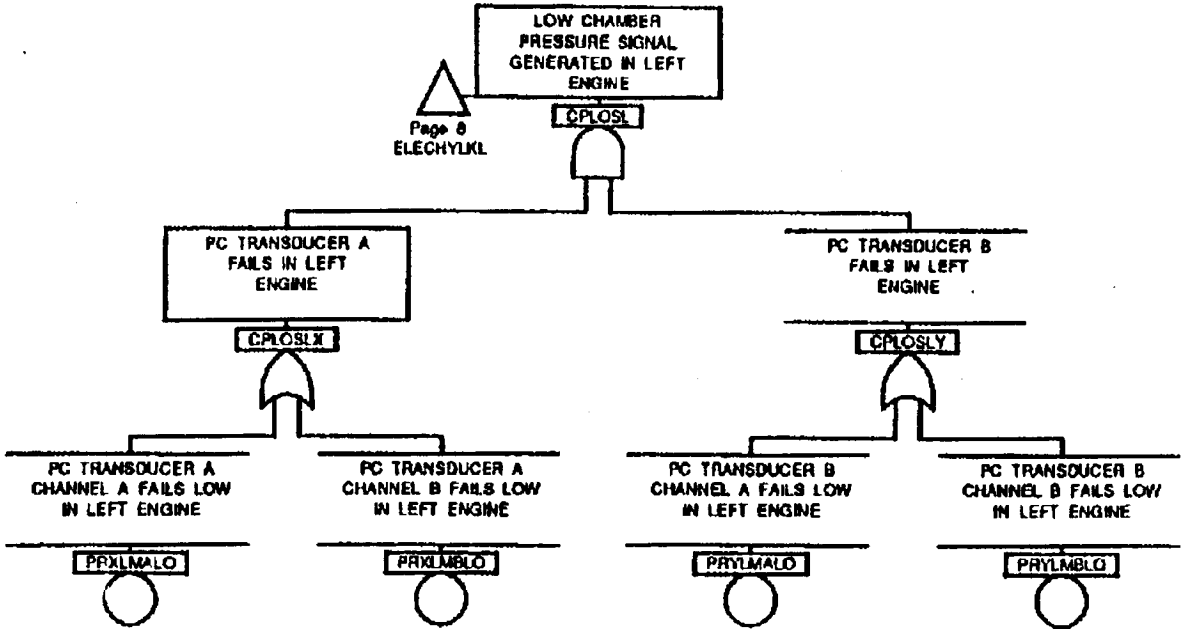
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 8	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

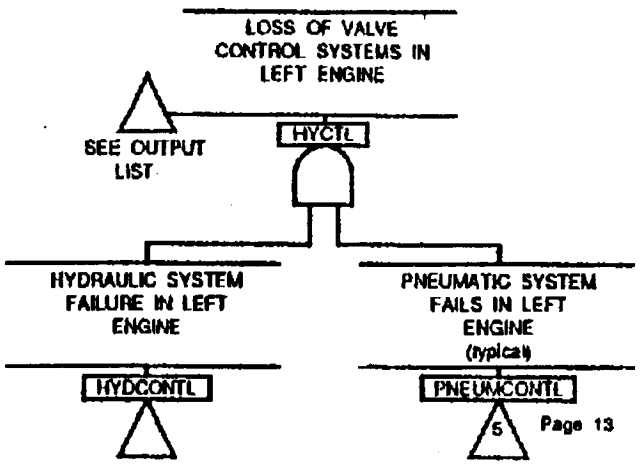
DRAWING NUMBER	DATE
Page 9	9/04/87



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 10	9/04/87

HYCTL OUTPUTS:
Page 3, Page 140, Page 133
Page 137, Page 147

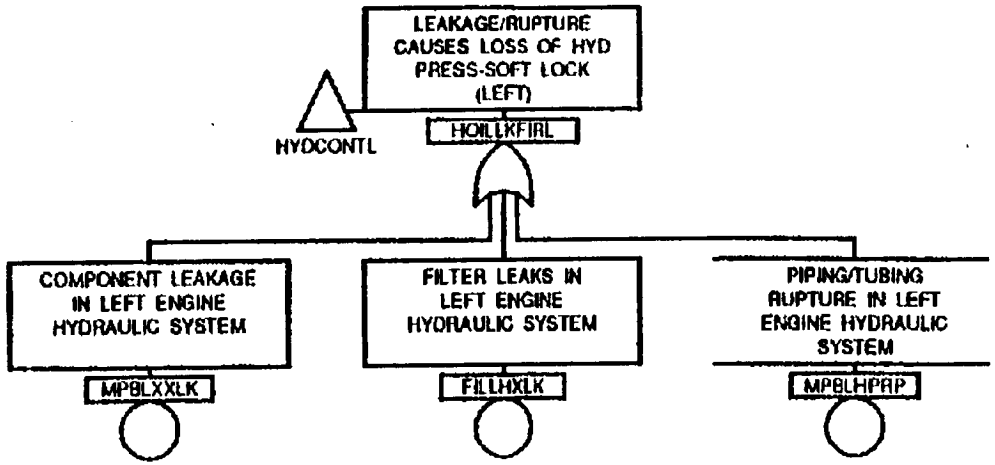
LMSC-F2230402



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 11	9/04/87



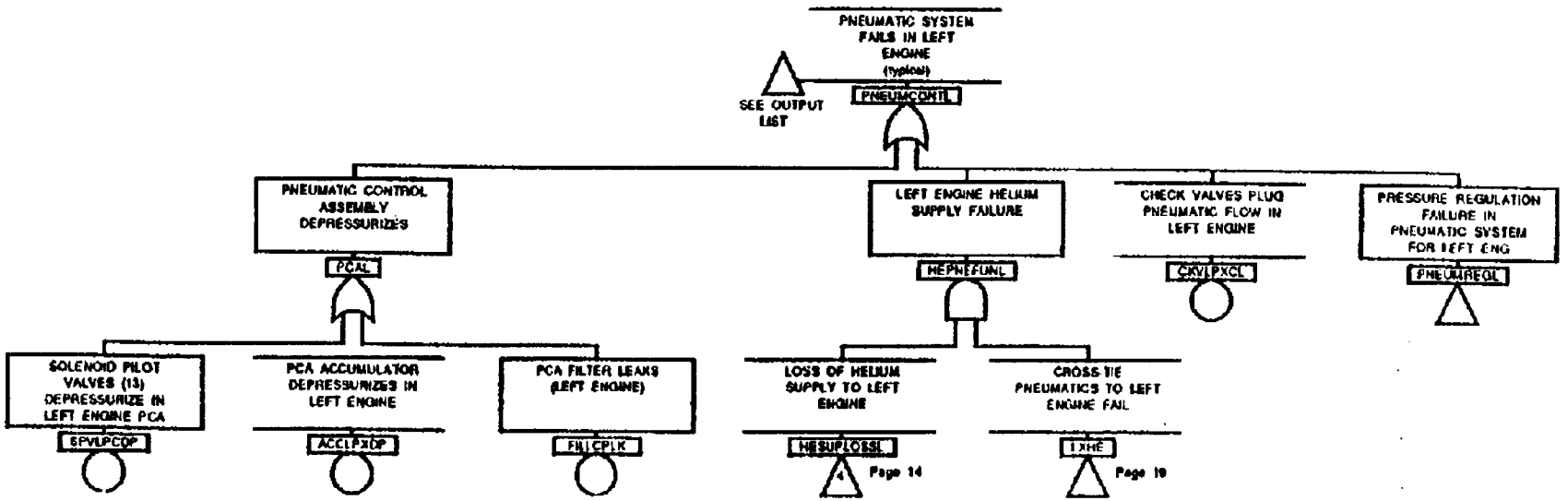
TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 12	9/04/87

PNEUMCONTL OUTPUTS:
Page 11, Page 93, Page 110
Page 140, Page 3

LMSC-F2230402



TITLE

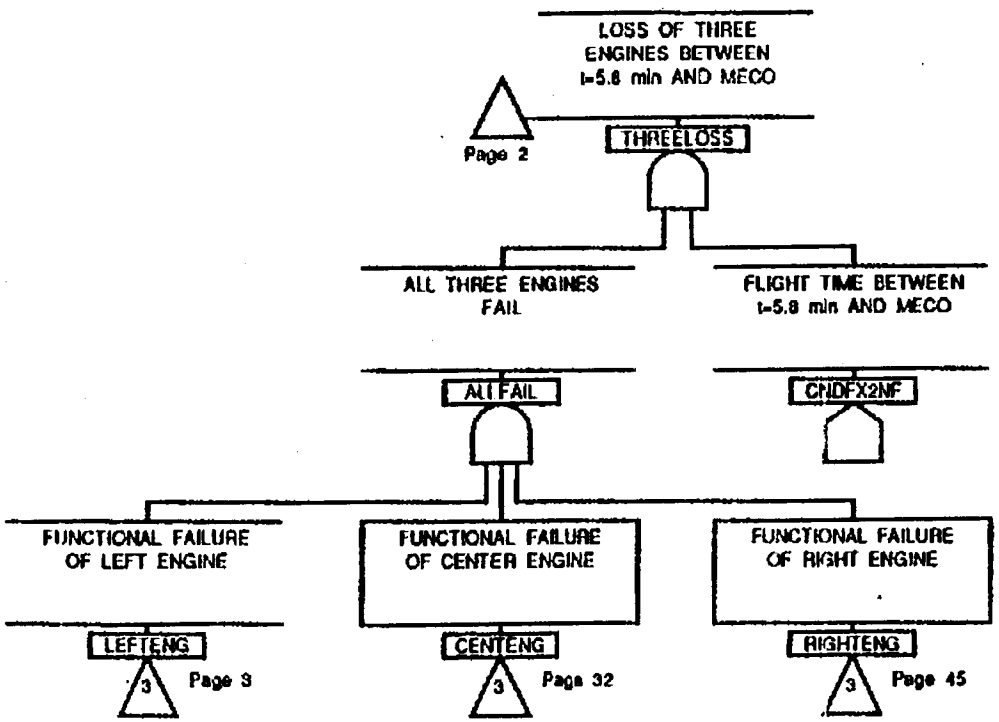
Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER

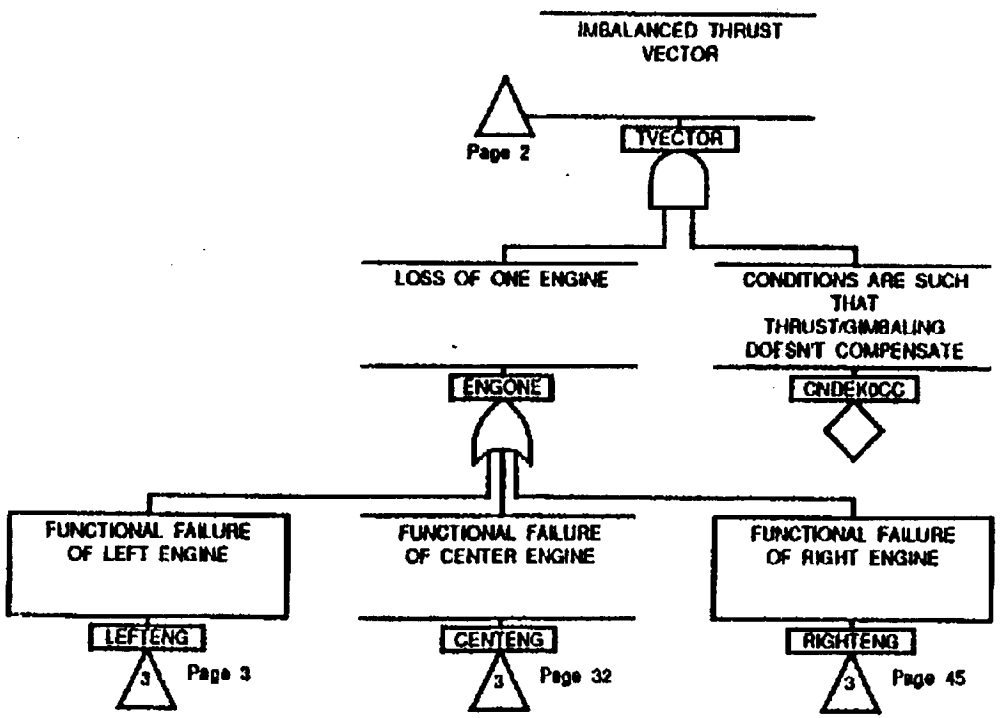
Page 13

DATE

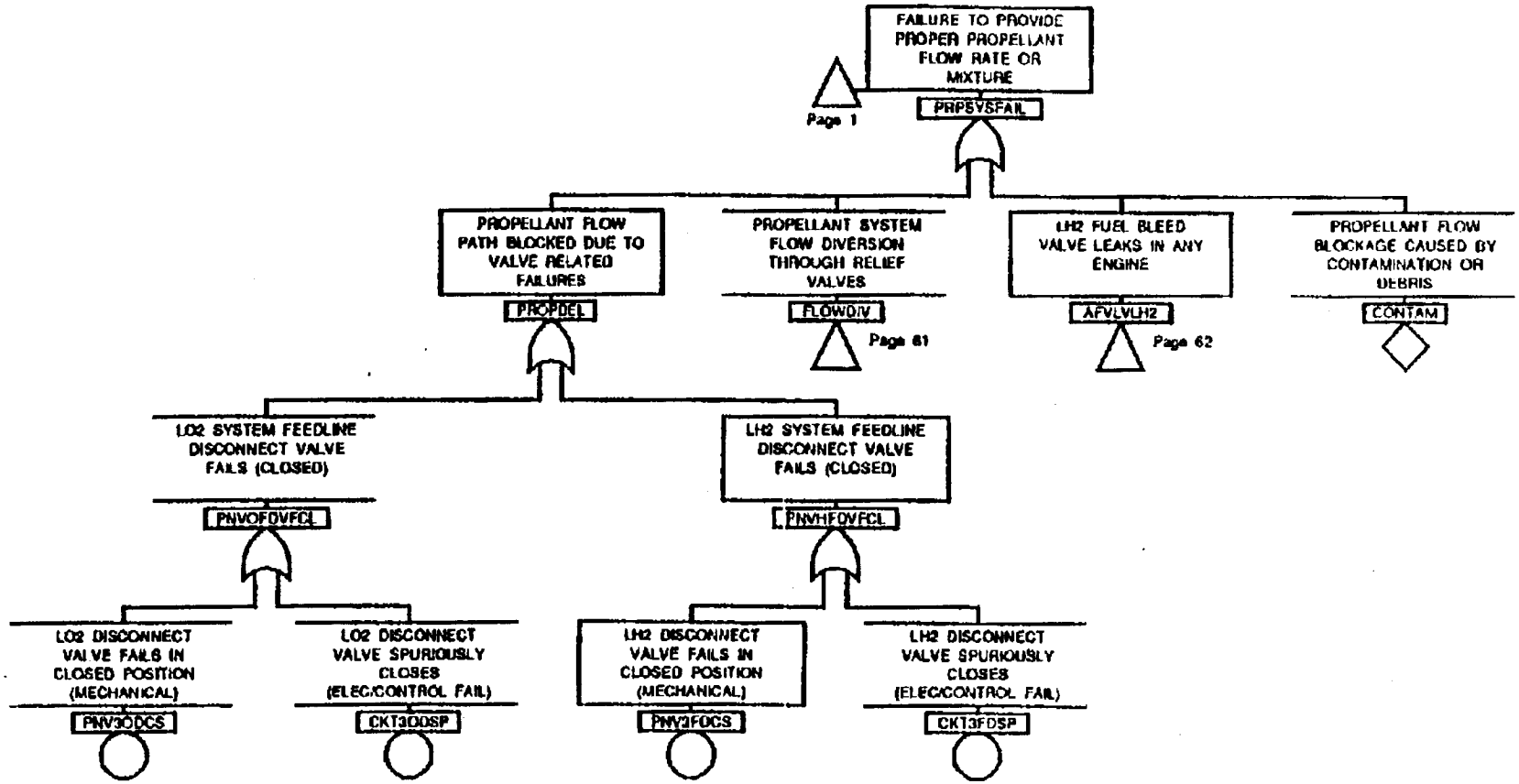
9/04/87



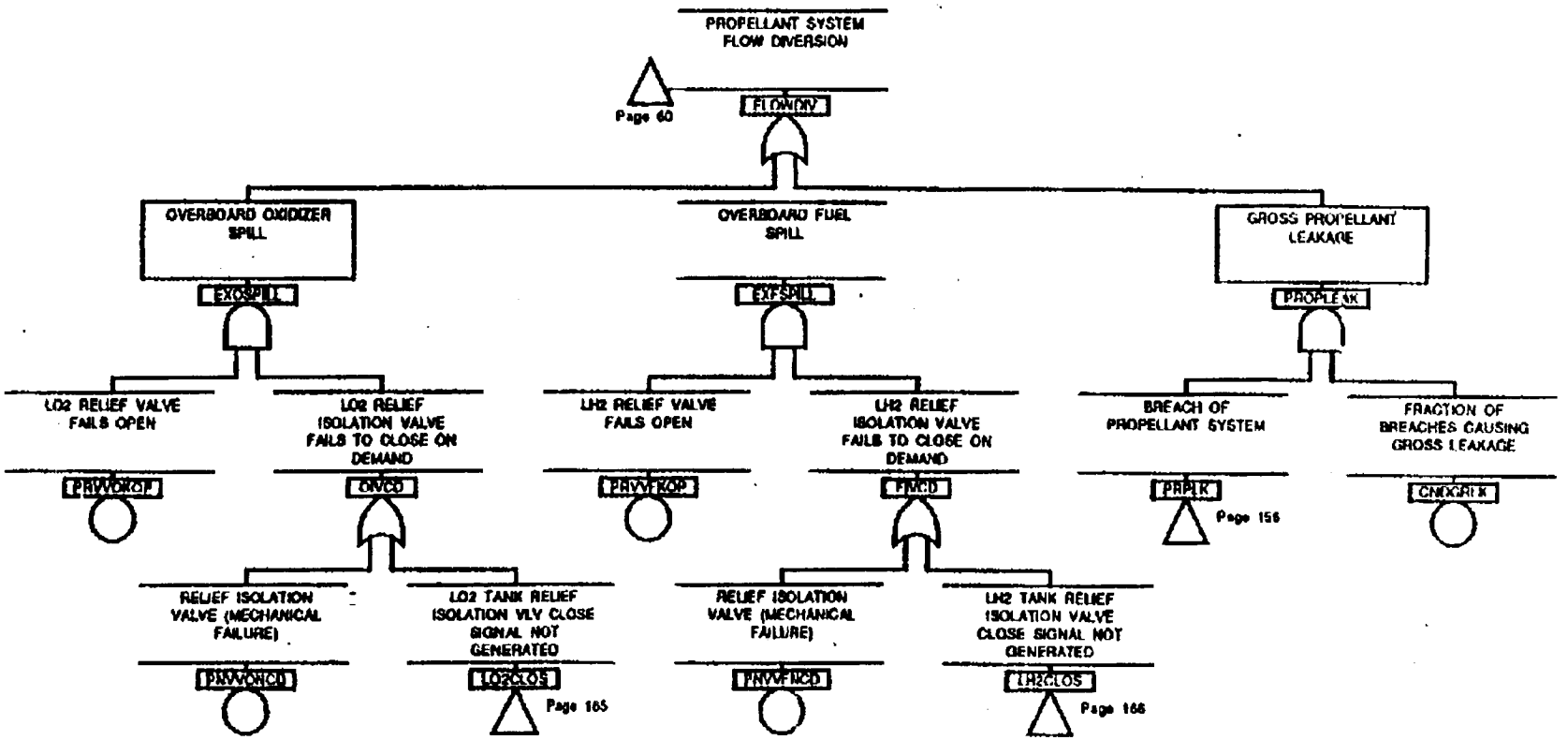
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER Page 58	DATE 9/04/87



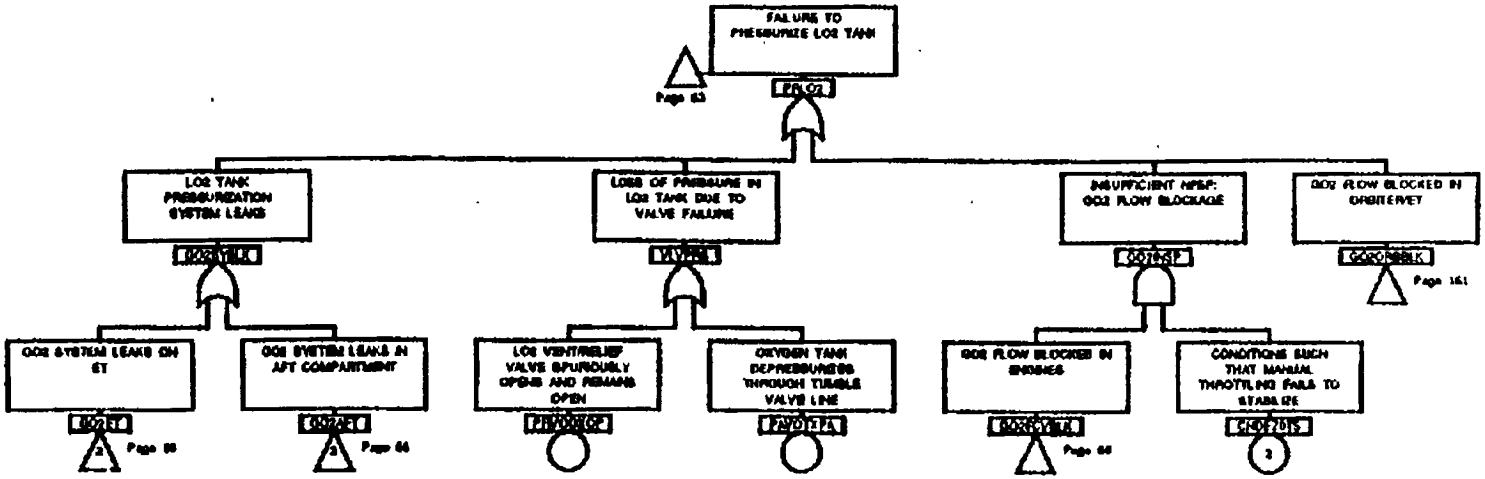
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 59	9/04/87



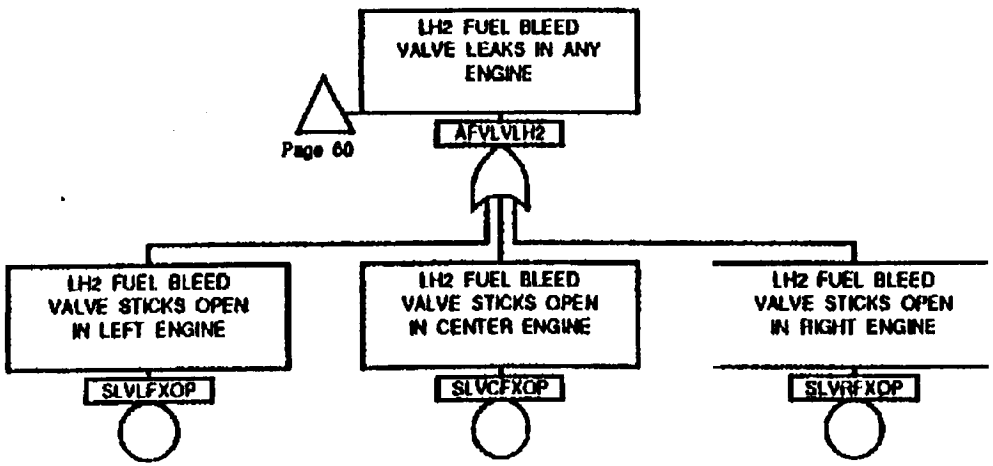
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 60	9/04/87



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 61	1/05/88



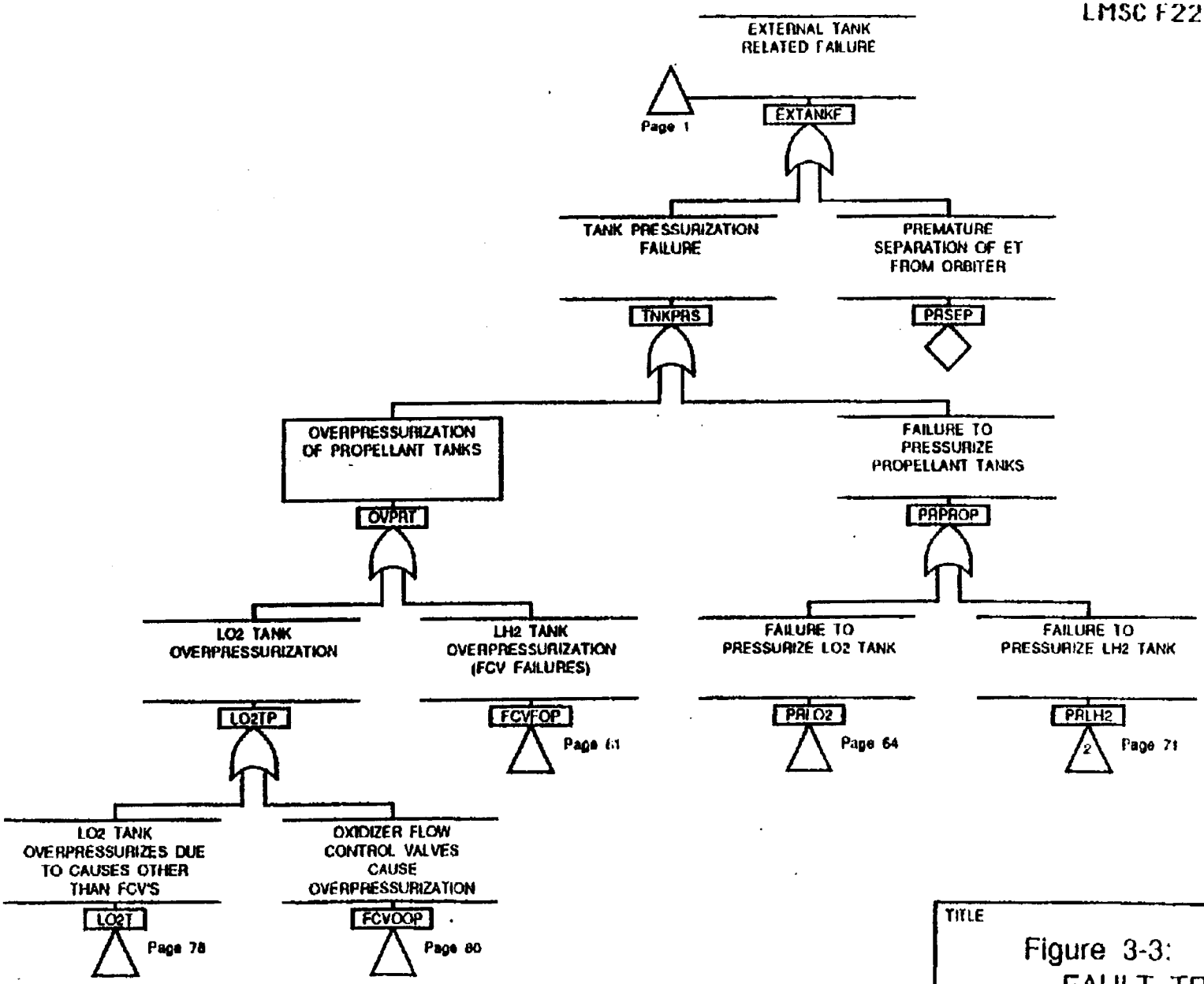
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 64	1/05/88



TITLE

Figure 3-3: MPPS FAULT TREE

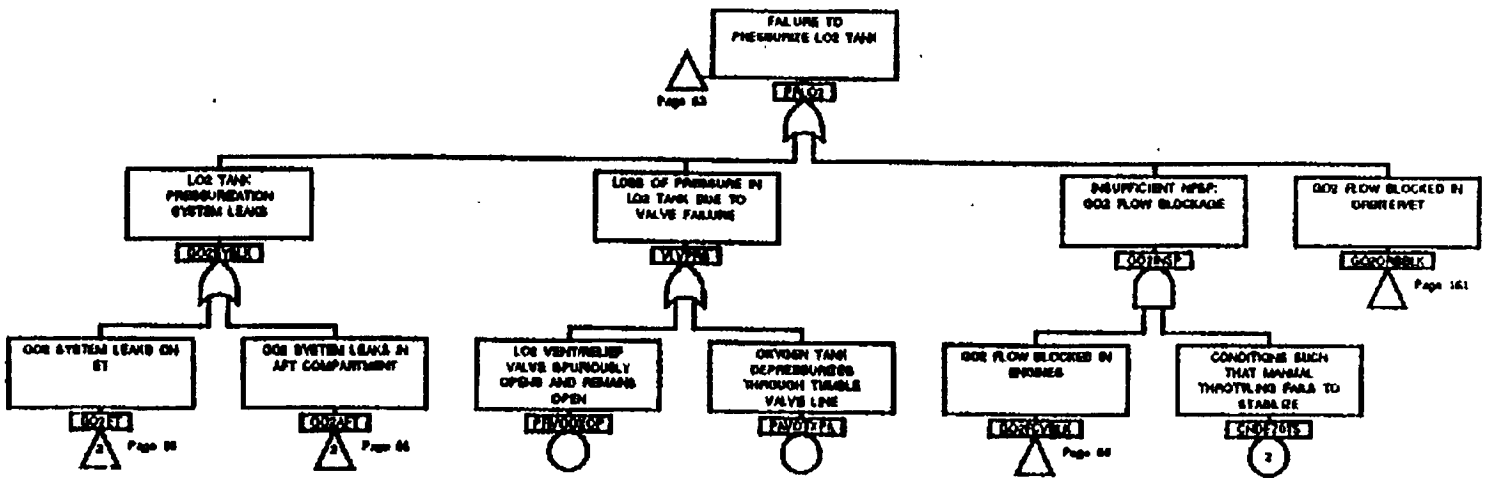
DRAWING NUMBER	DATE
Page 62	9/04/87



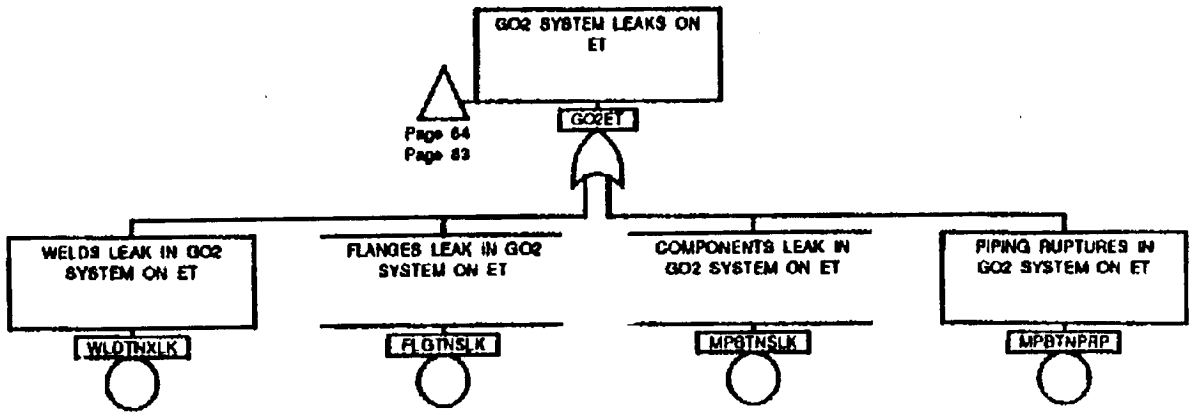
TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 63	1/05/88



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER Page 64	DATE 1/05/88



TITLE

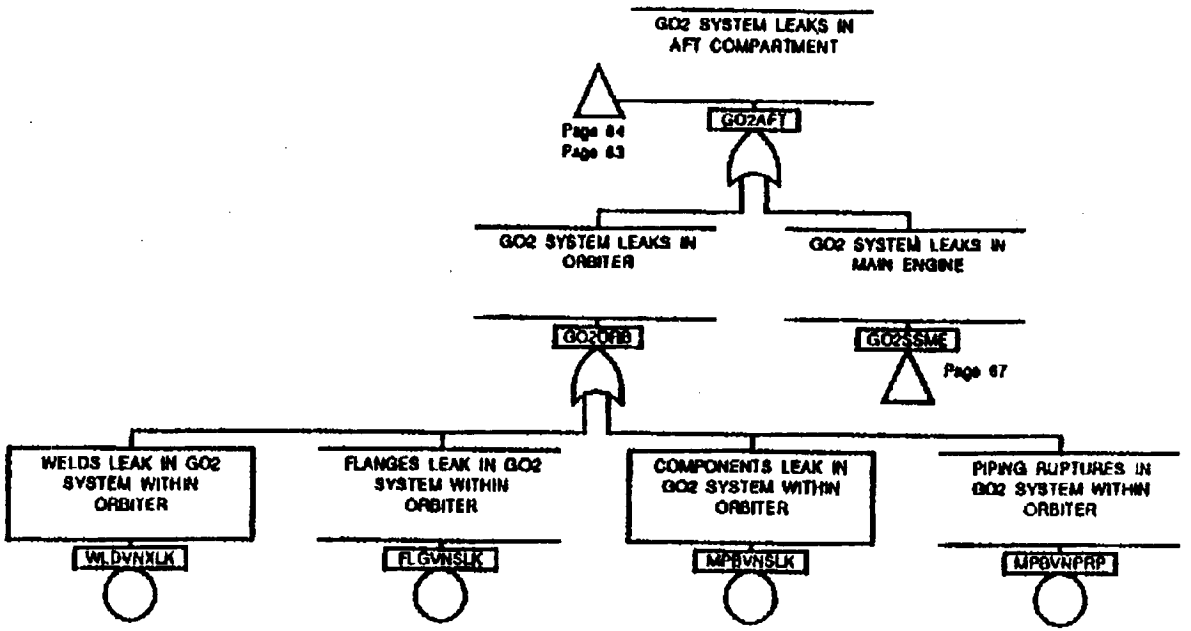
Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER

Page 65

DATE

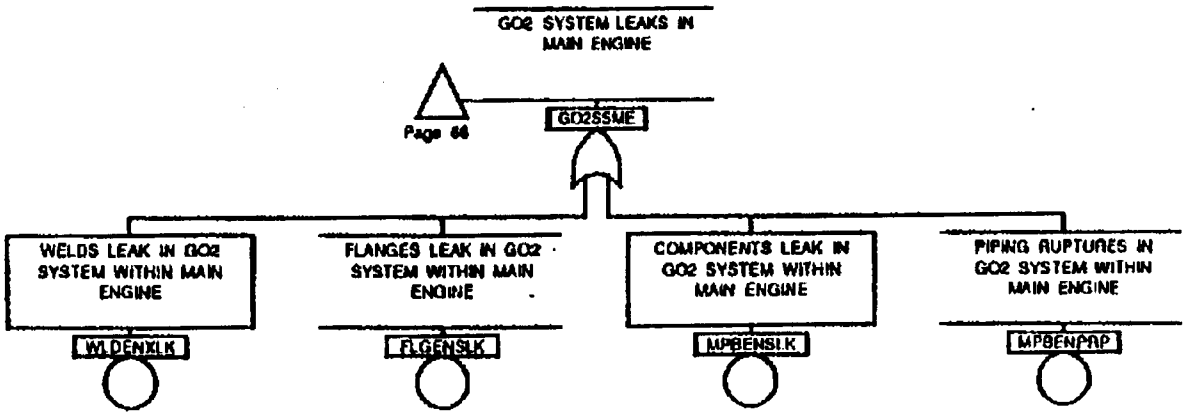
1/05/88



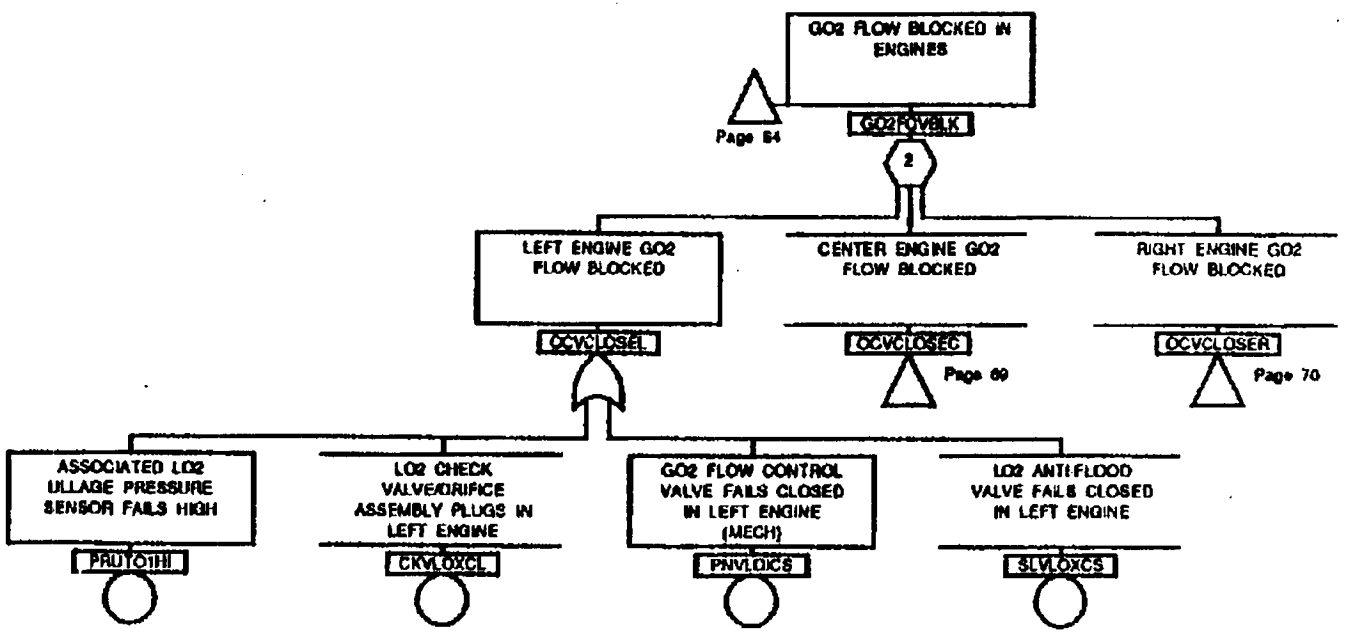
TITLE

Figure 3-3: MPPS FAULT TREE

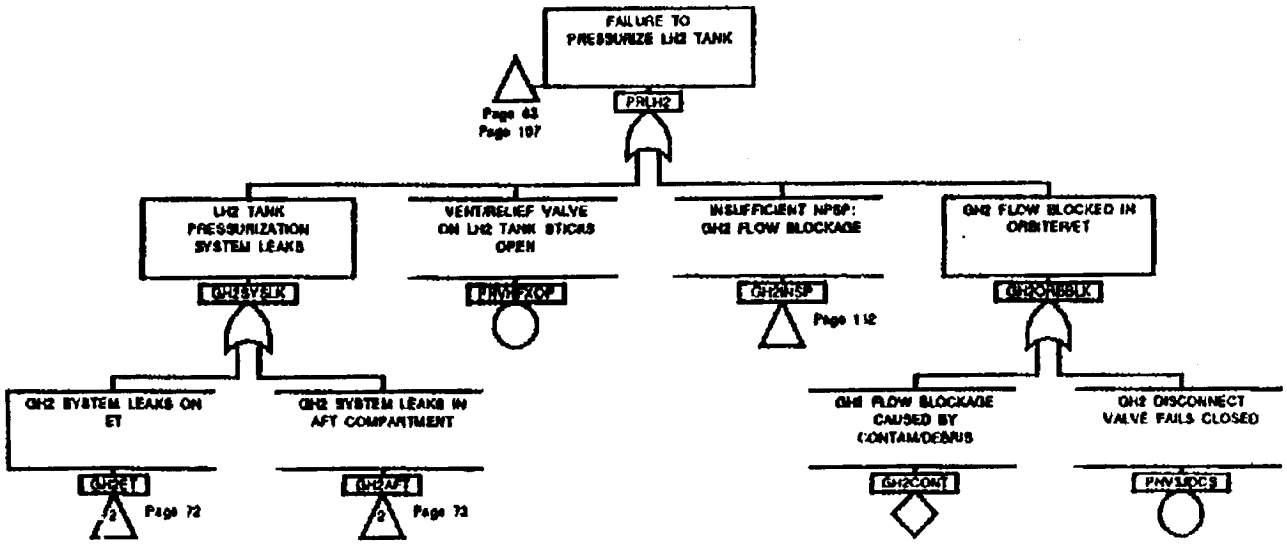
DRAWING NUMBER	DATE
Page 66	9/04/87



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 67	9/04/87



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 68	1/05/88

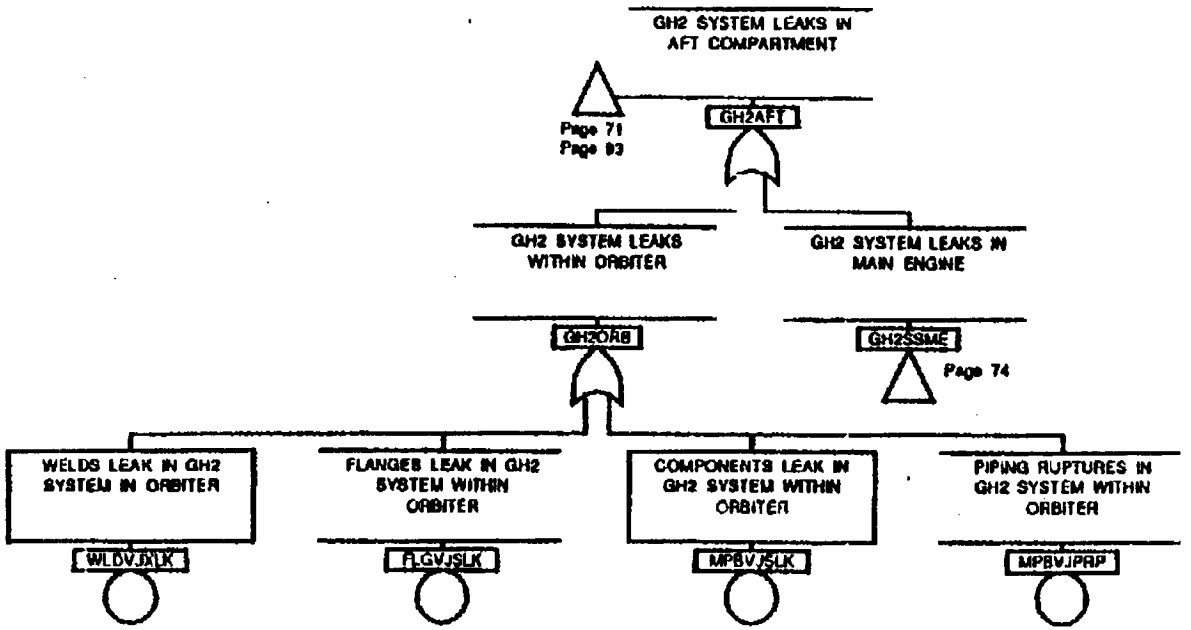


TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 71	1/05/88

69-70
PRECEDING PAGE BLANK NOT FILMED



TITLE

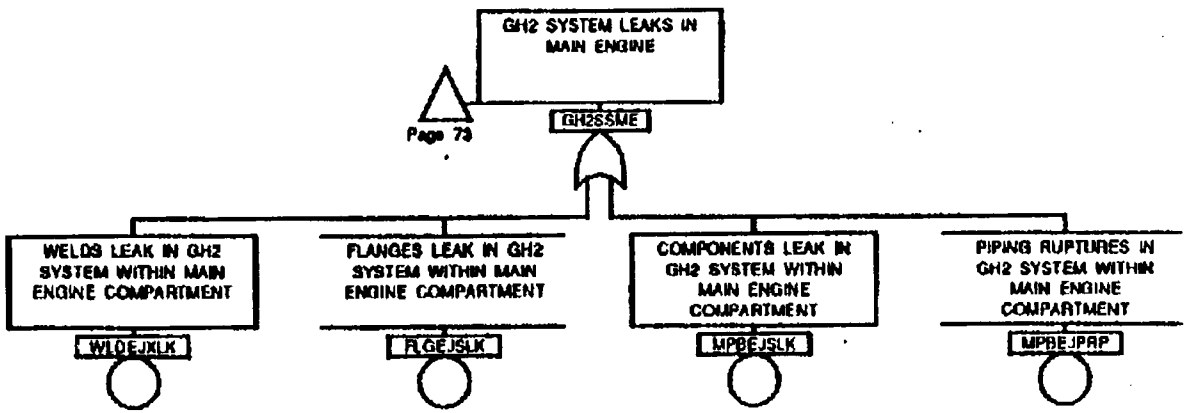
Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER

Page 73

DATE

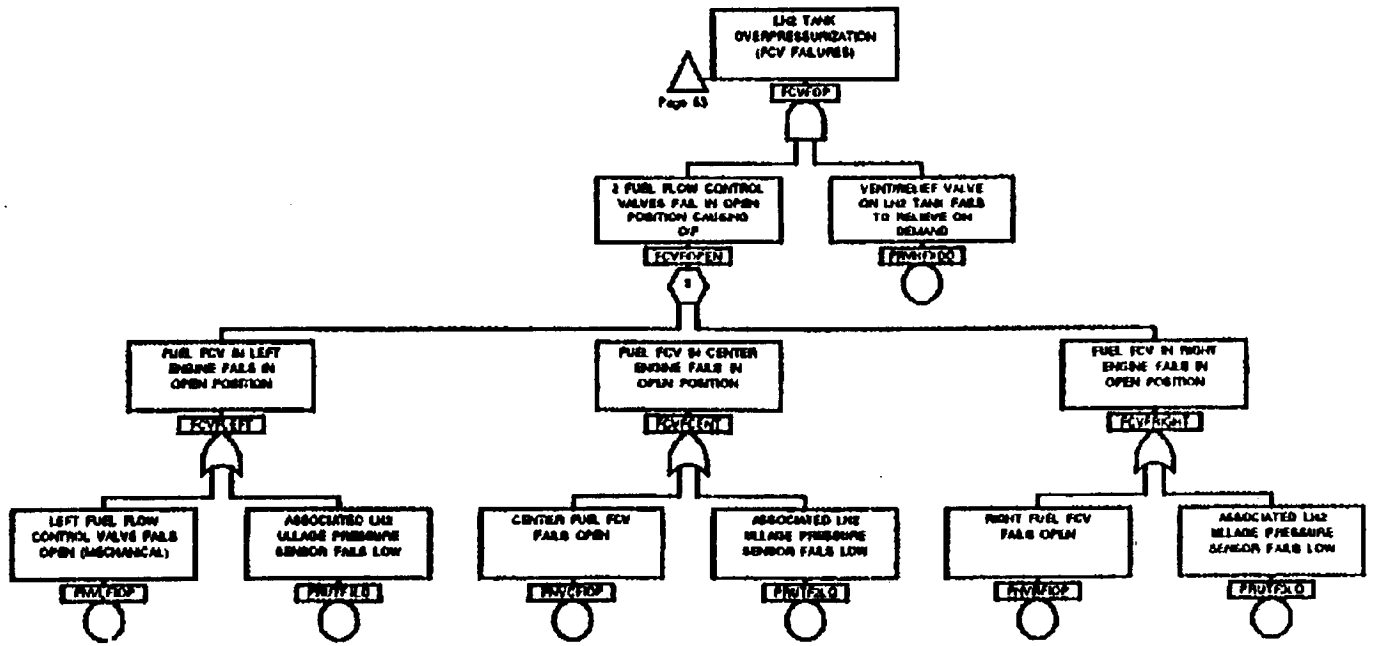
9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 74	9/04/87

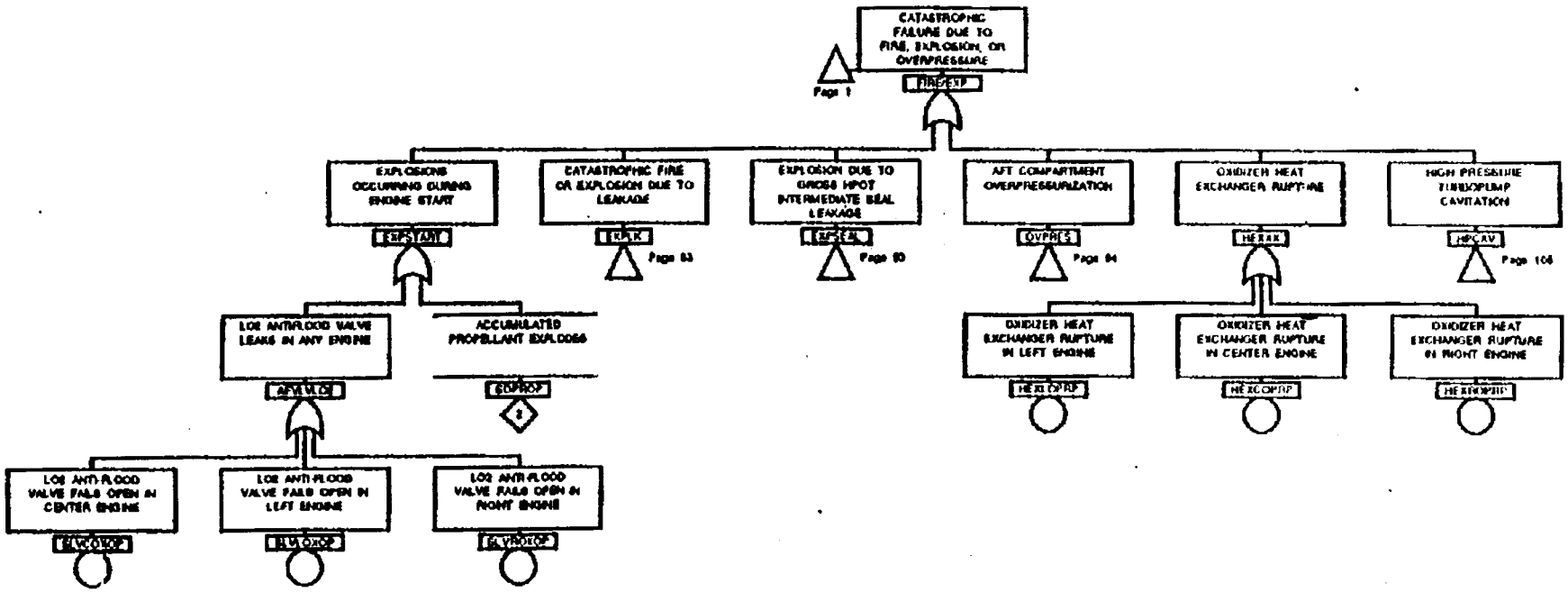


TITLE

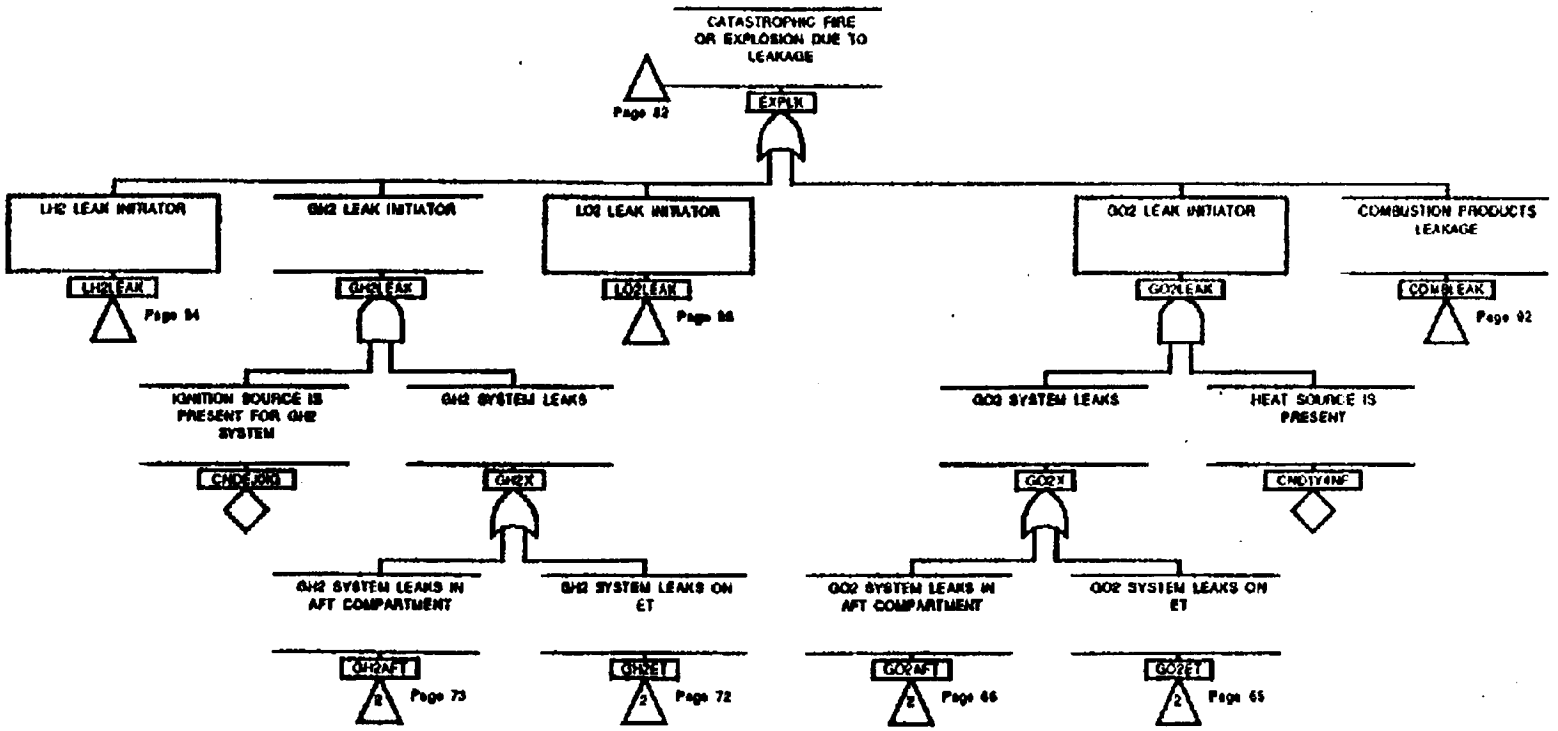
Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 81	9/04/87

PRECEDING PAGE BLANK NOT FILMED



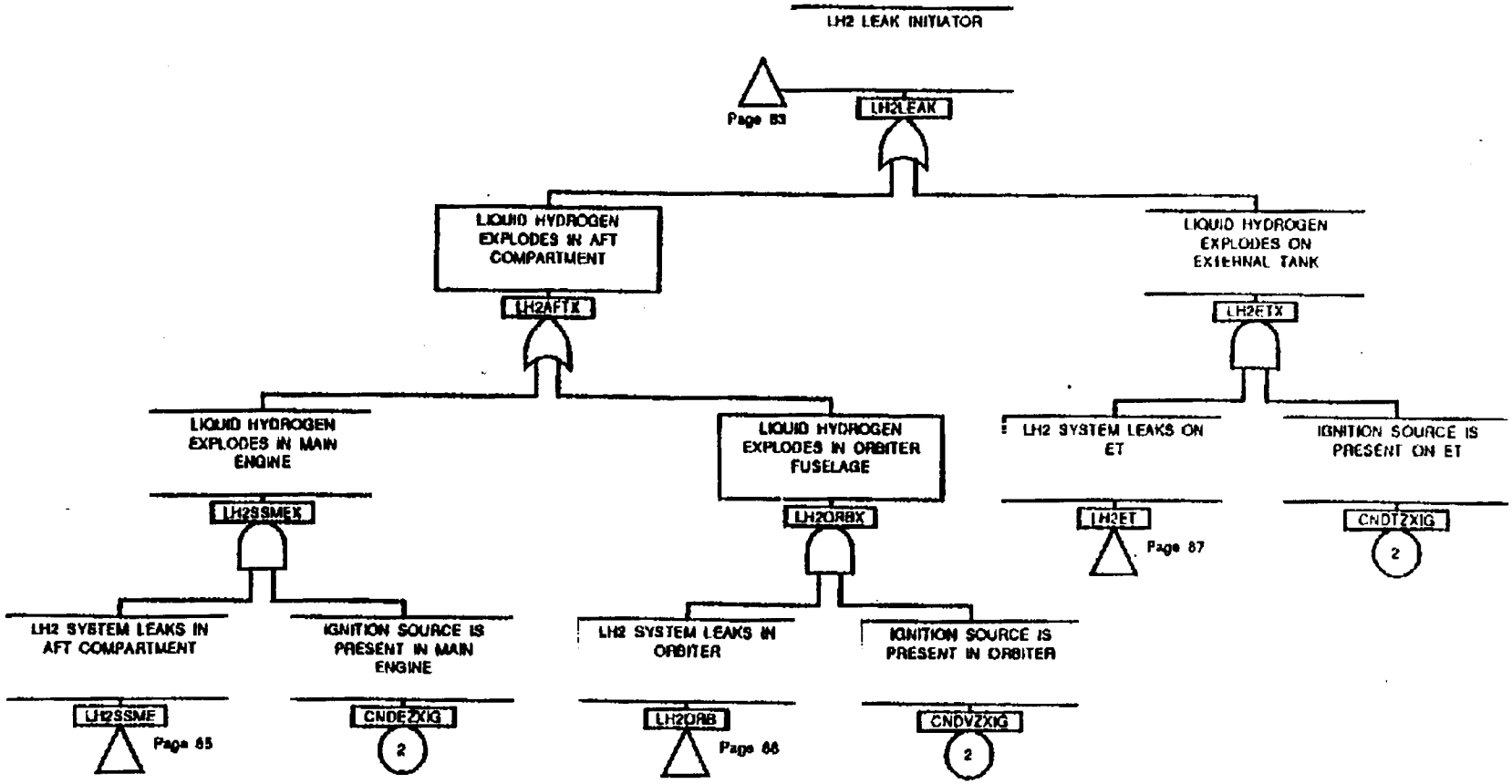
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 82	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

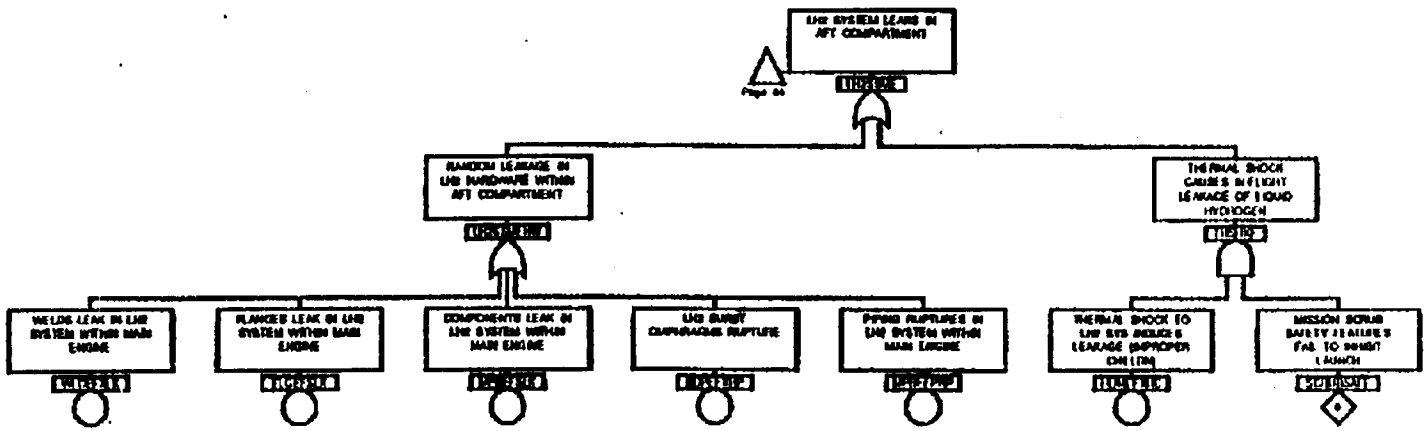
DRAWING NUMBER	DATE
Page 83	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

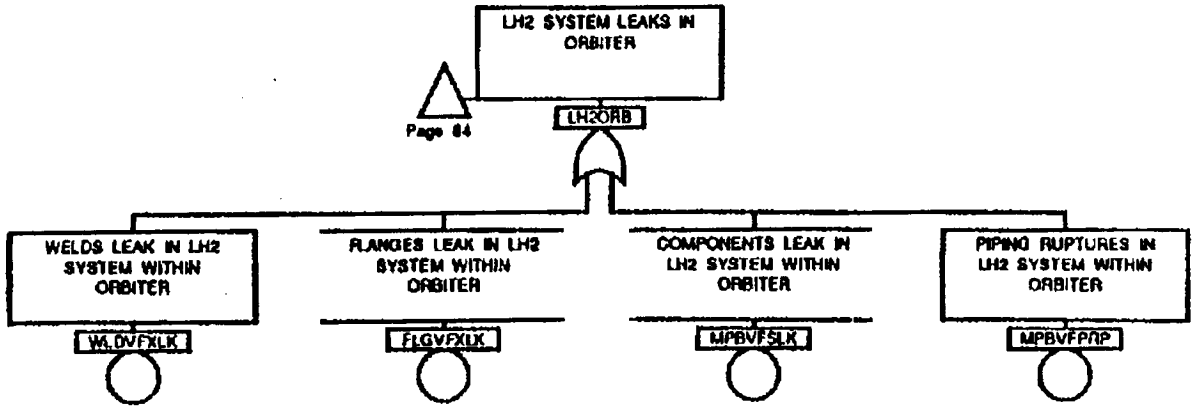
DRAWING NUMBER	DATE
Page 84	9/04/87



TITLE

Figure 3-3: MPPS
FAULT TREE

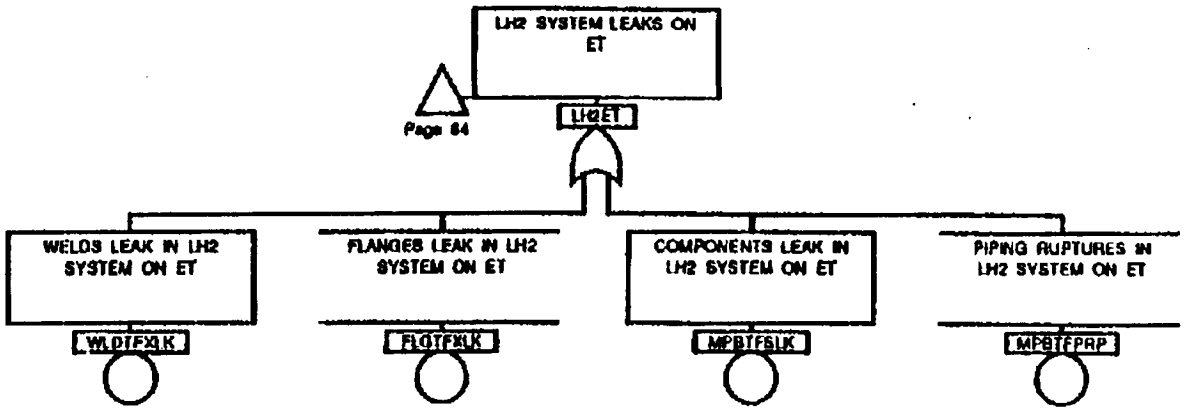
DRAWING NUMBER	DATE
Page 85	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

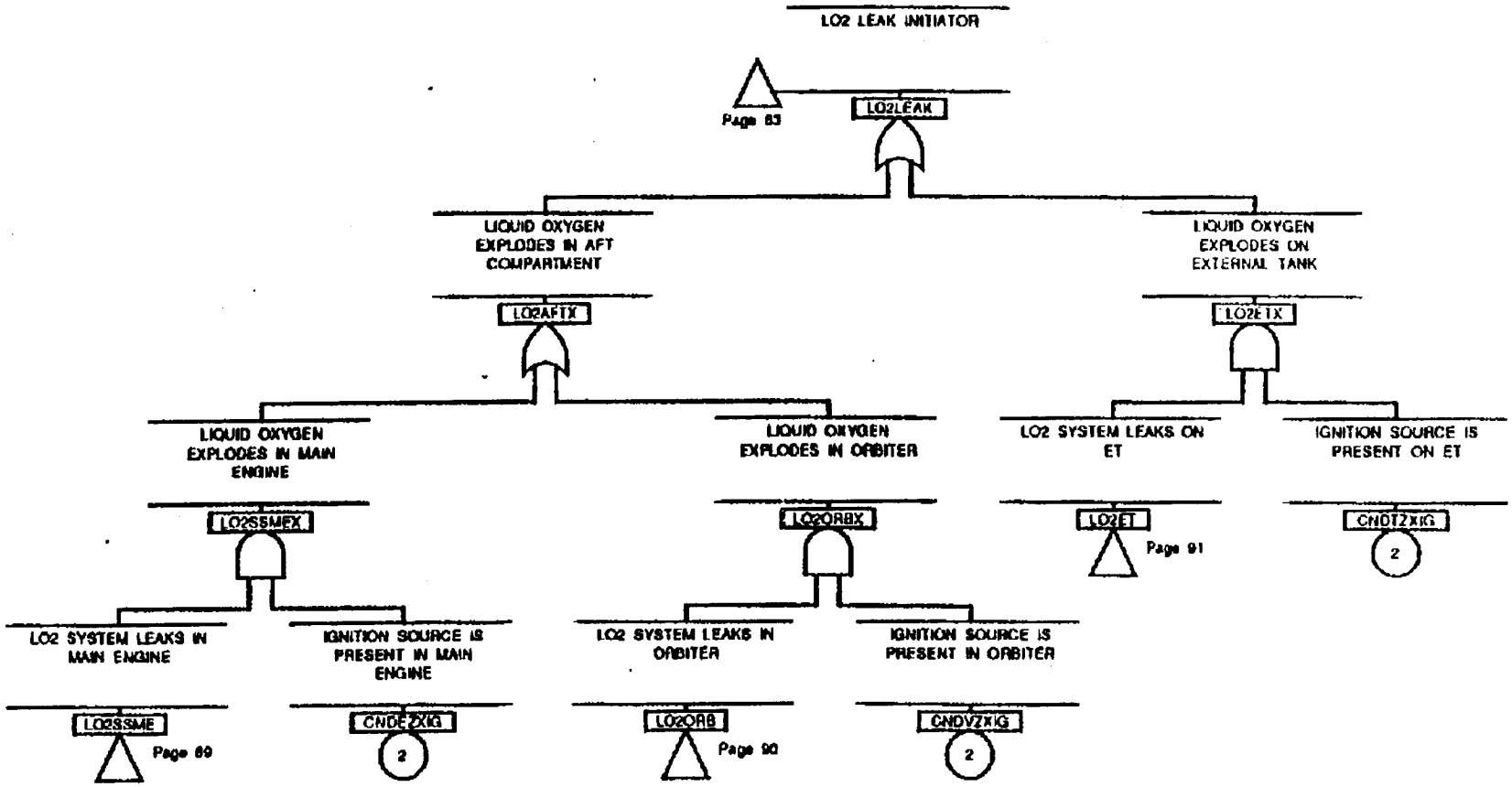
DRAWING NUMBER	DATE
Page 86	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

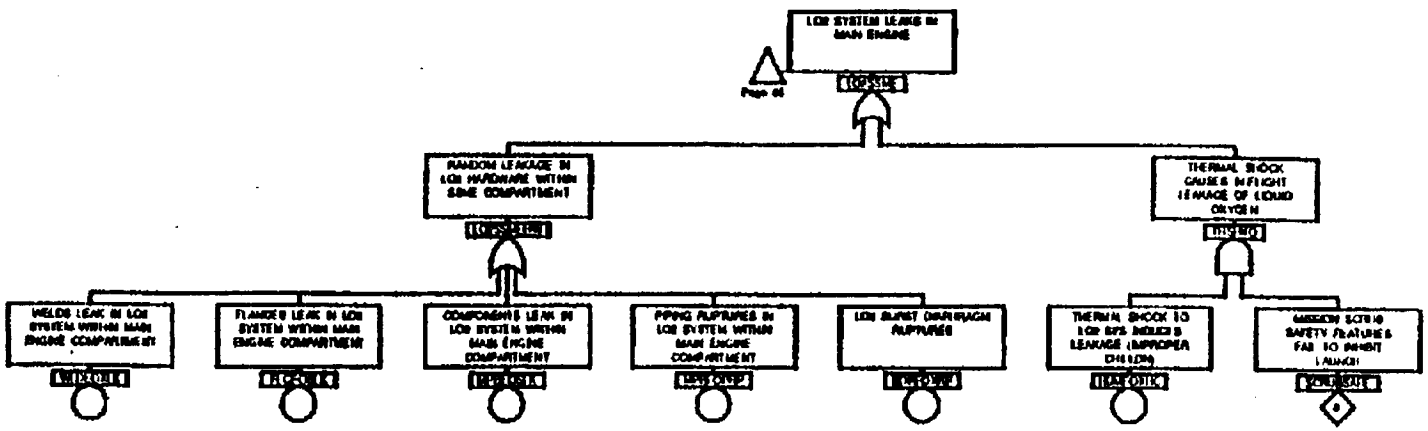
DRAWING NUMBER	DATE
Page 87	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 88	9/04/87



TITLE

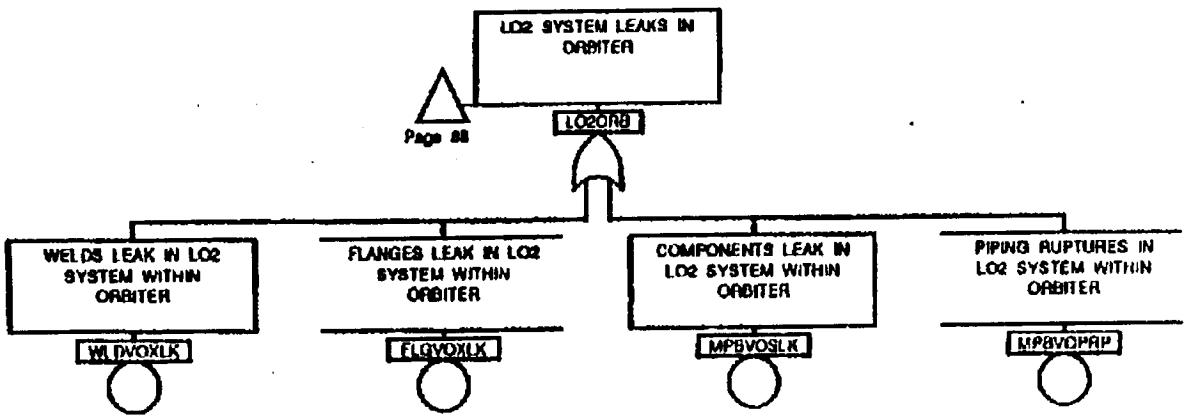
Figure 3-3: MPPS
FAULT TREE

DRAWING NUMBER

Page 89

DATE

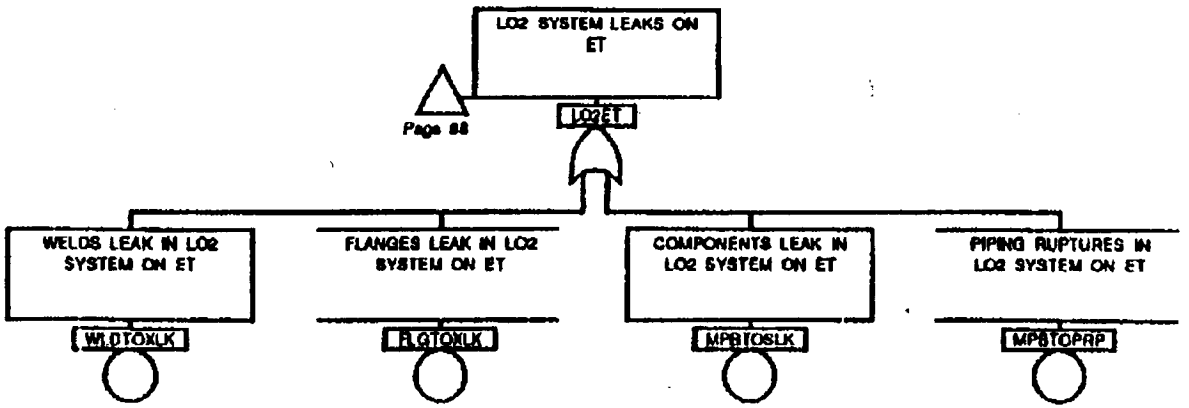
9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

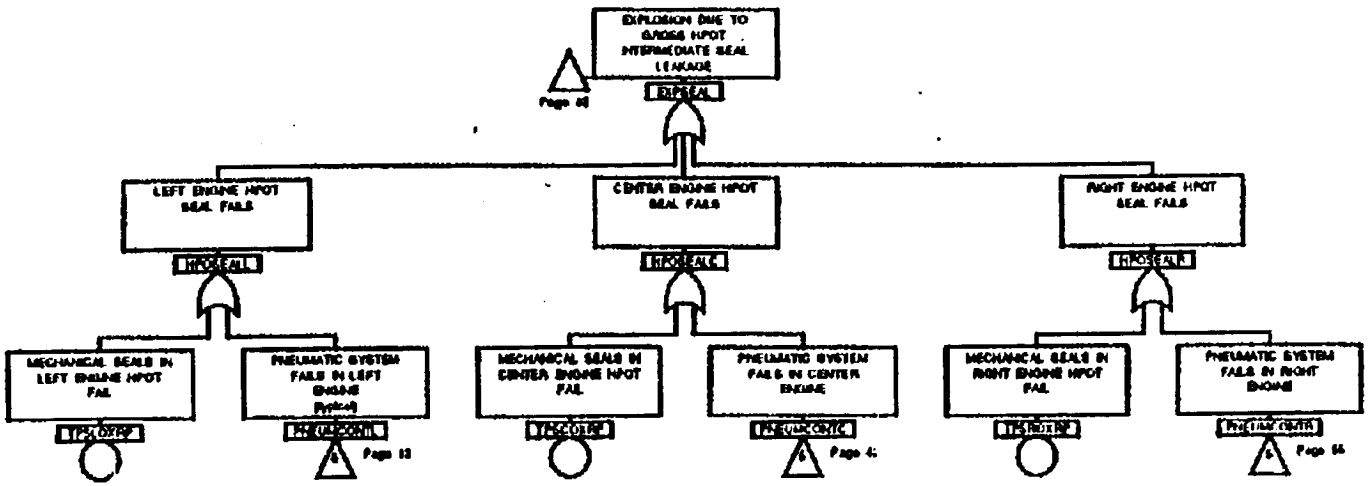
DRAWING NUMBER	DATE
Page 90	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

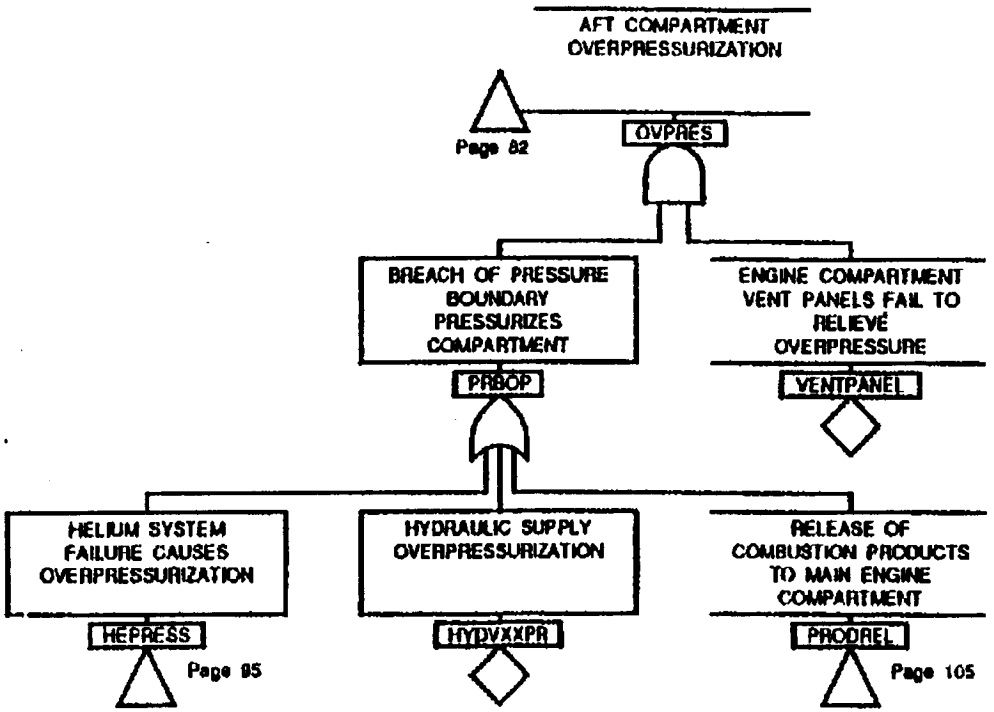
DRAWING NUMBER	DATE
Page 91	9/04/87



TITLE

Figure 3-3: MPPS
FAULT TREE

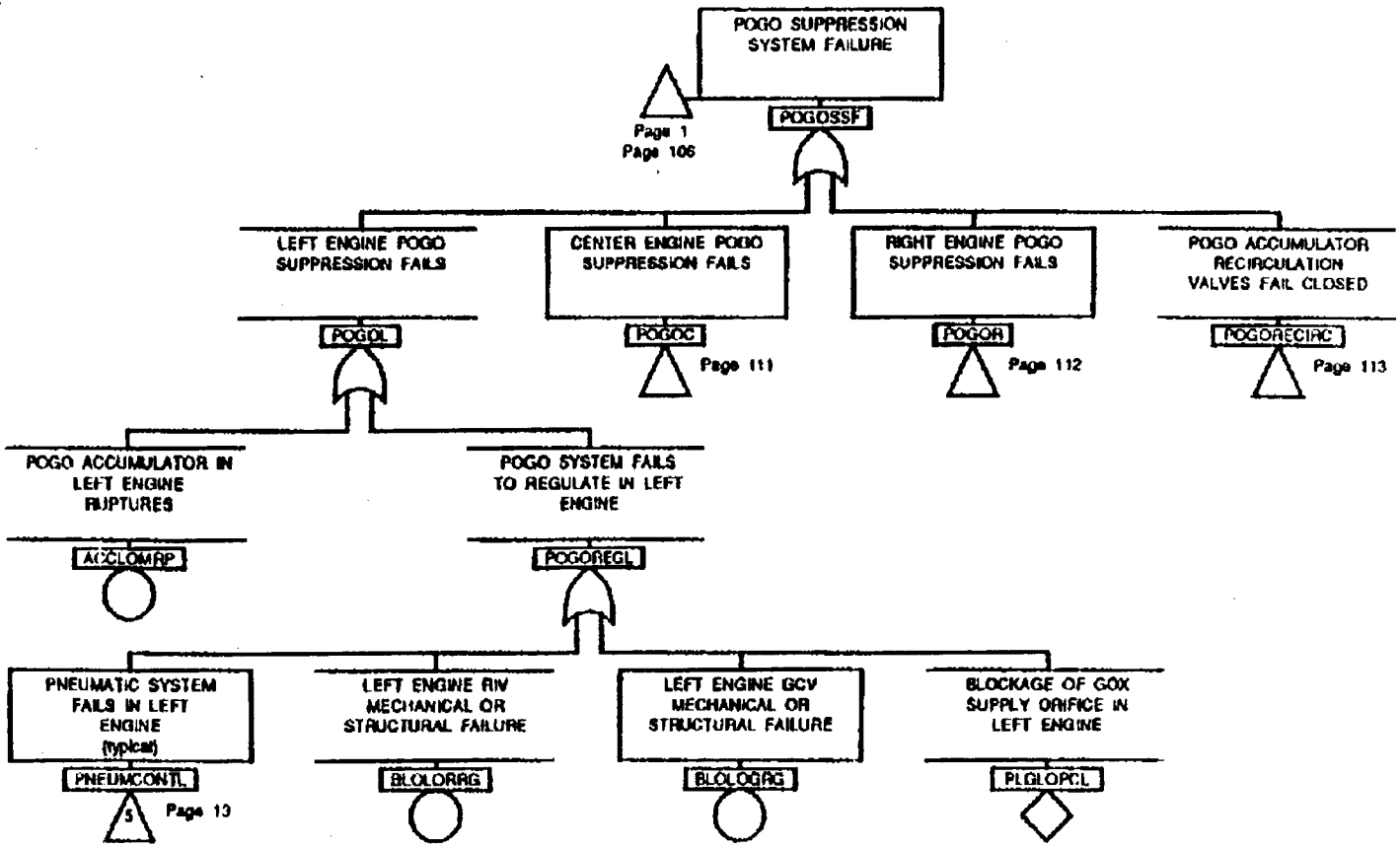
DRAWING NUMBER	DATE
Page 93	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 94	9/04/87

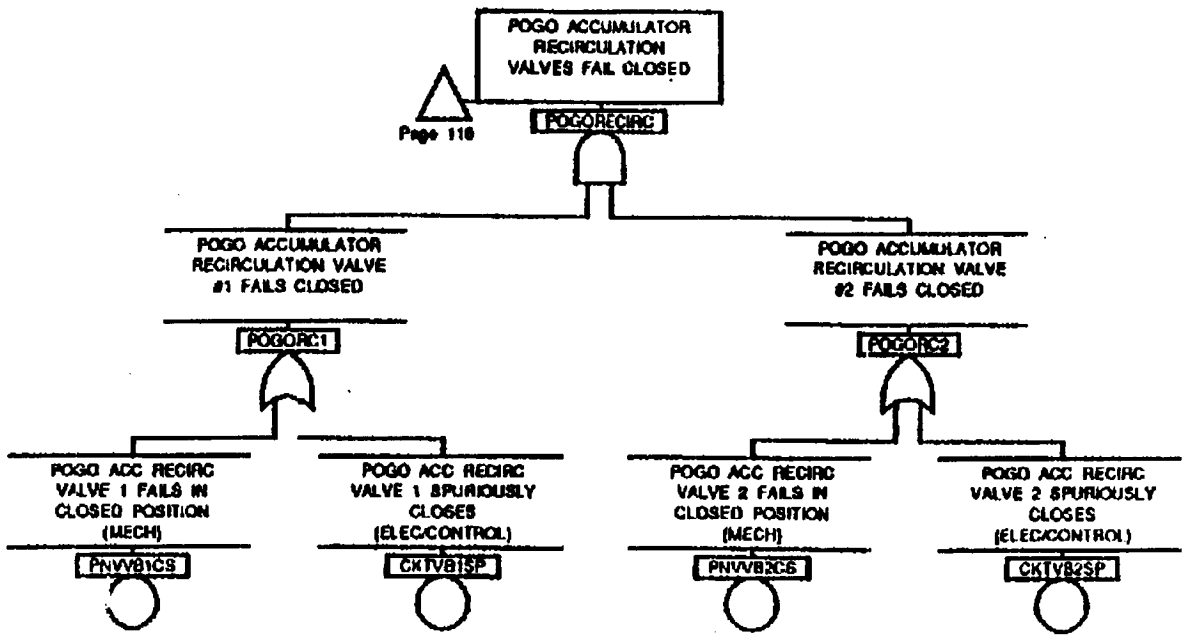


TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 110	9/04/87

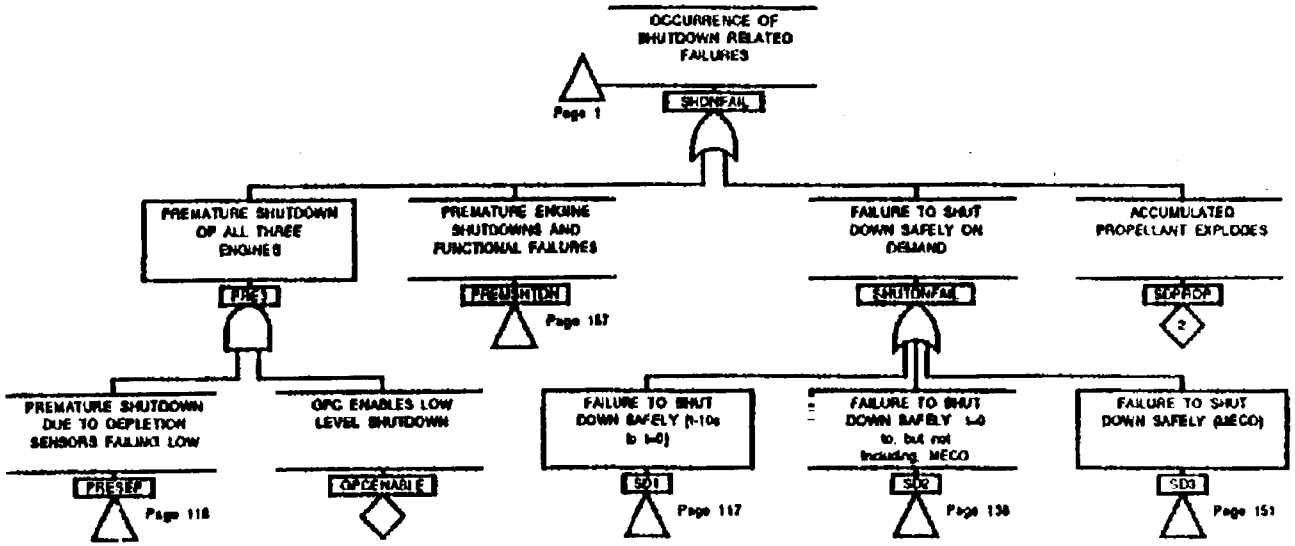
PRECEDING PAGE BLANK-NOT FILMED MISSING



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER Page 113	DATE 9/04/87

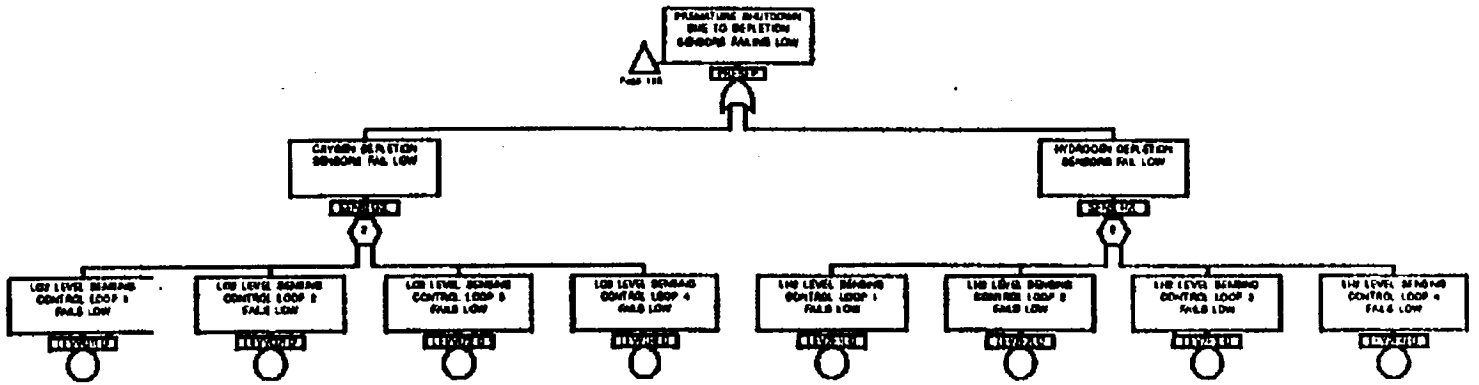
PRECEDING PAGE BLANK NOT FILMED

MISSING



MISSING PRECEDING PAGE BLANK NOT FILMED

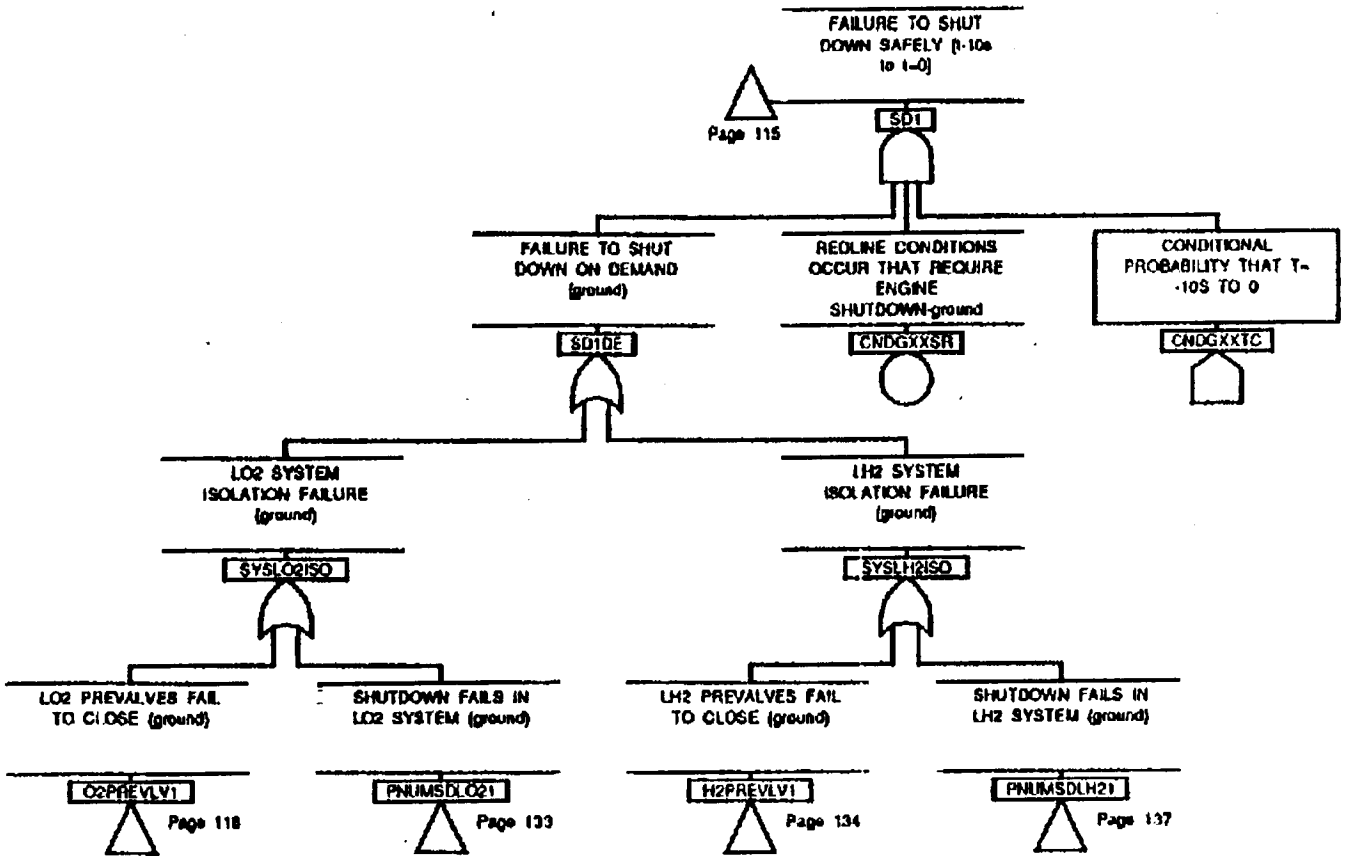
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 115	9/04/87



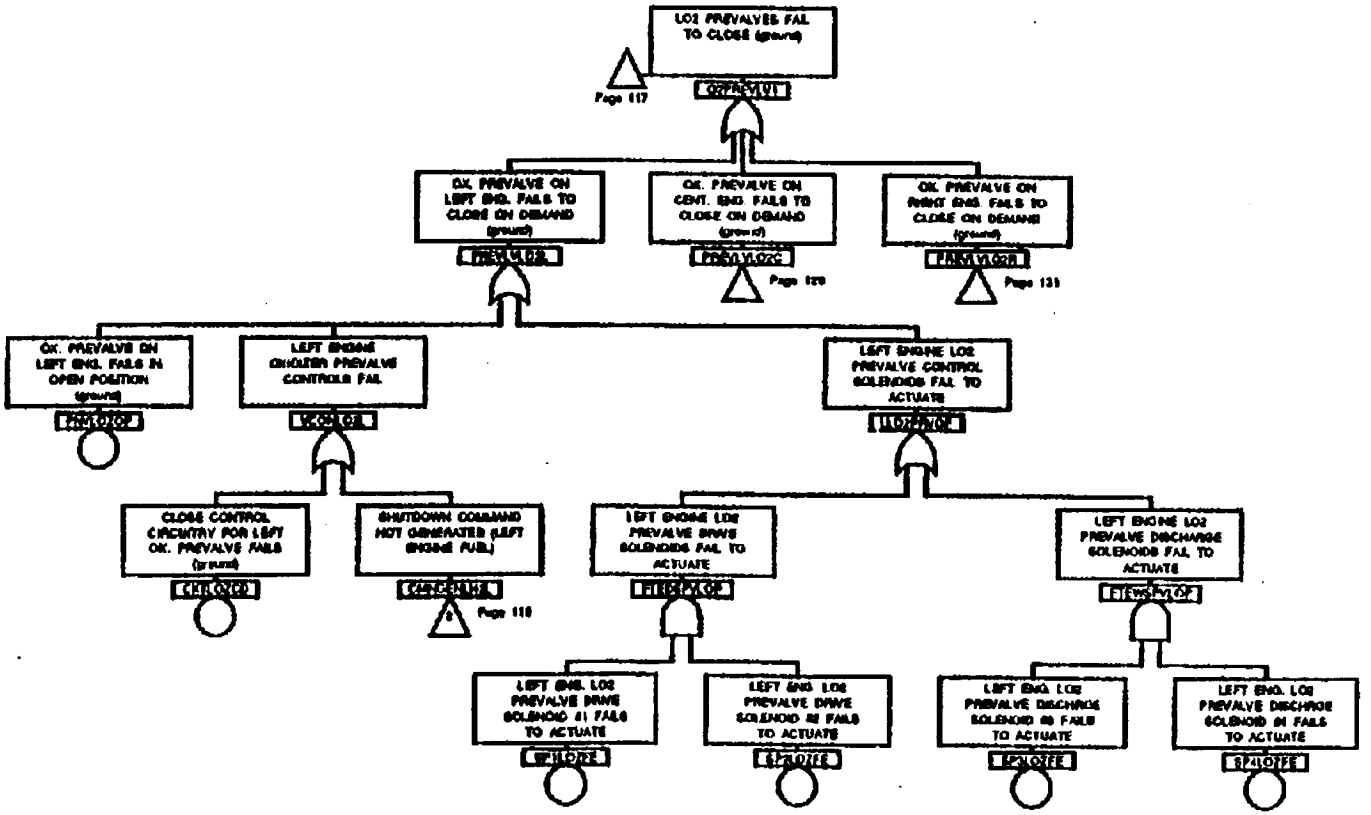
TITLE

Figure 3-3: MPPS
FAULT TREE

DRAWING NUMBER	DATE
Page 116	9/04/87



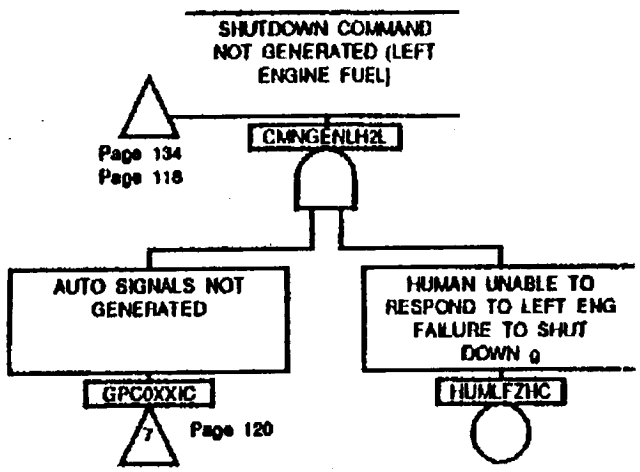
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 117	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 118	1/05/88



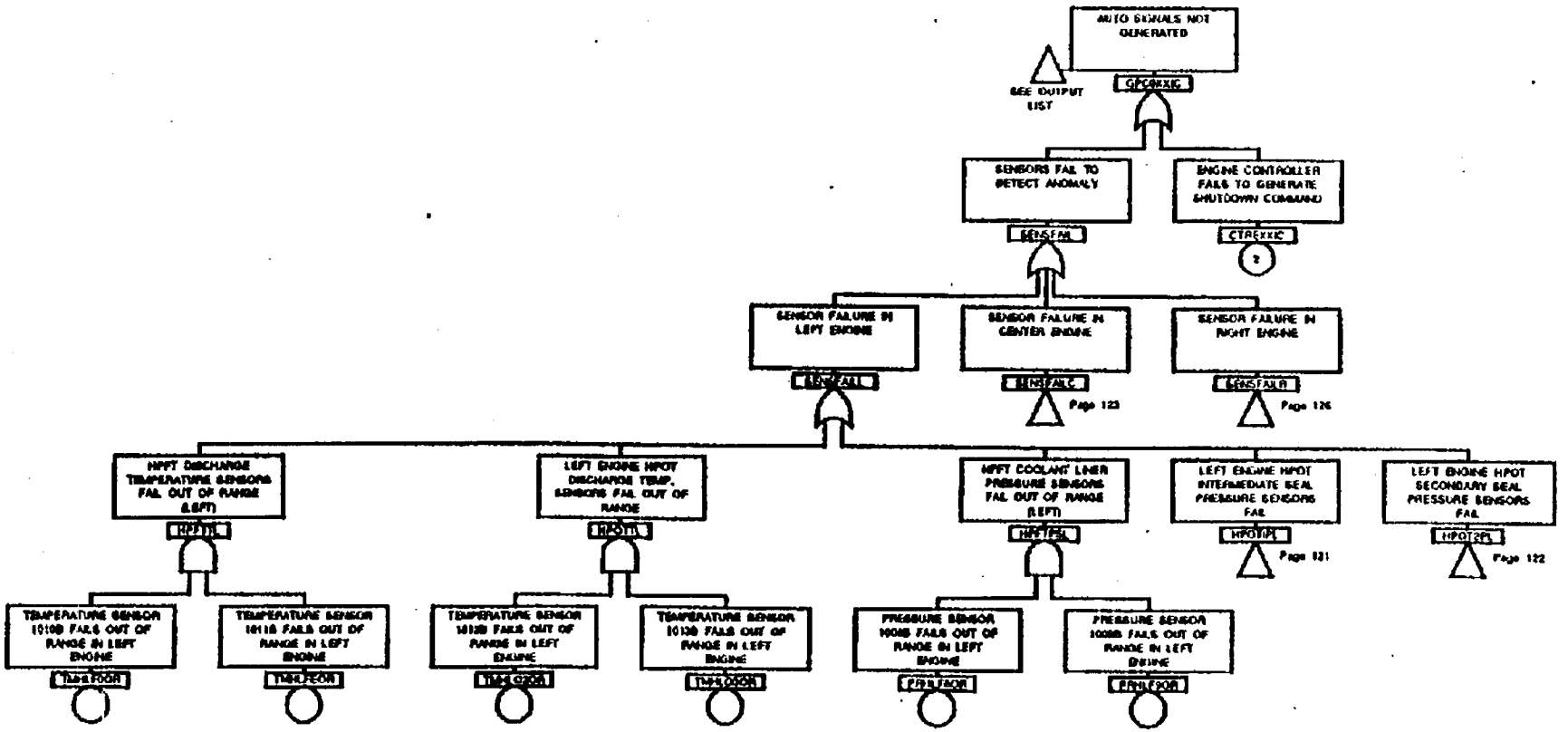
TITLE

Figure 3-3: MPPS FAULT TREE

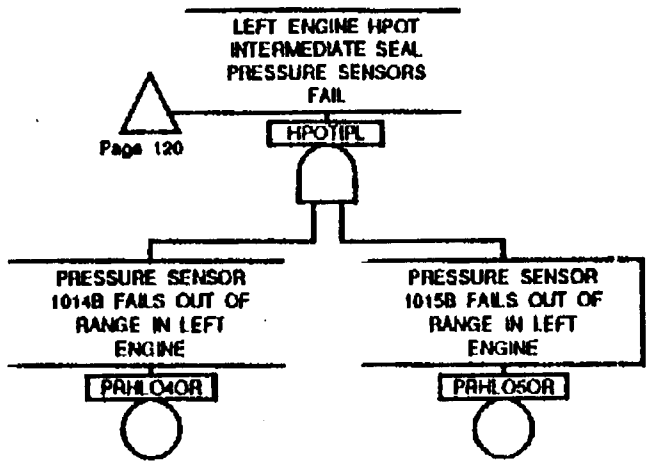
DRAWING NUMBER	DATE
Page 119	9/04/87

GPC0XXIC OUTPUTS:
Page 119, Page 130, Page 132
Page 150, Page 141, Page 143
Page 145

LMSC-F2230402



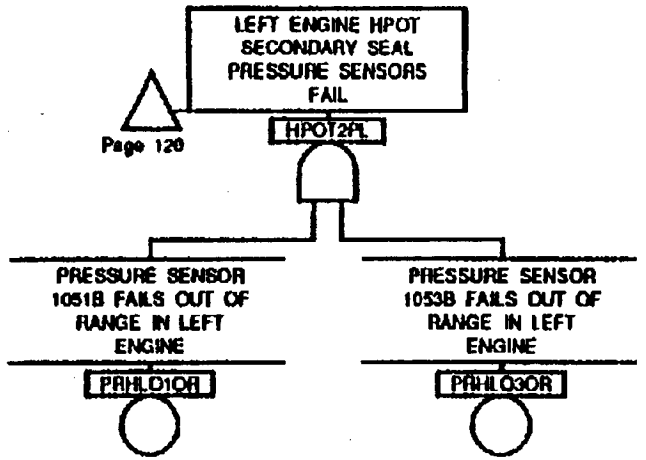
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 120	9/04/87



TITLE

Figure 3-3: MPPS
FAULT TREE

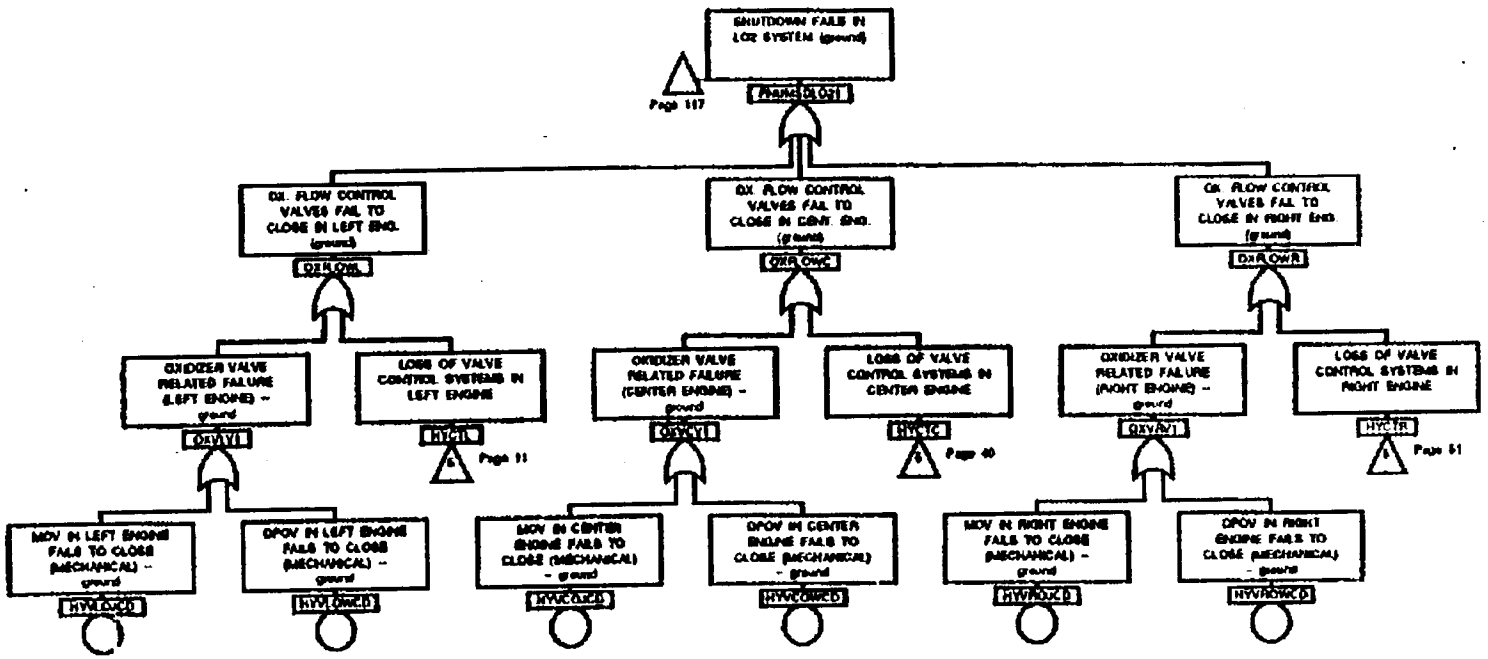
DRAWING NUMBER	DATE
Page 121	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

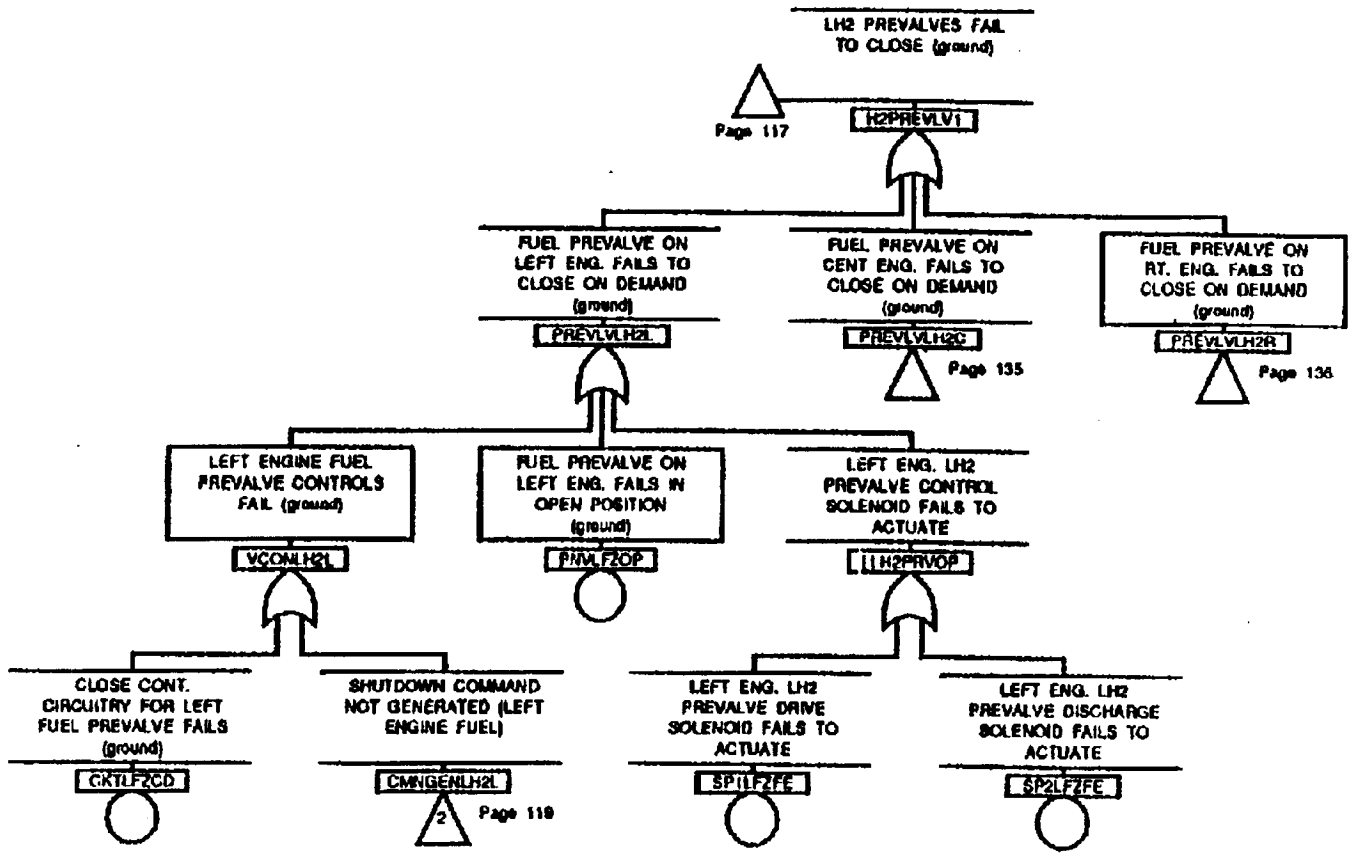
DRAWING NUMBER	DATE
Page 122	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

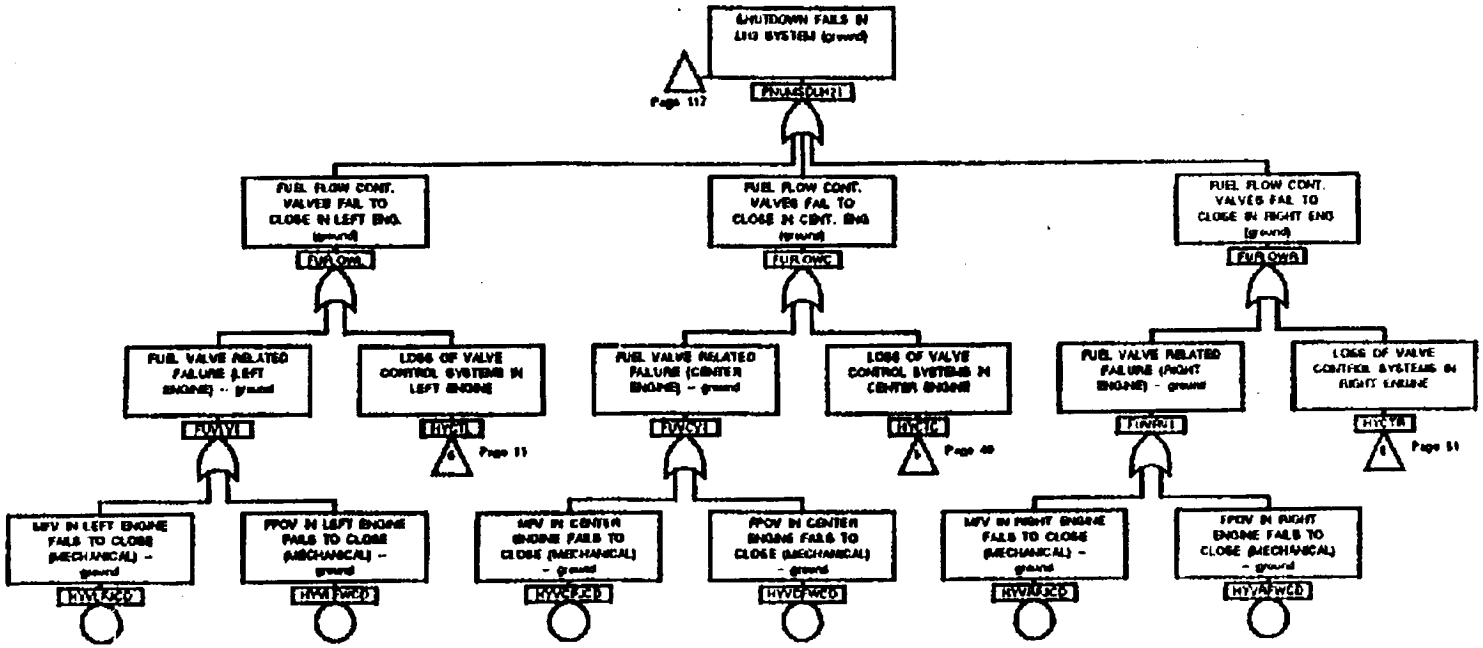
DRAWING NUMBER	DATE
Page 133	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 134	1/05/88



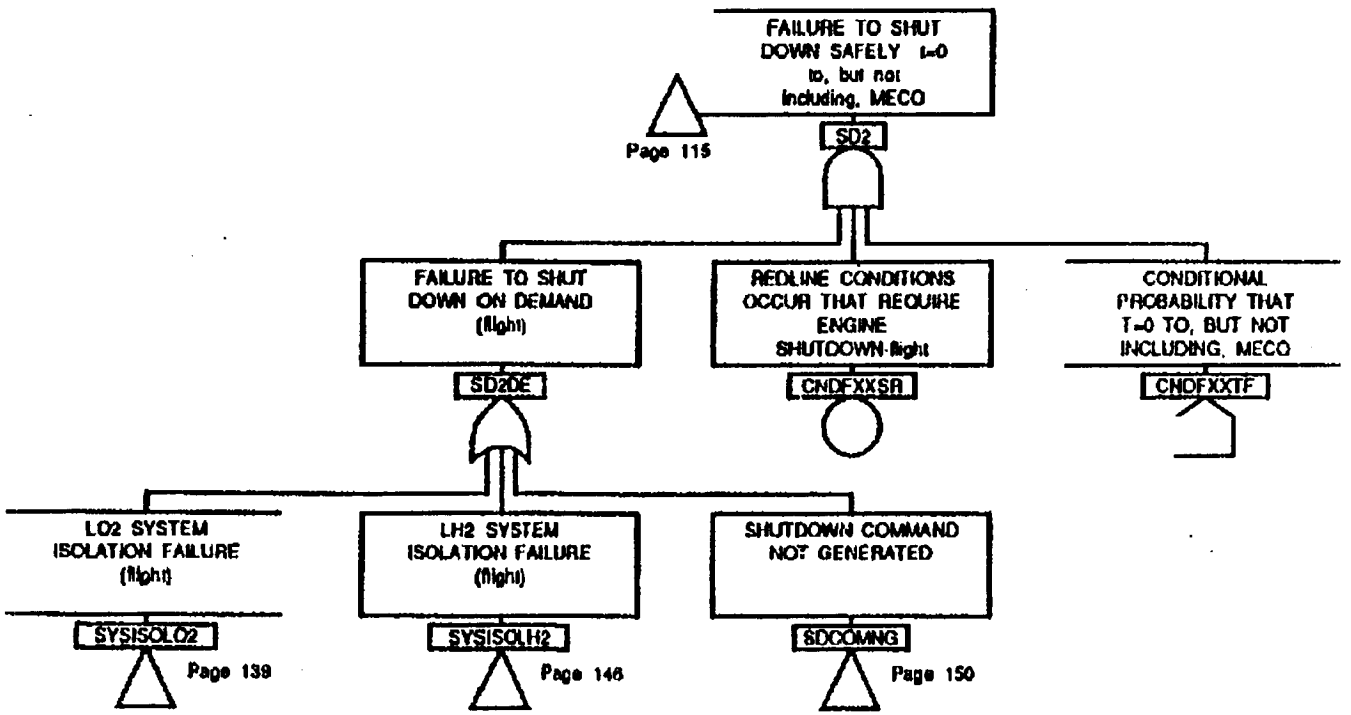
TITLE

Figure 3-3: MPPS FAULT TREE

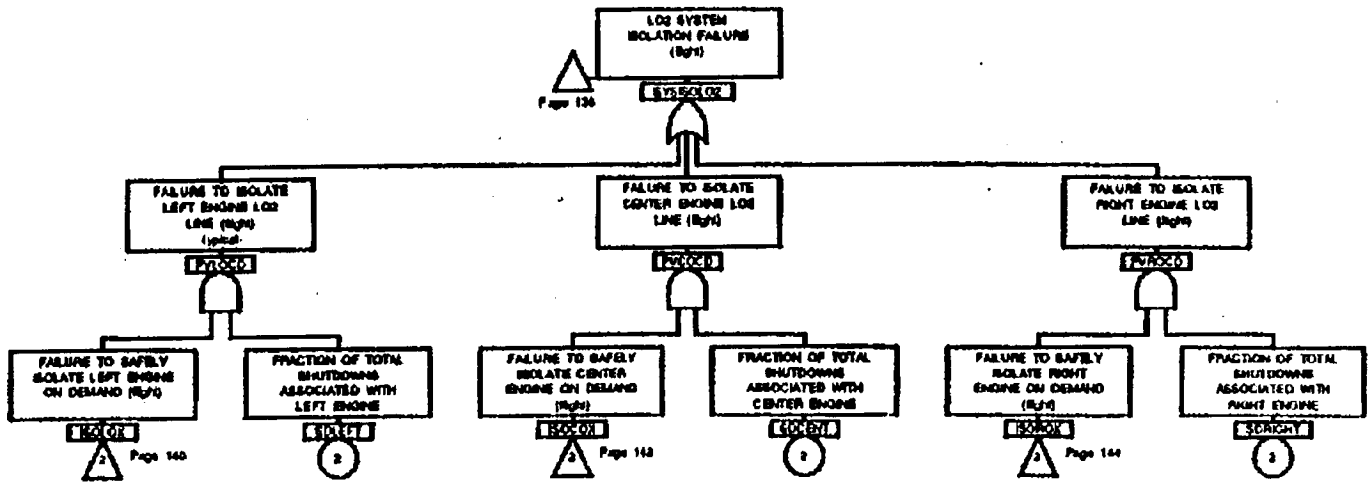
DRAWING NUMBER	DATE
Page 137	9/04/87

PRECEDING PAGE BLANK NOT FILMED

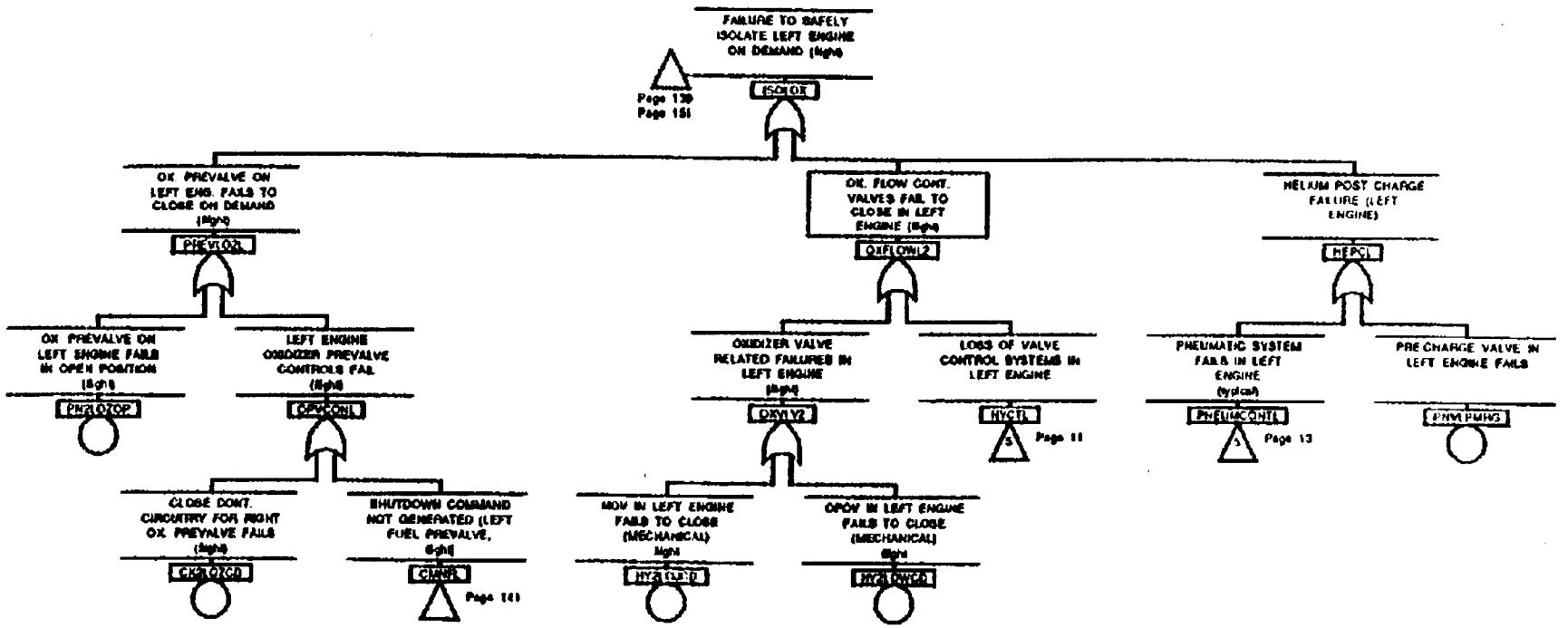
MISSING



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 138	9/04/87



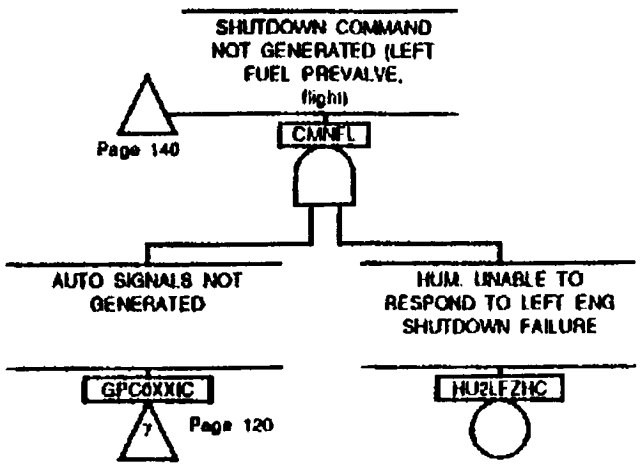
TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 139	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

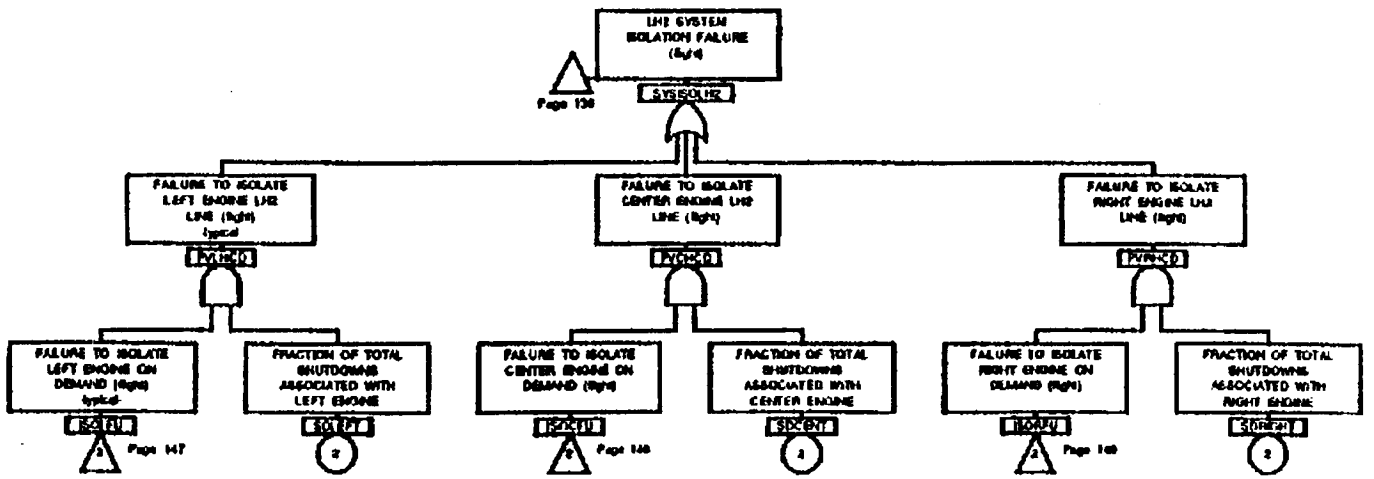
DRAWING NUMBER	DATE
Page 140	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

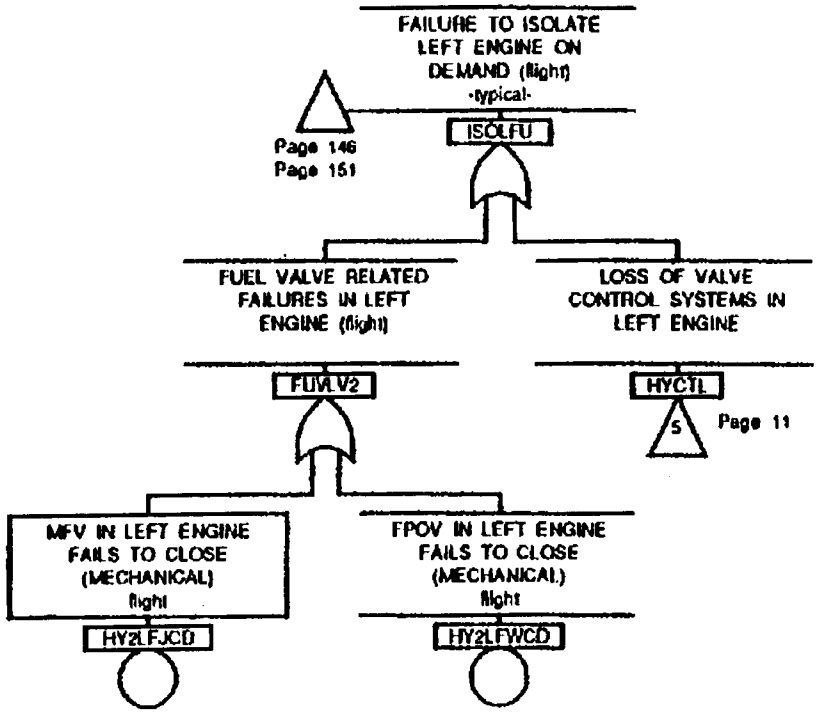
DRAWING NUMBER	DATE
Page 141	9/04/87



TITLE

Figure 3-3: MPPS
FAULT TREE

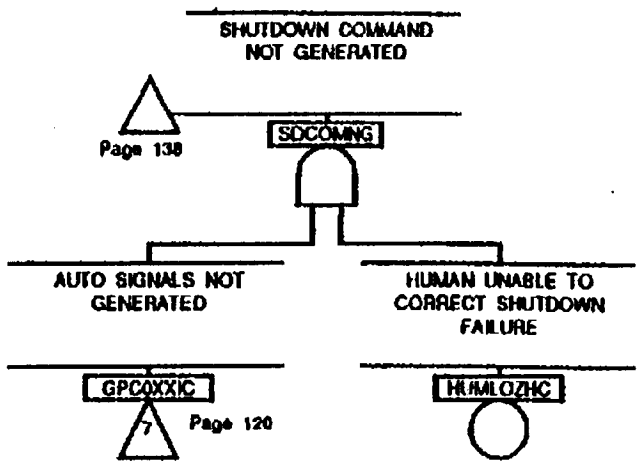
DRAWING NUMBER	DATE
Page 146	9/04/87



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 147	9/04/87

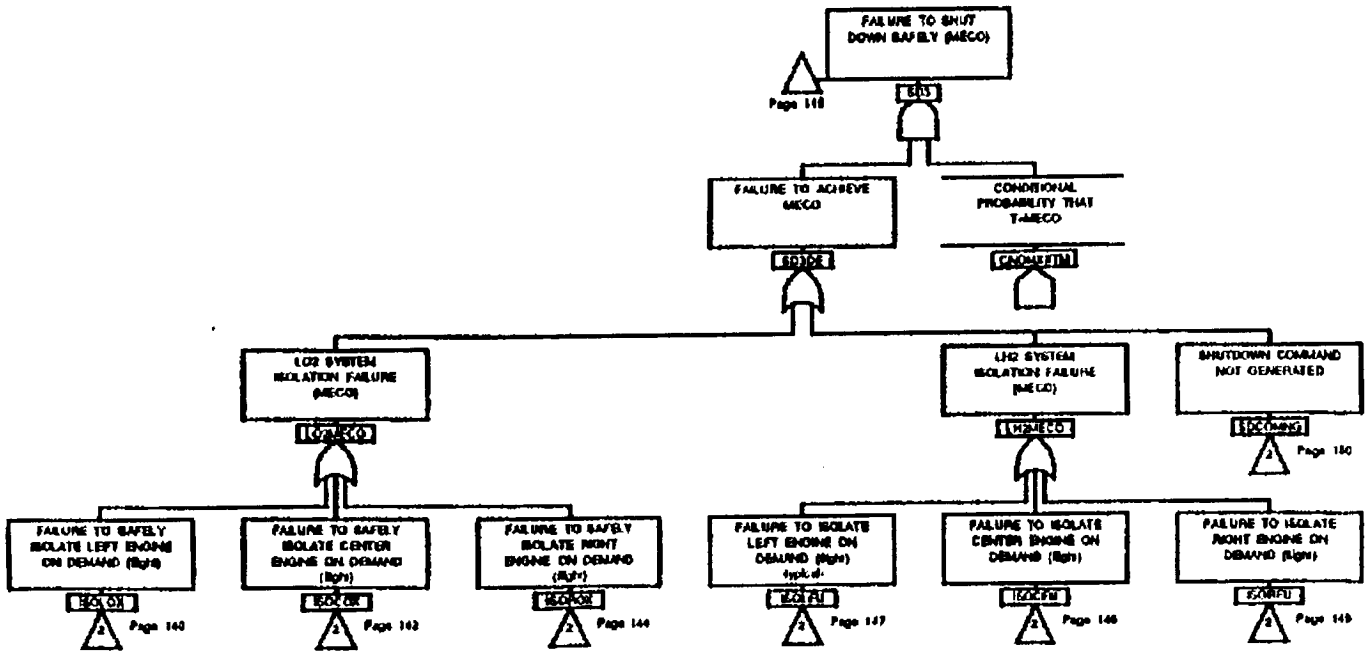


TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 150	9/04/87

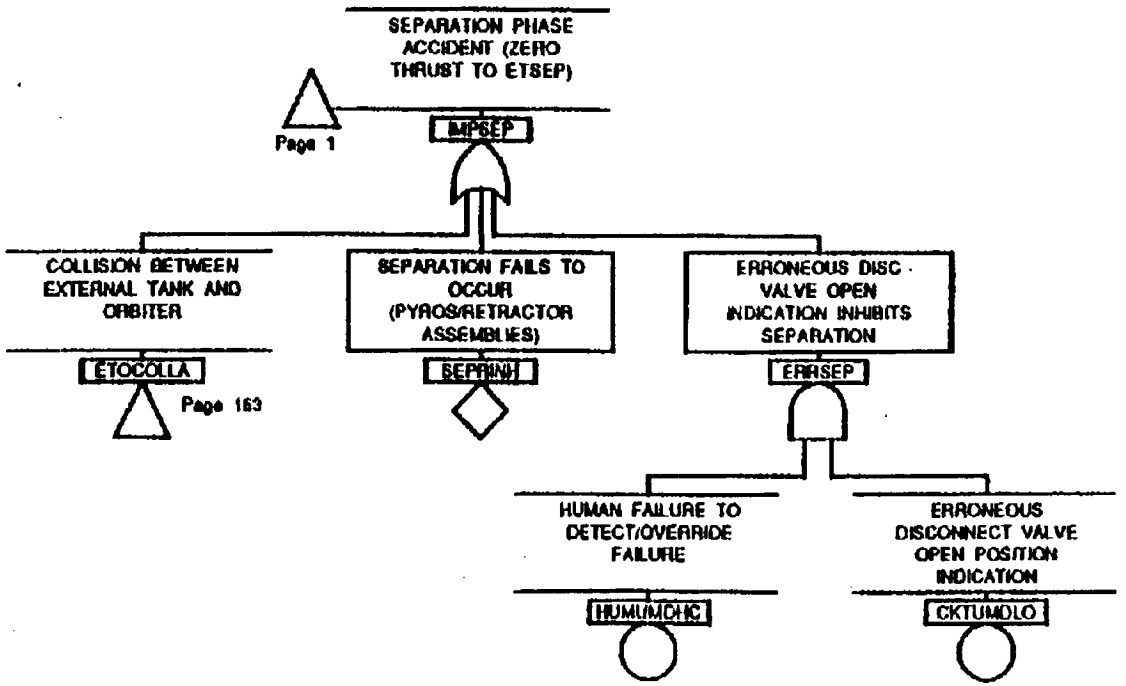
PRECEDING PAGE BLANK NOT FILMED MISSING



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 151	1/05/88



TITLE

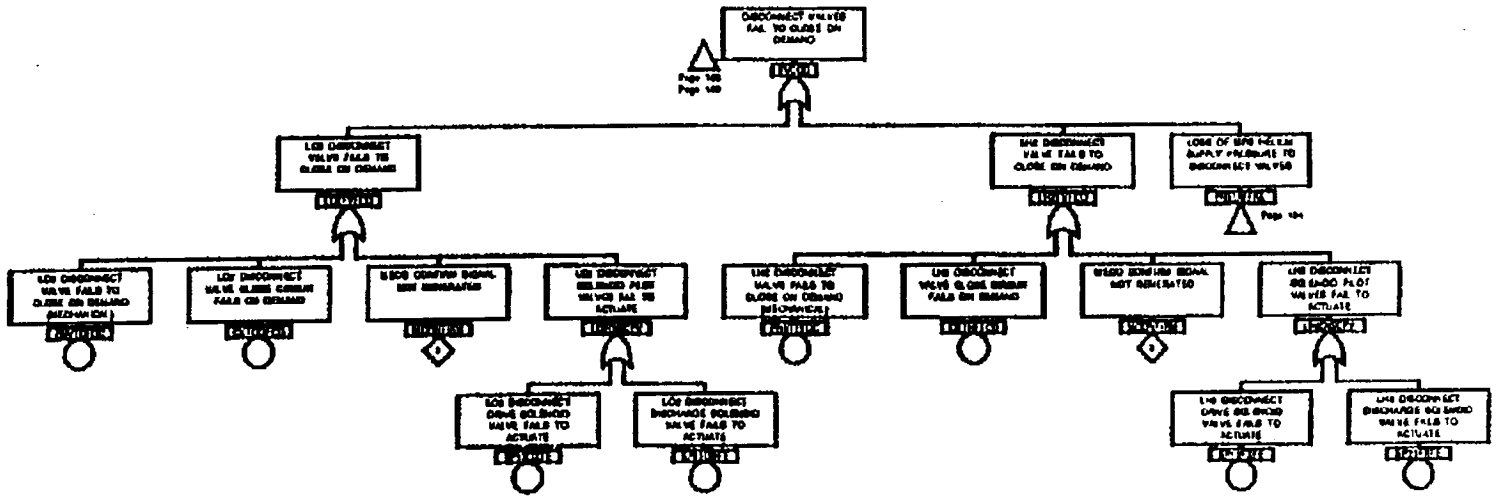
Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER

Page 152

DATE

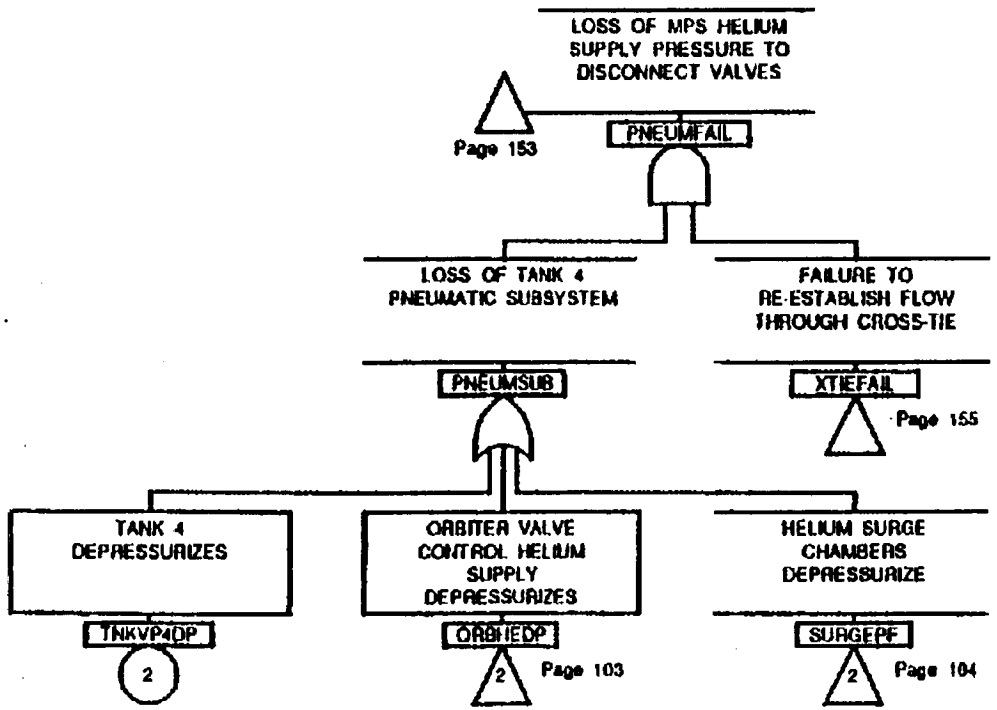
1/05/88



TITLE

Figure 3-3: MPPS FAULT TREE

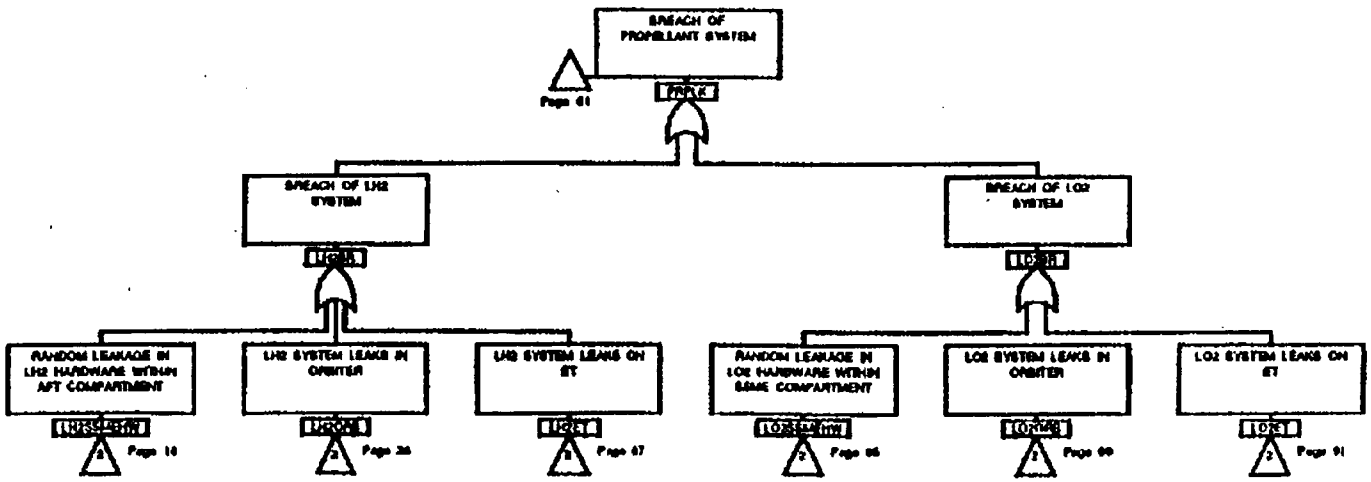
DRAWING NUMBER	DATE
Page 153	1/05/88



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 154	9/04/87

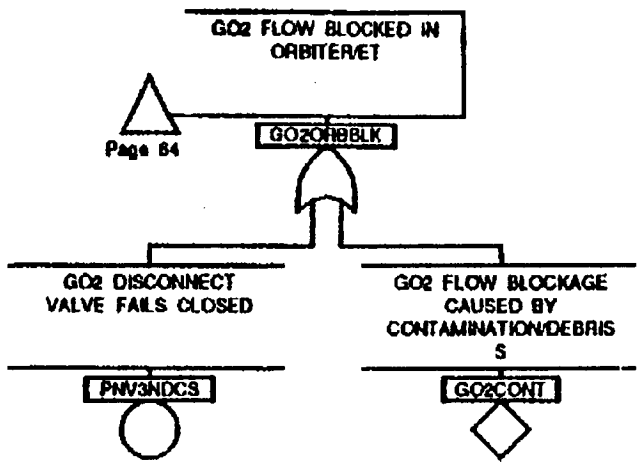


TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 156	1/05/88

PRECEDING PAGE BLANK NOT FILMED



TITLE

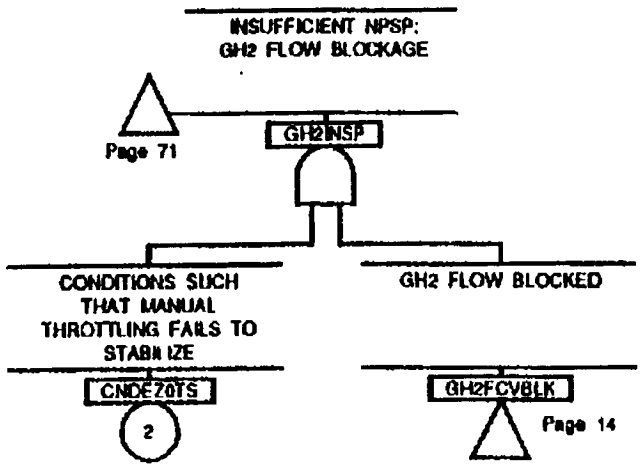
Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER

Page 161

DATE

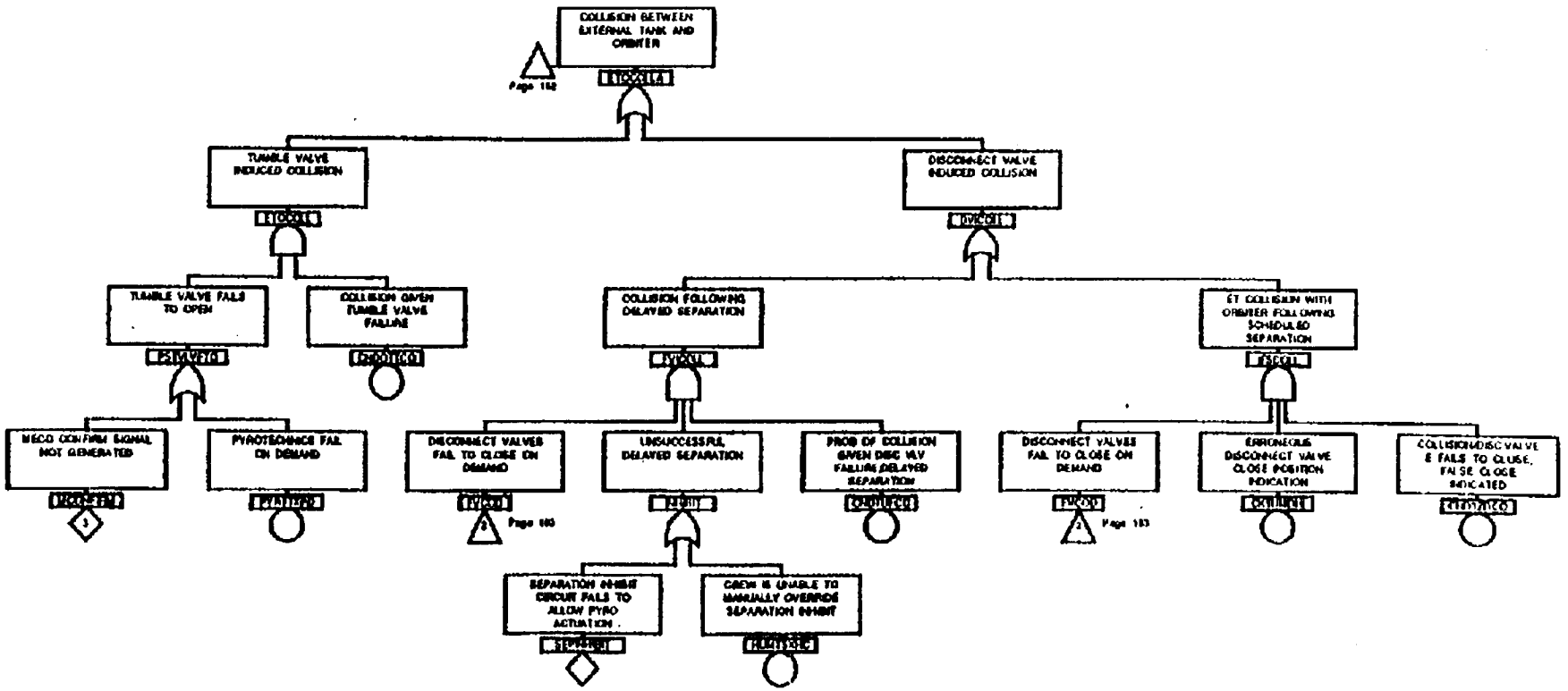
1/05/88



TITLE

Figure 3-3: MPPS FAULT TREE

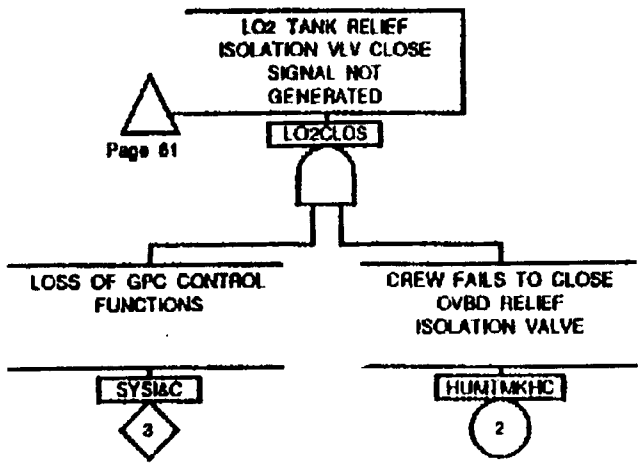
DRAWING NUMBER	DATE
Page 162	1/05/88



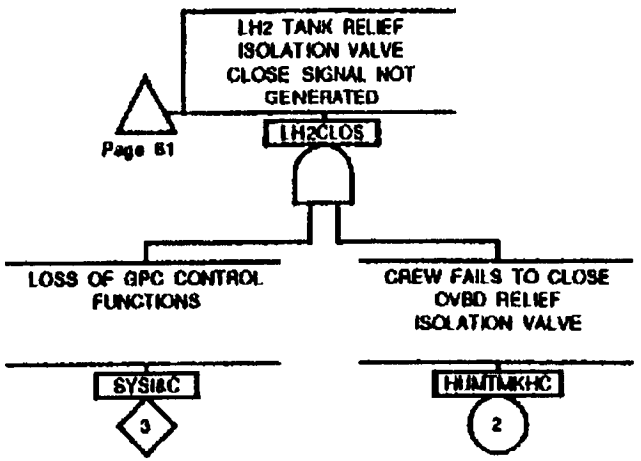
TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 163	1/05/88



TITLE	
Figure 3-3: MPPS FAULT TREE	
DRAWING NUMBER	DATE
Page 165	1/05/88



TITLE

Figure 3-3: MPPS FAULT TREE

DRAWING NUMBER	DATE
Page 166	1/05/88

NOTE:

FIGURE 3-3 IS AN EDITED VERSION OF THE FAULT TREE CONTAINING ALL ESSENTIAL BRANCHES.

IF FURTHER DETAIL IS REQUIRED, FIGURE D-2 (EXPANDED FAULT TREE) SHOULD BE CONSULTED.

NOTES TO FIGURE 3-4

Valve Schematic Designation	Fault Tree Mnemonic	Description of Basic Event or Gate
Tumble Valve	PYRTTXPD	Pyrotechnics on tumble valve fail to open the tumble valve at the time of ET separation. This basic event includes only pyrotechnic assembly failures and not the actuation circuitry failures.
Vent Relief	PRVOOXOP PRVHFXOP	Vent valve on external tank opens and sticks open. This mechanical malfunction depressurizes the tanks.
	PRVHFXDO PRVOOXDO	Vent valves on external tanks fail to open when ullage pressure is too high, resulting in overpressurization of the tank and hydrodynamic instabilities in the propellant lines.
OB DISC (PD1) **IB DISC (PD1)**	PNVTOFDC	LO2 flapper valve failure to close on demand (i.e. mechanical failure of valve actuators) causes a possible collision between external tank and orbiter. Pneumatic supply or control system failures which prevent valve from closing are not part of this basic event.
OB DISC (PD2) **IB DISC (PD2)**	PNVTFFDC	LH2 disconnect valve failure to close on demand (i.e. mech. failure of valve actuators) causes a possible collision between external tank and orbiter. Pneumatic supply or control system failures which prevent valve from closing are not part of this basic event.
OB DISC **IB DISC**	PNV3FDCS PNV3ODCS	LH2 or LO2 disconnect valve fails in closed position due to mechanical causes, resulting in blockage of the corresponding propellant flow path.
FLOW CTRL LV54, LV52	PNVCOICS PNVLOICS PNVROICS PNVCFICS PNVLFICS PNVRFICS	Tank ullage pressure (flow) control valves fail in the closed or partially closed position, restricting the pressurization flow from the engines to the external propellant tanks. This mechanical failure is associated with the flow control valves or their actuators. These basic events do not include spurious control signals which cause the valves to close.
	PNVCOICD PNVLOICD PNVROICD	Tank ullage pressure (flow) control valves fail to close when required (e.g. due to overpressure conditions). This pressure regulation failure occurs due to mechanical causes associated with the flow control valves or their actuators. These basic events do not include spurious control signals which cause the valves to close.

NOTES TO FIGURE 3-4

Valve Schematic Designation	Fault Tree Mnemonic	Description of Basic Event or Gate
RIV	PNYVB1CS PNYVB2CS	Pogo accumulator recirculation valves fail in the closed position so as to prevent LO2 from recirculating. These basic events represent mechanical malfunctions associated with the valve and valve actuator. Spurious control signals which force the valve to close are treated separately. Note: failure to establish recirculation flow is assumed to cause pogo accumulator flooding and subsequent loss of pogo suppression subsystem.
PV2	PN2COZOP PNVCOZOP PN2LOZOP PNVLOZOP PN2ROZOP PNVROZOP	Oxidizer prevalve fails in open position, preventing shutdown. PN2 denotes events occurring in flight; PNV denotes events occurring prior to SRB ignition. The cause of such failures is mechanical, internal to either the valve or valve actuator.
	PNVCOZCS PNVLOZCS PNVROZCS	Oxidizer prevalve fails in closed position due to mechanical failures, resulting in cavitation of the high pressure fuel turbopump, turbine blade failure, and internal missile generation; this event also contributes to failure of the LH2 system in that engine. Pneumatic supply or control system failures which cause spurious valve closure are not part of these basic events.
PV5	PNVCFZOP PNVLFZOP PNVRFZOP	Fuel prevalve fails in open position, preventing shutdown. The cause of such failures is mechanical, internal to either the valve or valve actuator.
	PNVCFZCS PNVLFZCS PNVRFZCS	Fuel prevalve fails in closed position due to mechanical failures, resulting in cavitation of the high pressure fuel turbopump, turbine blade failure, and internal missile generation; this event also contributes to failure of the LH2 system in that engine. Pneumatic supply or control system failures which cause spurious valve closure are not part of these basic events.
LPOT **LPFT**	TDPCFLSZ TDPCOLSZ TDPLFLSZ TDPLOLSZ TDPRFLSZ TDPROLSZ	Low pressure turbopumps fail in an overspeed or underspeed condition due to random mechanical failures internal to the pump. These failures are non-catastrophic and, if properly detected and corrected by shutdown, need not necessarily lead to loss of life or vehicle.

NOTES TO FIGURE 3-4

Valve Schematic Designation	Fault Tree Mnemonic	Description of Basic Event or Gate
HPOT HPFT	TDPCFHSZ TDPCOHSZ TDPLFHSZ TDPLOHSZ TDPRFHSZ TDPROHSZ	High pressure turbo pumps fail in an overspeed or underspeed condition due to random mechanical failures, internal to the pump These failures are non-catastrophic and, if properly detected and corrected by shutdown, need not necessarily lead to loss of life or vehicle.
HE	PNEUMCONTL PNEUMCONTC PNEUMCONTR	Pneumatic system is not available to each of the engines. All tanks, piping, regulators, control valves and associated hardware are contained within this gate.
HPOT HPFT	PRBCFSLK PRBCOSLK PRBLFSLK PRBLOSLK PRBRFSLK PRBROSLK	Preburners on high pressure turbopumps leak or release high pressure combustion produscts into the main engine compartment. This failure is caused by leakage through mechanical seals and joints between the preburner and pump assemblies.
OPOV FPOV	HY2CFWCD HYVCFWCD HY2LFWCD HYVLFWCD HY2RFWCD HYVRFWCD HY2COWCD HYVCOWCD HY2LOWCD HYVLOWCD HY2ROWCD HYVROWCD	Preburner valves (FPOV, OPOV) fail to close on demand due to structural failure, thereby preventing shutdown. HYV denotes event occurs prior to SRB ignition. HY2 denotes event occurs in flight. Hydraulic supply, pneumatic supply, and control system failures are not considered part of this basic event.
MFV	HY2CFJCD HYVCFJCD HY2LFJCD HYVLFJCD HY2RFJCD HYVRFJCD	Main Fuel Valve (MFV) fails to close on demand due to mechanical failures, thereby preventing shutdown. HYV denotes event occurs prior to SRB ignition. HY2 denotes event occurs in flight. Hydraulic supply, pneumatic supply, and control system failures are not considered part of this basic event.
MOV	HY2COJCD HYVCOJCD	Main Oxidizer Valve (MOV) fails to close on demand due to structural failures, thereby preventing shutdown. HYV

NOTES TO FIGURE 3-4

Valve Schematic Designation	Fault Tree Mnemonic	Description of Basic Event or Gate
	HY2LOJCD HYVLOJCD HY2ROJCD HYVROJCD	denotes event occurs prior to SRB ignition. HY2 denotes event occurs in HYVLOJCD flight. Hydraulic supply, pneumatic supply, and control system failures are not considered part of this basic event.
MOV **MFV** **OPOV** **FPOV**	HYVCFJCS HYVCFWCS HYVCOJCS HYVCOWCS HYVLFJCS HYVLFWCS HYVLOJCS HYVLOWCS HYVRFJCS HYVRFWCS HYVROJCS HYVROWCS	Engine propellant valves (MOV, MFV, FPOV, OPOV) fail in a closed or flow restricting position after SRB ignition. These mechanical failures include failures of the valves and valve actuators. Hydraulic supply, pneumatic supply, or control system failures which cause spurious valve closure are not part of these basic events.
HPOT	HEXCOPRP HEXLOPRP HEXROPRP	Oxidizer high pressure turbopump (HPOT) heat exchanger ruptures. The rupture is assumed to create a breach of HPOT preburner pressure integrity.
MCC	CHBURN	Main combustion chamber burns through due to corrosion, random factors, or excessive chamber temperature. These events are outside the scope of analysis and are undeveloped.
POGO	ACCCOMRP ACCLOMRP ACCROMRP	POGO accumulator leaks or ruptures. The leakage will probably result from breach of pressure boundary at or near the flanged seal. Other material migration paths include the interface with the helium precharge valves and RIVs. Ruptures are assumed to be random in nature, resulting from a major breach in any part of the accumulator tank.
RIV	BLOCORRG BLOLORRG BLORORRG	Recirculation/isolation valve fails (mechanical or structural) in POGO suppression system, resulting in regulation failure in that engine. Note: Inability to maintain LO2 bleed/GO2 recirculation flow back into the main oxidizer feedline would cause the SSME POGO accumulators to dump excess GO2 pressurant into the inlet to the HPOT, causing possible pump cavitation and

NOTES TO FIGURE 3-4

Valve Schematic Designation	Fault Tree Mnemonic	Description of Basic Event or Gate
		overspeed with potential for uncontained engine damage. (Ref. 7, p. 10-3)
GOX CNTL VLV	BLOCOGRG BLOLOGRG BLOROGRG	Gas control valve fails (mechanical or structural) in the POGO suppression system, resulting in regulation failure in that engine. A major rupture in the valve will cause pump cavitation and subsequent explosion.
RELIEF RV5 RV6	PRVVFKOP PRVVOKOP	Liquid propellant overboard relief valves fail in the open position, releasing propellant at an uncontrolled rate overboard and diverting flow en route to the main engines. These failures are mechanical malfunctions of the relief valves.
ISOL. VLV PV7 PV8	PNVVONCD PNVVFNCD	Isolation valves upstream of the liquid propellant overboard relief valves fail to close on demand. That is, given that the overboard relief valve fails open, these pneumatically actuated valves fail to isolate the flow. These failures are mechanical failures associated with valve or valve actuator malfunction. Spurious signals which prevent the valve from closing are not included in this basic event.

NOTES TO FIGURE 3-4

Valve Schematic Designation	Fault Tree Mnemonic	Description of Basic Event or Gate
POGO	ACCCOMRP ACCLOMRP ACCROMRP	POGO accumulator leaks or ruptures. The leakage will probably result from breach of pressure boundary at or near the flanged seal. Other material migration paths include the interface with the helium precharge valves and RIVs. Ruptures are assumed to be random in nature, resulting from a major breach in any part of the accumulator tank.
RIV	BLOCORRG BLOLORRG BLORORRG	Recirculation/isolation valve fails (mechanical or structural) in POGO suppression system, resulting in regulation failure in that engine. Note: Inability to maintain LO2 bleed/GO2 recirculation flow back into the main oxidizer feedline would cause the SSME POGO accumulators to dump excess GO2 pressurant into the inlet to the HPOT, causing possible pump cavitation and overspeed with potential for uncontained engine damage. (Ref. 7, p. 10-3)
GOX CNTL VLV	BLOCOGRG BLOLOGRG BLOROGRG	Gas control valve fails (mechanical or structural) in the POGO suppression system, resulting in regulation failure in that engine.A major rupture in the valve will cause pump cavitation and subsequent explosion.
RELIEF RV5 RV6	PRVVFKOP PRVVOKOP	Liquid propellant overboard relief valves fail in the open position, releasing propellant at an uncontrolled rate overboard and diverting flow en route to the main engines. These failures are mechanical malfunctions of the relief valves.
ISOL. VLV PV7 PV8	PNVVONCD PNVVFNCD	Isolation valves upstream of the liquid propellant overboard relief valves fail to close on demand. That is, given that the overboard relief valve fails open, these pneumatically actuated valves fail to isolate the flow. These failures are mechanical failures associated with valve or valve actuator malfunction. Spurious signals which prevent the valve from closing are not included in this basic event.

Section 4

QUANTITATIVE EVALUATION

4.1 SYSTEM AND COMPONENT FAILURE RATES

Component failure rates and associated exposure times are used to calculate failure probabilities for continously operating components. Each basic event failure rate depends on its component type, failure mode, operating mode, and environmental application. The results of this data compilation effort are summarized in Appendix C. The rationale for the established failure rates is similarly included in the data summary.

The generic failure rates in Appendix C, Table C-1 are used in the development of individual basic event failure rates. That is, a specific failure rate or set of failure rates are derived for each basic event in the fault tree. The data base derived from the generic failure rate and used in fault tree computations is also provided in Appendix C. Because much of the failure rate data is time-dependent or conditional, several sets of probabilities are calculated. The rationale behind the use of time-dependent data is contained in Section 6.

Structural failures, such as failure of the ET within its design envelope, are not included within scope. Such failures are shown for modeling completeness on the master fault trees but are not quantified in the final computations.

4.2 HUMAN ERROR

Man-machine interactions are examined in two distinct ways: 1) as a source introducing potential risk due to human error, and 2) as a means of recovering from system failures or reducing an existing hazardous condition through corrective action.

From T-10 seconds to T+8 minutes, human actions (either introducing or recovering errors) become secondary to automatic controls. In contrast, ground operation errors may result in delayed sources of catastrophic accidents if flight scrub safeguards fail to detect the error. Delayed effects include those failures which do not manifest themselves until flight; for example a latent ground error will not cause an accident until after SSME ignition.

Table C-2 summarizes the various human failure rates per task or specific operation. During ground fill operations, the human is assumed to provide only backup and status monitoring functions. Fill operations are assumed to be software controlled and fully automatic. For all tasks in which the operator takes responses to a software or hardware failure it is assumed that the operators follows written procedures and that there is at least one other independent check. Other major assumptions regarding human errors and response characteristics are provided in Appendix C, Table C-3.

4.3 FAILURE PROBABILITY CALCULATIONS

The top event probability was determined using the CAFTA code developed by Science Applications International Corporation. A description of the code and its method of generating cutsets and event probabilities from failure rate and exposure is provided in Section 3.2 and in Appendix I. The failure rate data described in Appendix C were used to determine the input (basic event) probabilities for the code. The probability was approximated by the product of the failure rate ( ) and the exposure time ( ). This approximation is fairly accurate for probabilities below .001. This is the case for all basic events in the ESMF fault tree model.

Timing of a catastrophic failure is very important in determining the total impact on the STS, STS crew, and surrounding facilities and personnel. Therefore, different time intervals were defined to account for various system configurations and consequences. In addition, the exposure time varies depending on the functional requirements of the component (i.e., certain components can only induce catastrophic failures during specific time intervals, operations or system configurations). In this manner, the exposure time is set as the longest period of time in which the postulated basic event failure can occur. Components which are inactive (until required to operate) assume the entire time duration from the start of launch as the exposure time: this assumption errors in the direction of conservation. A detailed description of the time intervals and the basis for those intervals is described in Section 6.

The sum of top event probabilities for each of the mutually exclusive time intervals yields the total probability of a catastrophic failure during the period T-8 hours to ET separation.

Most of the failure probability occurs during the time interval T-10 seconds to zero thrust. Any failures which result from component leakages, ice plugging, or related failures will most likely be realized during the early seconds of flight. Subsequent portions of the flight are important contributors, but add only a fractional contribution to the probability of catastrophic failure.

It is important to note, however, that the initial calculation of the top event is based on point estimate values for each of the basic events. In other words, the input probabilities do not carry with them information regarding their statistical distribution. The top event, therefore, does not contain any information regarding its distribution.

4.4 SENSITIVITY ANALYSIS

Because of the unavailability of shuttle - specific failure data, generic failure data was substituted. The subsequent uncertainty introduced by using generic data may be addressed through sensitivity analysis. In sensitivity analysis, the probabilities assumed for certain basic events are varied and the effect on the top event probability noted.

Two commonly used sensitivity techniques are parametric variation and Monte Carlo simulation. A brief discussion of how each technique is used and the results produced by each approach is provided below.

Parametric Variation

The most straight forward means of performing a sensitivity analysis is by changing the basic event probabilities for those events of highest importance ranking. In addition, sensitivity analysis are performed for components of special interest to design/analysis teams.

The sensitivity analysis is based on varying the following parameters:

- Reduce all seal failure rates to the 20% lower confidence interval value as dictated by the failure rate data base.
- Change undeveloped event VENTPANEL (i.e. orbiter aft compartment vent panel/door). Assume successful relief of pressure (following gross helium leakage or pneumatic system component rupture) 90% of the time.
- Change the availability of ignition source following gross leakage of propellant in aft compartment form 1.0 to 0.1.
- Reduce bleed valve/anti-flood valve failure rate to the lower 90% confidence limit established by the failure rate data base.
- Increase heat exchanger rupture/gross leakage failure rate by one order of magnitude (i.e., multiply failure rate by 10). NOTE: This great variation in failure rate is to illustrate the insensitivity of the top event to changes in the heat exchanger failure rate.

The sensitivity parameters are changed individually, and then changed collectively. The results are presented in Table 4-1.

Synthetic Sampling

A second method of assessing the risk model's sensitivity to changes in basic event failure probabilities is throughout the use of synthetic sampling techniques such as Monte Carlo. Monte Carlo relies on the generation of random sample of basic event failure probabilities from appropriate distributors. For each set of basic event probabilities, a top event is calculated. If sufficient sample (e.g. sets of basic event probabilities) are drawn, a distribution may be determined for the top event. More details regarding this technique provided in Appendix J.

Various distributions were used to represent the basic event failure probabilities to assess sensitivities in the fault tree model. The resulting top event distribution exhibited that 90% of the top event probabilities were expected to occur between 1.40E-04 and 4.50E-03. This range was computed by TEMAC code using a "Latin Hypercube" sampling algorithm. The computed point estimate value in CAFTA was 2.20e-03. The range confirms that variations in top event probability are subtantially small. This increases the confidence in that point estimate data used in the analysis gives a fairly accurate representation of expected system performance.

Other TEMAC computer run was presented in Appendix J for general reference.

4.5 IMPORTANCE CALCULATION OF DOMINANT EVENTS

The CAFTA processor automatically computes five measures of quantitative importance and one qualitative measure of structural importance. The results of the CAFTA importance computations are presented in Appendix I for all events which appear in cutsets whose probability is greater than 10(-8).

By focusing on those events which are the dominant contributors to top event probability, according to their importance ranking, one can prioritize those design efforts which reduce risk most effectively. Two measures of importance are selected to illustrate this technique. Fussell-Vesely is selected to represent a quantitative measure (e.g. importance is based on the assigned probabilities). Qualitative or structural importance is also summarized. The results of these computations are presented in Tables 4-2a and 4-2b for the Fussell-Vesely and structural measures, respectively. The expressions used to compute these values are discussed in Section 3.3.2.

4.5.1 Results of Fussell-Vesely Importance Ranking

Fussel-Vesely Importance was computed for all basic events appearing in cuts sets of probability 10 -8 or greater.

The highest ranking basic event is leakage through LO2 system seals. This is closely followed by failure of aft compartment 3-way solenoid pilot valves which control orbiter valves. The "vent-to-port" failure mode of the valves may overpressurize the aft compartment if the vent door fails to relieve overpressure condition. Most other major terms are associated with leaks or ruptures in the balance of LO2/LH2 system components, seals and piping.

4.5.2 Results of Structural Importance Ranking

It is necessary for computational purposes, to limit structural ranking to those basic events which appear in sequences above 3.6 E -05, or the presence of too many singletons immediately below this truncation limit causes the importance value to approach zero. It is important to observe that those basic events which appear in singleton cut sets are all given a structural importance of 1. This is an inherent limitation of structural importance, but the measure does provide some insight for those dominant basic events appearing above the truncation limit.

The highest ranking basic events are CNDEZXIG and VENTPANEL which corresponds to the presence of an ignition source in the aft compartment and the ability of the aft compartment to relieve overpressure, respectively. These basic events appear in most of the cutsets above the truncation limits and are expected to be very high in structural importance.

Loss of HPOT seal purge due to gross depressurization of the pneumatic control assembly also ranks high in structural importance. All remaining basic events rank equally since they all appear in one and only one doubleton cutset. These events are primarily related to propellant leaks or component ruptures within the aft compartment.

TABLE 4-1

SENSITIVITY ANALYSIS SUMMARY

Description of Basic Event Change	New Top Event Probability	% Change With Respect to Baseline
Seal failure rate reduced to 20% lower confidence interval valve of 1.71E -5 failures/hour (previously 2.09E-5 failure/hours)	2.36E-3	-2.9%
Probability of orbiter vent panel failing to relieve pressure on demand = 0.1 instead of 1.0. This condition follows gross leakage or component rupture in helium pneumatic system.	1.66E-3	-32%
Change probability of ignition given a major propellant spill in the orbiter from 1.0 to 0. This affects basic event CNDEZXIG.	1.93E-3	-20%
Reduce bleed valves and anti-flood valve failure rate by one order of magnitude.	2.37E-3	-2.5%
Increase failure rate of all electrical/electronic equipment by a factor of 10	2.49E-3	+2.5%
Pneumatic regulator failure rate reduced from 1.16E -4 failures/hour to 1.10 E -4 failures/hour.	2.42E-3	-.41%
Increase heat exchanger failure rate by one order of magnitude.	2.43E-3	Negligible
Collective change of items 1) thru 6).	1.14E-3	-53%

TABLE 4- 2a

SUMMARY OF HIGHEST RANKING BASIC EVENT IMPORTANCE VALUES

◇ USING FUSSELL-VESELY MEASURES ◇

Basic Event	Description	Importance
VENTPANEL	VENT DOOR ON ORBITER AFT COMPARTMENT FAILS TO RELIEVE PRESSURE WHEN COMPARTMENT OVERPRESSURIZATION OCCURS. THIS EVENT IS APPLICABLE DURING ALL PHASES OF FLIGHT. THE MECHANISMS AND DETAILS REGARDING FAILURE REMAIN UNDEVELOPED.	3.5E-01
CNDEZXIG	AN IGNITION SOURCE IS PRESENT TO IGNITE PROPELLANT RELEASED WITHIN THE ENGINE COMPARTMENTS. THE PRIMARY SOURCE OF IGNITION ARE THE HOT SURFACES OF THE SSME PREBURNERS, AND HOT GAS MANIFOLD.	2.0E-01
FLGEOSLK	FLANGE FAILURES IN THE LO2 SYSTEM WITHIN THE MAIN ENGINE COMPARTMENT RESULT IN LEAKAGE THROUGH SEALS. LEAKAGE THROUGH SEALS COMBINED WITH AN IGNITION SOURCE IS ASSUMED TO BE CATASTROPHIC.	6.6E -02
CNDVZXIG	AN IGNITION SOURCE IS PRESENT TO IGNITE PROPELLANT LEAKS WITHIN THE ORBITER. SOURCES OF IGNITION HAVE NOT BEEN IDENTIFIED FOR LEAKS IN THIS LOCATION.	4.5E-02
SPVVPXDP	PILOT VALVES ON ORBITER PNEUMATIC ACTUATORS SPURIOUSLY VENT TO PORT, DEPRESSURIZING PNEUMATIC SUPPLY TO THE ACTUATORS AND RENDERING VALVE CONTROLS INOPERATIVE. THIS BASIC EVENT REPRESENTS THE SUM TOTAL OF ALL PILOT VALVES ON MANIFOLDS FOR ORBITER VALVE ACTUATORS.	4.4E-02
MPBVP3LK MPBVP5LK MPBVP1LK	GROSS LEAKAGE THROUGH COMPONENT SEALS CAUSE DEPRESSURIZATION OF THE HELIUM SUPPLY SYSTEM. LEAKAGE CONFINED INTERNALLY TO THE COMPONENT IS NOT INCLUDED IN THESE BASIC EVENTS. THE BASIC EVENT REPRESENTS THE SUM TOTAL OF WELDS IN A SECTION OF HELIUM SYSTEM PIPING AS DESCRIBED IN THE FAULT TREE. EACH VALVE WAS ASSUMED TO HAVE ONE SEAL.	4.1E-02 4.0E-02 4.0E-02

TABLE 4- 2a

SUMMARY OF HIGHEST RANKING BASIC EVENT IMPORTANCE VALUES

◇ USING FUSSELL-VESELY MEASURES ◇

Basic Event	Description	Importance
MPBEOSLK	COMPONENTS SUCH AS VALVES AND RELIEF DEVICES ON THE OXIDIZER SYSTEM WHICH ARE LOCATED IN THE ENGINE COMPARTMENT RUPTURE OR LEAK. RUPTURE IS SUFFICIENT TO CAUSE MAJOR LOSS OF LO2.	3.5E-02
FLGEFSLK	FLANGE FAILURES IN THE LH2 SYSTEM WITHIN THE MAIN ENGINE COMPARTMENT RESULT IN LEAKAGE THROUGH SEALS. LEAKAGE THROUGH SEALS COMBINED WITH AN IGNITION SOURCE IS ASSUMED TO BE CATASTROPHIC.	3.1E-02
MPBEFSLK	COMPONENTS SUCH AS VALVES AND RELIEF DEVICES OF THE LH2 SYSTEM WHICH ARE LOCATED IN THE ENGINE COMPARTMENT LEAK OR RUPTURE. RUPTURE IS SUFFICIENT TO CAUSE MAJOR LOSS OF LH2.	2.3E -02
MPBVOSLK MPBVFSLK	COMPONENTS SUCH AS VALVES AND RELIEF DEVICES ON THE PROPELLANT SYSTEM WHICH ARE LOCATED IN THE ORBITER RUPTURE OR LEAK. RUPTURE IS SUFFICIENT TO CAUSE MAJOR LOSS OF PROPELLANT FROM EITHER THE LO2 OR LH2 SYSTEMS.	2.1E-02 2.1E-02
MPBEOPRP	PROPELLANT SYSTEM PIPING ASSOCIATED WITH THE LO2 SYSTEM IN THE MAIN ENGINE COMPARTMENT RUPTURES, THEREBY RELEASING LIQUID INTO THE ENGINE COMPARTMENT. RUPTURE IS SUFFICIENT TO CAUSE MAJOR LOSS OF PROPELLANT FROM THE LO2 SYSTEM.	2.0E-02
FLGEJSLK	FLANGE FAILURES IN THE GH2 SYSTEM WITHIN THE MAIN ENGINE COMPARTMENT RESULT IN LEAKAGE THROUGH SEALS. LEAKAGE THROUGH SEALS COMBINED WITH AN IGNITION SOURCE IS ASSUMED TO BE CATASTROPHIC.	1.8E-02

TABLE 4- 2a

SUMMARY OF HIGHEST RANKING BASIC EVENT IMPORTANCE VALUES

◇ USING FUSSELL-VESELY MEASURES ◇

Basic Event	Description	Importance
SPVLPCDP SPVCPCDP SPVRPCDP	LEAKAGE OR RUPTURE CAUSES SOLENOID VALVES IN THE PNEUMATIC CONTROL ASSEMBLY (PCA) TO DEPRESSURIZE THE HELIUM SYSTEM. DEPRESSURIZATION MAY OCCUR THROUGH CRACKS IN THE VALVE WALLS OR THROUGH THE VALVES' WELDED CONNECTIONS TO PCA PIPING.	1.6E-02 1.6E-02 1.6E-02
BDPEFXRP BDPEOXRP	BURST DIAPHRAGM LEAKS OR PREMATURELY RUPTURES SO AS TO CAUSE PROPELLANT SYSTEM PRESSURE BOUNDARY FAILURE. THIS FAILURE CAN OCCUR IN BOTH THE LO2 AND LH2 SYSTEMS.	1.6E-02 1.6E-02
MPBEJPRP	PROPELLANT SYSTEM PIPING ASSOCIATED WITH THE GH2 SYSTEM IN THE MAIN ENGINE COMPARTMENT RUPTURES. RUPTURE IS SUFFICIENT TO PREVENT LH2 TANK PRESSURIZATION.	1.5E -02

TABLE 4-2b

SUMMARY OF HIGHEST RANKING BASIC EVENT IMPORTANCE VALUES

◇ USING STRUCTURAL MEASURES ◇

Basic Event	Description	Importance
CNDEZXIG	CONDITONAL PROBABILITY THAT AN IGNITION SOURCE IS PRESENT TO IGNITE PROPELLANT RELEASED WITHIN THE MAIN ENGINE THE PRIMARY SOURCE OF IGNITION IS HOT SURFACES OF SSME PREBURNERS. COMBUSTION PRODUCT EXHAUST PIPING. ETC.	1.10 E -02
VENTPANEL	VENT DOOR ON ORBITER AFT COMPARTMENT FAILS TO RELIEVE PRESSURE WHEN COMPARTMENT OVERPRESSURIZATION OCCURS.	4.40 E -03
FLGEJSLK	FLANGE FAILURES RESULT IN LEAKAGE THROUGH GH2 SYSTEM SEALS. LEAKAGE THROUGH SEALS COMBINED WITH AN IGNITION SOURCE IS ASSUMED TO BE CATASTROPHIC. THIS BASIC EVENT REPRESENTS THE SUM TOTAL OF FLANGE-RELATED FAILURES WITHIN THE AFT COMPARTMENT.	2.97 E -03
SPVCPCDP SPVLPCDP SPVRPCDP	LEAKAGE OR RUPTURE CAUSES SOLENOID VALVES IN THE PNEUMATIC CONTROL ASSEMBLY (PCA) TO DEPRESSURIZE THE HELIUM SYSTEM.	2.97 E -03 (EACH)
CNDVZXIG	CONDITIONAL PROBABILITY THAT AN IGNITION SOURCE IS PRESENT TO INGNITE PROPELLANT RELEASED WITHIN THE ORBITER FUSELAGE. SOURCES OF IGNITION HAVE NOT BEEN IDENTIFIED FOR LEAKS IN THIS LOCATION.	1.98 E -03
BDPEFXRP BDPEOXRP	BURST DIAPHRAGM LEAKS OR PREMATURELY RUPTURES SO AS TO CAUSE PROPELLANT SYSTEM PRESSURE BOUNDARY FAILURE. THIS FAILURE CAN OCCUR IN BOTH THE LO2 AND LH2 SYSTEM.	9.90 E -4 (EACH)
FLGEFSLK FLGEOSLK	FLANGE FAILURES RESULT IN LEAKAGE THROUGH SEALS. LEAKAGE THROUGH SEALS COMBINED WITH AN IGNITION SOURCE IS ASSUMED TO BE CATASTROPHIC. THESE BASIC EVENTS REPRESENT THE SUM TOTAL OF FLANGE-RELATED FAILURES OF BOTH THE LIQUID FUEL AND OXIDIZER SYSTEMS WITHIN THE AFT COMPARTMENT.	9.90 E -04 (EACH)

TABLE 4-2b

SUMMARY OF HIGHEST RANKING BASIC EVENT IMPORTANCE VALUES

◇ USING STRUCTURAL MEASURES ◇

Basic Event	Description	Importance
MPBEFSLK MPBEOSLK	COMPONENTS SUCH AS VALVES AND RELIEF DEVICES ON THE PROPELLANT SYSTEM WHICH ARE LOCATED IN THE MAIN ENGINES RUPTURE OR LEAK. RUPTURE IS SUFFICIENT TO CAUSE MAJOR LOSS OF PROPELLANT FROM EITHER THE LO2 OR LH2 SYSTEM.	9.90 E -04 (EACH)
MPBEOPRP	PROPELLANT SYSTEM PIPING ASSOCIATED WITH THE MAIN ENGINE RUPTURES, THEREBY RELEASING LIQUID OXIDIZER INTO THE AFT COMPARTMENT. RUPTURE IS SUFFICIENT TO CAUSE MAJOR LOSS OF PROPELLANT FROM THE LO2 SYSTEM.	9.90 E -04
MPBVFSLK MPBVOSLK	COMPONENTS SUCH AS VALVES AND RELIEF DEVICES ON THE PROPELLANT SYSTEM WHICH ARE LOCATED IN THE ORBITER RUPTURE OR LEAK. RUPTURE IS SUFFICIENT TO CAUSE MAJOR LOSS OF PROPELLANT FROM EITHER THE LO2 OR LH2 SYSTEM.	9.90 E -04 (EACH)
MPBVP1LK MPBVP3LK MPBVP5LK	GROSS LEAKAGE THROUGH COMPONENT SEALS CAUSES DEPRESSURIZATION OF THE HELIUM SUPPLY SYSTEM.	9.90 E -04
SPVVPXDP	PILOT VALVES ON ORBITER PNEUMATIC ACTUATORS SPURIOUSLY VENT TO PORT, DEPRESSURIZING PNEUMATIC SUPPLY TO THE ACTUATORS AND RENDERING VALVE CONTROLS INOPERATIVE.	9.90 E -04

Section 5

SYSTEMS DESCRIPTION
(Reference 22)

The MPPS furnishes the pressurant gas at the conditions necessary for proper operation of the Main Propulsion System (MPS) from the beginning of ground operations until successful return of the Shuttle Orbiter to Earth. The MPPS consists of the external tank (ET), the Space Shuttle main engine (SSME), and those components of the Orbiter which connect the ET to the SSME and provide the necessary services for safe operation within the normal Space Transportation System (STS) requirements. The system also includes the facility equipment and the ground support equipment (GSE) necessary for servicing the Helium Pressurization System and providing the necessary ET fuel and oxidizer pressurization prior to SSME ignition. The MPPS must allow the SSME to shut down safely during normal operation and protect the engine from catastrophic damage when malfunctions within the engine or in any supporting system are detected. Where possible, the system must provide backup to malfunctioning systems and allow continuation of a mission or allow the mission to be safely aborted.

The MPPS is designed to provide pressurization services from prior to SSME ignition throughout ascent and insertion. Pressurization services terminate with successful separation of the ET and purge of the residual propellants in the Orbiter feed lines and the SSME. ET separation occurs approximately 8 minutes after lift-off at the vehicle velocity state vector of 25,700 ft/sec and an altitude of 65 n. mi. The MPPS has the ability to overcome failures, which allows successful mission completion or safe abort, depending upon the time at which a failure occurs. The mission abort modes and strategies will be discussed.

This section was adapted from Reference 22, with background from Ref. 6.

A description of systems operations, physical characteristics and significant failure modes is provided in the paragraphs below.

5.1 LH2 AND LO2 PROPELLANT FLOW FUNCTIONS

The LH2 and LO2 systems are operationally very similar. Both systems draw propellant from their respective external tanks and both direct the flow through orbiter piping into the main engine assembly. The systems vary slightly in 1) external tank/orbiter interface connections, and 2) provisions for POGO suppression. Other differences are noted in Table 5-1.

Figures 5-1a, b, and 5-2a, b, are simplified schematics illustrating the main propellant process flow for the LH2 and LO2 systems for ground and flight configurations.

5.1.1 Propellant Flow Path

During flight, propellant is drawn from the external tank (ET) through an ET/orbiter disconnect valve. The flow is split equally into three separate paths from a common manifold. Each flow path corresponds to one of these main engines.

Prior to reaching the main engine, each propellant flow passes through a prevalve (i.e., one prevalve per flow path to the engine). The prevalves are bi-stable valves in that they can only assume a full open or full closed position. The full closed position serves an isolation function. When full open, a flow path to the main engine is maintained.

Downstream of the prevalves, the flow enters the suction side of a low pressure turbo pump. A second high pressure pump draws the propellant from the low pressure pump discharge and directs most of the flow towards the main burner through a main flow control valve. The main process flow configuration is schematically identical for both the LH2 and LO2 lines. All three engines are likewise identical in configuration.

5.1.2 Propellant Pressure Boundary

The ET contains the liquid propellants, liquid hydrogen (LH2) fuel and liquid oxygen (LO2) oxidizer at the required ratio (approximately 6:1), and supplies them with the proper temperature, density, and pressure required to prevent pump cavitation to the three Space Shuttle main engines (SSME's) from lift-off through ascent to main engine cutoff (MECO). After MECO, the ET is jettisoned, enters the Earth's atmosphere, and impacts in a remote area of the Indian Ocean.

The LO2 tank is located in the forward part of the ET. It contains approximately 1,361,200 pounds of liquid oxygen. The tank feeds a 17-inch-diameter feed line passing from the bottom of the tank through the intertank structure, then external to the aft right-hand ET/Orbiter disconnect. The intertank is a cylindrical structure which houses the ET instrumentation components and provides an umbilical plate that interfaces with the GSE arm for helium gas supply, hazardous gas detection, and gaseous hydrogen boil off during prelaunch operations. The LH2 tank, which is located aft, contains approximately 227,650 pounds of liquid hydrogen and supplies fuel through a 17-inch-diameter feed line to the aft left-hand disconnect.

Because of the great difference in density of fuel and oxidizer, the hydrogen tank contains one-sixth the total weight of propellants and is approximatley 2.7 times the volume of the LO2 propellant tank. The LO2 tank is located forward to obtain a favorable center of gravity (c.g.) location for the entire vehicle.

The Propellant Piping in the Orbiter consists of manifolds, distribution lines and valves which circulate propellant to condition the system and route the fuel and oxidizer through prevalves to each of the three SSME's. This subsystem also consists of the distribution lines and valves which furnish pressurant gas to the ET after SSME ignition and until MECO.

5.1.3 Control of Major Mechanical Components

Valves within the main process flow are hydraulically or pneumatically actuated, or both.

Flow is regulated by adjusting the speed on the high pressure pump. The high pressure pump consists of a preburner/tubine pump mechanism from LO2 and LH2 extraction lines. The oxidizer flow is adjusted by a throttling valve, a preburner oxidizer valve which controls the rate of combustion in the pump preburner and thus pump speed. The high pressure pump configurations are identical for the LO2 and LH2 systems.

The low pressure oxidizer pump is driven by an extraction line from the discharge of the high pressure oxidizer turbopump.. The low pressure LH2 turbopump is driven off the main engine burner combustion pressure. Exhausts from the turbopump are combined with the exhausts from the LH2 and LO2 preburners and recycled into the main engine burner.

5.1.4 External Tank Pressurization

This section describes the pressurization of the LO2 and LH2 tanks. Effects of failures assume that all three engines are running. Engine out failure modes are discussed in Section 5.5

5.1.4.1 LO2 Tank

High pressure liquid oxygen from the HPOT is fed to the MCC and the preburner pump. Small quantities are bled through the anti-flood valve (AFV) to the heat exchanger (HEX). Part of the resulting gaseous oxygen (GO2) is used for Pogo suppression, and the rest is routed through the oxygen FCV's for pressurization of the ET (Ref 17, p. 1.2-1).

The LO2 tank pressurization line provides the means of transporting the pressurant to the ullage area to assure the required LO2 interface pressure and tank pressure. (Ref. 8, p. P-6) Loss of ullage pressurant flow from the period of engine start to one second after lift-off could violate the 18.3 psig minimum ullage pressure requirement at lift-off plus one second causing potential tank damage (shear buckling) with the potential for TPS loss and eventual tank rupture. (Ref. 7, p. 4-10A) Loss of LO2 ullage pressure during flight could result in ET structural failure.

Described below are the major constituents and failure modes of the LO2 tank pressurization subsystem.

Components Forming GO2 Pressure Boundary

Major external leakage of GO2 components (line segments, flex couplings, bellows, seals) may cause loss of GO2 and possible structural failure of the LO2 tank. (Ref. 8, p. PA-6)

Failure of one GO2 engine isolation check valve to open would prevent pressurization gas from that engine from reaching the tank. This could also cause possible rupture of SSME heat exchanger coil allowing mixture of fuel rich exhaust gas and LO2. (Ref. 18, p. 354)

Flow Control Valve

Each pressure sensor controls a flow control valve for one of the three orbiter main engines. At engine start, the three orbiter flow control valves are closed since the tanks are pressurized. (Ref. 8, p. E-9)

To maintain the desired ullage pressure, the flow control valves are automatically opened if the tank pressure drops to of the control band. There is no manual control for the LO2 flow control valves. (Ref. 17, p. 2.1-4)

Failure of a single LO2 pressurant flow control valve to open to increase GO2 pressurant flow will not affect the system. A second valve failing closed, or a GO2 engine isolation check valve failing closed in another engine will result in low ullage pressure, possibly violating the ET structural safety factor. All 3 flow control valves failing closed may result in ET structural failure and loss of crew/vehicle. (Ref. 18, p. 365)

A clogged orifice in one leg of a flow control assembly results in loss of only 1/2 flow capacity of one valves. Other valves will maintain adequate ET pressure. (Ref. 18, p.367)

Body burn-through of a LO2 flow control valve caused by impact of particles or excessive GO2 temperatures will cause loss of GO2 pressurant to ET. Release of hot GO2 into orbiter aft bay may result in overpressurization and orbiter structural damage. Hot HO2 impingement may cause damage to surrounding system/components. (Ref. 18, p. 368)

Disconnect Valve

The LO2 tank pressurization disconnect transmits pressurant flow from the Orbiter to the external tank in flight and from the ground during tank prepressurization operations. The ET/Orbiter interface consists of a 2-in.-diameter disconnect valve. The disconnect contains coaxial poppets which are held open mechanically when the disconnect halves are engaged and closed with spring force once disengaged. Sealing is accomplished by metal-to-metal seal with internal gas pressure assisting the effectiveness of the seal. The gas trapped between the two poppet closures during disengagement is allowed to dump freely. After umbilical separation the Orbiter half of the disconnect serves as a closeout for the main engine pressurization system, preventing contamination of this system during atmospheric exposure. The tank half of the disconnect prevents loss of pressurant from the tank, minimizing thrust reaction on the tank during tank separation and free fall.

External leakage caused by seal fracture can possibly reduce ullage pressure. This reduction is not sufficient to be critical, since the mating flange design restricts the flow path to 0.008 squared inches with total seal failure. Failure of the disconnect to remain open during ascent can result in possible rupture of the pressurization line and low LO2 ullage pressure. This can lead to possibly early LO2 depletion and SSME shutdown. There is a

possibility of the loss of crew/vehicle if the line ruptures and the aft bay compartment is overpressurized. Failure of the disconnect to close during ET separation will result in contamination of the Orbiter pressurization line during reentry.

Diffuser Assembly

A cylindrical diffuser is located internal to the LO2 tank at the pressurization line outlet. The diffuser is equipped with a perforated cylindrical core with more than 1500 holes. The external portion of the diffuser is a mesh screen. The diffuser reduces the entrance velocity of the incoming pressurant gas to provide uniform distribution of the gases in the ullage. A pressure reduction orifice is located at the inlet to the diffuser to avoid problems with high Mach Number flow in the pressurized line. (Ref. 8, p. P-7)

Structural failure of the diffuser assembly or screen could cause loss of capability to diffuse pressurant flow which would result in ullage pressure collapse. (Ref. 8, p. PA-7)

Vent/Relief Valve

The LO2 vent/relief valve is a normally closed, spring-loaded valve which is actuated open by Ground Support Equipment (GSE) helium prior to prepressurization and launch.

The valve is held open during loading to allow the escape of purge and pressurant gas as it is displaced by the propellant and the propellant boil-off.

In the event that the tank pressure gets too high, the valve will relieve to protect the tank structure. The LO2 relief pressure is 24 +- 1 (plus or minus 1) psig. The LO2 valve vents directly to the atmosphere. (Ref. 17, p. 2.3-1)

For valve relief mode operations, the two stage valve design utilizes a primary sensing pilot and a secondary slave pilot. The primary pilot uses local ambient pressure as a reference pressure (sensed at ambient pressure sense port). The primary pilot provides control so that valve relief will occur. The secondary pilot allows flow to the main piston in response to signal from the primary pilot during relief operation. The primary and secondary pilot inlets are connected to the main valve inlet cavity. (Ref. 17, p.2.3-1)

The inlet of the vent/relief valve is fastened to the LO2 tank forward dome ogive coverplate. The valve outlet is tee connected to plenums on opposite sides of the nose fairings to provide non-propulsive venting. (Ref. 8, p. P-7)

Failure of the vent/relief valve to remain closed or structural failure of the valve assembly resulting in external leakage will cause loss of ullage pressure. (Ref. 7, pp. PA-11 - PA-18)

The LO2 vent/relief valve position indicator switch tolerance allows valve to indicate closed when it may be open up to 0.30 inches. This condition could allow undetected ullage gas leakage prior to launch. Hot GO2 may autoignite TPS during flight.

5.1.4.2 LH2 Tank

Components Forming GH2 Pressure Boundary

Major external leakage of GH2 components (line segments, flex couplings, bellows, seals) may cause loss of GH2 and possible structural failure of the LH2 tank. (Ref. 8, p. PA-46)

Failure of an engine isolation check valve to open would prevent pressurization gas from that engine from reaching the tank. Failure of a second check valve or a flow control valve in another engine will result in insufficient LH2 ullage pressure. (Ref. 18, p.341)

Flow Control Valves

Each pressure sensor controls a flow control valve for one of the three orbiter main engines. At engines start, the three orbiter flow control valves are closed since the tanks are pressurized (Ref. 8, p. E-91)

To maintain the desired ullage pressure, the flow control valves are automatically opened if the tank pressure drops out of the control band. The LH2 flow control valves can be manually opened by the crew if necessary. (Ref. 17, p. 2.1-4)

Failure of a single LH2 pressurant flow control valve to open to increase GH2 pressurant flow will not affect the system. A second valve failing closed, or a GH2 engine isolation check valve failing closed in another engine will result in insufficient ullage pressure, resulting in 3 SSME shutdown. All 3 flow control valves failing closed may result in ET structural failure and loss of crew/vehicle. (Ref. 18, p. 338)

A clogged orifice in one leg of a flow control assembly results in loss of 1/2 the flow capacity from one engine. Pressurization flow from the other two engines will maintain adequate ET pressure. (Ref. 18, p. 340)

Disconnect Valve

The LH2 tank pressurization disconnect transmits pressurant flow from the Orbiter to the external tank in flight and from the ground during tank prepressurization operations. The ET/Orbiter interface consists of a 2-in.-diameter disconnect valve. The disconnect contains coaxial poppets which are held open mechanically when the disconnect halves are engaged and closed with spring force once disengaged. Sealing is accomplished by metal-to-metal seal with internal gas pressure assisting the effectiveness of the seal. The gas trapped between the two poppet closures during disengagement is allowed to dump freely. After umbilical separation the Orbiter half of the disconnect serves as a closeout for the main engine pressurization system, preventing contamination of this system during atmospheric exposure. The tank half of the disconnect prevents loss of pressurant from the tank, minimizing thrust reaction on the tank during tank separation and free fall.

External leakage caused by seal fracture can possibly reduce ullage pressure. This reduction is not sufficient to be critical, since the mating flange design restricts the flow path to 0.008 square inches with total seal

failure. Failure of the disconnect to remain open during ascent can result in possible rupture of the pressurization line and low LH2 ullage pressure. This can lead to possible early LH2 depletion and SSME shutdown. There is a possibility of the loss of crew/vehicle if the line ruptures and the aft bay compartment is overpressurized. Failure of the disconnect to close during ET separation will result in contamination of Orbiter pressurization line during reentry.

Diffuser

A cylindrical diffuser is located internal to the LH2 tank at the pressurization line outlet. The diffuser is equipped with a perforated cylindrical core with more than 1500 holes. The external portion of the diffuser is a mesh screen. The diffuser reduces the entrance velocity of the incoming pressurant gas to provide uniform distribution of the gases in the ullage. A pressure reduction orifice is located at the inlet to the diffuser to maintain back pressure on the pressurization line. (Ref. 8, p. P-10)

Vent/Relief Valve

In the event of excessive tank pressure, the valve will relieve to protect the tank structure. The LH2 relief and reseat pressures are 36 +- 1 psig and 34 psig (minimum). The LH2 valve vents through the ET/ground carrier umbilical prior to launch. (Ref. 17, p. 2.3-1)

For valve relief mode operations, the two stage valve design utilizes a primary sensing pilot and a secondary slave pilot. The primary pilot uses local ambient pressure as a reference pressure (sensed at ambient pressure sense port). The primary pilot provides control so that valve relief will occur. The secondary pilot allows flow to the main piston in response to a signal from the primary pilot during relief operation. The primary and secondary pilot inlets are connected to the main valve inlet cavity. (Ref. 17, p. 2.3-1)

Failure of the vent/relief valve to remain closed or structural failure of the valve assembly resulting in external leakage will cause a loss of ullage pressure. (Ref. 8, pp. PA-50 - PA-58)

The LH2 vent/relief valve position indicator switch tolerance allows valve to indicate closed when it may be open up to 0.30 inches. This condition could allow undetected ullage gas leakage during flight.

HPOT Heat Exchanger

See Appendix E for details.

5.2 SUPPORT SYSTEMS

Support systems are those systems and individual components which are essential to the operation of the critical mechanical components. Examples of such systems include the pneumatic and hydraulic control. Electrical instrumentation and control (EI&C) and electrical power (EP) are sometimes considered support systems in that they act mainly to support the function of

the critical mechanical components. However, due to the complexity of these systems and their interrelations with systems outside the SSMP, EI&C and EP will be addressed only in a limited sense in this study.

5.2.1 Pneumatic System

The Pneumatic (Helium) Pressurization Subsystem consists of helium supply tanks, regulators, check valves, control valves, and distribution lines. The subsystem supplies helium used within the engine for purging the high-pressure oxidizer turbopump (HPOT) intermediate seal, for purging the engine after shut down, and for actuating the valves during emergency shutdown. The balance of the helium is used to actuate the pneumatically operated propellant valves within the Propellant Delivery Subsystem and to pressurize the propellant lines prior to re-entry.

A brief description of each of those functions is provided in the paragraphs below. A simplified schematic of the pneumatic system is illustrated in Figure 5-4.

Control of Pneumatically Actuated Valves

Helium pressure is used to close the ET/Orbiter disconnect valves and propellant prevalves. These valves are closed only once during launch. Disconnect valves are closed a few seconds prior to ET separation following MECO.

Under normal flight conditions, prevalves are opened at T-10 seconds (to allow propellant flow to the main engines). The valves remain open until MECO conditions are met. The valves then are actuated to a fully closed position. If emergency shutdown of an engine is required, prevalves will be sequentially closed following SSME valve closure.

Failure of the pneumatic system will cause both disconnect and prevalves to remain in the open position.

The helium system also provides supply pressure to pogo system valves described in Section 5.3.3. Loss of valve control and post MECO charging is considered to be a catastrophic event.

Control of Hydraulically Actuated Valves

SSME valves are regulated by the engine controller using hydraulic supply pressure. A sudden drop in hydraulic pressure will cause pneumatic backup to the valve actuators to be initiated. A pneumatic shutdown of the engines occurs when a hydraulic lock condition has occurred and engine isolation is required. A description of this process is provided in Sections 5.2.2 and 5.4.3.

HPOTP Intermediate Seal Purge

The high pressure oxidizer turbopump is powered by the oxidizer preburner. Combustion of LO2 and LH2 in the preburner creates a hydrogen rich mixture at the harsh temperature and pressure of 1405 deg. R and 5180 PSIA, respectively.

The HPOT pumps LO2 at an outlet temperature and pressure of 188 deg. R and 4624 PSIA, respectively. If the hot gas and cold oxidizer meet an immediate explosion may occur. (Ref. 17, p. 1.10-3)

Mixing of oxidizer and turbine gas is prevented by a dynamic shaft seal package that is between the main pump and the turbine. The seal package consists of a labyrinth-type primary oxidizer seal, a purged controlled-gap intermediate seal, and two controlled gap turbine hot-gas seals. Drain cavities with overboard drain lines are located between the primary oxidizer seal and the intermediate seal, between the intermediate seal and the secondary turbine seal, and between the secondary and primary turbine seals. To further insure against the mixing of oxidizer and turbine gas, a helium purge is applied between the elements of the intermediate seal during engine operation. (Ref. 21, p. 1-22)

During ground operations, the intermediate seal cavity is purged with nitrogen to remove any residual air or moisture and to inert the system. This purge medium changes to helium immediately proceding engine start. Start is inhibited by inability to verify adequate purge pressure during propellent conditioning. (Ref. 11, p. 2-31)

The limit control system initiates shutdown for loss of intermediate seal purge pressure, excessive secondary seal cavity pressure or primary LO2 drain pressure or HPOT turbine discharge temperature exceeding high or low limits. (Ref. 11, p. 2-28)

If redline limits are being violated and auto-shutdown has been inhibited due to an engine loss or earlier crew decision, immediate crew action is required to shutdown that engine. It is possible that complete engine failure will occur so quickly that neither the crew nor the ground will have time to react (Ref. 17, p. 1.10-3). Loss of the HPOT intermediate seal purge during engine shutdown could potentially cause mixing of LO2 and turbine gases resulting in possible engine damage. However, loss of the engine shutdown purge would occur only if the SSME LIMIT CONTROL ENABLE/INHIBIT switch was in the INHIBIT position.

A complete failure of the secondary seal may not result in an engine loss with the limits inhibited, since the hot gas still must pass the primary seal and the intermediate seal to get to the LO2 in the pump. Thus, if the engine is running with limits inhibited and the secondary seal redline is violated, but the intermediate seal redline is not violated, the engine has a high likelihood of running until a safe abort region is reached (Ref 17, p. 1.10-3).

5.2.2 Hydraulic System

The hydraulic system is included in the model only to the extent to which it services the flow control valves. Only the piping and other mechanical pressure boundary components within the SSME's have been reviewed. The hydraulic system also services other portions of the shuttle which are not related to the operation of flow control valves in the main engine. These functions are not included in the fault tree.

5.3 PRESSURE CONTROL

5.3.1 Pressure Sensing

It is essential that proper ullage pressure be maintained. Insufficient net positive suction pressure (NPSP) may cause engine pump cavitation and subsequent explosion.

LO2 Tank

LO2 tank pressure is maintained by the tank ullage pressure transducer control circuit providing discrete pressure/flow control valve open (full flow) and closed (reduced flow) signals in accordance with the sensed tank pressure. The external tank contains four ullage pressure transducers with three of the four transducers used for controlling the operation of the flow control valves. Each transducer is dedicated electronically assigned to an engine and provides direct control for that engine's flow control valve. The fourth transducer is switched into the control circuit should a ullage pressure transducer failure occur prior to launch. (Ref. 7, p. 6-1)

The LO2 tank has gauge type transducers. The gauge transducers have individual ambient sense ports that can fail due to plugging from contamination or icing and could result in a transducer reading low. (Ref. 8, p. E-10) Failure of one sensor reading lower than actual tank pressure will open the corresponding FCV early. Tank pressure will remain within nominal limits with one failed sensor. If two or three sensors read lower than actual pressures and the vent/relief valve fails closed, tank overpressurization will result. Relief valve operation could cause loss of usable propellant. (Ref. 8, p. E-A-41)

Two or three sensors reading higher than actual pressure will cause flow control valves to shut off too soon causing tank underpressurization. (Ref. 8, p. EA-9)

LH2 Tank

LH2 tank pressure is maintained by the tank ullage pressure transducer control circuit providing discrete pressure/flow control valve open (full flow) and closed (reduced flow) signals in accordance with the sensed tank pressure. The crew is provided with an override switch which provides backup for the condition of two failures in the tank ullage pressure tranducers/flow control valve circuits to provide adequate pressurant to the LH2 tank. The switch by-passes the control for the pressure/flow control valves and commands all of the pressure flow control valves to the normally open (full flow) position. The switch would be operated if the C & W gave an indication of lowering mainfold pressure. The external tank contains four ullage pressure transducers with three of the four transducers used for controlling the operation of the flow control valves. Each transducer is dedicated electronically assigned to an engine and provides direct control for that engine's flow control valve. The fourth transducer is switched into the control circuit should a ullage pressure transducer failure occur prior to launch. (Ref. 7, p. 6-1)

Failure of one sensor reading lower than actual tank pressure will open the corresponding FCV early. Tank pressure will remain within nominal limits with one failed sensor. If two or three sensors read lower than actual pressures,

relief valve actuation may be required to prevent overpressurization. Relief valve operation could cause fire damage to the (TPS) thermal protection system and loss of usable propellant. (Ref. 8, p. E-A-41)

Two of three sensors reading higher than actual pressure will cause flow control valves to shut off too soon causing tank underpressurization. (Ref. 8,p. EA-8)

5.3.2. Pressure Relief

The propellant tank vent/relief valve assemblies provides two functions, vent and relief. The vent function is only utilized during propellant loading launch countdown and hold periods, and the relief function is used to protect the tank structure when the vent is closed by automatically reducing the ullage pressure in the event that it exceeds a preset value.

During flight the vent valves assume their normally closed position and act as safety relief valves to protect against overpressurization. Failure of LO2 or LH2 relief functions would result in tank overpressurization if a secondary system failure (ie. flow control valve failure) exists. (Ref. 8, P-A-15, 52)

5.4 POGO SUPPRESSION

Pogo is self-induced longitudinal oscillation involving major vehicle components, structure, feedlines, turbopumps, and engine. Pogo results in undesirable low frequency oscillations (typically 5 to 25Hz) with potentially detrimental effects on the vehicle crew's ability to function and on vehicle structure and components. (Ref. 11, p. Z-127)

Loss of Pogo suppression capability from one engine after liftoff is considered to result in structural oscillations and feedline pressure of unpredictable amplitude which can lead to loss of crew/vehicle. (Ref. 23, p. 1-7)

A GO2 Pogo suppressor system is incorporated into the LO2 feed system at the HPOT inlet. The system utilizes a gas filled accumulator to suppress vehicle-induced flow oscillations. GO2 tapped off the heat exchange is used as the pressurization medium following an initial helium precharge. The system controls liquid level in the accumulator by means of an overflow line which routes overflow fluids through the recirculation isolation valve (RIV) and the LO2 bleed line to the manifold feedline upstream of the prevalves. (Ref. 9, p. 1-7) Refer to Figure 5-5.

The Pogo suppression system consists of a flanged accumulator, standpipe, helium precharge valve package, GO2 control valve, a recirculation isolation valve, and two recirculation control valves. The engine controller controls the valves. (Ref. 9, p. 1-7)

The accumulator is chilled by LO2 during engine chilldown operation. Free convection circulation within the accumulator, with optional cycling of the recirculation isolation valve, allows the accumulator to fill to the

recirculation line level. This level is sufficient to preclude gas ingestion at start. (Ref. 9, p. 3-128) At termination of engine chilldown, T-12.5 seconds, the Pogo recirculation control valves are opened. (Ref. 17, p. 2.2-7)

During engine start, charging of the accumulator with helium is delayed by 2.4 seconds after the engine start signal to permit the engine to reach a well behaved portion of its pressure/flow transient. At that point, the controller signals helium flow through the helium precharge valve. Helium entering the accumulator forces the LO2 level down to the nominal operating position in approximately 2.0 seconds. (Ref. 11, p. 2.2-8)

The helium precharge is utilized in the GO2 Pogo suppressor system to provide a rapid charge and thereby afford Pogo protection during liftoff and the early part of the flight until gaseous oxygen is available from the engine heat exchanger. The helium prechrarge valve (HPV) is also used to provide helium to the accumulator as a post charge at engine shutdown. The HPV contains a 15-micron filter at the helium inlet. (Ref. 17, p. 1.6-8)

The helium precharge solenoid valve also controls the normally open GO2 control valve. When the solenoid is de-energized, GO2 is supplied to the accumulator. (Ref. 11, p. 2.2-8)

The GO2 Control Valve (GCV) provides gaseous oxygen pressurant to the Pogo accumulator during engine operation after the engine heat exchanger is functioning. A bleed orifice provides fail-safe valve actuation to the open position. Pneumatic pressure to the closing side of the actuator is also applied to the opening side of the bleed orifice. This will cause the valve to reopen approximately 2 seconds after the application of closing pressure. (Ref. 17, p. 1.6-9)

The normally open Recirculation Isolation Valve (RIV) is actuated closed by the same pneumatic pressure that opens the normally closed Oxidizer Bleed Valve. RIV opening during engine operation is ensured by routing gaseous oxygen from the override port of the GCV to the opening side of the RIV actuator when the GCV is opened. (Ref. 17, p. 1.6-6)

5.5 ELECTRICAL INSTRUMENTATION AND CONTROL (EI&C) FUNCTIONS

The SSMP EI&C system can be generally classified as performing one of the following critical functions:

1) Propellant flow rate/mixture regulation
2) Engine shutdown on demand, and
3) Thrust vector adjustment (gimbaling, throttle-up etc.)
4) External fuel tank separation actuation.

A brief description of each of these systems operations and associated hardware is provided in the sections below. Functions provided by the on-board general purpose computer (GPC) will only be described insofar as system interfaces are concerned. Analysis of the GPC and EI&C functions (Avionics System) not strictly supporting SSMP operation is outside the scope of this effort. The boundaries of EI&C functions included in the analysis are shown in Figure 5-6.

5.5.1 Avionics System Features and Interfaces

Features associated with the Avionics System include the following:

1. The primary flight system (PFS) design is based on a centralized set of quad-redundant general-purpose computers (GPC's) within the data processing system (DPS) which provides the primary mode of acquiring flight-critical sensor data, processing the data, and, finally, generating and delivering guidance, navigation, and control (GN&C) commands to the various vehicle control elements.

2. Additionally, a single GPC with independently designed and coded flight software called the backup flight system (BFS), is available to take over vehicle control through the primary bus structure from the PFS, if necessary.

3. The DPS bus structure contains 24 separate serial digital input/output (I/O) buses including eight flight-critical (GN&C) and five intercomputer (ICC) buses, which provide for sensitive data communications and control through the GPC redundant set. The three engine interface units and two master events controllers are cross-strapped to the four Flight Critical (FC) buses and provide interface services between the GPCs and the Main Engine Controllers and associated events sequencing functions.

4. The various multiply redundant inertial navigation and flight control sensors and effectors must be in a constant state of readiness to perform the fault detection, isolation, and reconfiguration (FDIR) functions.

5. The avionics and nonavionics system management (SM) function is performed in conjunction with the operational instrumentation (OI).

6. A three-string electrical power distribution and control system provides single fault-tolerant power to non-flight-critical systems and dual fault-tolerant power to flight-critical systems.

5.5.2 Propellant Flow Rate/Mixture Control

The SSME's can be throttled over a range of 65 to 109 percent of rated power level in 1-percent increments. At sea level, the engine throttle range is restricted by nozzle flow separation. The 65-percent throttle setting is referred to as minimum power level (MPL).

All three engines normally receive the same throttle command simultaneously. The command comes from the GPC's to the MEC's. During certain contingency operations, manual crew control of engines is possible by use of the speed brake/MEC handle. Throttling reduces vehicle loads during maximum aerodynamic pressure, limits longitudinal acceleration to 3 g's during boost, and makes it possible to abort with all main engines thrusting or with one engine out.

The controller is an electronics package mounted on each SSME and contains two digital computers with associated electronics that control all main engine components and operations. The controller is attached to the main combustion chamber by mounting fittings.

Each controller operates in conjunction with engine sensors, valves, actuators, and spark igniters to provide a self-contained system for engine control, checkout, and monitoring. The controller provides engine flight readiness verification, engine start and shutdown sequencing, closed-loop thrust and propellant mixture ratio control, sensor excitation, valve actuator and spark igniter control signals, engine performance limit monitoring, onboard engine checkout and response to vehicle commands and transmission of engine status, and performance and maintenance data.

Each engine controller receives engine commands transmitted by the orbiter GPC's through an engine interface unit (EIU) dedicated to that engine controller. The engine controller provides its own commands to the main engine components. Engine data are sent to the engine controller, where the data are stored in a vehicle data table (VDT) in the controller's computer memory. Controller status compiled by the engine controller's computer are also added to the vehicle data table. The vehicle data table is periodically output by the controller to the EIU for transmission to the orbiter GPC's.

The EIU is a specialized multiplexer/demultiplexer (MDM) that interfaces with the orbiter GPC's and with the engine controller. When engine commands are received by the EIU, the data are held in a buffer until the EIU receives an orbiter GPC request for data. The EIU then sends data to each orbiter GPC. Each EIU is dedicated to one SSME and communicates only with the engine controller that controls the SSME. The EIU's have no interface with each other.

The controller provides responsive control of engine thrust and mixture ratio throughout the digital computer in the controller, updating the instructions to the engine control elements 50 times per second (evey 20 milliseconds). Engine reliability is enhanced by a dual redundant system that allows normal operation after the first failure and a fail-safe shutdown after a second failure. High-reliability electronic parts are used throughout the controller.

The digital computer is programmable, allowing modification of engine control equations and constants by change to the stored program (software). The controller is packaged in a sealed, pressurized chassis and is cooled by convection heat transfer through pin fins as part of the main chassis. The electronics are distributed on functional modules with special thermal and vibration protection.

The controller is divided into five subsystems: Input electronics, output electronics, computer interface electronics, digital computer, and power supply electronics. Each subsystem is duplicated to provide dually redundant capability. A simplified redundancy diagram of the controller is Figure 5-7.

The input electronics receive data from all engine sensors, condition the signals, and convert to digital values for processing by the digital computer. Engine control sensors are dual-redundant, and maintenance data sensors are non-redundant.

The output electronics convert the computer digital control commands into voltages suitable for powering the engine spark igniters, the off/on valves, and the engine propellant valve actuators.

The computer interface eletronics control the flow of data within the controller, input data to the computer, and computer output commands to the output electronics. They also provide the controller interface with the vehicle engine electronics interface unit for receiving engine commands which are triple-redundant channels from the vehicle and transmission of engine status and data through dual-redundant channels to the vehicle. The computer interface electronics includes the watchdog timers that determine which channel of the dual redundant mechanization is in control.

During prelaunch, the orbiter GPC's will look at both primary and secondary data. Loss of either primary or secondary data will result in data path failure and either engine ignition inhibit or launch pad shutdown of all three SSME's.

At T-0, the orbiter GPC's will request both primary and secondary data from each EIU. For no failures, only primary data are looked at. If there is a loss of primary data (which can occur between the engine controller Channel A electronics and SSME SOP), then the secondary data are examined.

5.5.3 Engine Isolation on Demand (Shutdown)

Engine shutdown is initiated when pre-established parametric conditions (redlines) are met and processed through the controller. Propellant flow to the engines is then cut off by means of the engine flow valves and the orbiter prevalves on the LO2 and LH2 system lines. This effectively isolates the external tanks and orbiter plumbing from the engines.

The controller may fail to generate a shutdown command if 1) the engine interface unit (EIU) or general purpose computer (GPC) fails to send the proper signals, 2) the electric power is lost to the valves/controller, and 3) if the pre-established redlines are violated.

The shutdown sequence is initiated when minimum power level (MPL) is detected. MPL is currently set to 90% of full power. Engines may also be shut down if high temperature is detected on either high pressure pump turbine exhaust. Other shutdown parameters include low main burner/ chamber pressures and low tank level.

More discussion regarding system response to shutdown of one or more engines is provided in Section 5.

5.5.4 External Tank Separation

External tank detachment from the orbiter is controlled by the GPC. Activation of ET/orbiter pyrotechnics occurs after isolation of disconnect flapper valves and MECO enables the firing.

Tumbling Subsystem

As a means of assuring ET impact in a defined landing area and avoiding Orbiter/ET collision, the tank is designed to tumble shortly after Orbiter/ET separation.

The tumble system is initiated just prior to separation by commands from the Orbiter. The tumble valve arm command is initiated 5 seconds after MECO is confirmed by the GPC's and the valve fire command is initiated 1 second later. (Ref. 7, p. S-19)

The first orbiter command arms the circuit by energizing the switch module relay. This closes the two normally open relay contacts which completes the firing circuit to the NASA Standard Detonator (NSD). The second command is the fire command which activates the NSD and fires the pyro cartridge that opens a two-inch valve mounted on the ogive forward ring forging. The residual GO2 is vented in the +Z axis providing the required tumble thrust.

5.6 MAIN ENGINE SHUTDOWN

The two failure situations discussed in this section, one and two engine shutdowns, are analyzed because each is related to the MPPS. However, they are grouped together for this report because they appear to represent a cross section of mission techniques. Failure to shut down an engine illustrates redundancy and two-engine shutdown poses a real-time mission decision.

5.6.1 Failure to Shutdown a Single Engine

Engine shutdown, whether initiated by the controller or by crew command, is a safe response to an unsafe operating condition. Serious consequences may result if a main engine fails to shut down on demand. To overcome such a failure, several shutdown methods have been designed into engine operation.

Emergency engine shutdown may be initiated from any steady state or transition thrust level, including engine start. The engine shutdown sequence is initiated by the controller upon receipt of a vehicle shutdown command or engine parameters which exceed predetermined redline limits. If the controller cannot accomplish shutdown via hydraulic actuators, it will perform shutdown with helium pneumatic pressure via the Pneumatic Control Assembly (PCA). If malfunctions are such that the engine is still operating, the crew can take action, first, by cutting off electrical power to the engine and, finally, by closing the prevalves to stop the fuel flow.

5.6.2 Two Engine Shutdowns

Other considerations aside, the three engines on the Shuttle represent redundancy. However, this is true only for a single-engine-out situation; i.e., the Shuttle can safely return to the launch site or perform one of the other preplanned aborts on two engines. If two engines shut down, or the second engine must be shut down by the crew, a safe abort is possible only of the Orbiter has achieved the velocity threshold that would allow at least a TAL abort on the one remaining engine. Thus, should a second engine drift out of

safe operating boundaries between the time the first engine shuts down and the time the ascent trajectory reaches single-engine TAL, mission operations personnel and the crew may have a very difficult decision to make.

Consider a scenario beginning with the shutdown of a single engine soon after lift-off. When this event occurs, the Orbiter computers send a command to inhibit shutdown of either of the other two engines.

To enable a second automatic shutdown, the inhibit of one or both of the remaining engines must fail. This is a credible situation if a communication path failure between the Orbiter GPC's and an engine had occurred. For the same reason, the crew would also be unable to inhibit engine shutdown. Such a situation exposes the flight to the possibility of a second automatic shutdown.

Presuming the remaining two engines have been inhibited from an automatic shutdown, ground operations personnel and the crew will monitor engine parameters to identify off-nominal operations of either of the two remaining engines. The loss of intermediate seal purge is a singularly serious malfunction. If this happens, the crew may have to shut down the second engine, even at the risk of a dangerous abort. Another conceivable, though hypothetical, situation is the shutdown of a second engine with a contained failure.

Thus, the two-engines-out situation can result in a loss of life or vehicle if the event occurs between lift-off and single-engine TAL.

5.7 GROUND OPERATIONS (MPS)

Flight preparations between T-8 hours and the end of ET pressurization consist primarily of four major functions:

1. System purge
2. System chilldown
3. Propellant fill
4. ET Pressurization

Appendix F describes the individual tasks and readings needed to successfully accomplish these operations. Propellant fill is the process by which the external tank (LO2 and LH2) is slow and quick-filled to 100% level. Chilldown is the process by which system piping and components are cooled by the propellants in order to minimize thermal shock. Failure to properly chill propellant system pressure boundary may result in gross leakage or piping rupture due to overstress conditions. System purge and anti-icing is performed to prevent the accumulation of contamination (mainly water) from plugging lines upon the introduction of propellents.

Pneumatic System GSE used in the MPPS consists of three independent subsystems. Two of the subsystems are identical. The LO2 and LH2 ET prepressurizaton syubsystems provide gaseous helium to their respective tank in order to pressurize those tanks sufficiently to permit SSME start. The GSE then

continues to provide helium pressure to the tanks until lift-off. Each pressurization subsystem consists of three valves, two in parallel and one as a shutoff to the other two. These valves are controlled by the Launch Processing System (LPS), which senses the ullage pressure in the ET and opens and closes the valves accordingly. The helium is provided by a 3000 psig facility source.

The onboard helium system is pressurized prior to flight by the third GSE subsystem, the primary helium pressurization reduction and bottle fill panel. This panel regulates helium down to 4450 ± 50 psig through two parallel circuits. The helium flow is controlled by shutoff valves, which are opened and closed by the LPS in order to pressurize the onboard helium tanks without exceeding temperature limits. The helium is provided by 6000 psig facility source.

5.8 MISSION ACCOMODATIONS OF IN-FLIGHT FAILURES

The Space Shuttle mission has been designed to accomodate operational failures within the flight systems. During the ascent-to-orbit phase of a mission, a series of abort strategies has been devised to ensure a "fail operational-fail safe" capability. Simply stated, the strategies may be defined as follows:

1) Return to launch site (RTLS) is the initial abort mode, which allows the vehicle to abort anytime after launch and to return to the Kennedy Space Center (KSC) runway. The constants are (a) the loss of no more than one engine and (b) sufficient main engine propellant to steer the Shuttle on a return course to KSC with the desired position and velocity state prior to engine cutoff. Although a critical failure may occur earlier, this mode will not be activated until approximately 2 minutes 30 seconds after lift-off when the solid rocket boosters (SRBs) have burned out and separated from the Shuttle.

2) Transoceanic abort landing (TAL) is the second abort mode and overlaps the RTLS capability at approximately 4 minutes after lift-off. This mode provides the capability for the Orbiter to land at a contingency site, generally in North Africa or Spain. This option is usually activated following a critical system failure in order to land as soon as possible. This mode has full capability to accommodate one failed engine and a limited capability to accommodate two failed engines (velocities approximately > 13,000 ft/sec).

3) Abort once around (AOA) provides for an abort landing at Edwards Air Force Base or at White Sands by achieving the desired hypersonic suborbital flight state at MECO. This mode, which provides engine-out accommodation similar to TAL, is initiated because the vehicle flight energy state has progressed past the autoguidance TAL capability (velocity approximately > 20,000 ft/sec).

4) Abort to orbit (ATO), the final mode, is an option from the AOA. If sufficient onboard propulsion capability exists and the critical failure does not affect mission completion, the Orbiter will be propelled by the Orbital Maneuvering System (OMS) engines to the desired orbit after ET separation. The mission may be continued or aborted, depending on the criticality of the system failure.

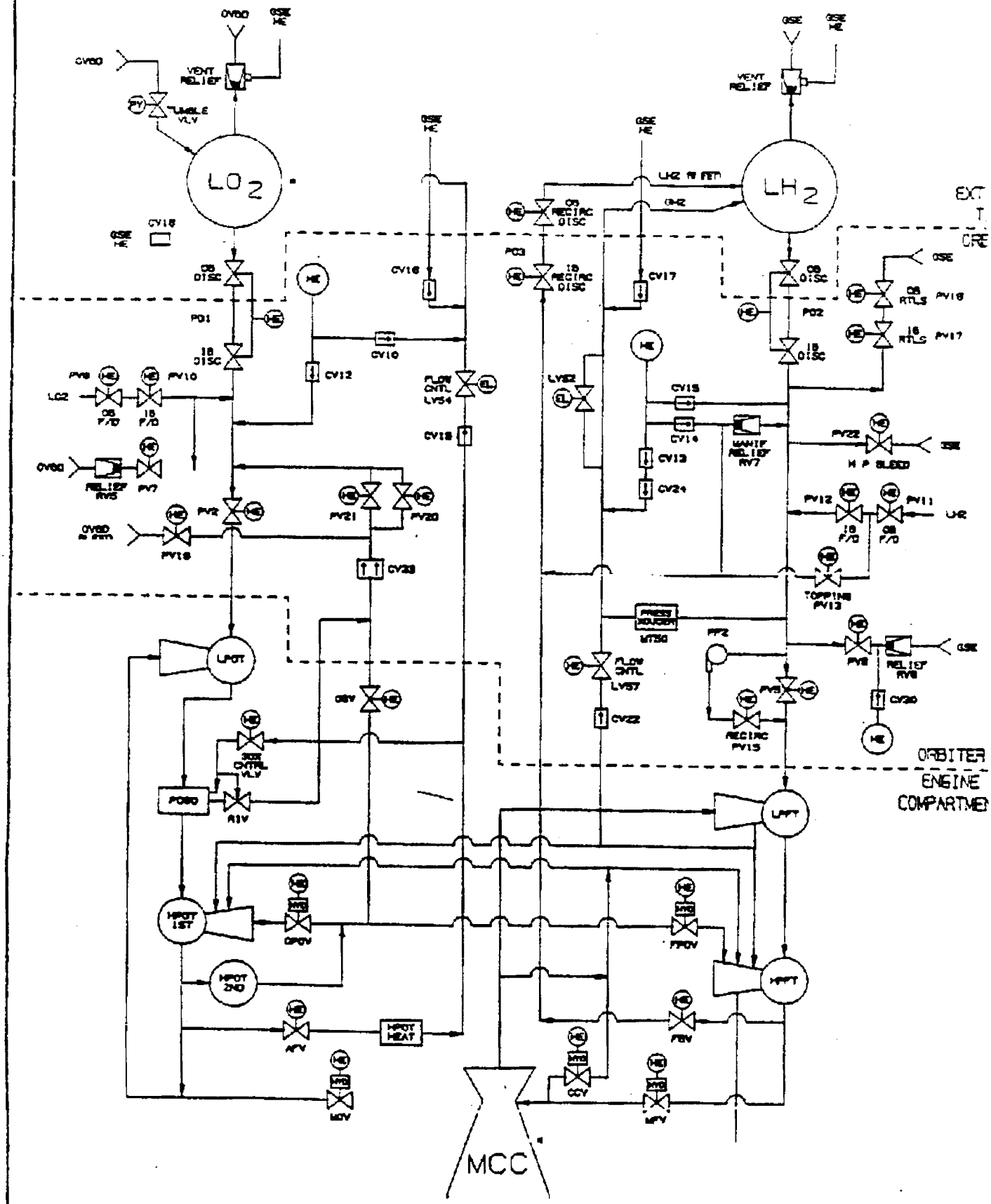
TABLE 5-1

Salient Differences and Points of Asymmetry
Between LO2 and LH2 Propellant Systems

Component/Subsystem	LO2	LH2
External Tank (ET)	Propellant tank on the top portion of ET. Has a tumble valve	Propellant tank on the bottom portion of ET. No tumble valve
Location of ET low level sensing devices (ET separation parameter)	Inside orbiter on main flow line downstream of the ET/orbiter disconnect valves	On ET
Propellant prevalves	Open/close circuitry and valve pneumatic actuator differences	Open/close circuitry and pneumatic actuator differences
POGO Suppression and antigeysering line	POGO accumulator and isolation valves and antigeysering line	No POGO suppression or antigeysering line
Low pressure turbo pumps	Driven by high pressure turbopump discharge pressure. No recirculation pump system used.	Driven by main engine chamber coolant pressure
High pressure turbo pumps	Regulated by LO2 flow control valves on LPOT preburners. Heat exchanger coils on the pump preburner	Regulated by LO2 flow control valves on preburners. No LH2 flow control valves are used on the LPFT preburners. No heat exchange.
Recirculation pumps	No recirculation pump system is used	Recirculation flow initiated for propellant system downstream of prevalves

Figure 3-4

LH2 / LO2 VALVE SCHEMATIC



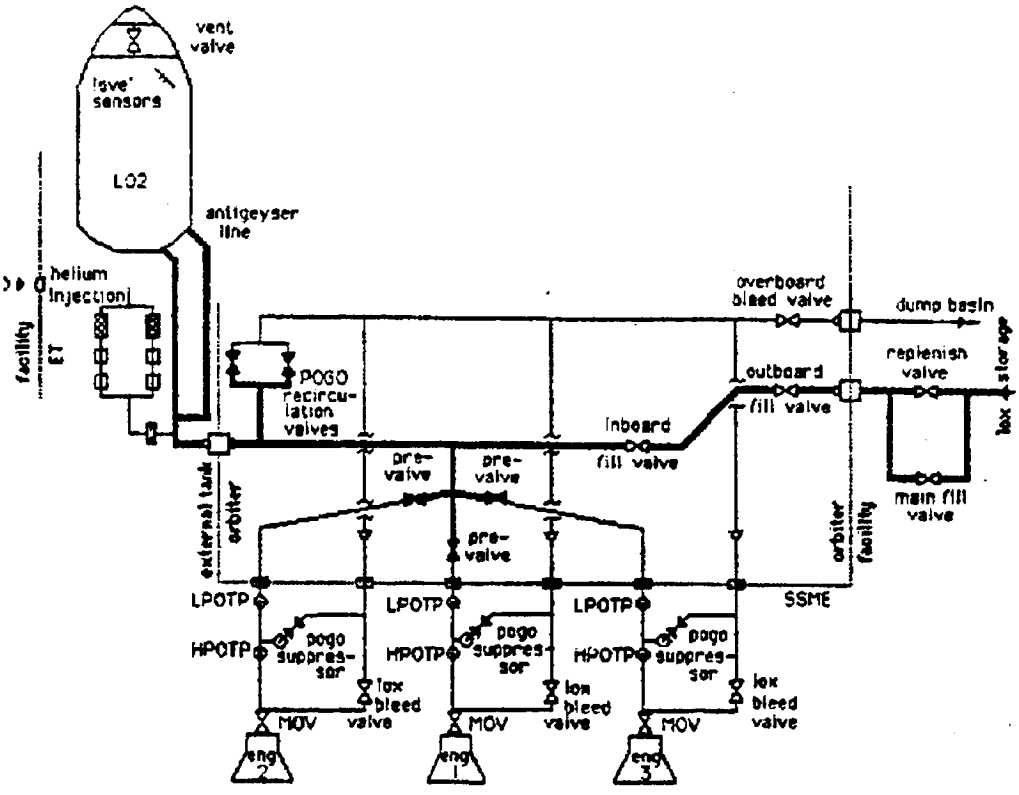


FIGURE 5-1a

LO2 PROPELLANT DELIVERY SYSTEM

(During Fill Operations)

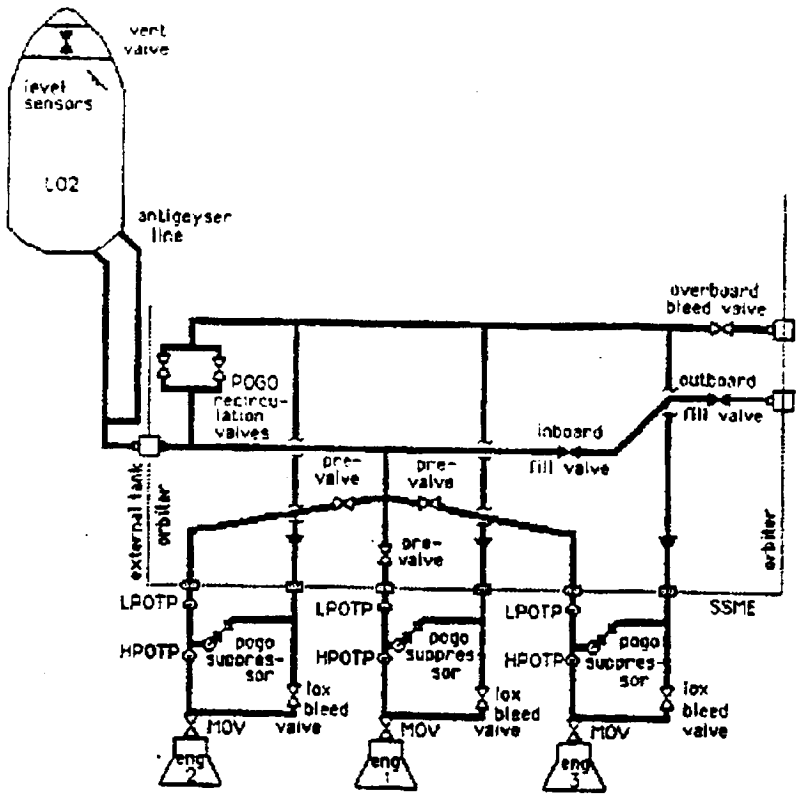


FIGURE 5-1b

LO2 PROPELLANT DELIVERY SYSTEM
(During Flight)

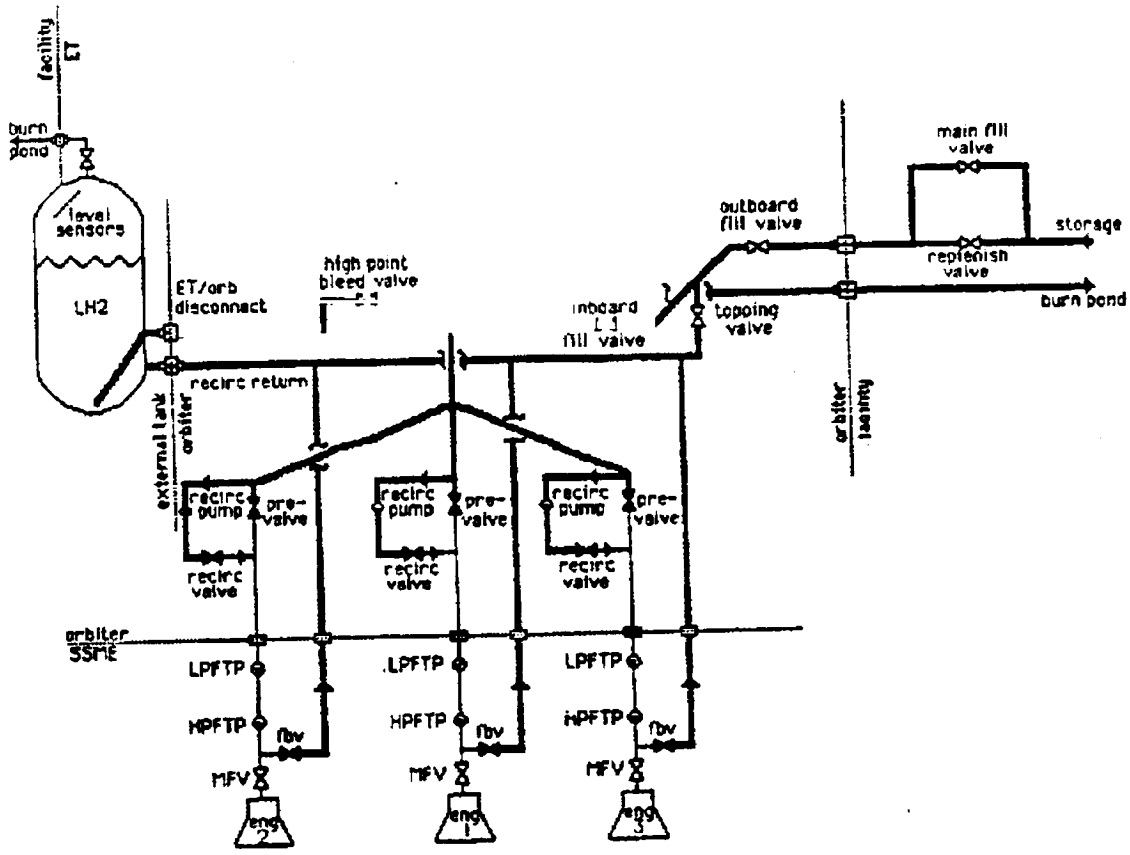


FIGURE 5-2a

LH2 PROPELLANT DELIVERY SYSTEM

(During Fill Operations)

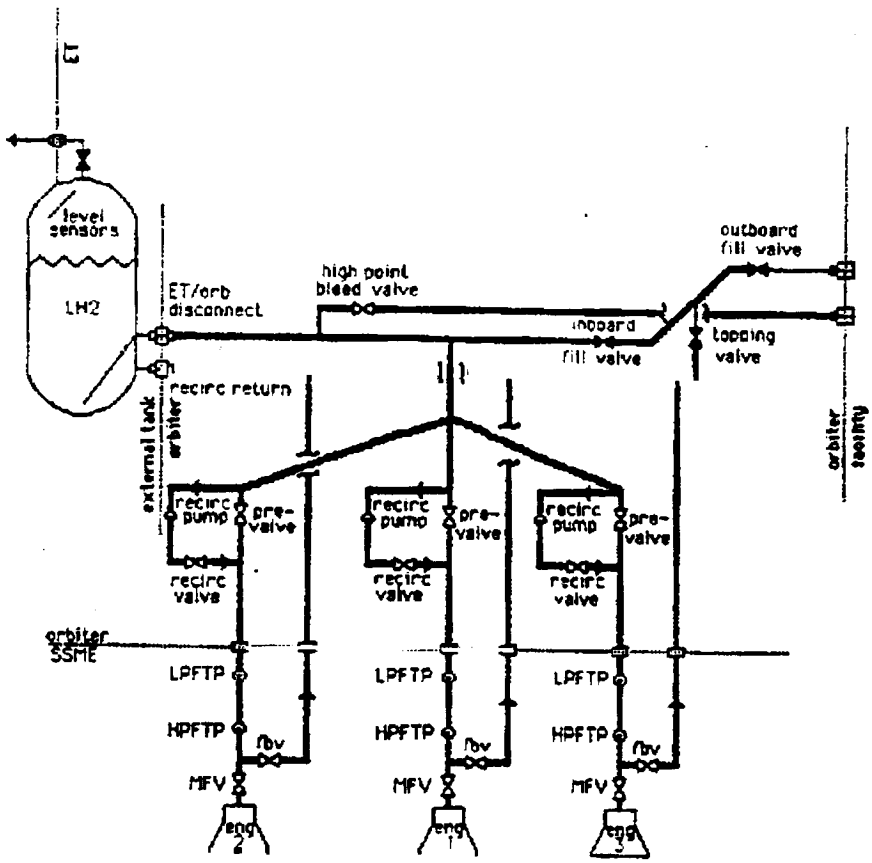


FIGURE 5-2b

LH2 PROPELLANT DELIVERY SYSTEM

(During Flight)

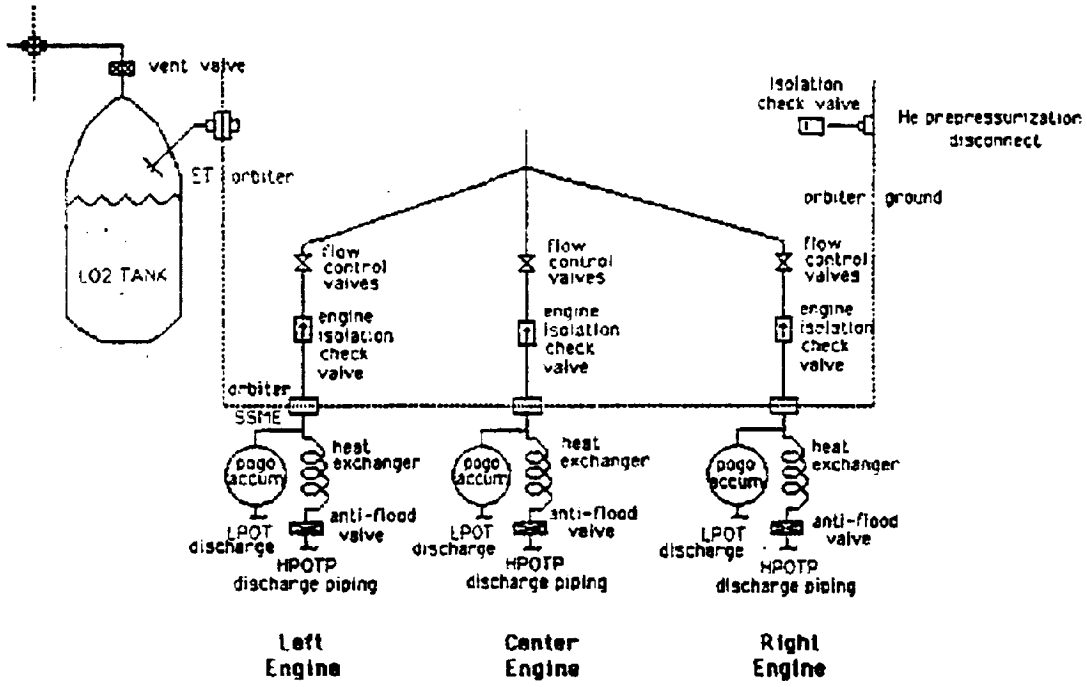


Figure S-3a

LO2 TANK PRESSURIZATION SCHEMATIC

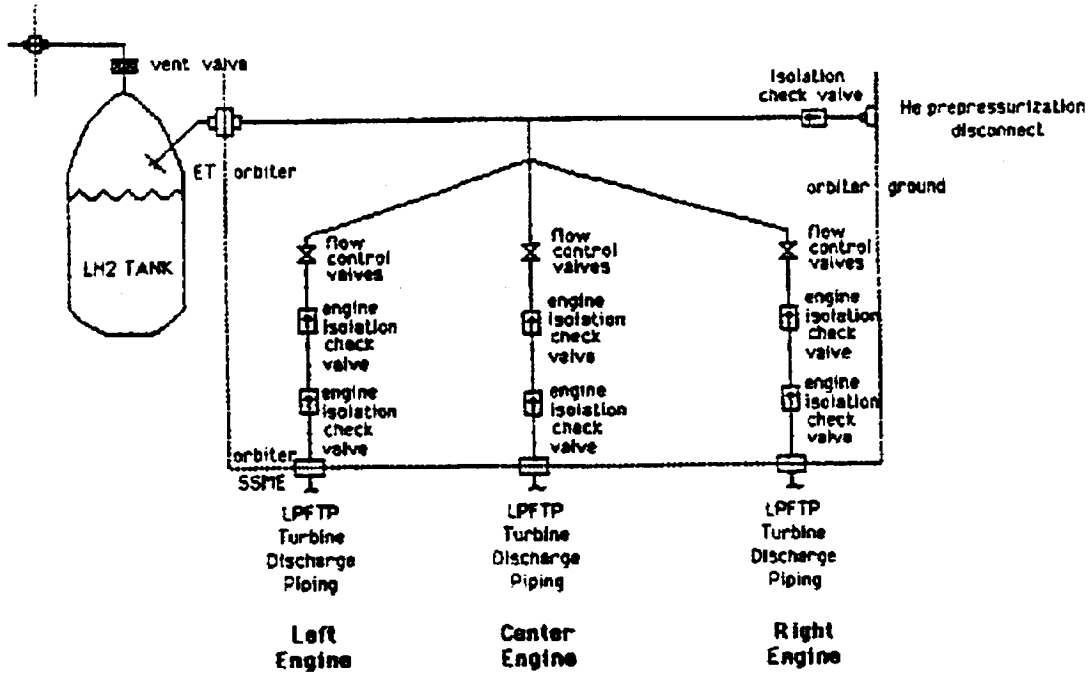


Figure S-3b

LH2 TANK PRESSURIZATION SCHEMATIC

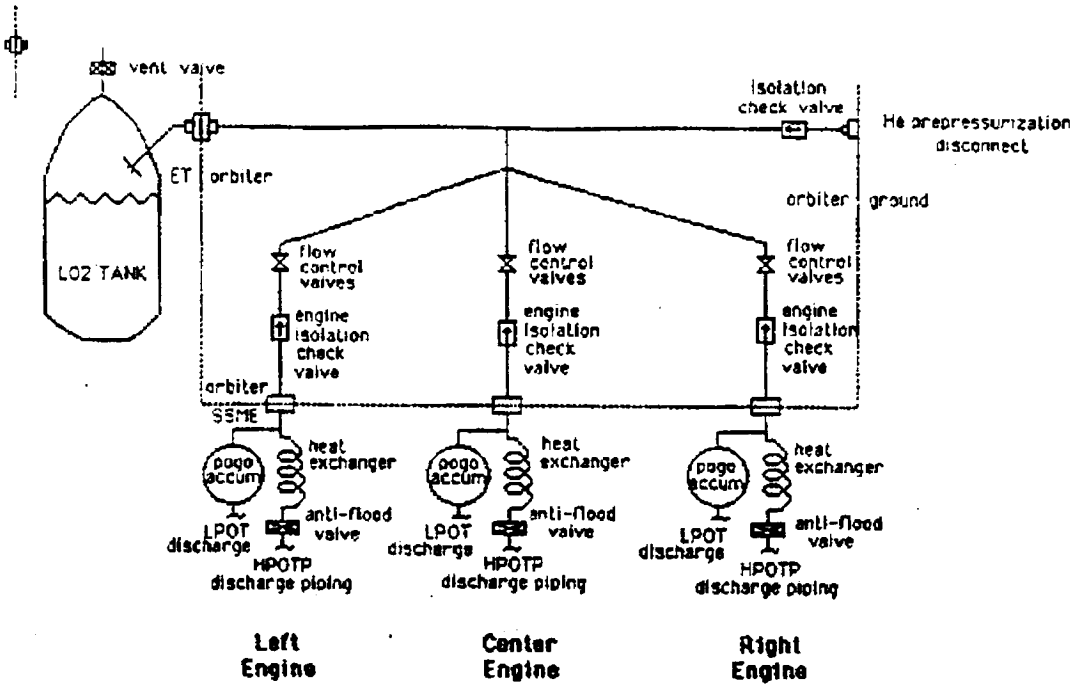


Figure 5-3a

LO2 TANK PRESSURIZATION SCHEMATIC

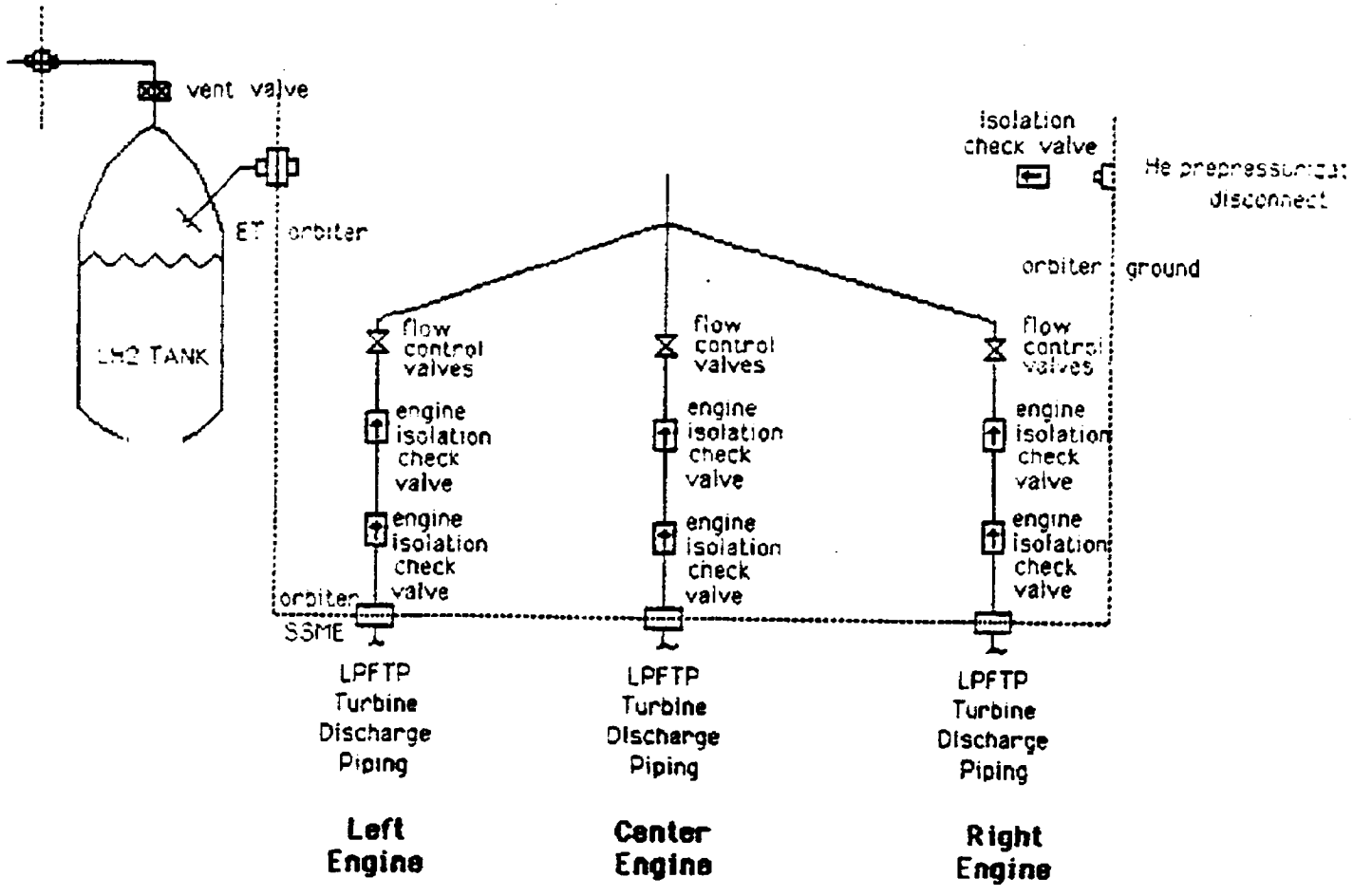
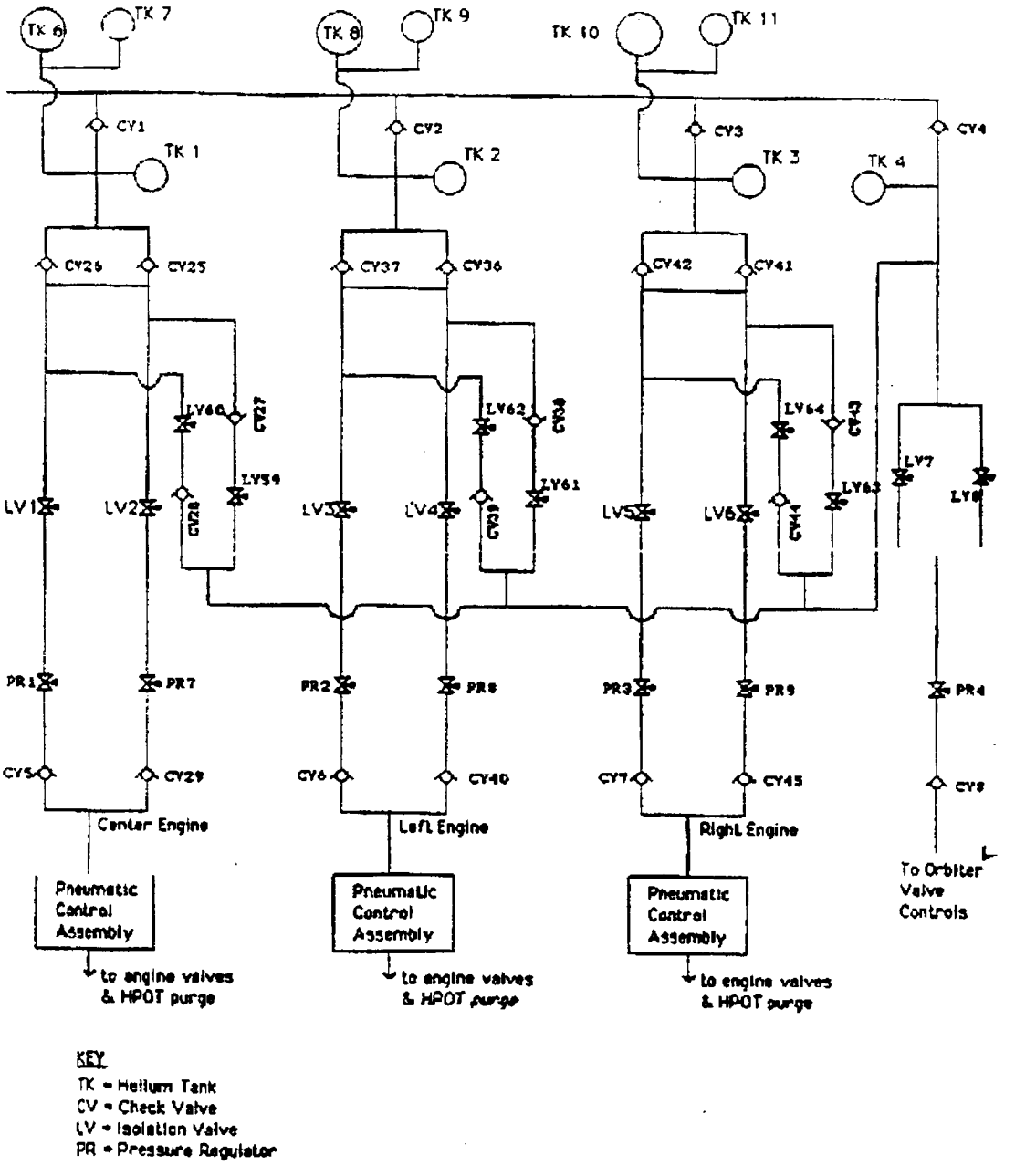


Figure 5-3b

LH2 TANK PRESSURIZATION SCHEMATIC

FIGURE 5-4 SIMPLIFIED HELIUM SYSTEM SCHEMATIC



KEY
TK = Helium Tank
CV = Check Valve
LV = Isolation Valve
PR = Pressure Regulator

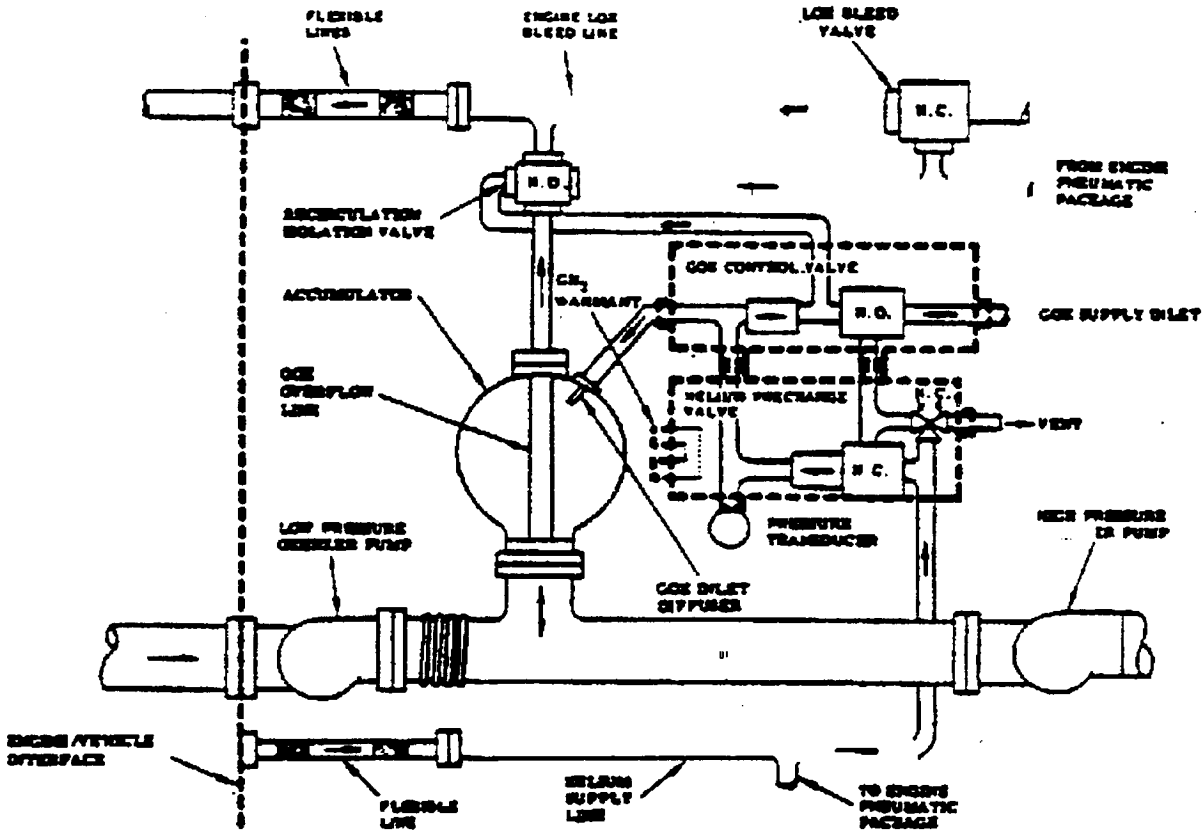


Figure 5-5, Pogo suppression system schematic.

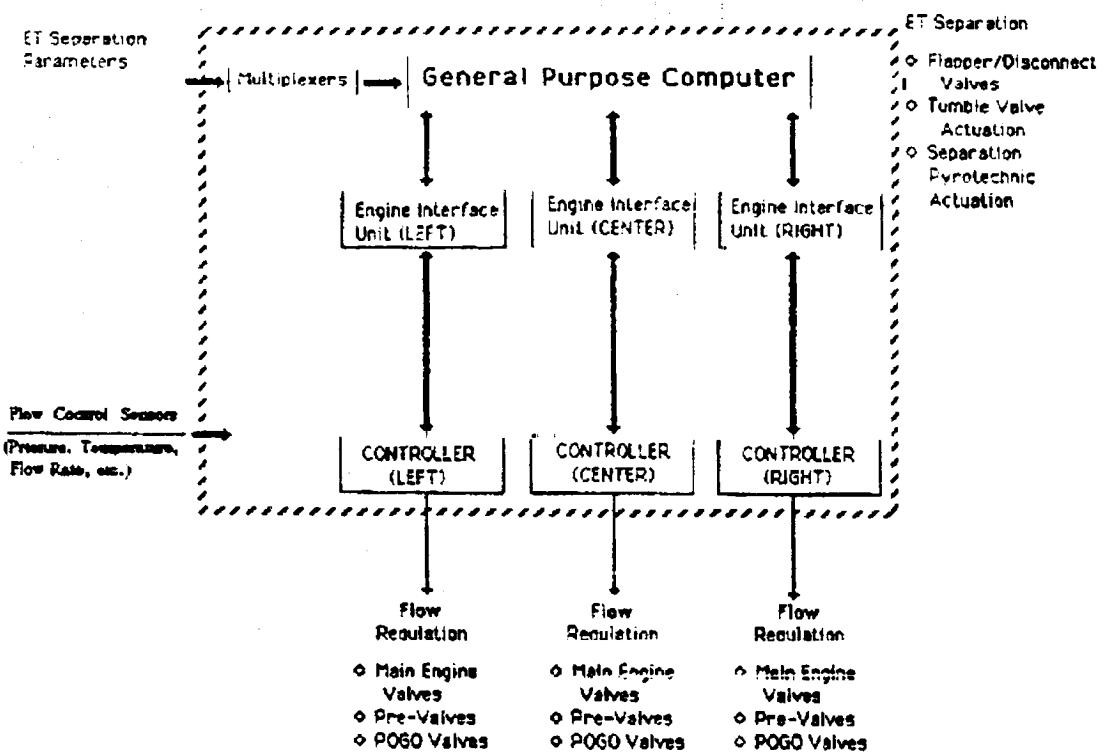


FIGURE 5-6

SIMPLIFIED FUNCTIONAL BLOCK DIAGRAM OF MPPS ELECTRICAL CONTROL SYSTEM *

* DASHED LINE SIGNIFIES THE CONTROL SYSTEM BOUNDARY NOT ANALYZED IN THIS STUDY.

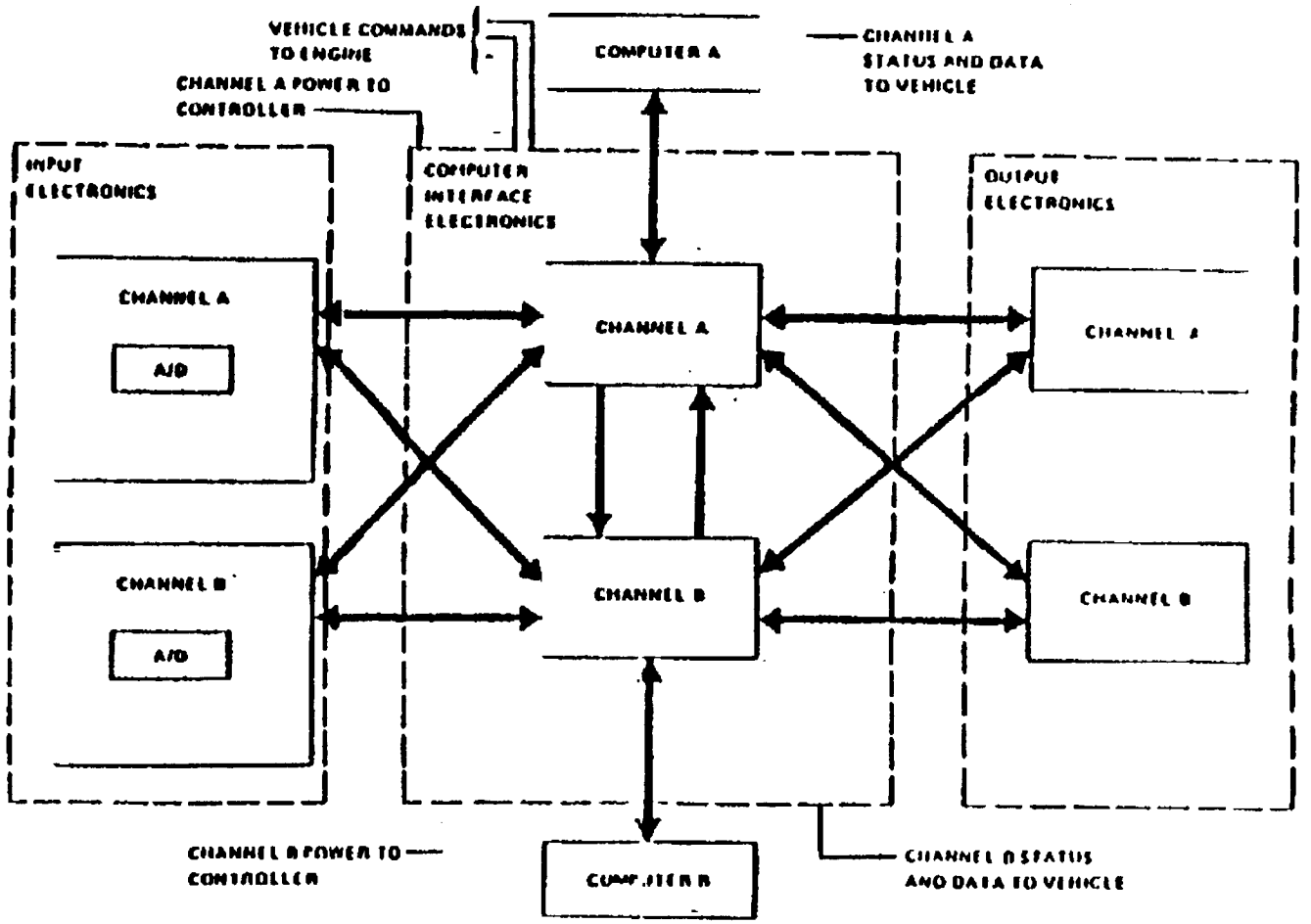


Figure 5-7, SSME controller simplified redundancy diagram

Section 6

RISK ASSESSMENT

Risk is typically defined as the product of the probability of an event occurrence and the severity of its consequences, or

$$\text{Risk} = \text{Probability} \times \text{Severity} \qquad \text{Equation 6-1}$$

For this study, the risk is a loss of life and/or vehicle due to a combination of MPPS related failures. The probability is that of loss of life and/or vehicle during a mission. Severity is measured in terms of the number of potential fatalities and hardware losses resulting from a catastrophic failure.

Equation 6-1 is, however, a simplistic representation of risk. The severity of an accident varies as a function of the specific failure scenario or combination. Consider, for example, a catastrophic loss of engine thrust within the first few seconds following lift-off. The severity of this failure will vary depending on whether or not the STS has cleared the launch facility. Timing of the failure is just one crucial factor in assessing the total resulting damage. Risk can thus be redefined as the sum of the risks created during various stages of the mission, or

$$\text{Risk} = \sum (F \times S)i \qquad \text{Equation 6-2}$$

Where F = The probability of catastrophic failure during a mission time interval "i"

S = The severity of the catastrophic failure during interval "i".

Throughout this section, emphasis will be placed on consequence as a function of mission time.

6.1 LAUNCH AND PRELAUNCH TIME SEQUENCE

An event tree may be used as a method of depicting the various outcomes (or levels of severity) for time dependent failures. Figures 6-1a and 6-1b show a time-sequence event tree representing scenarios which would result if a catastrophic accident occurred during the different intervals of the mission. The lower branches represent either a failure to successfully avoid a catastrophic event or a failure to accomplish a critical recovery operation (e.g., abort landing). Upper branches represent success.

Two separate event trees are developed to provide some distinction between those events which are not recoverable or immediately catastrophic (i.e. fire, explosion, aft compartment overpressurization and other non-recoverable events) and those events for which an abort is possible. Leakage and rupture of propellant system or other pressure boundary create situations in which the recovery time is very compressed. Figure 6-1a, therefore, represents fairly straight forward outcome status in which an immediate catastrophy is expected. Figure 6-1b, however, includes many potential abort scenarios. The consequences

are similarly dependent on the time phase. That is, ground facilities and personnel associated with the various abort landing sites will be affected by the abort sequence attempted (i.e. PTLS, TAL, etc.)

Using the cutsets generated by CAFTA, a determination is made regarding which cutsets are applicable to the various branches of the event tree. The exposure times for each basic event in the cutsets is then carefully reviewed to ensure that proper probabilities are assigned for each of the time intervals (Refer to Appendix C, Table C-5 for time-phased probabilities). Tables 6-1a and 6-1b identify the pertinant cutsets for each event tree branch. It is necessary, for practical purposes, to truncate cutsets whose probabilities fall below 10 -8.

The probability of an outcome state is the product of all event tree branches leading to that state. The probability of each branch of the tree is obtained by selecting the appropriate portions of the master fault tree and applying probabilities to the basic events corresponding to the respective exposure times (i.e., time intervals). Abort scenarios have not been probabilistically quantified since these are outside the scope of analysis. For time intervals between T + 30 seconds and zero thrust, fault tree probabilities were adjusted for fractional exposure times (e.g. subdivisions of flight phases). The fractions are shown along side the fault tree mnemonics on the event trees.

6.1.1 Basis for Division of Time Intervals

The divisions shown in the event tree represent time intervals which define distinct outcomes. In other words, by subdividing the time intervals further, one would obtain the same number of outcome states, but a greater number of individual sequences dependent on the subdivided time interval; no significant additional information regarding risk is obtained from such a subdivision.

The time-line for our mission profile begins with flight preparation operations at approximately T-8 hours. Major flight preparation operations, including cryogen fill, system purging and initial system checkout are performed mainly during the interval between T-8 hours and crew boarding at T-2 hours. This interval is chosen as a convenient segment of time because any catastrophic accidents resulting during these six hours primarily affect the ground support equipment and launch facility. At the time of crew boarding, the consequences of a major accident would at least potentially include loss of flight crew life. Other consequence categories are identified in Table 6-2.

Time intervals during ignition and the flight are similarly divided into milestone changes in the accident outcome. From T-10 seconds until the time STS clears all ground facilities, a catastrophic accident may not be limited solely to the loss of STS and crew. Ground facilities may be affected from scattered debris following explosion. The STS is conservatively assumed to pose no threat to the ground facilities and non-crew members after 30 seconds. All other flight operations and sequences are grouped into a single time interval which extends until MECO and ET separation. It is important to note that unsuccessful abort landing scenarios have risks associated not only with the STS/crew, but potentially with personnel, facilities, and other hardware at the abort landing site.

Events which do not necessarily lead to an immediate catastrophic accident (e.g. recoverable events) have time intervals subdivided. This is necessary because abort scenarios resulting from system failures are highly dependent on the timing of the event. The three subdivisions of the fault tree time interval T + 30 seconds to zero thrust are as follows:

- T + 30 seconds to T + 2.5 minutes
- T + 2.5 minutes to T + 4.0 minutes
- T + 4.0 minutes to zero thrust

This corresponds to an RTLS, TAL and orbital abort, respectively.

6.1.2 Consequence Data

As previously discussed, consequence are measured as expected number of fatalities and hardware/facilities losses (in $). No attempt is made in this analysis to combine these two categories of losses.

Some conservative assumptions are made regarding loss of human life following an accident:

- Catastrophic explosions/fires on the launch pad between T-8 hours and crew boarding at T-2.1 hours are assumed to cause only hardware damage.
- Catastrophic exposions/fires between the time of crew boarding and engine start sequence are assumed to cause death of crew.
- Accidents occuring between engine start and T+30 seconds are assumed to cause death of crew. Additionally, depending on the time of failure, flying debris, explosion fragments and shock waves are assumed to damage surrounding buildings and structures and potentially cause additional injuries/deaths.
- Major accidents after T+30 seconds are assumed to affect only the crew with the exception of potential loss of ground personnel at abort landing sites if abort is possible.

Similarly, hardware and facilities are affected according to the interval. Any catastrophic explosion prior to T+30 seconds affects the STS plus the pad. Except for abort landing scenarios, only the STS and ships in the trajectory footprint are assumed to be affected once the STS has cleared the launch facility.

A summary of consequence data is provided in Table 6-3. These losses are reflected in terms of a probability density function discussed later in this section.

6.2 SUMMARY OF RISK COMPUTATIONS

The branch probabilities on Figure 6-1a and 6-1b are used to compute each of the consequence probabilities.

The consequence categories are then quantified according to their risk value using Equation 6-2. The severity is based on the expected human and hardware losses specified in Table 6-3. The aggregate probability of each of the consequence categories is shown for both human and hardware losses in Tables 6-4a and 6-4b, respectively. It is important to note that the losses are strictly represented by those failures represented by the scope of this PRA. Other risks not within the scope defined by the fault tree cut sets are necessarily not factored into these results.

Two separate estimates of aggregate probabilities are presented in Tables 6-1a and 6-1b in order to distinguish between events in which successful abort was achieved and those events which end in ultimate loss of life/vehicle. No attempt is made to quantify the likelihood of successful abort landing given a disabling failure. Therefore the specified total probability (for each of the consequence categories) is provided to show a range of probabilities with and without abort recovery.

Abort landings can at best be expected to reduce overall risk of MPPS-related accidents by less than 10%. The importance of abort landing towards risk reduction varies depending on the system involved. MPPS failures are seldom recoverable ones and, therefore, abort scenarios provide minor overall risk reduction. Most failure probability contributions are due to non-recoverable failures such as immediate explosions or aft compartment overpressurization events. In total, non-recoverable events are more than one order of magnitude higher than recoverable events, or events in which abort landing is a viable option.

Risk to human life, as may be expected, is almost exclusively the result of loss of STS crew. The expected loss of life due to MPPS failure is more than one death per hundred flights. A residual, but insignificant, risk is posed to other persons in the general vicinity of the launch facility if a catastrophic explosion occurs during the first 30 seconds of flight.

Risk to hardware consists primarily of the loss of the STS vehicle and payload (note: payload loss is not included in cost estimates of STS loss). The average loss per launch is estimated to be approximately $3M. Facility damage is the next greatest source of monetary loss totalling under $0.1 M per launch. The remaining sequences contribute minimally to the total expected losses.

EVENT TREE QUANTIFICATION USING FAULT TREE CUTSETS FOR EXPLOSION, OVERPRESSURIZATION AND OTHER NON-RECOVERABLE EVENTS

Event Tree Branch (figure 6-1a)	Applicable Cutsets		Cutset Probability	TOTAL
A	CND4ZO1G	GSEUXXST	*	*
B	CND4ZO1G	GSEUXXST	*	*
C	FLGEOSLK	CNDEZX1G	1.24E-05	2.02E-04
	SPVVPXDP	VENTPANEL	8.94E-06	
	VENTPANEL	MPBVP3LK	8.32E-06	
	MPBVP5LK	VENTPANEL	8.07E-06	
	MPBVP1LK	VENTPANEL	8.07E-06	
	MPBEOSLK	CNDEZX1G	6.57E-06	
	CNDEZX1G	FLGEFSLK	5.84E-06	
	MPBEFSLK	CNDEZX1G	4.39E-06	
	MPBVOSLK	CNDVZX1G	3.98E-06	
	MPBVFSLK	CNDVZX1G	3.90E-06	
	MPBEOPRP	CNDEZX1G	3.72E-06	
	FLGEJSLK		3.65E-06	
	SPVCPCDP		3.30E-06	
	SPVRPCDP		3.30E-06	
	SPVLPCDP		3.30E-06	
	BDPEOXRP	CNDEZX1G	3.07E-06	
	CNDEZX1G	BDPEFXRP	3.07E-06	
	MPBEJPRP		2.99E-06	
	ACCRPXDP		2.68E-06	
	TNKVP0DP	VENTPANEL	2.68E-06	
	TNKVP6DP	VENTPANEL	2.68E-06	
	TNKVP1DP	VENTPANEL	2.68E-06	
	TNKVP8DP	VENTPANEL	2.68E-06	
	TNKVPEDP	VENTPANEL	2.68E-06	
	TNKVP2DP	VENTPANEL	2.68E-06	
	TNKVP7DP	VENTPANEL	2.68E-06	
	TNKVP9DP	VENTPANEL	2.68E-06	
	ACCLPXDP		2.68E-06	
	TNKVP3DP	VENTPANEL	2.68E-06	
	TNKVP4DP	VENTPANEL	2.68E-06	
	ACCCPXDP		2.68E-06	
	MPBVJSLK		2.67E-06	
	MPBEFPRP	CNDEZX1G	2.52E-06	
	FLGENSLK		2.19E-06	
	FLGTNSLK		2.19E-06	

MPBENSLK		2.19E-06	
MPBVNSLK		2.19E-06	
MPBLP3DP	VENTPANEL	2.11E-06	
MPBRP5DP	VENTPANEL	2.07E-06	
MPBCP1DP	VENTPANEL	2.07E-06	
MPBENPRP		1.73E-06	
FLGTJSLK		1.46E-06	
FLGEOSLK	CNDGRLK	1.24E-06	
SCHVP6RP	VENTPANEL	1.10E-06	
SCHVP5RP	VENTPANEL	1.10E-06	
ACCCOMRP		1.05E-06	
ACCLOMRP		1.05E-06	
ACCROMRP		1.05E-06	
SLVCFXOP		9.19E-07	
SLVCOXOP		9.19E-07	
SLVLFXOP		9.19E-07	
SLVRFXOP		9.19E-07	
SLVLOXOP		9.19E-07	
SLVROXOP		9.19E-07	
MPBVOPRP	CNDVZXIG	8.19E-07	
MPBVJPRP		7.74E-07	
REGRP3CS		7.00E-07	
REGVPXHI	VENTPANEL	7.00E-07	
REGRP3OP		7.00E-07	
REGLP8OP		7.00E-07	
REGLP2CS		7.00E-07	
REGCP1CS		7.00E-07	
REGRP9OP		7.00E-07	
REGCP7CS		7.00E-07	
REGCP1OP		7.00E-07	
REGCP7OP		7.00E-07	
REGLP8CS		7.00E-07	
REGRP9CS		7.00E-07	
REGLP2OP		7.00E-07	
TPSROXRP		6.77E-07	
TPSRFLLK		6.77E-07	
TPSLOXRP		6.77E-07	
TPSLFLLK		6.77E-07	
TPSCOXRP		6.77E-07	
TPSCFLLK		6.77E-07	
MPBEOSLK	CNDGRLK	6.57E-07	
MPBVNPRP		6.42E-07	
FLGEFSLK	CNDGRLK	5.84E-07	
MPBVFPRP	CNDVZXIG	5.75E-07	
MPBEFSLK	CNDGRLK	4.39E-07	
MPBTNPRP		3.98E-07	
MPBYOSLK	CNDGRLK	3.98E-07	
MPBVFSLK	CNDGRLK	3.90E-07	
PNYRFZCS		3.76E-07	

	PNV3NDCS		3.76E-07	
	PNV30DCS		3.76E-07	
	PNVL0ZCS		3.76E-07	
	PNVLFZCS		3.76E-07	
	PNV3JDCS		3.76E-07	
	PNVR0ZCS		3.76E-07	
	PNVCFZCS		3.76E-07	
	PNVC0ZCS		3.76E-07	
	PNV3FDCS		3.76E-07	
	MPBE0PRP	CNDGRLK	3.72E-07	
	BDPEFXRP	CNDGRLK	3.07E-07	
	BDPE0XRP	CNDGRLK	3.07E-07	
	MPBLP3LK	VENTPANEL	2.98E-07	
	MPBRP5LK	VENTPANEL	2.98E-07	
	MPBCP1LK	VENTPANEL	2.98E-07	
	MPBTJPRP		2.66E-07	
	MPBEFPRP	CNDGRLK	2.52E-07	
	MPBVP2LK	VENTPANEL	2.52E-07	
	MPBVP4LK	VENTPANEL	2.52E-07	
	MPBVP6LK	VENTPANEL	2.52E-07	
	PRBR0SLK		2.45E-07	
	PRBRFSLK		2.45E-07	
	PRBCFSLK		2.45E-07	
	PRBLFSLK		2.45E-07	
	PRBL0SLK		2.45E-07	
	PRBC0SLK		2.45E-07	
	MPETNSLK		2.44E-07	
	MPBTJSLK		2.44E-07	
	PAV0TXPA		2.44E-07	
	FILRCPLK		2.27E-07	
	FILLCPLK		2.27E-07	
	FILCPCLK		2.27E-07	
	FLGT0XLK	CNDGRLK	2.19E-07	
	CNDEZXIG	WLDE0XLK	1.76E-07	
	FILLFYRP		1.74E-07	
	FILRFYRP		1.74E-07	
	FILCFYRP		1.74E-07	
	FILR0YRP		1.74E-07	
	FILC0YRP		1.74E-07	
	FILL0YRP		1.74E-07	
	MPBCP2LK	VENTPANEL	1.60E-07	
	MPBRP6LK	VENTPANEL	1.60E-07	
	WLDEJXLK		1.42E-07	
	BLORORRG		1.40E-07	
	BLOC0GRG		1.40E-07	
	BLOL0GRG		1.40E-07	
	BLOLORRG		1.40E-07	
	BLOR0GRG		1.40E-07	
	BLOC0RRG		1.40E-07	

MPBLP4LK	VENTPANEL	1.37E-07	
TNKVP3DP	HUMRPXHC	1.34E-07	
TNKVP1DP	HUMCPXHC	1.34E-07	
TNKVP9DP	HUMLPXHC	1.34E-07	
TNKVP8DP	HUMLPXHC	1.34E-07	
TNKVP2DP	HUMLPXHC	1.34E-07	
TNKVP6DP	HUMCPXHC	1.34E-07	
TNKVP7DP	HUMCPXHC	1.34E-07	
TNKVPEDP	HUMRPXHC	1.34E-07	
TNKVPODP	HUMRPXHC	1.34E-07	
HGMEZSLK		1.19E-07	
MPBLP4DP	VENTPANEL	9.19E-08	
MPBCP2DP	VENTPANEL	9.19E-08	
MPBRP6DP	VENTPANEL	9.19E-08	
MPBVOPRP	CNDGRLK	8.19E-08	
WLDENXLK		8.17E-08	
MPBVFPRP	CNDGRLK	5.75E-08	
WLDVP3LK	VENTPANEL	5.05E-08	
WLDVP1LK	VENTPANEL	4.94E-08	
WLDVP5LK	VENTPANEL	4.94E-08	
CNDVZXIG	WLDVOXLK	3.88E-08	
MPBRPXLK	HUMRPXHC	3.78E-08	
MPBLPXLK	HUMLPXHC	3.78E-08	
MPBCPXLK	HUMCPXHC	3.78E-08	
MPBTOPRP	CNDGRLK	3.76E-08	
WLDVJXLK		3.67E-08	
PRVLP20P	VENTPANEL	3.62E-08	
PRVLP90P	VENTPANEL	3.62E-08	
PRVRP30P	VENTPANEL	3.62E-08	
PRVRP00P	VENTPANEL	3.62E-08	
PRVCP10P	VENTPANEL	3.62E-08	
PRVCP80P	VENTPANEL	3.62E-08	
PRVHFX0P		3.62E-08	
PRV00X0P		3.62E-08	
PRVVPX0P	VENTPANEL	3.62E-08	
PNVRPMRG	CNDMXXTM	3.21E-08	
PNVCPMRG	CNDMXXTM	3.21E-08	
PNVLPMRG	CNDMXXTM	3.21E-08	
WLDVNXLK		3.04E-08	
WLDVPXLK	VENTPANEL	2.77E-08	
WLDVFXLK	CNDVZXIG	2.72E-08	
HEXC0PRP		2.47E-08	
HEXR0PRP		2.47E-08	
HEXL0PRP		2.47E-08	
MPBTFSLK	CNDGRLK	2.44E-08	
FLGTFXLK	CNDGRLK	2.44E-08	
MPBTOSLK	CNDGRLK	2.44E-08	
WLDTNXLK		1.89E-08	
WLDE0XLK	CNDGRLK	1.76E-08	

	TPDCFLSZ		1.61E-08	
	TPDLFLSZ		1.61E-08	
	TPDRFLSZ		1.61E-08	
	TPDCOLSZ		1.61E-08	
	TPDLOLSZ		1.61E-08	
	TPDROLSZ		1.61E-08	
	MPBRP5LK	HUMRPXHC	1.49E-08	
	MPBLP3LK	HUMLPXHC	1.49E-08	
	MPBCP1LK	HUMCPXHC	1.49E-08	
	WLDTJXLK		1.26E-08	
	WLDEFXLK	CNDEZXIG	1.20E-08	
	CKVLPXCL		1.16E-08	
	CKVCPXCL		1.16E-08	
	CKVRPXCL		1.16E-08	
	MPBRP6LK	HUMRPXHC	8.01E-09	
	MPBCP2LK	HUMCPXHC	8.01E-09	
	MPBLP4LK	HUMLPXHC	6.87E-09	
	MPBTFPRP	CNDGRLK	6.64E-09	
	WLDVOXLK	CNDGRLK	3.88E-09	
	WLDVFXLK	CNDGRLK	2.72E-09	
	WLDVP4LK	VENTPANEL	2.72E-09	
	WLDVP2LK	VENTPANEL	2.72E-09	
	WLDVP6LK	VENTPANEL	2.72E-09	
	PLGLOPCL		1.97E-09	
	PLGCOPCL		1.97E-09	
	PLGROPCL		1.97E-09	
	WLDTOXLK	CNDGRLK	1.78E-09	
	WLDEFXLK	CNDGRLK	1.20E-09	
D	FLGEOSLK	CNDEZXIG	1.29E-04	2.05E-03
	SPVVPXDP	VENTPANEL	9.32E-05	
	VENTPANEL	MPBVP3LK	8.68E-05	
	MPBVP5LK	VENTPANEL	8.42E-05	
	MPBVP1LK	VENTPANEL	8.42E-05	
	MPBEOSLK	CNDEZXIG	6.85E-05	
	CNDEZXIG	FLGEFSLK	6.09E-05	
	MPBEFSLK	CNDEZXIG	4.57E-05	
	MPBVOSLK	CNDVZXIG	4.15E-05	
	MPBVFSLK	CNDVZXIG	4.06E-05	
	MPBEOPRP	CNDEZXIG	3.88E-05	
	FLGEJSLK		3.80E-05	
	SPVCPCDP		3.44E-05	
	SPRPCDP		3.44E-05	
	SPVLPCDP		3.44E-05	
	BDPEOXRP	CNDEZXIG	3.20E-05	
	CNDEZXIG	BDPEFXRP	3.20E-05	
	MPBEJPRP		3.11E-05	
	ACCRPXDP		2.80E-05	
	TNKVPODP	VENTPANEL	2.80E-05	
	TNKVP6DP	VENTPANEL	2.80E-05	

TNKVP1DP	VENTPANEL	2.80E-05	
TNKVP8DP	VENTPANEL	2.80E-05	
TNKVPEDP	VENTPANEL	2.80E-05	
TNKVP2DP	VENTPANEL	2.80E-05	
TNKVP7DP	VENTPANEL	2.80E-05	
TNKVP9DP	VENTPANEL	2.80E-05	
ACCLPXDP		2.80E-05	
TNKVP3DP	VENTPANEL	2.80E-05	
TNKVP4DP	VENTPANEL	2.80E-05	
ACCCPXDP		2.80E-05	
MPBVJSLK		2.79E-05	
MPBEFPRP	CNDEZXIG	2.63E-05	
FLGENSLK		2.29E-05	
FLGTNSLK		2.29E-05	
MPBENSLK		2.29E-05	
MPBVNSLK		2.29E-05	
MPBLP3DP	VENTPANEL	2.20E-05	
MPBRP5DP	VENTPANEL	2.15E-05	
MPBCP1DP	VENTPANEL	2.15E-05	
MPBENPRP		1.80E-05	
FLGTJSLK		1.52E-05	
FLGEOSLK	CNDGRLK	1.29E-05	
SCHVP6RP	VENTPANEL	1.14E-05	
SCHVP5RP	VENTPANEL	1.14E-05	
ACCCOMRP		1.10E-05	
ACCLOMRP		1.10E-05	
ACCROMRP		1.10E-05	
MPBVOPRP	CNDYZXIG	8.54E-06	
MPBVJPRP		8.07E-06	
REGCP1CS		7.30E-06	
REGCP10P		7.30E-06	
REGCP7CS		7.30E-06	
REGCP70P		7.30E-06	
REGLP2CS		7.30E-06	
REGLP20P		7.30E-06	
REGLP8CS		7.30E-06	
REGLP80P		7.30E-06	
REGRP3CS		7.30E-06	
REGRP30P		7.30E-06	
REGRP9CS		7.30E-06	
REGRP90P		7.30E-06	
REGVPXHI	VENTPANEL	7.30E-06	
TPSCFLLK		7.06E-06	
TPSLFLLK		7.06E-06	
TPSRFLLK		7.06E-06	
TPSCOXRP		7.06E-06	
TPSROXRP		7.06E-06	
TPSLOXRP		7.06E-06	
MPBEOSLK	CNDGRLK	6.85E-06	

MPBYNPRP			6.69E-06
FLGEFSLK	CNDGRLK		6.09E-06
MPBVFPRP	CNDVZXIG		6.00E-06
MPBEFSLK	CNDGRLK		4.57E-06
MPBTNPRP			4.15E-06
MPBVOSLK	CNDGRLK		4.15E-06
MPBVFSLK	CNDGRLK		4.06E-06
PNVCFZCS			3.92E-06
PNVLOZCS			3.92E-06
PNV3NDCS			3.92E-06
PNV30DCS			3.92E-06
PNV3FDCS			3.92E-06
PNVCOZCS			3.92E-06
PNVRFZCS			3.92E-06
PNVROZCS			3.92E-06
PNV3JDCS			3.92E-06
PNVLFZCS			3.92E-06
MPBEOPRP	CNDGRLK		3.88E-06
BDPEFXRP	CNDGRLK		3.20E-06
BDPEOXRP	CNDGRLK		3.20E-06
MPBLP3LK	VENTPANEL		3.10E-06
MPBRP5LK	VENTPANEL		3.10E-06
MPBCP1LK	VENTPANEL		3.10E-06
MPBTJPRP			2.77E-06
MPBEFPRP	CNDGRLK		2.63E-06
MPBVP2LK	VENTPANEL		2.63E-06
MPBVP4LK	VENTPANEL		2.63E-06
MPBVP6LK	VENTPANEL		2.63E-06
PRBROSLK			2.55E-06
PRBRFSLK			2.55E-06
PRBCFSLK			2.55E-06
PRBLFSLK			2.55E-06
PRBLOSLK			2.55E-06
PRBCOSLK			2.55E-06
MPBTNSLK			2.54E-06
MPBTJSLK			2.54E-06
PAVOTXPA			2.54E-06
FILRCPLK			2.37E-06
FILLCPLK			2.37E-06
FILRCPLK			2.37E-06
FLGTOXLK	CNDGRLK		2.29E-06
CNDEZXIG	WLDEOXLK		1.84E-06
FILLFYRP			1.81E-06
FILRFYRP			1.81E-06
FILCFYRP			1.81E-06
FILROYRP			1.81E-06
FILCOYRP			1.81E-06
FILLOYRP			1.81E-06
MPBCP2LK	VENTPANEL		1.67E-06

MPBRP6LK	VENTPANEL	1.67E-06
WLDEJXLK		1.48E-06
BLORORRG		1.46E-06
BLOCOGRG		1.46E-06
BLOLOGRG		1.46E-06
BLOLORRG		1.46E-06
BLOROGRG		1.46E-06
BLOCORRG		1.46E-06
MPBLP4LK	VENTPANEL	1.43E-06
TNKVP3DP	HUMRPXHC	1.40E-06
TNKVP1DP	HUMCPXHC	1.40E-06
TNKVP9DP	HUMLPXHC	1.40E-06
TNKVP8DP	HUMLPXHC	1.40E-06
TNKVP2DP	HUMLPXHC	1.40E-06
TNKVP6DP	HUMCPXHC	1.40E-06
TNKVP7DP	HUMCPXHC	1.40E-06
TNKVPEDP	HUMRPXHC	1.40E-06
TNKVP0DP	HUMRPXHC	1.40E-06
HGMEZSLK		1.24E-06
MPBLP4DP	VENTPANEL	9.59E-07
MPBCP2DP	VENTPANEL	9.59E-07
MPBRP6DP	VENTPANEL	9.59E-07
MPBV0PRP	CNDGRLK	8.54E-07
MPBVFPRP	CNDGRLK	6.00E-07
WLDVP3LK	VENTPANEL	5.27E-07
WLDVP1LK	VENTPANEL	5.15E-07
WLDVP5LK	VENTPANEL	5.15E-07
CNDVZXIG	WLDV0XCLK	4.05E-07
MPBRPXLK	HUMRPXHC	3.94E-07
MPBLPXLK	HUMLPXHC	3.94E-07
MPBCPXLK	HUMCPXHC	3.94E-07
MPBT0PRP	CNDGRLK	3.92E-07
WLDVJXLK		3.83E-07
PRVLP20P	VENTPANEL	3.77E-07
PRVLP90P	VENTPANEL	3.77E-07
PRVRP30P	VENTPANEL	3.77E-07
PRVRP00P	VENTPANEL	3.77E-07
PRVCP10P	VENTPANEL	3.77E-07
PRVCP80P	VENTPANEL	3.77E-07
PRVHFX0P		3.77E-07
PRV00X0P		3.77E-07
PRVVPX0P	VENTPANEL	3.77E-07
PNVRPMRG	CNDMXXTM	3.35E-07
PNVLPMRG	CNDMXXTM	3.35E-07
PNVCPMRG	CNDMXXTM	3.35E-07
WLDVNXLK		3.17E-07
WLDVPXLK	VENTPANEL	2.88E-07
WLDVFXLK	CNDVZXIG	2.84E-07
HEXC0PRP		2.58E-07

	HEXROPRP		2.58E-07	
	HEXLOPRP		2.58E-07	
	MPBTFSLK	CNDGRLK	2.54E-07	
	FLGTFXLK	CNDGRLK	2.54E-07	
	MPBTOSLK	CNDGRLK	2.54E-07	
	WLDTNXLK		1.97E-07	
	WLDEOXLK	CNDGRLK	1.84E-07	
	TPDCFLSZ		1.68E-07	
	TPDLFLSZ		1.68E-07	
	TPDRFLSZ		1.68E-07	
	TPDCOLSZ		1.68E-07	
	TPDLOLSZ		1.68E-07	
	TPDROLSZ		1.68E-07	
	MPBRP5LK	HUMRPXHC	1.55E-07	
	MPBLP3LK	HUMLPXHC	1.55E-07	
	MPBCP1LK	HUMCPXHC	1.55E-07	
	CKVLPXCL		1.20E-07	
	CKVCPXCL		1.20E-07	
	CKVRPXCL		1.20E-07	
	MPBRP6LK	HUMRPXHC	8.35E-08	
	MPBCP2LK	HUMCPXHC	8.35E-08	
	MPBLP4LK	HUMLPXHC	7.17E-08	
	MPBTFPRP	CNDGRLK	6.92E-08	
	PN2ROZOP	CNDMXXTM	4.49E-08	
	PN2COZOP	CNDMXXTM	4.49E-08	
	PN2LOZOP	CNDMXXTM	4.49E-08	
	WLDVOXLK	CNDGRLK	4.05E-08	
	WLDVP2LK	VENTPANEL	2.89E-08	
	WLDVP4LK	VENTPANEL	2.89E-08	
	WLDVP6LK	VENTPANEL	2.89E-08	
	WLDVFXLK	CNDGRLK	2.84E-08	
	WLDVP4LK	VENTPANEL	2.83E-08	
	WLDVP2LK	VENTPANEL	2.83E-08	
	WLDVP6LK	VENTPANEL	2.83E-08	
	WLDTOXLK	CNDGRLK	1.86E-08	
	WLDEFXLK	CNDGRLK	1.25E-08	
E	SPVCPCDP		1.41E-06	1.29E-05
	SPVRPCDP		1.41E-06	
	SPVLPCDP		1.41E-06	
	BDPEOXRP	CNDEZXIG	1.32E-06	
	BDPEFXRP	CNDEZXIG	1.32E-06	
	ACCRPXDP		1.15E-06	
	ACCLPXDP		1.15E-06	
	ACCCPXDP		1.15E-06	
	MPBCP1DP	VENTPANEL	8.85E-07	
	SCHVP6RP	VENTPANEL	4.70E-07	
	SCHVP5RP	VENTPANEL	4.70E-07	
	MPBLP3LK	VENTPANEL	1.28E-07	
	MPBRP5LK	VENTPANEL	1.28E-07	

	MPBCP1LK	VENTPANEL	1.28E-07	
	MPBLP4LK	VENTPANEL	5.89E-08	
	MPBCP2DP	VENTPANEL	3.94E-08	
	MPBLP4DP	VENTPANEL	3.94E-08	
	MPBRP6DP	VENTPANEL	3.94E-08	
	MPBRPXLK	HUMRPXHC	1.62E-08	
	MPBLPXLK	HUMLPXHC	1.62E-08	
	MPBCPXLK	HUMCPXHC	1.62E-08	
	PRVLP20P	VENTPANEL	1.55E-08	
	PRVLP90P	VENTPANEL	1.55E-08	
	PRVRP30P	VENTPANEL	1.55E-08	
	PRVRP00P	VENTPANEL	1.55E-08	
	PRVCP10P	VENTPANEL	1.55E-08	
	PRVCP80P	VENTPANEL	1.55E-08	
	PRVHFX0P		1.55E-08	
	PRV00X0P		1.55E-08	
	PRVVPX0P	VENTPANEL	1.55E-08	
	WLDVP4LK	VENTPANEL	1.16E-09	
	WLDVP2LK	VENTPANEL	1.16E-09	
	WLDVP6LK	VENTPANEL	1.16E-09	

Table 6-1b

EVENT TREE QUANTIFICATION USING FAULT TREE CUTSETS FOR RECOVERABLE EVENTS

Event Tree Branch (Figure 6-1b)	CUTSETS				CUTSET PROBABILITY
A				**TOTAL FOR A**	**2.25E-07**
	MPBRPXLK	HUMRPXHC			3.48E-08
	MPBLPXLK	HUMLPXHC			3.48E-08
	MPBCPXLK	HUMCPXHC			3.48E-08
	SPVLP3DC	HUMLPXHC	MPBVP3LK		1.92E-08
	SPVCP1DC	MPBVP1LK	HUMCPXHC		1.86E-08
	SPVRP5DC	MPBVP5LK	HUMRPXHC		1.86E-08
	MPBCP1LK	HUMCPXLK			1.37E-08
	MPBLP3LK	HUMLPXHC			1.37E-08
	MPBRP5LK	HUMRPXHC			1.37E-08
	MPBRP6LK	HUMRPXHC			7.39E-09
	MPBCP2LK	HUMCPXHC			7.39E-09
	MPBLP4LK	HUMLPXHC			6.33E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LOJCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDCENT	HY2CFJCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDCENT	HY2CFWCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2ROWCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2ROJCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDCENT	HY2COJCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDCENT	HY2COWCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2RFJCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2RFWCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LFJCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LOWCD	1.59E-10
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LFWCD	1.59E-10
	PNVLPMRG	CNDFXXTF	CNDFXXSR	SDLEFT	1.35E-10
	CNDFXXTF	CNDFXXSR	SDRIGHT	PNVRPMRG	1.35E-10
	CNDFXXTF	CNDFXXSR	SDRIGHT	CK2RFZCD	4.87E-11
	CNDFXXTF	CNDFXXSR	SDLEFT	CK2LFZCD	4.87E-11
	CNDFXXTF	CNDFXXSR	SDCENT	CK2CFZCD	4.87E-11

Table 6-1b

B					TOTAL FOR B:	7.19E-07
	MPBRPXLK	HUMRPXHC				1.05E-07
	MPBLPXLK	HUMLPXHC				1.05E-07
	MPBCPXLK	HUMCPXHC				1.05E-07
	SPVLP3DC	HUMLPXHC	MPBVP3LK			5.75E-08
	SPVRP5DC	MPBVP5LK	HUMRPXHC			5.57E-08
	SPVCP1DC	MPBVP1LK	HUMCPXHC			5.57E-08
	MPBCP1LK	HUMCPXLK				4.12E-08
	MPBLP3LK	HUMLPXHC				4.12E-08
	MPBRP5LK	HUMRPXHC				4.12E-08
	MPBRP6LK	HUMRPXHC				2.22E-08
	MPBCP2LK	HUMCPXHC				2.22E-08
	MPBLP4LK	HUMLPXHC				1.90E-08
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LOJCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2CFJCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2CFWCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2ROWCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2ROJCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2COJCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2COWCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2RFJCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2RFWCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LFJCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LOWCD		3.40E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LFWCD		3.40E-09
	PNVLPMRG	CNDFXXTF	CNDFXXSR	SDLEFT		2.88E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	PNVRPMRG		2.88E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	CK2RFZCD		1.04E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	CK2LFZCD		1.04E-09
	CNDFXXTF	CNDFXXSR	SDCENT	CK2CFZCD		1.04E-09

Table 6-1b

C				TOTAL FOR C:	5.39E-07
	MPBRPXLK	HUMRPXHC			7.84E-08
	MPBLPXLK	HUMLPXHC			7.84E-08
	MPBCPXLK	HUMCPXHC			7.84E-08
	SPVRP5DC	MPBVP5LK	HUMRPXHC		4.18E-08
	SPVCP1DC	MPBVP1LK	HUMCPXHC		4.18E-08
	SPVLP3DC	HUMLPXHC	MPBVP3LK		4.31E-08
	MPBCP1LK	HUMCPXLK			3.09E-08
	MPBLP3LK	HUMLPXHC			3.09E-08
	MPBRP5LK	HUMRPXHC			3.09E-08
	MPBRP6LK	HUMRPXHC			1.66E-08
	MPBCP2LK	HUMCPXHC			1.66E-08
	MPBLP4LK	HUMLPXHC			1.43E-08
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LOJCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2CFJCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2CFWCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2ROWCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2ROJCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2COJCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDCENT	HY2COWCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2RFJCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	HY2RFWCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LFJCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LOWCD	2.55E-09
	CNDFXXTF	CNDFXXSR	SDLEFT	HY2LFWCD	2.55E-09
	PNVLPMRG	CNDFXXTF	CNDFXXSR	SDLEFT	2.16E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	PNVRPMRG	2.16E-09
	CNDFXXTF	CNDFXXSR	SDRIGHT	CK2RFZCD	7.79E-10
	CNDFXXTF	CNDFXXSR	SDLEFT	CK2LFZCD	7.79E-10
	CNDFXXTF	CNDFXXSR	SDCENT	CK2CFZCD	7.79E-10

D				TOTAL FOR D:	1.65E-05
	SEPINHIBIT	CNDTUFCO	SP130XFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP230XFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP13FXFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP23FXFE		2.93E-06
	SEPINHIBIT	CKT00FCD	CNDTUFCO		2.03E-06
	CKTHFFCD	SEPINHIBIT	CNDTUFCO		2.03E-06
	CNDTUFCO	HUMTSXHC	SP130XFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP230XFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP13FXFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP23FXFE		1.47E-07
	MPBRPXLK	HUMRPXHC			1.48E-08
	MPBLPXLK	HUMLPXHC			1.48E-08
	MPBCPXLK	HUMCPXHC			1.48E-08
	SPVLP3DC	HUMLPXHC	MPBVP3LK		8.14E-09
	SPVRP5DC	MPBVP5LK	HUMRPXHC		7.90E-09
	SPVCP1DC	MPBVP1LK	HUMCPXHC		7.90E-09
	CKT00FCD	CNDTUFCO	HUMTSXHC		6.77E-09
	CKTHFFCD	CNDTUFCO	HUMTSXHC		6.77E-09
	MPBCP1LK	HUMCPXLK			5.83E-09
	MPBLP3LK	HUMLPXHC			5.83E-09
	MPBRP5LK	HUMRPXHC			5.83E-09
	CNDTUFCO	PNVTFFDC	HUMTSXHC		5.07E-09
	CNDTUFCO	PNVT0FDC	HUMTSXHC		5.07E-09
	MPBCP2LK	HUMCPXHC			3.14E-09
	MPBRP6LK	HUMRPXHC			3.14E-09
	MPBLP4LK	HUMLPXHC			2.69E-09

Table 6-1b

E:				TOTAL FOR E:	1.04E-04
	HY2LOWCD	CNDMXXTM			6.19E-06
	HY2ROJCD	CNDMXXTM			6.19E-06
	HY2LOJCD	CNDMXXTM			6.19E-06
	HY2LFJCD	CNDMXXTM			6.19E-06
	HY2LFWCD	CNDMXXTM			6.19E-06
	HY2ROWCD	CNDMXXTM			6.19E-06
	HY2COJCD	CNDMXXTM			6.19E-06
	HY2COWCD	CNDMXXTM			6.19E-06
	HY2RFJCD	CNDMXXTM			6.19E-06
	HY2RFWCD	CNDMXXTM			6.19E-06
	HY2CFJCD	CNDMXXTM			6.19E-06
	HY2CFWCD	CNDMXXTM			6.19E-06
	CK2COZCD	CNDMXXTM			3.72E-06
	CK2LOZCD	CNDMXXTM			3.72E-06
	CK2ROZCD	CNDMXXTM			3.72E-06
	CK2CFZCD	CNDMXXTM			1.89E-06
	CK2LFZCD	CNDMXXTM			1.89E-06
	CK2RFZCD	CNDMXXTM			1.89E-06
	PN2LOZOP	CNDMXXTM			7.20E-07
	PN2ROZOP	CNDMXXTM			7.20E-07
	PN2COZOP	CNDMXXTM			7.20E-07
	PN2LFZOP	CNDMXXTM			7.20E-07
	PN2CFZOP	CNDMXXTM			7.20E-07
	PN2RFZOP	CNDMXXTM			7.20E-07
	HY2CFWCD	CNDMXXTM			4.37E-07
	HY2RFWCD	CNDMXXTM			4.37E-07
	HY2COJCD	CNDMXXTM			4.37E-07
	HY2ROJCD	CNDMXXTM			4.37E-07
	HY2COWCD	CNDMXXTM			4.37E-07
	HY2ROWCD	CNDMXXTM			4.37E-07
	HY2CFJCD	CNDMXXTM			4.37E-07
	HY2RFJCD	CNDMXXTM			4.37E-07
	HY2LFJCD	CNDMXXTM			4.37E-07
	HY2LOJCD	CNDMXXTM			4.37E-07
	HY2LFWCD	CNDMXXTM			4.37E-07
	HY2LOWCD	CNDMXXTM			4.37E-07
	CK2COZCD	CNDMXXTM			2.63E-07
	CK2LOZCD	CNDMXXTM			2.63E-07
	CK2ROZCD	CNDMXXTM			2.63E-07
	CKT30DSP				2.63E-07
	CKT3FDSP				2.63E-07
	MPBRPXLK	HUMRPXHC			2.09E-07
	MPBRPXLK	HUMRPXHC			2.09E-07
	MPBLPXLK	HUMLPXHC			2.09E-07
	MPBCPXLK	HUMCPXHC			2.09E-07
	SPVRP5DC	MPBVP5LK	HUMRPXHC		1.11E-07
	SPVCP1DC	MPBVP1LK	HUMCPXHC		1.11E-07

Table 6-1b

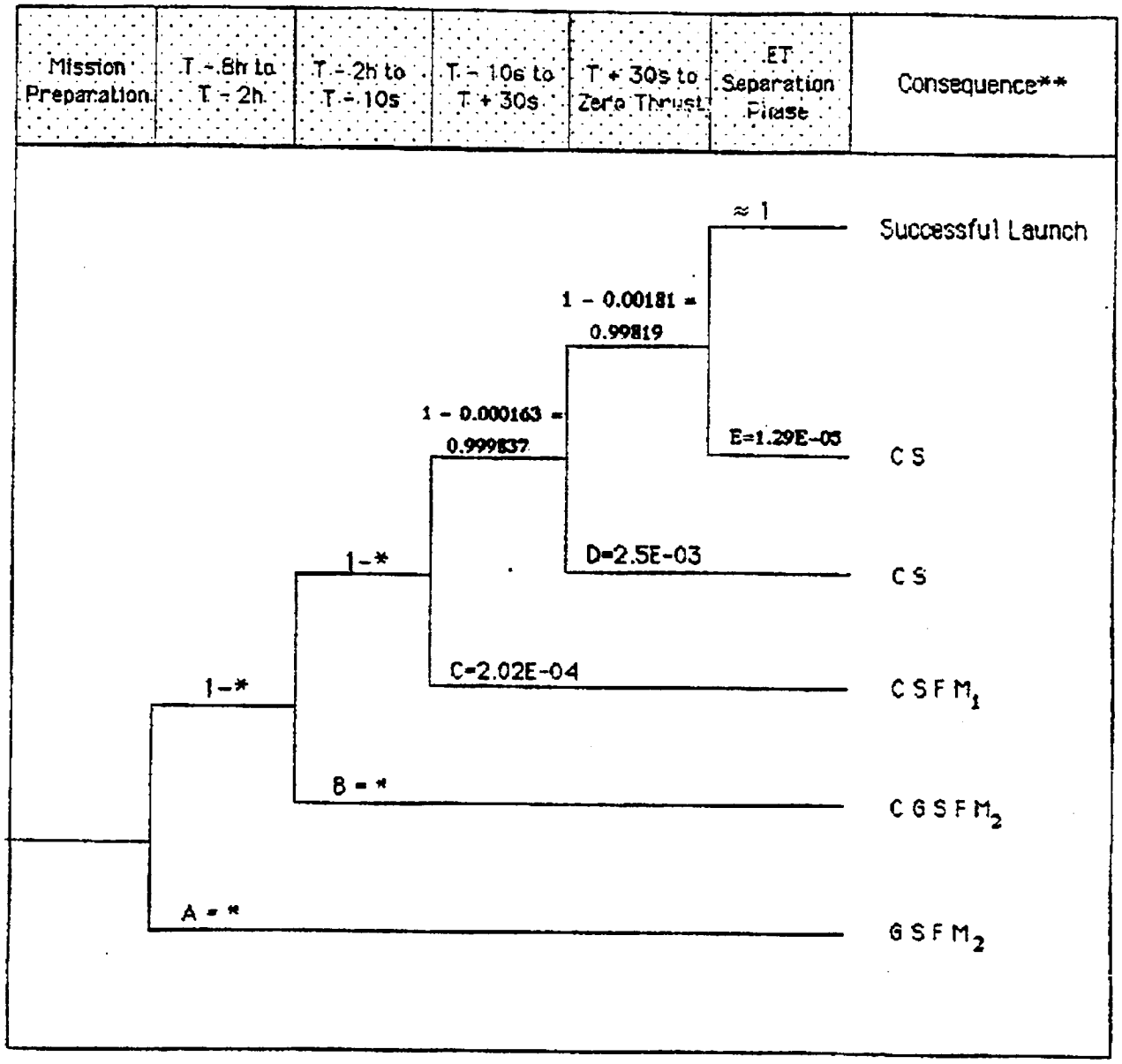
	SPVLP3DC	HUMLPXHC	MPBVP3LK		1.15E-07
	MPBCP1LK	HUMCPXLK			8.23E-08
	MPBLP3LK	HUMLPXHC			8.23E-08
	MPBRP5LK	HUMRPXHC			8.23E-08
	MPBRP6LK	HUMRPXHC			4.43E-08
	MPBCP2LK	HUMCPXHC			4.43E-08
	MPBLP4LK	HUMLPXHC			3.80E-08
F-				**TOTAL FOR F:**	**1.65E-05**
	SEPINHIBIT	CNDTUFCO	SP13OXFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP23OXFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP13FXFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP23FXFE		2.93E-06
	SEPINHIBIT	CKTOOFCD	CNDTUFCO		2.03E-06
	CKTHFFCD	SEPINHIBIT	CNDTUFCO		2.03E-06
	CNDTUFCO	HUMTSXHC	SP13OXFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP23OXFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP13FXFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP23FXFE		1.47E-07
	MPBRPXLK	HUMRPXHC			1.48E-08
	MPBLPXLK	HUMLPXHC			1.48E-08
	MPBCPXLK	HUMCPXHC			1.48E-08
	CKTOOFCD	CNDTUFCO	HUMTSXHC		1.37E-08
	CKTHFFCD	CNDTUFCO	HUMTSXHC		1.37E-08
	CNDTUFCO	PNVTFFDC	HUMTSXHC		1.03E-08
	CNDTUFCO	PNVTOFDC	HUMTSXHC		1.03E-08
	SPVLP3DC	HUMLPXHC	MPBVP3LK		8.14E-09
	SPVRP5DC	MPBVP5LK	HUMRPXHC		7.90E-09
	SPVCP1DC	MPBVP1LK	HUMCPXHC		7.90E-09
	MPBCP1LK	HUMCPXLK			5.83E-09
	MPBLP3LK	HUMLPXHC			5.83E-09
	MPBRP5LK	HUMRPXHC			5.83E-09
	MPBCP2LK	HUMCPXHC			3.14E-09
	MPBRP6LK	HUMRPXHC			3.14E-09
	MPBLP4LK	HUMLPXHC			2.69E-09

6				TOTAL FOR 6:	1.65E-05
	SEPINHIBIT	CNDTUFCO	SP130XFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP230XFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP13FXFE		2.93E-06
	SEPINHIBIT	CNDTUFCO	SP23FXFE		2.93E-06
	SEPINHIBIT	CKTOOFCD	CNDTUFCO		2.03E-06
	CKTHFFCD	SEPINHIBIT	CNDTUFCO		2.03E-06
	CNDTUFCO	HUMTSXHC	SP130XFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP230XFE		1.47E-07
	CNDTUFCO	HUMTSXHC	SP13FXFE		1.47E-07
	CNDTUFCO	HUMTYSXHC	SP23FXFE		1.47E-07
	MPBRPXLK	HUMRPXHC			1.48E-08
	MPBLPXLK	HUMLPXHC			1.48E-08
	MPBCPXLK	HUMCPXHC			1.48E-08
	CKTOOFCD	CNDTUFCO	HUMTSXHC		1.37E-08
	CKTHFFCD	CNDTUFCO	HUMTSXHC		1.37E-08
	CNDTUFCO	PNVTFFDC	HUMTSXHC		1.03E-08
	CNDTUFCO	PNVTOFDC	HUMTSXHC		1.03E-08
	SPVLP3DC	HUMLPXHC	MPBVP3LK		8.14E-09
	SPVRP5DC	MPBVP5LK	HUMRPXHC		7.90E-09
	SPVCP1DC	MPBVP1LK	HUMCPXHC		7.90E-09
	MPBCP1LK	HUMCPXLK			5.83E-09
	MPBLP3LK	HUMLPXHC			5.83E-09
	MPBRP5LK	HUMRPXHC			5.83E-09
	MPBCP2LK	HUMCPXHC			3.14E-09
	MPBRP6LK	HUMRPXHC			3.14E-09
	MPBLP4LK	HUMLPXHC			2.69E-09

PHASE H: No cutsets above probability = E-10

FIGURE 6-1a: MISSION TIME SEQUENCE EVENT TREE

Explosion, Overpressurization, & Non-recoverable Events

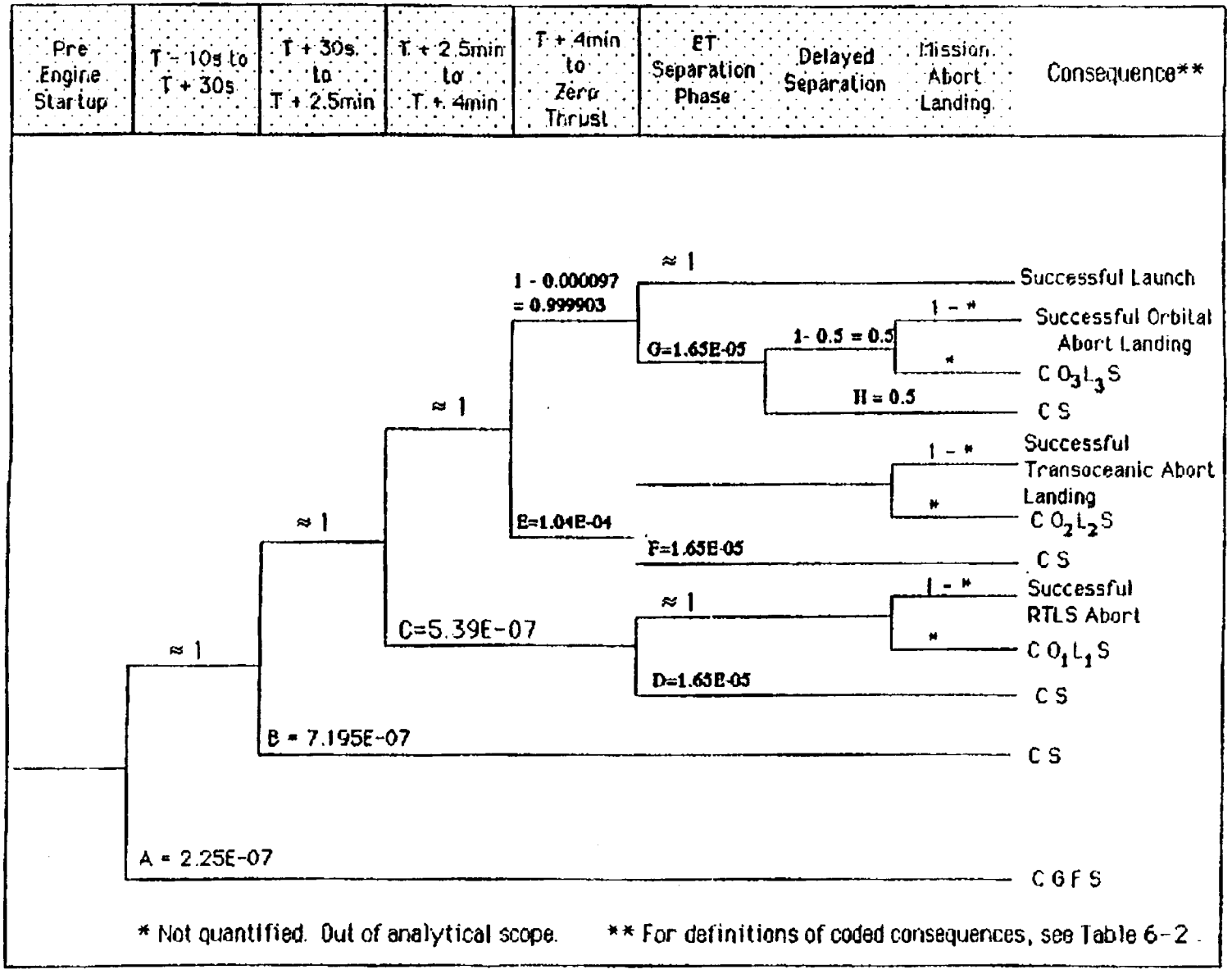


* Not qualified. Out of Analytical scope.

** For definitions of coded consequences, see Table 6-2

FIGURE 6-1b: MISSION TIME SEQUENCE EVENT TREE

Recoverable Events (Functional Failures)



* Not quantified. Out of analytical scope. ** For definitions of coded consequences, see Table 6-2.

TABLE 6-2
Definition of Consequence Categories and Specific Consequences

HUMAN LOSSES

C = Mission Crew
G = Ground Support Team
O_1 = Other persons in vicinity susceptible to fatalities incurred during RTLS abort landing or explosions during flight near the launch facility.
O_2 = Other persons in vicinity susceptible to fatalities incurred during TAL abort landing
O_3 = Other persons in vicinity susceptible to

HARDWARE LOSSES

S = Space Transportation System
F = Ground Facilities and Support Equipment
L_1 = Abort Landing Facilities - RTLS
L_2 = Abort Landing Facilities - TAL
L_3 = Abort Landing Facilities - orbit abort
M_1 = Miscellaneous damage resulting from dispersion of explosion debris prior to T + 30s.
M_2 = Miscellaneous damage resulting from dispersion of explosion debris when STS is on the launch pad

TABLE 6-3
Consequence Data Summary

	HUMAN LOSS (Expected Number of Fatalities)			HARDWARE LOSS (Million Dollars Lost)			
TIME (t)	Crew	Ground Support Team	Other	STS	Ground Facilities (3)	Abort Landing Facilities (4)	Misc
-8 hours to -2 hours	N/A	(1) negligible	N/A	1300	500	N/A	(10
-2 hours to -10 seconds	7	(1) negligible	N/A	1300	500	N/A	(10
-10 seconds to +30 seconds	7	(1) negligible	N/A	1300	500	N/A	(10
+30 seconds to +2.5 minutes	7	N/A	(2) 6.5e-7	1300	N/A	N/A	(.01
+ 2.5 minutes to + 4 minutes	7	N/A	negligible	1300	N/A	50	(6) negligi
+ 4 minutes to + 8.1 minutes	7	N/A	negligible	1300	N/A	50	(6) negligi
+8.1 minutes to abort landing	7	N/A	N/A	1300	N/A	50	N/A

NOTES: (1) Reference 34, Table 10-3, Case No. 1.
(2) Reference 34, Table 10-3. Modify Ec by scaling by 1.78e-4/1.1e-3 to accommodate Figur 6-1a, branch C probability of hazard versus that computed in Table 10-3.
(3) Reference (to be provided).
(4) RTLS, TAL and Orbital Abort landing sites.
(5) Assume $10 million per incident for surrounding buildings & structures.
(6) Reference 34, Table 10-3, take computed value of PI for stage 1 and assume $10M per incid

TABLE 6-4a

Aggregate Probabilities and Risk

Probability of MPPS-Related Events Potentially leading to Loss of Human Life:
Successful Abort Scenario

Category	C	G	01	02	03
applicable sequence probabilities (Fig. 6-1a)	- 2.02E-4 2.05E-3 1.29E-5	-	-	-	-
subtotal	2.26E-3	0.00E+0	0.00E+0	0.00E+0	0.00E+0
applicable sequence probabilities (Fig. 6-1b)	2.25E-7 7.19E-7 8.89E-12 1.72E-9 8.25E-6	2.25E-7	0.00E+0	0.00E+0	0.00E+0
subtotal	9.20E-6	2.25E-7	0.00E+0	0.00E+0	0.00E+0
TOTAL	2.3E-03	negligible	0.0E+00	0.0E+00	0.0E+00
RISK* Expected No. of lives lost	1.6E-02	negligible	0.0E+00	0.0E+00	0.0E+00

Probability of MPPS-Related Events Potentially leading to Loss of Human Life:
Unsuccessful Abort Scenario

Category	C	G	01	02	03
applicable sequence probabilities (Fig. 6-1a)	- 2.02E-4 2.05E-3 1.29E-5	-	-	-	-
subtotal	2.26E-3	0.00E+0	0.00E+0	0.00E+0	0.00E+0
applicable sequence probabilities (Fig. 6-1b)	2.25E-7 7.19E-7 5.39E-7 1.04E-4 8.25E-6	2.25E-7	5.38E-7	1.04E-4	8.25E-6
subtotal	1.14E-4	2.25E-7	5.38E-7	1.04E-4	8.25E-6
TOTAL	2.4E-03	negligible	5.4E-07	1.0E-04	8.3E-06
RISK* Expected No. of lives lost	1.7E-02	negligible	3.5E-13	negligible	negligible

* Derived from Table 6-3

Aggregate Probabilities and Risk

Probability of MPPS-Related Events Potentially Leading to Loss of Hardware or Facilities
Successful Abort Scenario

Category	S	F	L1	L2	L3	M1	M2
applicable sequence probabilities (Fig. 6-1a)	- - 2.02E-4 2.05E-3 1.29E-5	- - 2.02E-4	-	-	-	2.02E-4	- -
subtotal	2.26E-3	2.02E-4	0.00E+0	0.00E+0	0.00E+0	2.02E-4	0.00E+0
applicable sequence probabilities (Fig. 6-1b)	2.25E-7 7.19E-7 8.89E-12 1.72E-9 8.25E-6	2.25E-7	-	-	-	-	-
subtotal	9.20E-6	2.25E-7	0.00E+0	0.00E+0	0.00E+0	0.00E+0	0.00E+0
TOTAL	2.3E-3	2.0E-4	0.0E+0	0.0E+0	0.0E+0	2.0E-4	0.0E+0
RISK* Expected loss of hardware (in $M)	3	0.1	0	0	0	negligible	negligible

Probability of MPPS-Related Events Potentially Leading to Loss of Hardware or Facilities
Unsuccessful Abort Scenario

Category	S	F	L1	L2	L3	M1	M2
applicable sequence probabilities (Fig. 6-1a)	- - 2.02E-4 2.05E-3 1.29E-5	- - 2.02E-4	-	-	-	2.02E-4	- -
subtotal	2.26E-3	2.00E-4	0.00E+0	0.00E+0	0.00E+0	2.02E-4	0.00E+0
applicable sequence probabilities (Fig. 6-1b)	2.25E-7 7.19E-7 5.38E-7 1.04E-4 8.25E-6	2.25E-7	5.38E-7	1.04E-4	8.25E-6	-	-
subtotal	1.14E-4	2.25E-7	5.38E-7	1.04E-4	8.25E-6	0.00E+0	0.00E+0
TOTAL	2.4E-3	2.0E-4	5.4E-7	1.0E-4	8.3E-6	2.0E-4	0.0E+0
RISK* Expected loss of hardware (in $M)	3	0.1	negligible	0.0005	negligible	negligible	negligible

* Derived from Table 6-3

Section 7

REFERENCES

1. "Nonelectric (Mechanical) Parts Failure Rates", Revision C, November 26, 1985, prepared by J. T. Yee.

2. "Nonelectronic Parts Reliability Data", NPRD-3, RADC, Fall 1985, prepared by Michael J. Ross.

3. "RADC Nonelectronic Reliability Notebook", RADC-TR-85-194, Interim Report, Hughes Aircraft Company, October 1985.

4. "Nonelectric Reliability Notebook", RADC-TR-75-22, AD/A005-657, RADC, January, 1975.

5. IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Stations, IEEE Std. 500-1977, June 30, 1977.

6. "Space Transportation System" description document, NASA General Distribution Material, comprising pp. 46-107.

7. "Shuttle Element Interface Functional Analysis", for the Space Shuttle Main Engine/Orbiter Contract NAS-9-14000, Phase I Report, Rockwell International, February 1987.

8. "External Tank Space Shuttle Lightweight Tanks Failure Modes and Effects Analysis (FMEA)", Document MMC-ET-RA04a-F, dated 1 October, 1984 (incorporating change notices through #11, dated 1-9-86).

9. "SSME Failure Mode and Effects Analysis and Critical Items List", Document Number RSS-8553-10, May 30 1986.

10. "Space Shuttle External Tank, External Tank Hazard Catalog, Block Baseline ET-30 through ET-39", Rev. 30, Document No. MMC-ET-RA01a-30, 5 March 1985, approved with comments by CCBD ET3-00-590S, date 17 June 1985.

11. "Detail Design Hazard Analysis Space Shuttle Main Engine Operational Flights", Rockwell International, Report Number RSS-8545-19, 15 January 1983.

12. "Systems Assurance Analysis of the Main Propulsion Liquid Oxygen Control System for the Launch Operation Area (PAD A/B) and the Vehicle Assembly Area, OMB Baseline No.: 9 & 32", KSC Drawing No. SAA09PP02-001, Rev. F, January 1987.

13. "System Assurance Analysis of the Main Propulsion Liquid Hydrogen Control System at the LoA and VAA, OMB Baseline No.: 8 & 31", KSC Drawing No. SAA09PP03-001, November 1980.

14. "Reuseable Rocket Engine Maintenance Study", NASA Final Report, NASA CR-165569; RI/RD81-226 January, 1982.

15. "SSME Main Combustion Chamber Life Prediction", NASA Final Report No., NASA CR-168215; RI/RD83-150 May 1983.

16. "Space Shuttle Main Engine Detection", H. A. Cikanek, IEEE Control Systems Magazine 6 (3) 1986.

17. "Mission Operations Directorate Booster Systems Brief", NASA Report No. JSC-19041, October 1, 1984.

18. "Orbiter Vehicle Operational Configuration Failure Mode Effects Analysis, Main Propulsion Subsystem", Document Number STS82-0022, dated 28 January 1983 (Change #2), incorporating Change Package #3, dated 15 August 1985. V. P. Ostrander and G. Cadwell, Rockwell International, Space Systems Group.

19. "Reliability Prediction of Electronic Equipment", MIL-HDBK-217E, 15 January 1986.

20. "Main Engine Hydraulics And Pneumatics", NASA JSC Space Shuttle Drawing No. 10.9, Basic Rev. C.

21. "Space Transportation System Technical Manual, SSME Description and Operation", JSC E41000, Rockwell International Report No. RSS-8559-1 ! !, Replacement Report, September 1983.

22. "Shuttle Main Propulsion Pressurization System, Probabilistic Risk Assessment System Description Document", LEMSCO Report No. 24120, August 1987.

23. STS Operational Flight Rules, JSC12820, February 2, 1986, PCN-1.

24. "A User's Guide for the Top Event Matrix Analysis Code (TEMAC)", NUREG/CR-4598, SAND86-0960, August 1986, R. Iman, M. Shortencarier.

25. Letter: Guy Thibodaux to Ed Smith, dated May 11, 1987, Subject: Contamination, Compatibility, Cleaniness and Leakage.

26. "Preliminary Fault Tree Study of Fire & Explosion and of Controller/Electronics Malfunctions within the Space Shuttle Main Propulsion System", Dr. Howard Lambert, Rev. 2, June 23, 1987.

27. Handbook of Piece Part Failure Rates, Martin Marietta Corp., Denver Division, GIDEP 031-1273

28. "CAFTA: A Comprehensive Fault Tree Development Workstation", Proceedings of the Annual Reliability and Maintainability Symposium, Las Vegas, Nevada, 28 January 1986

29. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, SAND 80-0200, August 1983.

30. "Update to Orbiter FMEA - Section 2 Helium System", dated May 29, 1987.

31. "External Tank", NASA JSC Space Shuttle Drawing No. 10.10, Basic Rev. C-4.

32. "Main Engine LOX System", NASA JSC Space Shuttle Drawing No. 10.11, Basic C-4.

33. "Main Engine LH2 System", NASA JSC Space Shuttle Drawing No. 10.12, Basic Rev. C-4.

34. "Space Shuttle Range Safety Hazards Analysis", Technical Report No. 81-1309, J. H. Wiggin's Co., July 1981.

35. "Main Engine", NASA JSC Space Shuttle Drawing No. 10.13, Basic Rev. C-5

36. "Helium System Schematic", Dwg. 5.2, MPS 5-4, Rev. A.

SPACE SHUTTLE
PROBABILISTIC RISK ASSESSMENT
PROOF – OF – CONCEPT STUDY

VOLUME III
AUXILIARY POWER UNIT
AND HYDRAULIC POWER UNIT
ANALYSIS REPORT

18 DECEMBER 1987

C 6

MCDONNELL DOUGLAS ASTRONAUTICS COMPANY
ENGINEERING SERVICES

SPACE TRANSPORTATION SYSTEM ENGINEERING AND OPERATIONS SUPPORT

WORKING PAPER NO. 1.0-WP-VA88004-03

SHUTTLE PROBABILISTIC RISK ASSESSMENT PROOF-OF-CONCEPT STUDY

VOLUME III
AUXILIARY POWER UNIT AND HYDRAULIC POWER UNIT PROBABILISTIC RISK ASSESSMENT ANALYSIS REPORT

18 DECEMBER 1987

This Working Paper is Submitted to NASA under
Task Order No. VA88004, Contract NAS 9-17650

PREPARED BY:

J. E. Barnes

M. L. McNeely

J. J. Ewell, Jr.

T. E. Emmons

APPROVED BY:

G. W. Knori
Technical Manager
Independent Orbiter
Assessment

J. I. McPherson
Deputy Program Manager
STSEOS

VOLUME III

AUXILIARY POWER UNIT AND HYDRAULIC POWER UNIT

PROBABILISTIC RISK ASSESSMENT ANALYSIS REPORT

18 DECEMBER 1987

ACKNOWLEDGEMENTS

McDonnell Douglas

W. R. Davidson
L. M. Rater
C. A. McCants
J. W. Homol
(Word Processing)

Pickard, Lowe & Garrick, Inc.

B. J. Garrick
M. V. Frank
V. M. Bier
D. C. Bley
S. A. Epstein
B. A. Fagen
Y. M. Hou
J. C. Lin
S. Kaplan
P. H. Raabe

CONTENTS

Section	Section Title	Page
1.0	EXECUTIVE SUMMARY	1-1
2.0	INTRODUCTION	2-1
3.0	SUMMARY CONCLUSIONS AND INSIGHTS	
	3.1 PRA Technology Transfer	3-1
	3.2 Conclusions and Insights into the Risk of the APU and HPU	3-2
	3.3 PRA Implementation Lessons	3-7
4.0	SYSTEM DESCRIPTIONS	
	4.1 APU System Description & Overview	4-1
	4.2 APU Mission Operations	4-1
	4.3 APU Design and Function	4-3
	4.4 HPU System Description & Overview	4-6
	4.5 HPU Mission Operations	4-8
	4.6 HPU Design and Function	4-8
5.0	STUDY METHODOLOGY	
	5.1 The Purpose of PRA	5-1
	5.2 The Structure of a Decision	5-1
	5.3 The Quantitative Definition of Risk	5-3
	5.4 The Damage Index, Xi	5-4
	5.5 Quantifying Likelihood: The Probability of Frequency Format	5-4
	5.6 Identifying Scenarios	5-5
	5.7 Structuring the Scenario List	5-7
	5.8 Multistage Modeling	5-14
	5.9 Determination of Split Fractions	5-15
	5.10 Quantifying Scenarios	5-21
	5.11 Risk Diagnosis	5-23
	5.12 Summary of PRA Methodology	5-25
6.0	APU SCENARIO PRESENTATION	
	6.1 Damage States	6-3
	6.2 Master Logic Diagram Development	6-4
	6.3 Event Sequence Diagrams	6-11
	6.4 APU Event Tree Development	6-35
	6.5 Split Fraction Model Development	6-64
	6.6 Spatial Interactive Events (SIEs)	6-93

Section	Section Title	Page
7.0	APU DATA DEVELOPMENT	
	7.1 Raw Data Sources	7-4
	7.2 Spatial Interactive Event Data	7-11
	7.3 Raw Data Table Development	7-14
	7.4 Failure History Data Categorization	7-17
	7.5 Failure Rates	7-25
	7.6 Spatial Interactive Event Data Development	7-60
8.0	QUANTITATIVE RESULTS OF THE APU PRA	
	8.1 Risk Profiles	8-2
	8.2 Description of Risk Contributors	8-9
	8.3 Assessment of Study Results	8-15
9.0	HPU SCENARIO PRESENTATION	
	9.1 HPU Damage States	9-2
	9.2 Master Logic Diagram (MLD) Development	9-2
	9.3 Event Sequence Diagram For HPU Initiated Scenarios	9-4
	9.4 Event Tree For HPU Initiated Scenarios	9-14
	9.5 Split Fraction Model Development	9-23
	9.6 Spatial Interactive Events (SIEs)	9-33
10.0	HPU DATA DEVELOPMENT	
	10.1 HPU Raw Data Sources	10-4
	10.2 Spatial Interactive Event Data	10-7
	10.3 Data Categorization	10-7
	10.4 Failure Rates	10-9
	10.5 HPU SIE Data Development	10-30
11.0	QUANTITATIVE RESULTS OF THE HPU PRA	
	11.1 Risk Profiles	11-2
	11.2 Description of Risk Significant Scenarios	11-4
	11.3 Failure Mode Importance Ranking	11-10
	11.4 Interpretation of Results	11-10
12.0	REFERENCES	12-1
13.0	ACRONYMS	13-1
14.0	APPENDICES	
	A. Study Assumptions	A-1
	B. APU Tables	B-1
	C. HPU Tables	C-1

LIST OF FIGURES

Figure	Description	Page
3-1	Probability Distribution Comparison	3-3
4-1	Auxiliary Power Unit Location	4-2
4-2	Auxiliary Power Unit (APU) System Schematic	4-4
4-3	SRB TVC Components Location	4-7
4-4	Hydraulic Power Unit (HPU) System Schematic	4-10
5-1	Decision Model	5-2
5-2	State of Knowledge Probability Curve for the Frequency of the ith Scenario	5-6
5-3	The Initiating Failure Concept	5-8
5-4	Emanation of Scenarios from Initiating Failure	5-9
5-5	Master Logic Diagram	5-11
5-6	Simplified ESD and Associated Event Tree	5-13
5-7	Multistage Modeling	5-16
5-8	Relationship of Split Fraction Models to Event Trees	5-17
5-9	Event Tree Quantification	5-22
5-10	Risk Diagnosis	5-24
5-11	Procedure for APU/HPU Quantitative Risk Assessment	5-26
6-1	APU Operational Phases and Modeling Stages	6-2
8-1	Probability Distributions for Stage A	8-3
8-2	Probability Distributions for Stage A (Ascent)	8-4
8-3	Probability Distribution for LOC/V - Entire Mission	8-7
9.3-1	HPU Event Sequence Diagram	9-6
9.4-1	HPU Event Tree	9-16
11.1-1	HPU Failure Probability Distribution	11-3

LIST OF TABLES

Table	Description	Page
3-1	Importance Ranking of APU Failures, LOC/V - Whole Flight - 1st Iteration	3-10
3-2	Importance Ranking of APU Failures, LOC/V - Whole Flight - 2nd Iteration	3-12
3-3	Importance Ranking of APU Failure Scenarios - LOC/V - Whole Mission	3-14
3-4	Importance Ranking of HPU Failure Modes, Loss of Crew or Vehicle	3-18
3-5	Importance Ranking of HPU Failure Scenarios, LOC/V	3-19
6.1-1	Damage State Applicability	6-4
6.2-1	MLD Definitions	6-6
6.4.1	Damage Bin Assignments - Stage A	6-39
6.4.2	Top Event Definitions - APU Event Tree - Stage A	6-40
6.4.3	Relationship of Stage A Event Tree Top Events to APU ESD 1 - Prelaunch and Ascent	6-42
6.4.4	Top Event Definitions - APU Event Tree - Stage B	6-52
6.4.5	Relationship of Stage B Event Tree Top Events to APU ESDs 2, 3, and 4 - Orbit and Entry/ Descent/Landing	6-54
7.2-1	Spatial Interactive Event APU Ascent Distributions	7-12
7.2-2	Spatial Interactive Event APU Entry Distributions	7-13
7.4-1	Component Categories Considered in the APU Model	7-20
7.5-1	Prior Distributions	7-32
7.5-2	Prior Distributions and Observed Data for APU Basic Events	7-37
7.5-3	APU Component Failure Descriptions	7-47
7.5-4	APU Data Analysis Results	7-52
7.6-1	APU Split Fractions for SIEs	7-61
7.6-2	Turbine Hub Breakup Data	7-63
7.6-3	APU Uncontained Fragment Energies	7-66
7.6-4	Potential Targets of APU Turbine Fragments	7-67
7.6-5	Penetration Capability of Uncontained Fragments	7-68
7.6-6	Wall Thicknesses of Selected Equipment	7-69

LIST OF TABLES (Continued)

Table	Description	Page
8-1A	Importance Ranking of APU Failure Scenarios, LOC/V - Ascent	8-18
8-1B	Importance Ranking of APU Failure Scenarios, Launch Scrub - Ascent	8-20
8-1C	Importance Ranking of APU Failure Scenarios, Intact Abort - Ascent	8-22
8-1D	Importance Ranking of APU Failure Scenarios, APU Stage A (Ascent), Primary Landing Site	8-24
8-2	Importance Ranking of APU Failure Scenarios, LOC/V - Whole Mission	8-26
8-3	Importance Ranking of APU Failures, LOC/V - Ascent	8-30
8-4	Importance Ranking of APU Failures, Launch Scrub	8-31
8-5	Importance Ranking of APU Failures, Intact Intact Abort	8-32
8-6	Importance Ranking of APU Failures, PLS	8-33
8-7	Importance Ranking of APU Failures, LOC/V - Whole Flight - 1st Iteration	8-34
8-8	Importance Ranking of APU Failures, LOC/V - Whole Flight - 2nd Iteration	8-36
9.4-1	Top Event Definitions - HPU Event Tree	9-18
9.4-2	Relationship of Top Events to HPU ESD	9-19
10.2-1	Spatial Interactive Event HPU Ascent Distributions	10-8
10.3-1	Component Categories Considered in the HPU Model	10-10
10.4-1	Prior Distributions	10-15
10.4-2	Prior Distributions and Observed Data for APU Basic Events	10-20
10.4-3	Results of HPU Data Analysis	10-26
10.5-1	HPU Split Fractions	10-31
10.5-2	HPU Uncontained Fragment Energies	10-34
11.2-1A	Importance Ranking of HPU Failure Scenarios, LOC/V	11-6
11.2-1B	Importance Ranking of HPU Failure Scenarios, Launch Scrub	11-8
11.2-2	Importance Ranking of HPU Failure Modes	11-11

SPACE SHUTTLE
PROBABILISTIC RISK ASSESSMENT
PROOF-OF-CONCEPT STUDY
ANALYSIS REPORT

1.0 EXECUTIVE SUMMARY

This document focuses on the transfer of the Probabilistic Risk Assessment (PRA) methodology to a Space Shuttle environment utilizing the Auxiliary Power Unit (APU) and Hydraulic Power Unit (HPU) as typical examples of spacecraft subsystems. This volume presents specific PRA findings of this proof-of-concept study and attempts to answer the following question: Can the PRA methodology be transferred to a space system?

The study results resembled those of previous PRAs accomplished in other industries. The study produced a quantification of the frequency of certain undesired end states, along with a ranking of specific subsystem failure modes by their contribution to the risk of these end states.

For the APU, the study indicates that five failures account for about 80% of the total risk of Loss of Crew/Vehicle (LOC/V) during a typical flight. An additional five failures account for over 90% of the total risk. The common hazard associated with the first five failures is hydrazine leakage into the aft compartment. This creates the potential for fire, as demonstrated at the conclusion of the STS-9 mission when there were two APU fires.

The HPU has two failures that represent over 98% of the contribution to LOC/V. These contributions could arise from common cause lube oil contamination in two HPUs by fuel leaking into the gearbox, or by introduction of foreign substances into the gearbox, and from turbine wheel failures.

The APUs are about two orders of magnitude more of a risk to the safety of the Shuttle than are the HPUs. The bulk of the risk from the APUs arises from the potential for fire from any hydrazine leaks which manifest themselves as a fire during entry.

The PRA results indicate that for both the APU and HPU, only a few failures account for the majority of the risk during a typical flight. The results illuminated no new areas of concern or failures not previously known, but do identify the high risk failure scenarios that map the paths between the end states and individual APU and HPU failures.

The PRA, therefore, provided a quantitative way of prioritizing the known safety concerns and failure modes. It also provided an estimate of the magnitude of risk of each safety concern.

2.0 INTRODUCTION

McDonnell Douglas was selected by the National Aeronautics and Space Administration (NASA) to assess the Probabilistic Risk Assessment (PRA) methodology when applied to a space system. The PRA has been in use by other industries for many years. The study attempts to provide insight to answer several questions. One of these questions is: Can the PRA methodology be transferred to a space system?

This volume provides information for the evaluation of the PRA methodology transfer, the benefits to be gained from application of PRA methodology, and the information necessary for the FMEA/CIL comparison described in Volume II. Volume I discusses the management aspects of the study as related to the results. Volume IV documents the PRA preparation instructions.

Pickard, Lowe, and Garrick, Inc. (PLG), a firm experienced in the use of the PRA technique in other industries, was selected as a subcontractor to provide the expertise and software analysis tools necessary to adapt the PRA methodology to the Space Shuttle environment.

Two subsystems were chosen for this proof-of-concept study:

a. The Orbiter Auxiliary Power Unit (APU), designed and manufactured by the Sundstrand Corporation as a subcontractor to Rockwell International Corporation, and

b. The Solid Rocket Booster (SRB) Hydraulic Power Unit (HPU), also manufactured by the Sundstrand Corporation but under contract to United Space Boosters Incorporated (USBI).

The system configuration of the APU and HPU used in this study was that which existed as of January 1986. The "Improved" APU and post-51L flight modifications to the APU were not analyzed, except as specifically noted elsewhere in the report.

The PRA process offers a different type of risk analysis tool available to industries or agencies who must deal with risk assessment. The PRA begins with the consideration of effects that are deemed undesirable. The analysis proceeds from the top down through the system or systems via scenario paths that ultimately lead to the failed component or assembly. The process proceeds to the lowest level of detail that time, effort, funds, or available data permits.

The Probabilistic Risk Assessment involves:

a. An integrated model of the responses of an engineered system to disturbances during operation

b. A rigorous and systematic identification of the levels of damage that could conceivably result from those responses

c. A quantitative assessment of the frequency of such occurrences and of the uncertainty in that assessment

Although the PRA process produces a quantification of risk, the actual numbers produced are not the only important results. The important results from a risk management perspective are:

a. The insight gained into the system under study

b. The frequency of occurrence of the damage states

c. The relative ranking of failure scenarios and component failure modes

d. Identification of failure modes which account for the majority of the risk

e. How well the risk is known (uncertainty of the results)

The PRA is a decision-making tool for managing the risk associated with the system under investigation. It points out weak areas in the system, and aids in deciding where "fixes" are warranted. The numbers produced are valuable to the extent that they give a decision-maker a way to decide what is important and what is not important. Resources may then be allocated based on specific needs such as reduction of high risk, cost, or schedule impact.

The next section summarizes the conclusions and insights gained into the transfer of PRA methodology to these Shuttle subsystems, as well as insight gained into the APU and HPU risk. The individual risk contributors which comprise 99% of the risk to LOC/V were ranked according to their contribution to the likelihood of the damage state. The risk contributors that collectively represent 1% of the risk were grouped.

The remaining sections, 4 through 11, describe the APU and HPU system configuration used for this study, the PRA methodology, the application of that methodology, and the conclusions and insights that were obtained during the course of this study.

Assumptions are inherent to any analysis and PRA is no exception. Assumptions were made to define the boundaries of each system, the system interfaces, the boundary conditions of the interfaces, and the general modeling guidelines used to conduct the study. These assumptions and guidelines are described in detail in Appendix A and are discussed where appropriate in Sections 5 through 11.

The results presented in this volume are intended to be representative of the kind obtained by a PRA and not indicative of actual Shuttle results. The numerical predictions of LOC/V from the pilot study are not deemed reliable, because the database used was uncertified, the various designs and diagrams had not been subjected to any configuration control, and the PRA process itself was not conducted with any peer review or management oversight function. For this reason, any risk numbers or probability curves discussed in the later volumes of this report are purely representational in nature, and should not be used for hardware certification, flight readiness review, nor should they be regarded as being an accurate expression of the reliability of either the APU or HPU. The results are intended only as a "template" to test fit the PRA methodology, and should not be taken out of context or used for any other engineering purpose.

3.0 SUMMARY CONCLUSIONS AND INSIGHTS

This section presents a summary of the technical conclusions and lessons learned concerning the transfer of PRA technology to the Space Shuttle. It also provides insights into the risk posed by operation of the Auxiliary Power Unit (APU) and Hydraulic Power Unit (HPU) on a typical Shuttle mission, and lessons learned which may be of value for implementing PRA on other space systems.

3.1 PRA TECHNOLOGY TRANSFER

The PRA techniques (such as fault trees and event trees) applied in this study have reached various states of sophistication through application in the nuclear, chemical, and aircraft industries. Space Shuttle systems, their interfaces with each other, with operators, and with operating procedures, share much in common with systems in these industries. It was, therefore, expected that PRA techniques could be applied to the Space Shuttle; the difficulty of the task was the unknown.

A successful application of PRA techniques requires a balance of knowledgeable PRA personnel and system experts; each must acquire some of the skills of the other. This proof-of-concept study successfully demonstrated the adaptation of PRA techniques on two Shuttle subsystems in the following manner: The damage states on which the study was based were identified; the study groundrules and constraints were developed; the PRA models were developed; the historical records of past missions and of the APU and HPU were obtained and analyzed; action items were generated to resolve important issues concerning hydrazine and its properties; data-bases were developed to compile and correlate failure history data; the models were quantified; the uncertainties in the data and models were developed using probability distributions; the risk profiles were obtained; and the contributors to the Shuttle's risk due to the APU and HPU were identified and ranked.

PRA may be considered an "engineering art" in which the combined skills and knowledge of many are required to apply the basic PRA techniques in combinations which accurately and logically model the risk posed by the system. There were no standard "cook book" procedures for applying PRA techniques to the Space Shuttle systems. A generalized set of PRA techniques were developed as part of this study which may have application to other space systems.

This study identified and documented how failures initiated by the APU or HPU can propagate through a subsystem to cause

degraded performance, shuttle damage, or mission curtailment. This was accomplished by identifying damage states, and by identifying failure scenarios emanating from initial failures in the APU or HPU that lead to the damage states. The damage states used in this study were Loss of Crew/Vehicle, and Loss of Mission. Loss of mission was further divided into intact abort, Primary Landing Site (PLS) entry, and launch scrub. A risk profile, which represents the likelihood of the damage state occurring and the uncertainty about that likelihood, was assessed for each of these damage states. The study was able to divide the mission into stages that allowed the assessment of risk for ascent as distinct from orbit and entry. The PRA addressed mechanical, electrical and electronic failures, interactions caused by functional and spatial relationships, and failures of multiple components due to a common cause.

It should be noted that additional damage states could have been selected which, for example, allow for the identification of equipment damage and subsequent cost of repairing failures. Additional damage states such as these add unnecessary complexity when one is primarily interested in damage states that pose risk of LOC/V. However, the techniques appear quite capable of quantifying risk to equipment just as reliably as they handle the more serious cases.

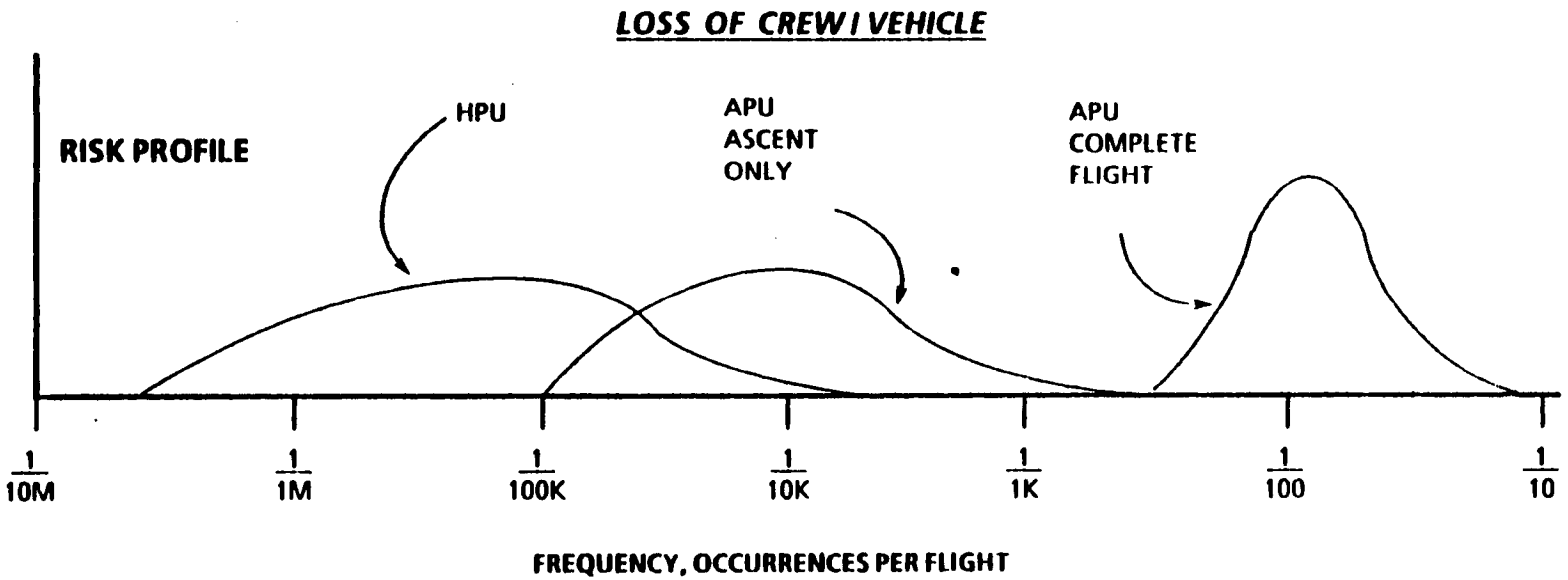
3.2 CONCLUSIONS AND INSIGHTS INTO THE RISK OF THE APU AND HPU

The PRA results present risk-related information about the APU and HPU in several ways. They provide risk profiles, a ranked order of scenarios contributing to the risk profiles, a ranked order of APU/HPU failures contributing to the failure scenarios, and a ranking of component failure modes that contribute to the risk profile.

The risk profiles for loss of crew/vehicle for the APU and HPU are shown in Figure 3-1. These data are proof-of-concept study results and are not to be used for engineering, design evaluation, or flight certification. The contribution of HPU risk to the Shuttle is clearly much lower than the contribution of APU risk, even with uncertainties included.

3.2.1 Insights Into APU Risk

What are the major risk contributors of the APU? Table 3-1, at the end of this section, presents the APU risk contributors



PROOF-OF-CONCEPT STUDY RESULTS - NOT APPROVED FOR DESIGN EVALUATION OR FLIGHT CERTIFICATION

FIGURE 3-1 PROBABILITY DISTRIBUTION COMPARISON

(failure modes) that contribute over 99% of the likelihood of loss of crew/vehicle during a flight. The risk from all other contributors combined, therefore, makes a negligible contribution to the overall risk associated with APUs. The first three major contributors are: (1) hydrazine leakage into the aft compartment from at least one APU during orbit or entry with potential for fire or corrosion damage to other equipment, (2) hydrazine leakage into either isolation valve solenoid cavity, and (3) failure of the APU turbine wheel. This includes all failures of the turbine such as bearing seizure and fragmentation of the wheel causing shrapnel damage to other equipment. Hydrazine leakage contributes about four times more to risk than all the others combined. Therefore, reducing either the likelihood or effects of this leakage would provide the most benefit in terms of risk reduction for invested resources.

The large (74.6%) contribution from the general category of hydrazine leaks downstream of the isolation valves, and the desire to rank the risk contributors to a finer detail, led to a second iteration. Table 3-2 identifies, more specifically, the risk points of leakage downstream of the isolation valves. For example, 71.6% of this risk can be attributed to the first three leak sources. Fuel leakage into the fuel isolation valve remains high on the risk table.

Hydrazine leakage was the initial failure in many scenarios. The PRA identified and documented the leakage related scenarios via event sequence diagrams and event trees as shown in Appendices B6.3 and B6.4, respectively. Table 3-3 summarizes the quantified result of this process by presenting the percent of the LOC/V risk attributable to each category of scenarios and the percent contribution of the categories of scenarios attributable to individual APU failure modes. The risk profile was also broken down directly into failed components or assemblies as shown in Tables 3-1 and 3-2.

The LOC/V risk from APUs is clearly dominated by leakage of hydrazine leading to the cascading effects of fire, hydrazine corrosion, hydrazine decomposition reactions, and possibly detonation. These effects were assessed to lead to failure of either an adjacent APU or other flight critical equipment in the aft compartment with a relatively high frequency. This assessment resulted from historical Shuttle data and from the recognition that the aft compartment is very crowded. The compartment contains main propulsion equipment, electronics, and exposed wiring whose insulation (such as Kapton) is susceptible to the damaging effects of hydrazine. All are in close proximity

to hydrazine sources. There are no effective barriers between the hydrazine sources and the rest of the equipment in the aft compartment. When the Shuttle descends to an altitude of about 60,000 feet during entry, sufficient atmospheric oxygen is available to support combustion of free hydrazine in the aft compartment, provided that an ignition source exists. The APUs themselves provide sufficiently hot surfaces to ignite leaking hydrazine. The effects of hydrazine ignition were dramatically demonstrated by the two APU fires that occurred at the end of the STS-9 flight.

The study also revealed that propagating failure effects from common cause failures (as revealed in the APU failure history database) led to a risk that was far greater than would be expected if APUs were failing independently. The benefits of redundant APUs are not being realized. The STS-9 fire demonstrated that a single hydrazine leak can fail two APUs. Restricted lube oil flow has affected the same APU on two separate missions due to contamination introduced during ground servicing. Restricted circulation of lube oil due to contamination has already caused a launch scrub. However, it is recognized that procedures have been instituted to minimize the possibility of lube oil contamination. In addition, a new design in the seal cavity drain of the Improved APU will eliminate the common fuel and lube oil seal drain that exists on the present APUs.

Since hydrazine leakages can occur from any one of the APUs and a single leak can lead to LOC/V, the presence of three APUs (two of three of which are required to operate), from a purely mathematical point of view, is more detrimental to flight safety than are two. Even without cascading failures, a configuration in which one out of two must operate for success tends to be more reliable than a two out of three configuration. One approach that would significantly reduce the risk would be to affect a design wherein each of the three APUs is independently capable of supporting the demands of the Orbiter hydraulic system. Another less rigorous approach might be to erect barriers to isolate each APU from the rest of the aft compartment. The barriers would also serve to reduce the detrimental effects of shrapnel produced by turbine breakup while operating during the flight.

Because of the high probability of hydrazine leakage, inspection and leak check procedures should be reviewed for adequacy. Another approach is to certify that the vehicle is capable of operating throughout the flight envelope (ascent as well as entry) on a single APU. This would result in significant reduction in the risk of LOC/V as determined from this study. The study results

were heavily influenced by the assumption that two APUs were required for safe flight.

Further results of this study are discussed in Section 8 of this Volume and include APU risk associated with launch scrub and with the ascent phase of a typical flight. This Section has summarized the orbit/entry phase which poses the greater risk to flight.

3.2.2 Insights Into HPU Risk

The HPU has been assessed as posing very little risk of loss of crew/vehicle. Table 3-4 presents a breakdown of the risk profile into its risk contributors (failure modes). Two failures contribute over 98% of the risk posed by the HPU. These two failures are lube oil circulation restriction due to common cause contamination, and failure of the HPU turbine wheel. As in the APU this includes all failures of the turbine including wheel fragmentation leading to shrapnel damage to other equipment. The risk from all other failures combined, therefore, makes only a 2% contribution to the LOC/V risk due to the HPUs. Table 3-5 provides a breakdown of the risk profile into scenarios and the HPU failures associated with the scenarios.

The risk posed by the HPUs appears to be far less than that of the APU for five fundamental reasons.

a. Risk is directly proportional to flight duration. The HPU operates in-flight for about 3% as long as the APU.

b. The dominant contributor to APU risk is not appropriate to the HPU. The risk from hydrazine leakage on the APU is associated with the long duration that hydrazine must be contained during orbit, coupled with the potential for fire during entry. The HPU need contain hydrazine for only about 2 minutes during ascent and the environment around the HPU in the aft skirt is purged with nitrogen to prevent fires.

c. The SRB aft skirt is much less crowded with flight critical equipment than the Orbiter aft compartment, and the two HPUs appear to be well separated. In addition, damage from the shrapnel spray pattern is minimized by the orientation of the turbine wheel. Therefore, cascading effects from either hydrazine leakage or turbine fragmentation have relatively little chance of harming a second HPU or flight critical equipment.

d. The HPU is similar in design to the APU and is constructed by the same manufacturer. The APU requirements for duration of service and ability to cope with the environmental extremes of

ascent, orbit, entry and landing are more demanding than is required for the HPU. From a reliability viewpoint, the HPU appears to have a large design margin.

e. The HPU undergoes a stringent post flight disassembly and refurbishment. It also undergoes a thorough pre-flight reassembly and checkout procedure. The failure history indicates that these procedures are effective in reducing the frequency of failures during hot fire tests as well as flight, despite the detrimental effects of immersing the HPUs in sea water at the end of each flight. Essentially, new HPUs are flown each flight.

3.3 PRA IMPLEMENTATION LESSONS

The application of PRA to a Shuttle subsystem yielded some lessons about methodology, data acquisition, and management aspects of this study which may be of benefit for future application to PRA in other space systems.

3.3.1 Methodology Lessons

A number of challenges appeared during the course of this study and several insights were gained into the PRA process as applied to an aerospace subsystem as a result. They are as follows:

a. Multi-stage modeling may be required in which the risk model is divided into stages. In this study these stages were defined on the basis of mission time intervals. Each time interval was characterized by a different APU mode of operation, a different set of flight rules, and different potential damage states.

b. Evaluation of cascading failure effects, such as hydrazine leakage which can propagate damage, requires extensive modeling and analysis of physical processes. The results of these analyses then must be converted to a form suitable for use in a risk model.

c. The highly interactive nature of the APU with its surroundings requires careful event tree design to capture all important dependencies.

d. Coupling of propagating failure effects with random equipment failures requires highly coupled fault tree and event tree models.

Some of the challenges were typical of any first-of-a-kind study. A PRA cannot be completed without a thorough knowledge of the system, its interfaces, procedures, operator interactions and failure and success history. All task members must share some degree of this knowledge, as well as to acquire certain PRA skills. The unfamiliarity with the relative importance of various APU/HPU failure modes caused a number of false starts with respect to the risk model development. In particular, the study task group could not draw on a deep well of experience to unambiguously define, on the first try, which aspects of the scenarios could be treated by event trees, which by fault trees, which by data, and which by physical process modeling.

The study task group believes that the optimal use of the techniques has not yet been found and that application of PRA techniques will continue to evolve toward an aerospace specific methodology.

3.3.2 Data Acquisition Lessons

Although manned spaceflight dictates a certain level of record keeping in support of safety and reliability, it was known from the outset that data collection and validation was no small driver in the successful completion of the study. Databases developed to support the needs of various organizations are not necessarily in the format needed to support a PRA. In addition, the type of data needed for a PRA can be distinctly different from that required for other types of analyses. This is especially true when dealing with spatial considerations of the subsystem under study.

Examples of further data difficulties encountered are as follows:

a. Some failures were written against the APU, using its part number rather than the specific component part number, within the APU that failed. Extra time was required to identify the actual component that failed.

b. Incomplete failure records or partial data entries were not uncommon. Extra time was required to resolve the issue, or the data was eventually discarded for lack of substantiating information.

c. Different data sources use different computer software and hardware. This hampered the task of automating the data for compiling and sorting.

d. Inconsistencies exist in formatting. Failures were tied to an expected mission or mission date, not a calendar date. Run times were in different units of time. Extra time was required for correlating failures and tabulating data.

e. The inability to determine exactly when design changes were implemented made data screening difficult. What component design should be used to establish failure rates?

f. It was difficult to use "borrowed" data base material which lacked proper documentation (e.g., data file size, content and attributes). Extra time was required to establish electronic data transfer.

g. Access to the data sources was difficult. NASA vendors are reluctant to provide information without formal authorization and, in most cases, without compensation.

A great cost savings could be realized in conducting a PRA if the appropriate data could be assembled into coherent and consistent electronic databases that are easily accessible.

3.3.3 Management Aspects

Successful performance of a PRA requires continuous interaction among members of the PRA study group. These members must have a great depth of understanding of the system under investigation, as well as being thoroughly familiar with PRA methodology and techniques. The model development and data analysis requires a disciplined and organized effort; each step and intermediate result must be well documented.

While individual team members may work on different aspects of the analysis, all aspects must merge into the same risk model. All these factors point to the necessity for continuous, effective intra-team communication in order to achieve a coordinated effort. There is, of course, an additional need for effective communication between the study team and other NASA or contractor organizations from which the team must acquire needed information.

TABLE 3-1

IMPORTANCE RANKING OF APU FAILURES

LOC/V - WHOLE FLIGHT - 1st ITERATION

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Fuel System Leak Into Aft Compartment From Location Downstream of Isolation Valve	74.6
2	Leak Into Fuel Isolation Valve Solenoid Cavity	3.8
3	Turbine Wheel Failure	3.8
4	Leak Into Primary Valve Solenoid Cavity (GGVM Detonation)	2.9
5	Primary Valve Fails Closed at APU Start	2.4
6	Lube Oil Circulation Restricted	2.3
7	Fuel Tank GN2 Fill Q.D. Leakage (Low Fuel Tank Pressure)	1.8
8	Any MPU Fails High at APU Start*	1.3
9	Fuel Tank Diaphragm Leakage	1.2
10	Secondary Fuel Valve Fails to Open at APU Start	0.9
11	Heater Pair 116/117 Fails Off on Orbit	0.8
12	Any MPU Fails High While APU is Running*	0.7
13	MPU 1 Fails Low at APU Start	0.7
14	Loss of Power to Secondary Fuel Valve at APU Start	0.6

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 3-1 (Concluded)

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
15	Loss of Power to Fuel Tank Isolation Valves at APU Start	0.6
16	Fuel Tank GN2 Leakage	0.5
17	Fuel Pump Bypass Valve Fails to Close After APU Start	0.4
18	Heater Pair 111/112 Fails Off On Orbit	0.3
19	Secondary Fuel Valve Controller Output Fails Off at APU Start	0.1
20	Fuel Isolation Valve Fails to Close at APU Shutdown (GGVM Large Leak)	0.08
21	Fuel Isolation Valve Leaks at Closure After Ascent	0.08
22	Loss of Power to Secondary Fuel Valve While APU is Running	0.02
23	Primary Fuel Valve Controller Output Fails On While APU Running	0.01
24	Secondary Fuel Valve Controller Output Fails Off While APU Running	0.01
25	All Other Failures	0.10
	Total	100.00

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

TABLE 3-2

IMPORTANCE RANKING OF APU FAILURES

LOC/V - WHOLE FLIGHT - 2nd ITERATION

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Leakage From Gas Generator Injector Tube	35.5
2	Leakage From Fuel Lines and Fittings	23.3
3	Leakage From Fuel Pump	12.8
4	Leak Into Fuel Isolation Valve Solenoid Cavity	4.0
5	Leak Into Primary Valve Solenoid Cavity (GGVM Detonation)	3.3
6	Primary Valve Fails Closed While Pulsing	3.1
7	External Leakage From GGVM	3.0
8	Lube Oil Circulation Restricted	2.8
9	Fuel Pump Shaft Seal Detonation	1.8
10	Fuel Tank GN2 Fill Q.D. Leakage (Low Fuel Tank Pressure)	1.7
11	Heater Pair 111/112 Fails Off On Orbit	1.6
12	Heater Pair 116/117 Fails Off On Orbit	1.4
13	Fuel Tank Diaphragm Leakage	1.1
14	Secondary Fuel Valve Fails To Open At APU Start	0.9
15	MPU 1 Fails Low At APU Start Valves At APU Start	0.7
16	Loss Of Power To Secondary Fuel Valve At APU Start	0.5
17	Loss of Power To Fuel Tank Isolation Valves At APU Start	0.5

TABLE 3-2 (Concluded)

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
18	Turbine Wheel Failure	0.4
19	Fuel Tank GN2 Leakage	0.4
20	Fuel Pump Bypass Valve Fails To Close After APU Start	0.3
	Subtotal	**99.1**
21	Leakage From Fuel Line Flex Hose	0.30
22	Secondary Fuel Valve Controller Output Fails Off At APU Start	0.09
23	Leakage From Fuel High Point Bleed Q.D.	0.05
24	Leakage From Fuel Test Port Q.D.	0.04
25	Fuel Isolation Valve Fails To Close At APU Shutdown	0.04
26	Fuel Isolation Valve Leaks At Closure After Ascent	0.04
27	Loss of Power To Secondary Fuel Valve While APU Is Running	0.04
28	Primary Fuel Valve Controller Output Fails On While APU Is Running	0.01
29	Secondary Fuel Valve Controller Output Fails Off While APU Is Running	0.01
30	All Other Failures	0.28
	Total	**100.00**

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

TABLE 3-3

IMPORTANCE RANKING OF APU FAILURE SCENARIOS

LOC/V - WHOLE MISSION

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Hydrazine leak downstream of fuel isolation valves and into aft compartment during orbit or entry that leads to failure of two APUs or flight critical equipment	39.1
	Contributors:	
	a. Leakage from any one APU (100%)	
2	Hydrazine leak as above, but from two or three APUs concurrently	26.5
	Contributors:	
	a. Leakage from combinations of two APUs (91%) b. Leakage from three APUs (9%)	
3	Hydrazine leak from a single APU as above, with an independent failure of another APU	6.4
	Contributors:	
	a. Hydrazine leak in one APU, with equipment failure of another APU while running (see below for breakdown into APU failure modes) (88%)	
	b. Hydrazine leak in one APU, with start failure of another APU (see below for breakdown into APU failure modes) (12%)	
4	Equipment failure of two APUs during orbit, entry, or landing (failures not related to APU start)	5.0
	a. Lube oil circulation restricted on two APUs (16%)	
	b. Primary fuel valve fails closed while pulsing on one APU and fuel tank GN2 quick disconnect leaks on another APU (7%)	

TABLE 3-3 (Continued)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
	c. Lube oil circulation restricted in one APU, and primary fuel valve fails open while pulsing on another APU (6%)	
	d. Primary fuel valve fails closed while pulsing in two APUs (6%)	
	e. Primary fuel valve fails closed while pulsing on one APU, and fuel tank diaphragm leaks on another APU (4%)	
	f. Lube oil circulation restricted in one APU, and fuel tank GN2 quick disconnect leaks on another APU (4%)	
	g. Fuel tank diaphragm leak on one APU, and fuel tank GN2 quick disconnect leaks on another APU (3%)	
	h. Next 36 scenarios have combinations of lube oil circulation restricted, tank diaphragm leaks, primary fuel valve closure, nitrogen leak from fuel tank, MPU failures, turbine failures, and loss of power to fuel tank isolation valves (34%)	
5	Fail to start one APU at TIG-5 in orbit and equipment failure of second APU while running	4.0
	Contributors:	
	IMPORTANT APU START FAILURES:	
	a. Secondary fuel valve fails to open on demand to start (18%)	
	b. MPU 1 fails low on demand to start (14%)	
	c. Electric power to secondary fuel valve fails at start (11%)	
	d. MPU 1 fails high* (9%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 3-3 (Continued)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
	e. MPU 2 fails high* (9%)	
	f. MPU 3 fails high* (9%)	
	g. Fuel pump bypass valve fails closed (9%)	
	h. Fuel pump bypass valve fails open (9%)	
	i. Electric power to fuel tank isolation valve fails at start (7%)	
	IMPORTANT APU EQUIPMENT FAILURES:	
	j. Primary fuel valve fails closed during pulsing (19%)	
	k. Fuel tank GN2 fill quick disconnect fails open (13%)	
	l. Heaters fail off by common cause (14%)	
	m. Lube oil circulation restricted (12%)	
	n. Fuel tank diaphragm leaks (8%)	
	o. Fuel tank nitrogen leakage (3%)	
	p. MPU 2 fails high* (3%)	
	q. MPU 3 fails high* (3%)	
	r. Turbine wheel failure (3%)	
6	Hydrazine leaks into isolation valve solenoid, auto-decomposes, ruptures valve cover, and contents of fuel tank are dumped into aft compartment	3.8
	Contributors:	
	a. Leakage into solenoid cavity (100%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 3-3 (Concluded)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
7	Turbine comes apart at normal speed during entry; shrapnel and hydrazine effects fail a second APU or flight critical equipment	3.1
	Contributors:	
	a. Turbine wheel comes apart and escapes housing (100%)	
8	Hydrazine leak from two APUs as above, with an independent failure of another APU	1.9
	Contributors:	
	a. Leakage with equipment failure of APU while running (100%)	
9	Turbine comes apart at normal speed during ascent; shrapnel effects fail a second APU or flight critical equipment	0.9
	Contributors:	
	a. Turbine wheel comes apart and escapes housing (100%)	
10	Equipment failure of one APU during ascent and another during orbit or entry	0.9
	Contributors:	
	a. Breakdown of APU failures provided previously	
11	All Others	8.4
	TOTAL	100.0

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

TABLE 3-4

IMPORTANCE RANKING OF HPU FAILURE MODES

LOSS OF CREW OR VEHICLE

RANKING	COMPONENT/ASSEMBLY RISK CONTRIBUTORS	% CONTRIBUTION
1	Lube oil circulation restricted	55.0
2	Turbine wheel failure	43.0
3	Primary control valve transfers closed while pulsing	1.0
4	All other failures	1.0
	TOTAL	**100.0**

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

TABLE 3-5

IMPORTANCE RANKING OF HPU FAILURE SCENARIOS

LOC/V

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Equipment failure of 2 HPUs on the same SRB between lift-off and SRB SEP	56.8
	Contributors and % Contribution to Scenario 1:	
	a. Common cause restriction of lube oil circulation causing bearing overheat and failure of rotating equipment in the gearbox (99%)	
2	Turbine failure leading to shrapnel induced failure of a second HPU or other flight critical equipment between lift-off and SRB SEP	43.0
	Contributors and % Contribution to Scenario 2:	
	a. Turbine fragmentation at normal speed (100%)	
3	All Others	0.2
	TOTAL	**100.0**

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

4.0 SYSTEM DESCRIPTIONS

This section provides a brief technical description of the two Space Shuttle subsystems which were the subjects of this pilot study. These two subsystems, the Orbiter Auxiliary Power Unit (APU) and the Solid Rocket Booster Hydraulic Power Unit (HPU), are similar in form and function, and share many common hardware components. However, there are also numerous differences between them, due to the HPU's less demanding operational requirements. The HPU operates for about 2.5 minutes during a flight, whereas the APU operates for approximately 1.5 hours. In addition, it is not necessary for the HPU to start or run under zero gravity conditions.

The two subsystems are discussed separately in Sections 4.1 through 4.6. The reader desiring a more detailed description is referred to the references listed in Section 12.0.

4.1 APU SYSTEM DESCRIPTION AND OVERVIEW

The Space Shuttle Orbiter has three independent hydraulic systems similar to those found on large aircraft. These hydraulic systems are used to actuate the Orbiter aero-surfaces, throttle and gimbal the Orbiter main engines, deploy and steer the landing gear, apply the landing gear brakes, and retract the external tank/umbilical plates when the external tank separates from the Orbiter.

Power for the Orbiter hydraulic systems is provided by three identical APUs, one for each hydraulic system. These APUs and their controllers are mounted on the forward bulkhead of the Orbiter aft compartment, as shown in Figure 4-1, and generate power by means of a catalytic reaction of liquid hydrazine.

4.2 APU MISSION OPERATIONS

The APUs are operated by the Orbiter flight crew, using flight deck controls and displays. The APUs cannot be controlled by ground command uplink. However, extensive telemetry on APU status is available to Space Shuttle ground controllers.

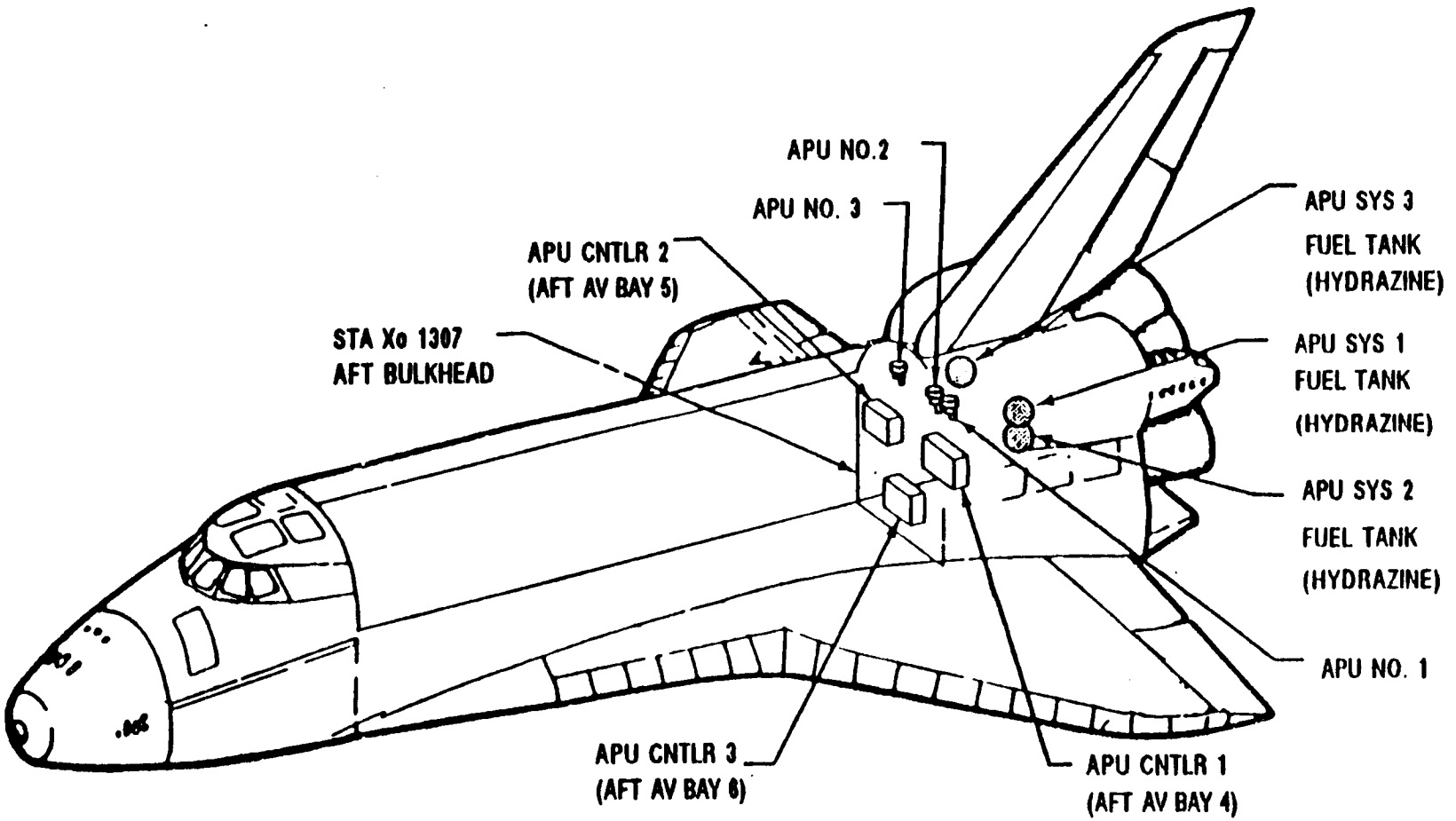


Figure 4-1. Auxiliary power unit location.

In a typical flight, the three APUs are started 5 minutes before lift-off and operate throughout the launch phase. They are shut down after the Orbital Maneuvering System (OMS) orbit insertion burn when hydraulic power is no longer required. The APUs are re-started for the deorbit burn and entry, and are shut down shortly after landing. In addition, one APU is usually run briefly the day before de-orbit to support a checkout of the Orbiter flight control system.

While the APUs are operating, they obtain lube oil cooling from three separate water spray boilers, one for each APU. During the inactive period on orbit, APU fluids are maintained within desired temperature ranges by thermostatically controlled heaters.

4.3 APU DESIGN AND FUNCTION

The APU is designed to achieve a high output of power in a compact package. It accomplishes this by means of a catalytic reaction of liquid hydrazine. This reaction produces a high velocity flow of hot gas, which is used to spin a turbine. A speed reduction gearbox transmits the power of the spinning turbine to the associated Orbiter main hydraulic pump.

Each APU consists of the following subassemblies:

(a) Fuel tank and fuel lines
(b) Fuel isolation valves (two in parallel)
(c) Fuel pump
(d) Gas generator valve module (two control valves)
(e) Gas generator
(f) Turbine
(g) Gearbox
(h) Electronic controller
(i) Exhaust duct assembly
(j) System of heaters for orbit thermal control
(k) Post-shutdown cooling system for the fuel pump/valve module
(l) Hot start cooling system for the gas generator injector
(m) Fuel/lube oil seal cavity drain system

Figure 4-2 is a schematic diagram of the APU system.

Since the APU interfaces directly with other subsystems, the diagram also depicts the APU boundary limits for the purposes of this study.

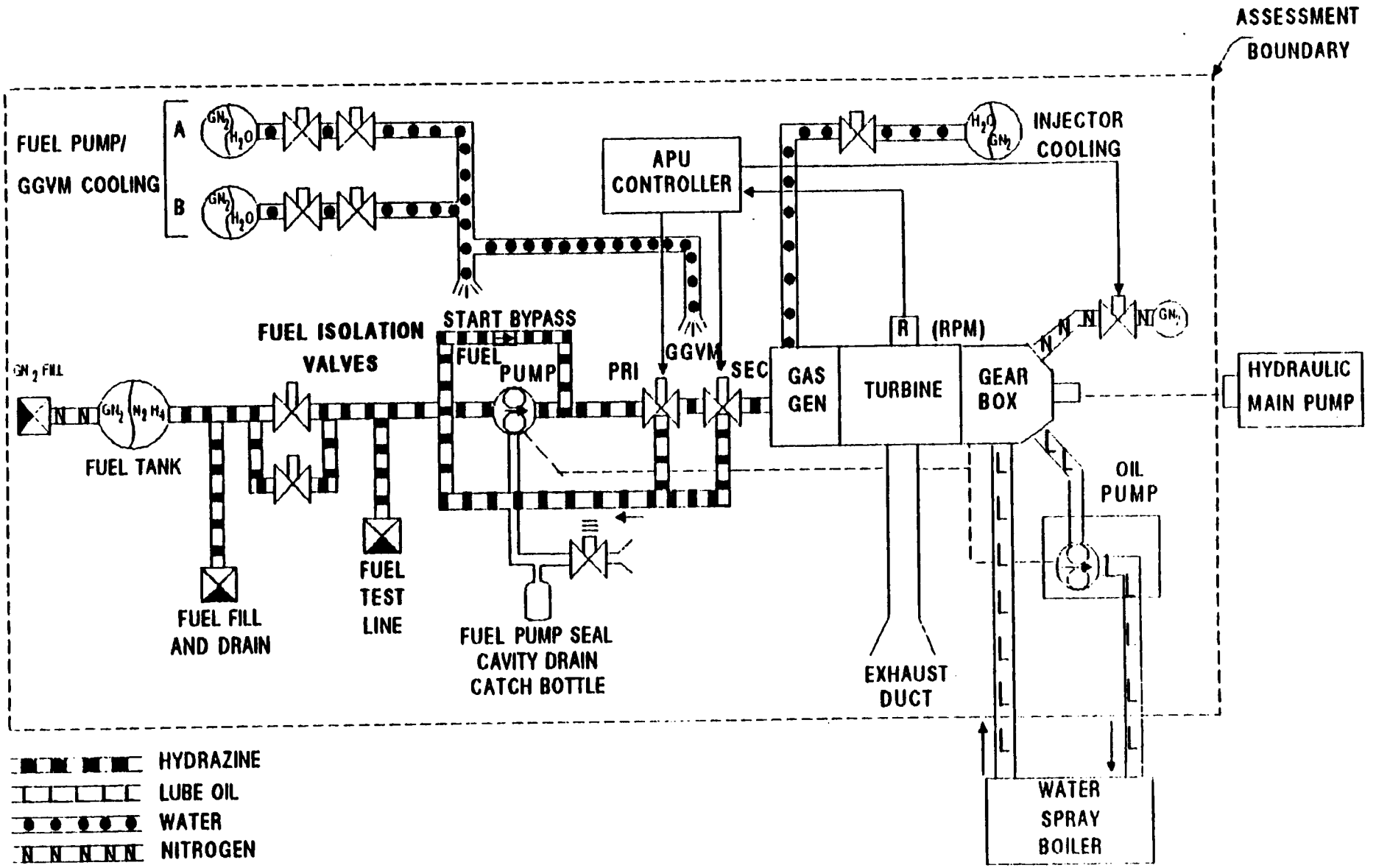


Figure 4-2. AUXILIARY POWER UNIT (APU) SYSTEM SCHEMATIC

The hydrazine fuel supply is stored in a 28-inch diameter titanium fuel tank and is pressurized with nitrogen during servicing. The gas pressure provides start capability through the fuel pump bypass valve until the fuel pump is running, and acts against the tank diaphragm to positively expel fuel to the APU. The fixed-displacement APU fuel pump provides a constant flow of hydrazine to the Gas Generator Valve Module (GGVM) after the initial bootstrap start. Approximately 325 lbs. of fuel is loaded into each fuel tank for a typical mission.

The APU turbine speed is controlled by the GGVM. The valve module consists of two flapper-type valves in series. The primary or modulating valve downstream of the pump is normally open and allows flow to the secondary or shutoff valve. The secondary valve is normally in by-pass, which directs hydrazine flow back to the pump inlet. In the powered state, it allows hydrazine flow to the gas generator. The APU controller cycles the primary valve to maintain proper turbine speed (about 74,000 rpm). In the high speed mode, the controller cycles the secondary valve to maintain a speed of about 81,000 rpm. For safety, the primary valve will begin pulsing again to maintain a speed of about 83,000 rpm if the secondary valve fails open. The gas generator (GG) is a pressure vessel containing a granular catalyst. Hydrazine flowing into the GG is decomposed by the catalyst, producing hot gases which are directed to the turbine assembly.

The dual-pass turbine assembly converts hot gas kinetic energy into mechanical shaft power at the desired speeds to operate the hydraulic pump, APU lube oil pump, and APU fuel pump.

The speed-reducing gearbox contains gears, bearings, seals, and a scavenger lubrication system. The gearbox is pressurized with nitrogen to prevent vaporization of the lubricant. A lube oil pump circulates the lube oil to the hydraulic system water boiler for cooling. The gearbox has a make-up pressurization system consisting of a small GN2 bottle and a solenoid shutoff valve actuated by the controller.

The APU electronic controller provides turbine speed control based on rotational speed sensors, logic for APU startup and shutdown, signal conditioning, gas generator catalyst bed heater control, gearbox make-up pressure control, and malfunction detection capability (flight crew alert signals to the Orbiter caution and warning system). Each controller is located remotely from its respective APU. One is located in each of the three aft avionics bays.

The APU fuel tanks are mounted on the sidewalls of the Orbiter aft compartment. Fuel tanks are located 7 to 9 feet away from their respective APUs.

The exhaust duct assembly directs the APU exhaust products overboard through an exit at the upper aft fuselage skin. Exhaust duct assemblies 1 and 2 are located on the port side and duct 3 is on the starboard side of the aft fuselage at the base of the vertical stabilizer.

All APU fluid components (pumps, valves, lines) are equipped with thermostat-controlled heaters to maintain fluid temperatures in proper ranges during the APU quiescent period on orbit and pre-launch. Heaters are also used to maintain the gas generator bed at a proper temperature for APU start-up.

The fuel pump and gas generator valve modules are maintained below 200°F during the heat soakback period, after APU shut down, by a water spray system consisting of two water tanks and associated lines, switches, thermostats, and timers. This system is only required on orbit when convective cooling is insufficient to cool these components. Temperatures above 200°F can cause partial decomposition of the hydrazine fuel, with potential for detonation at APU start-up if hydrazine bubbles have not collapsed as the APU cools down.

A single water tank with lines to all three APUs is provided to cool the gas generator injector should an APU restart be required before the gas generator can cool naturally. Control is via the APU controller. Starting a hot APU without this cooling risks detonation of the APU.

4.4 HPU SYSTEM DESCRIPTION AND OVERVIEW

The Space Shuttle SRB Solid Rocket Motor nozzle steering is controlled by the SRB Thrust Vector Control (TVC) system.

The SRB TVC System for each SRB consists of two HPUs, two servoactuators, and two APU control assemblies. The HPUs are located on the SRB aft skirt between the two servoactuators, as shown in Figure 4-3. Each HPU is driven by a hydrazine-powered turbine. The HPU provides hydraulic fluid flow to the servoactuator to obtain the proper thrust vectoring.

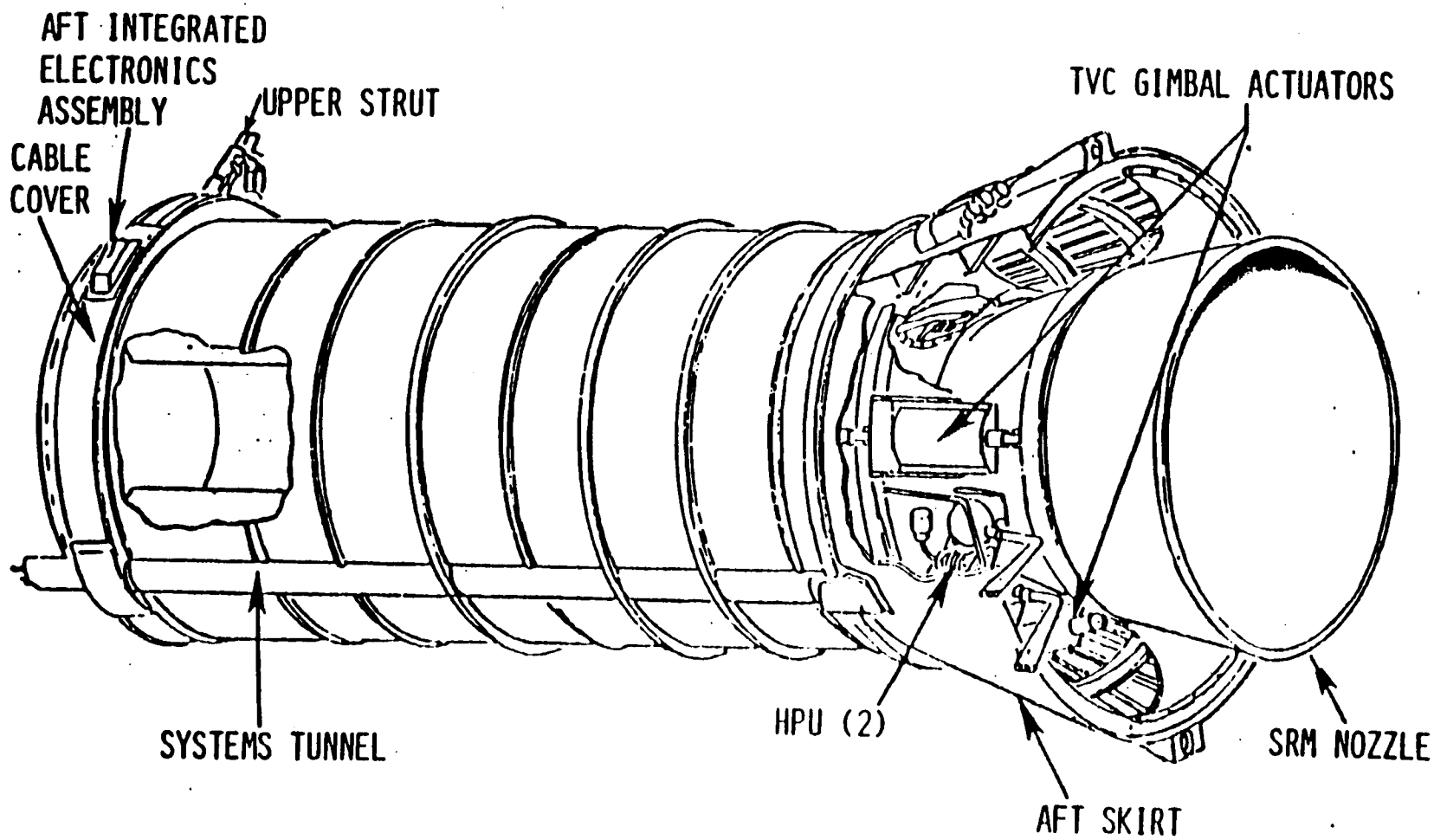


Figure 4-3 SRB TVC components location.

The two servoactuators provide nozzle gimbaling in the SRB rock and tilt axes (one dedicated servoactuator for each axis). Each HPU is dedicated to a single servoactuator during normal operation. If a single HPU fails, the remaining unit increases its power output and controls the nozzle position in both the rock and tilt planes at slightly reduced gimbal rates.

4.5 HPU MISSION OPERATIONS

The HPUs are started by a signal from the Launch Processing System (LPS) and operate autonomously through the SRB boost phase. The HPUs are not controlled by the crew or ground command uplink. However, extensive HPU telemetry is available to Space Shuttle ground controllers.

In a typical flight, the four HPUs are started 31 seconds before lift-off and operate until HPU power deadfacing at SRB separation (approximately 2 minutes after lift-off).

4.6 HPU DESIGN AND FUNCTION

The HPU is very similar to the Orbiter APU, but differs in the following ways:

a. No active cooling of any kind
b. No external insulation, except on the fuel tank
c. No fluid system heaters
d. Smaller fuel tank
e. Simpler electronic controller
f. No automatic overspeed or underspeed shutdown
g. No flight crew control or monitoring interface
h. No in-flight restart capability
i. Different type of fuel control valves
j. Different speed selection scheme
k. One fuel tank isolation valve rather than two in parallel
l. No active gearbox pressurization system
m. Stronger turbine containment ring

The Hydraulic Power Unit comprises the following subassemblies:

a. Fuel Supply Module (FSM)
b. Fuel Isolation Valve (FIV)
c. Fuel Pump

d. Gas Generator Valve Module (two Control Valves)
e. Gas Generator
f. Turbine
g. Gearbox
h. Electronic Controller
i. Exhaust Duct Assembly
j. Fuel/Lube Oil Seal Cavity Drain System

A schematic diagram of the HPU System is provided in Figure 4-4.

The FSM is a spherical pressure vessel, 15 inches in diameter, which contains approximately 32 pounds of hydrazine (N_2H_4) at mission start. The FSM is pressurized with GN_2 to deliver the N_2H_4 to the HPU fuel pump at start up. Fuel is introduced to the HPU by electrically commanding the fuel isolation valve and the secondary control valve open. The GN_2 pressure provides start capability through the fuel pump bypass valve until the pump is running. The fixed-displacement fuel pump, driven by the turbine/gearbox, provides a constant flow of hydrazine to the valve module after the initial bootstrap start.

The power generating portion of the HPU is referred to as the APU. The APU consists of a fuel pump, a gas generator valve module (which consists of a primary and a secondary speed control valve connected in series), a gas generator, a dual pass turbine, a fixed-ratio gearbox, and various check, service and relief valves to effect control for the APU.

Turbine speed is controlled by the Gas Generator Valve Module and the HPU controller. The primary or modulating valve downstream of the pump is normally open and allows flow to the secondary or shutoff valve. The secondary valve is normally in by-pass, which directs hydrazine flow back to the pump inlet. In the powered state, it allows hydrazine flow to the gas generator. The HPU controller cycles these valves to maintain proper turbine speed.

The HPU controller, located in the Aft Integrated Electronics Assembly (IEA) of the SRB, provides control of the HPU. The IEA is located on the exterior surface of the SRB casing, above the aft skirt. It monitors the turbine speed through signals received from two Magnetic Pickup Units (MPU) located on the APU turbine shaft and controls the fuel flow to the APU. Fuel flow is controlled by opening and closing the pulse (primary) control valve and/or the shut off (secondary) control valve. Prior to HPU start-up, the primary valve is normally

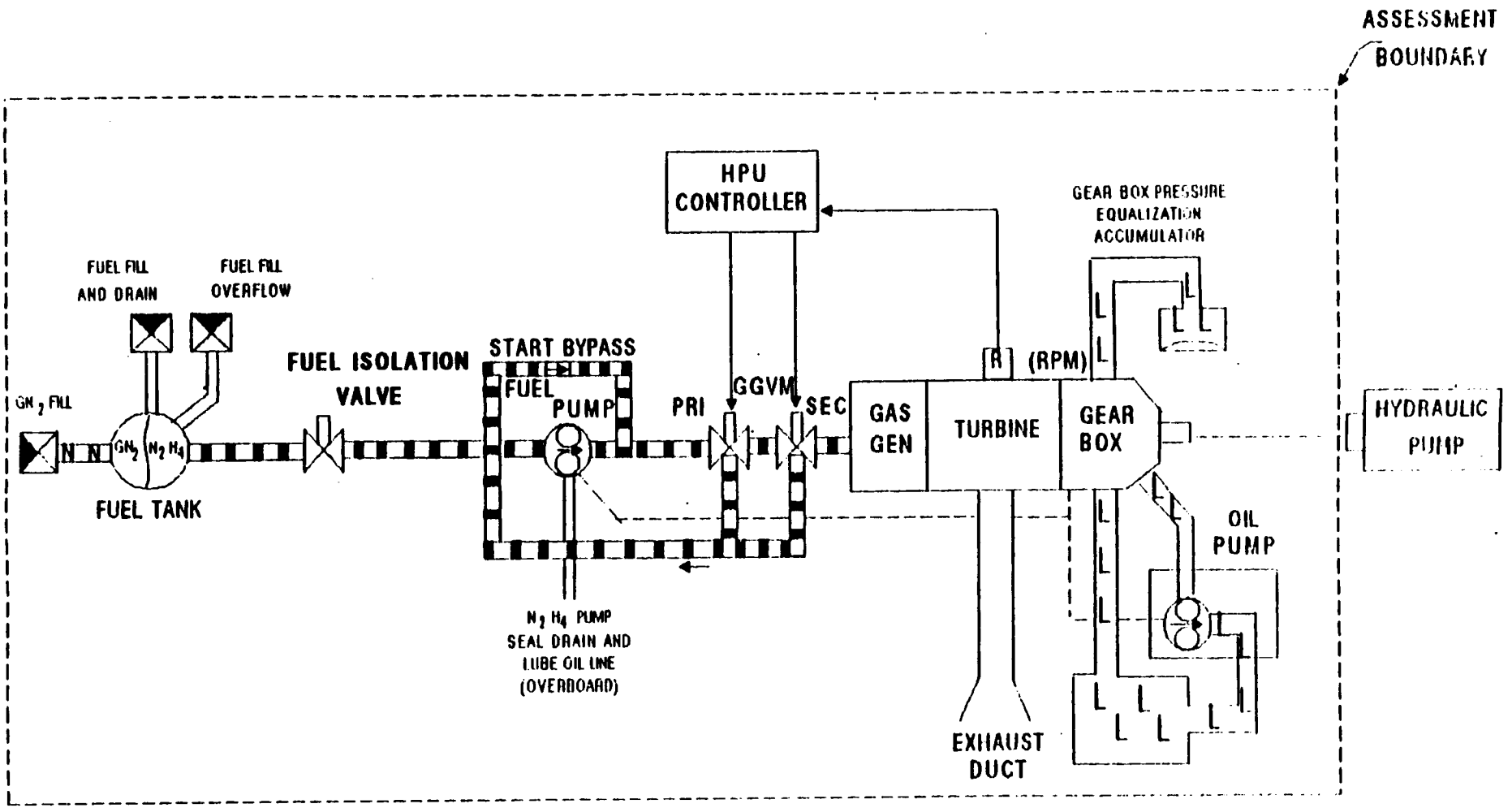


Figure 4-4. HYDRAULIC POWER UNIT (HPU) SYSTEM SCHEMATIC

open and the secondary valve is normally closed. The fuel isolation valve and the secondary control valve are opened at start-up, allowing pressurized fuel from the FSM to flow to the gas generator. As the turbine reaches 100 percent speed (74,000 rpm) a signal from the controller pulses the primary control valve to maintain 100 percent speed.

A reduction or loss of primary HPU hydraulic pressure will cause closure of a switch in the associated servoactuator which will inhibit the secondary HPU 100 percent circuit and enable its 110 percent (79,200 rpm) primary valve controller circuit. This increased APU speed provides additional hydraulic flow capacity for driving two servo-actuators. Restoration of hydraulic pressure in the failed system will move the servo-actuator switching valve back to the primary position allowing the formerly failed system to again supply hydraulic pressure to its actuator.

The secondary control valve is controlled by the 112 percent control circuit. A primary valve-open failure will cause the APU speed to increase. When the shaft speed reaches 112 percent (80,640 rpm) the secondary valve and control circuit will maintain that speed.

The exhaust duct assembly directs the APU exhaust products overboard through an exit at the outboard side of the SRB aft skirt.

5.0 STUDY METHODOLOGY

5.1 THE PURPOSE OF PRA

The purpose of Probabilistic Risk Assessment (PRA) is to provide a basis for making decisions. When PRA is applied to existing equipment, like the Auxiliary Power Unit (APU) and Hydraulic Power Unit (HPU) subsystems, the purpose is to identify and evaluate the risks and to assure that any weak spots are not overlooked. These results can be used to make day-to-day decisions, for example, how to allocate scarce resources, to improve performance, reduce cost, or increase safety.

5.2 THE STRUCTURE OF A DECISION

Like most other engineered systems, a space vehicle necessarily involves a degree of risk in its operation. Intelligent design and operating decisions can, however, control the amount of risk. Sometimes it is possible through a flash of insight to change or simplify a design in a way that not only reduces risk but also improves performance and reduces the cost. Often, however, risk reduction involves increased cost or reduced performance. The task of engineering, mission operations, and program management is to strike an optimal balance between risk, cost, and performance. The balance is struck and fine-tuned through day-by-day decisions, as the design, construction, and operation continue. In the flash of insight cases, the decisions are easy to make. In the usual case though, tradeoffs are required. In these situations, it is useful and necessary to have quantitative measures that show how much risk is being weighed against how much cost and performance. These variables are often difficult to analyze and require complex models to quantify. Cost, for example, increases by redesign but may be reduced by future performance at reduced risk. All these variables can and should be quantified for informed decisions about resource allocation.

Figure 5-1 shows the anatomy of a general decision problem. Each decision option brings with it a certain risk, cost, and performance. If these three factors were precisely known, it would be easy to make the decision. What makes the problem interesting in real life is that these variables are never known with complete certainty. It is important, then, to quantify these uncertainties as part of the input to the

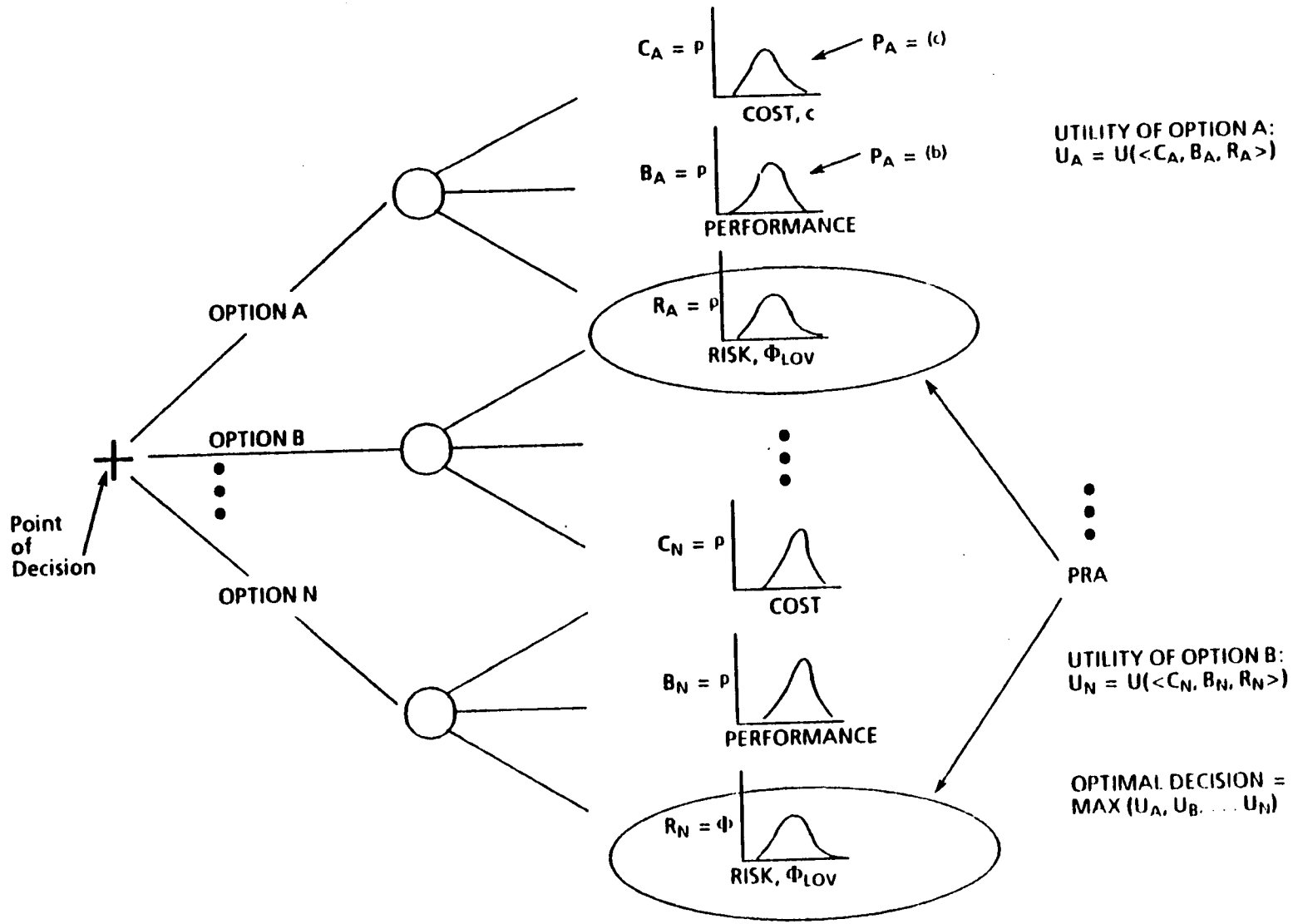


Figure 5-1 DECISION MODEL

decision analysis. Figure 5-1 also shows the uncertainties quantified in the form of probability curves. Each option can be characterized by a triplet of three probability curves. The decision maker must then choose which triplet (i.e., which option) he prefers. The role of PRA, as shown in the figure, is to provide the assessment of risk, including uncertainty, as of the input to decision problems. Strictly speaking, PRA per se is limited to the risk part of the problem, but the same quantitative way of thinking, the same probabilistic methodology, can be applied to the cost and performance factors as well.

Quantification is thus a necessary part of optimal decision making. It also serves admirably as a discipline for separating facts and evidence from hunches and wishful thinking; for discriminating between information that is truly relevant to risk and that which is irrelevant or convenient rationalization; and very importantly, for providing a uniform framework and language for documentation and communication among all parties involved in the project.

5.3 THE QUANTITATIVE DEFINITION OF RISK

A probabilistic risk assessment of the APU and HPU equipment is fundamentally the same as a PRA of anything else since, in all cases, we seek to answer the same three basic questions:

a. What can happen; i.e., what can go wrong?
b. How likely is it to happen?
c. If it does happen, what are the consequences?

The answers can be grouped as a triplet,

$$\langle s_i, L_i, x_i \rangle$$

where

s_i = a name and/or description of the ith scenario; i.e., an answer to "what can happen"

L_i = the likelihood of the ith scenario

x_i = the damage state, i.e., a measure of the damage consequent to the ith scenario

Each such triplet thus constitutes "an" answer to the three questions. The set of all possible such triplets then constitutes "the" answer to the questions. This set may therefore be adopted as the quantitative definition of risk.

Notionally, if we use braces, {}, to denote "set of" and R to denote "risk", then we may write

$$R = \{ \langle s_i, L_i, x_i \rangle \}.$$

Applying this definition, a PRA of the APU and HPU is a list of all the possible scenarios that we can envision originating in failure or malfunctions of the APU or HPU equipment and, along with each scenario, a measure of its likelihood and its consequences. Damage states (x_i), likelihoods (L_i), and scenarios (s_i) are discussed in the following three sections.

5.4 THE DAMAGE INDEX, x_i

In the case of the APU and HPU, the damage state, x, of most interest is Loss of Crew or Vehicle (LOC/V). Other damage states involved in this study include Intact Aborts (IA), entry at next Primary Landing Site (PLS) opportunity, and launch delay or Launch Scrub (LS).

5.5 QUANTIFYING LIKELIHOOD: THE PROBABILITY OF FREQUENCY FORMAT

To quantify the notion of likelihood for APU and HPU scenarios, we adopt the "probability of frequency" format. That is, we imagine a model or thought experiment in which we have launched many millions of shuttles under varying conditions. At the end of this experiment we could look at the records and ask "in what fraction of missions did scenario s_i occur?".

We shall denote this fraction by ϕ_i, and call it the "frequency" of scenario i, expressed in units of occurrences per mission. The ϕ_i are thus the output of our thought experiment.

If we had actually run this experiment, we would know these frequencies exactly. We have not run it but have, instead, the benefit of 24 successful shuttle missions and numerous tests. Thus, we know something about these frequencies but do not know them exactly. This gives rise to uncertainty about predicting the likelihood of success of future APU and HPU performance.

We also have the benefit of a data base of APU and HPU malfunctions, and of analytical calculations about the equipment and the consequences of failures. Additionally, we have the benefit

of numerous tests of individual APU and HPU components, and the opinions and insights of experts who have been working with Shuttle systems and equipment for many years. We have knowledge of similar equipment used in other applications, and finally, we have our general engineering knowledge.

All this information can be used to make inferences about the numerical values of the frequencies, ϕ_i. The format in which such inferences are expressed is that of a probability distribution, hence the name "probability of frequency format."

Such distributions will typically have the appearance of Figure 5-2. We refer to these curves as "state of knowledge" curves since they express our total knowledge (and lack of knowledge) about the values of the parameters ϕ_i, based on all the information sources mentioned above.

These curves constitute an important numerical output of the PRA, which is sometimes called a risk profile. They are one set of information useful for a decision analysis. However, of equal or greater value is what is learned in the process of arriving at these curves.

The discipline and rigor of getting these curves, assembling the information, and asking the right questions, produces great clarity and communication. It allows us to make decisions with all of our knowledge brought to bear, rather than with our knowledge of worst case scenarios only.

Furthermore, the structured, scenario-based methodology allows us to determine the reasons that the probability distribution has the shape that it does. That is, it allows us to identify the scenarios and equipment that contribute to the risk profile, and to rank the contributors to risk in order of importance.

5.6 IDENTIFYING SCENARIOS

According to our definition of risk in terms of a set of failure scenarios, the first and most important step in a risk assessment is to identify these scenarios. First, any scenario that we can describe in a finite number of words is actually a category of scenarios. Thus "the pipe breaks" is a category that includes as subcategories, "the pipe breaks longitudinally," "there is a double-ended guillotine break," "the pipe breaks in such and such location," etc. Our first principle therefore is that the word "scenario" is taken to mean "category of scenarios."

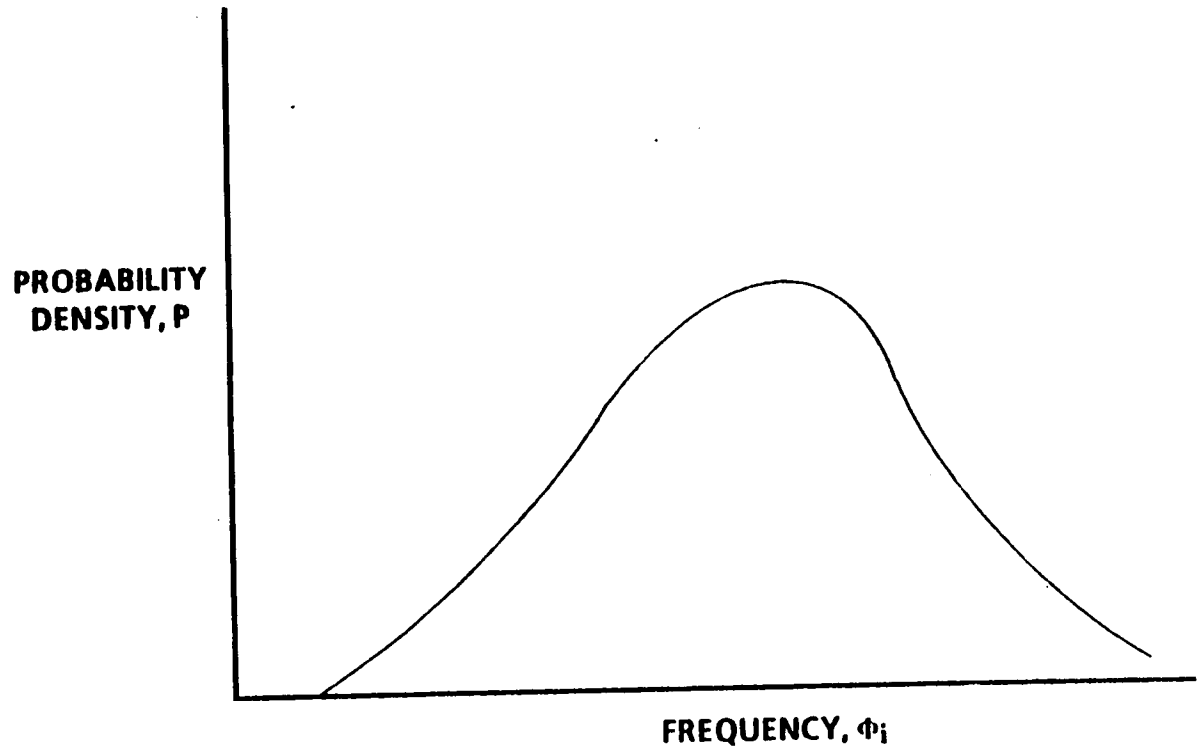


Figure 5-2 STATE OF KNOWLEDGE PROBABILITY CURVE FOR THE FREQUENCY OF THE iTH SCENARIO

A second point is that since our objective is to identify all possible significant scenarios, any method that helps us do that is good. Any new way of looking, any new way of categorizing that helps us be sure we have not overlooked any significant scenarios is good, so it is perfectly all right to use more than one approach to scenario identification.

A third point is that in any specific PRA application there are likely to be a huge number of possible scenarios. Clearly then, the scenario list must be organized in some way to allow it to be analyzed efficiently. How this is done in any instance is partly a matter of personal preference and partly a matter of modeling skill. A general methodology for this structuring of scenarios is presented in Section 5.7.

5.7 STRUCTURING THE SCENARIO LIST

To structure the scenario list for the APU and HPU, we adopt the following concepts.

a. What we call a scenario is by definition a departure from the "as planned" flight of the vehicle.

b. Any such departure from plan must originate in some initiating failure as in Figure 5-3.

c. From each such initiating failure, or initiating event, a "tree" of possible scenarios emerges as shown in Figure 5-4. The branch points in this tree represent further events which can be new failures, independent of the initiating event, or which can be dependent or cascade failures. A cascade or dependent failure is one which happens as a consequence of the original failure.

These three concepts provide us with key ideas for structuring the set of scenarios; namely, first define a finite set of possible initiating failure categories and then define, from each initiating failure category, a finite set of subsequent failure scenarios. Since each initiating failure is a category, just as each scenario is a category, we can achieve finiteness by judicious definition of the categories. The categories should be mutually exclusive and complete. Thus, any actual physical initiating failure must fall in one and only one of our set of initiating failure categories. Similarly, any actual emerging scenario must fall in one and only one of the finite set of scenario categories that we define for that initiating failure.

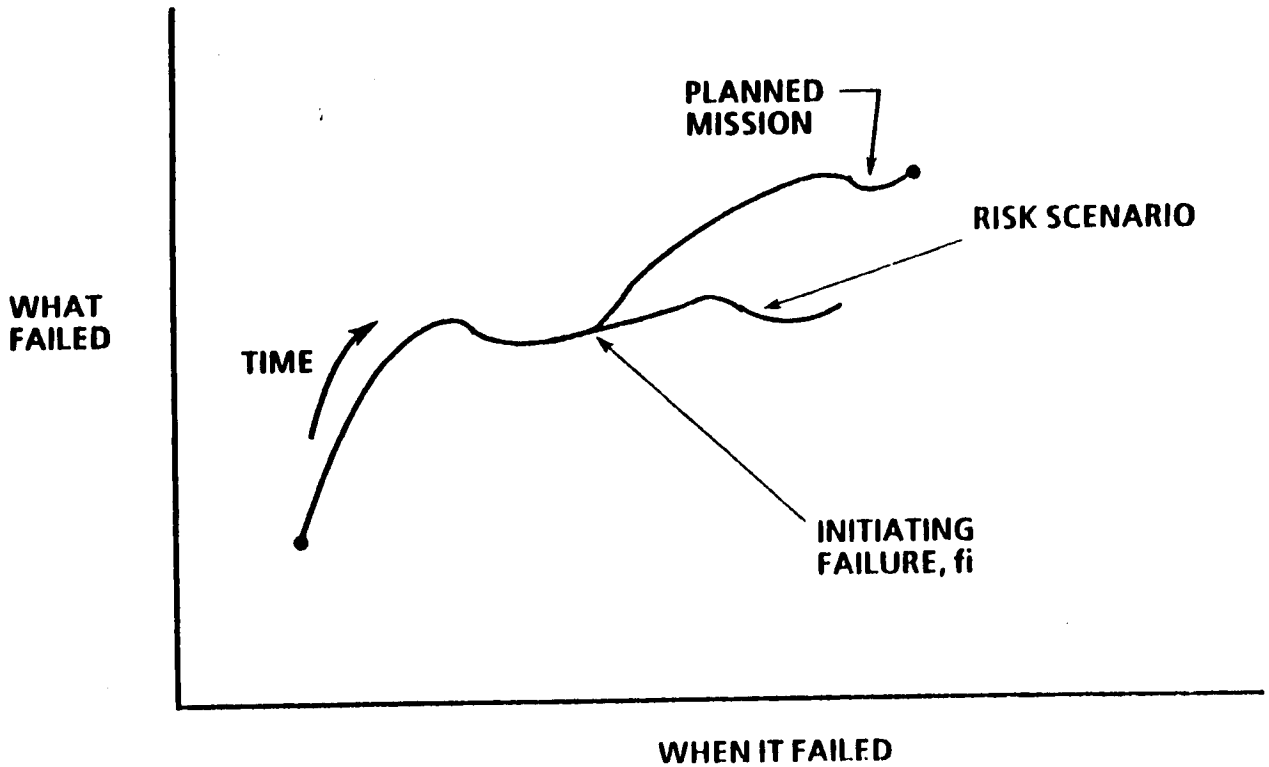
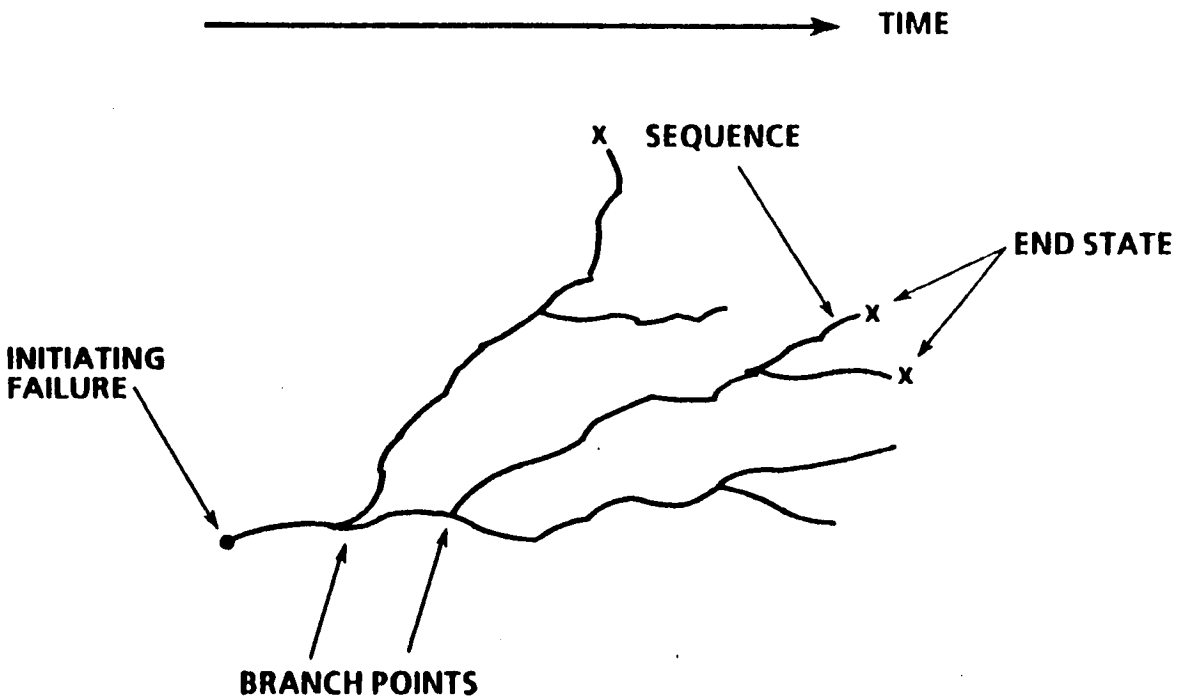


Figure 5-3 THE INITIATING FAILURE CONCEPT



TYPES OF SEQUENCES:

SINGLE EVENT
MULTI-EVENT – COINCIDENTAL
PROPAGATING FAILURE
PROPAGATING AND COINCIDENCE

Figure 5-4 EMANATION OF SCENARIOS FROM INITIATING FAILURE

We refer to the process of defining a complete and finite set of mutually exclusive categories as "partitioning" the set of possible scenarios. Let us then continue our line of thought by looking more deeply into how this partitioning can be accomplished. We begin with the initiating failures.

d. The initiating failure must occur in some part or subsystem of the vehicle and it must occur at some time or during some phase of the mission. Thus, we can label an initiating failure by saying what happened and when it happened.

e. Furthermore, by partitioning the mission time and the set of possible failures into discrete units we can establish a categorization scheme for initiating failures.

5.7.1 Master Logic Diagrams

For the purpose of the present study we have partitioned the mission time into five mission phases: prelaunch, ascent, orbit, entry/landing, and post wheelstop.

To partition and structure the set of possible failures, i.e., the "what happened" coordinate of the initiating event, we adopt a device called a master logic diagram (MLD). This device allows us to systematically think out a question like: During ascent, how can LOC/V occur? At the top level of Figure 5-5, for example, LOC/V can occur only if there is loss of thrust, loss of control, loss of structural integrity, etc. Thus, at the second level we have partitioned the set of possible failures. In the third level, each of these partitions is subdivided further, and so on. The bottom level provides failure mode categories associated with an APU or HPU.

The lowest level of breakdown constitutes a complete set of discrete initiating failure categories. For the present study we pursue only those few of these categories that involve initiating failures in the APU or HPU equipment.

In this way, for example, we arrive at the following APU and HPU initiating failures, which have the potential to lead to one of the damage states:

a. Turbine overspeed
b. Fuel (hydrazine) leak
c. Exhaust gas leak

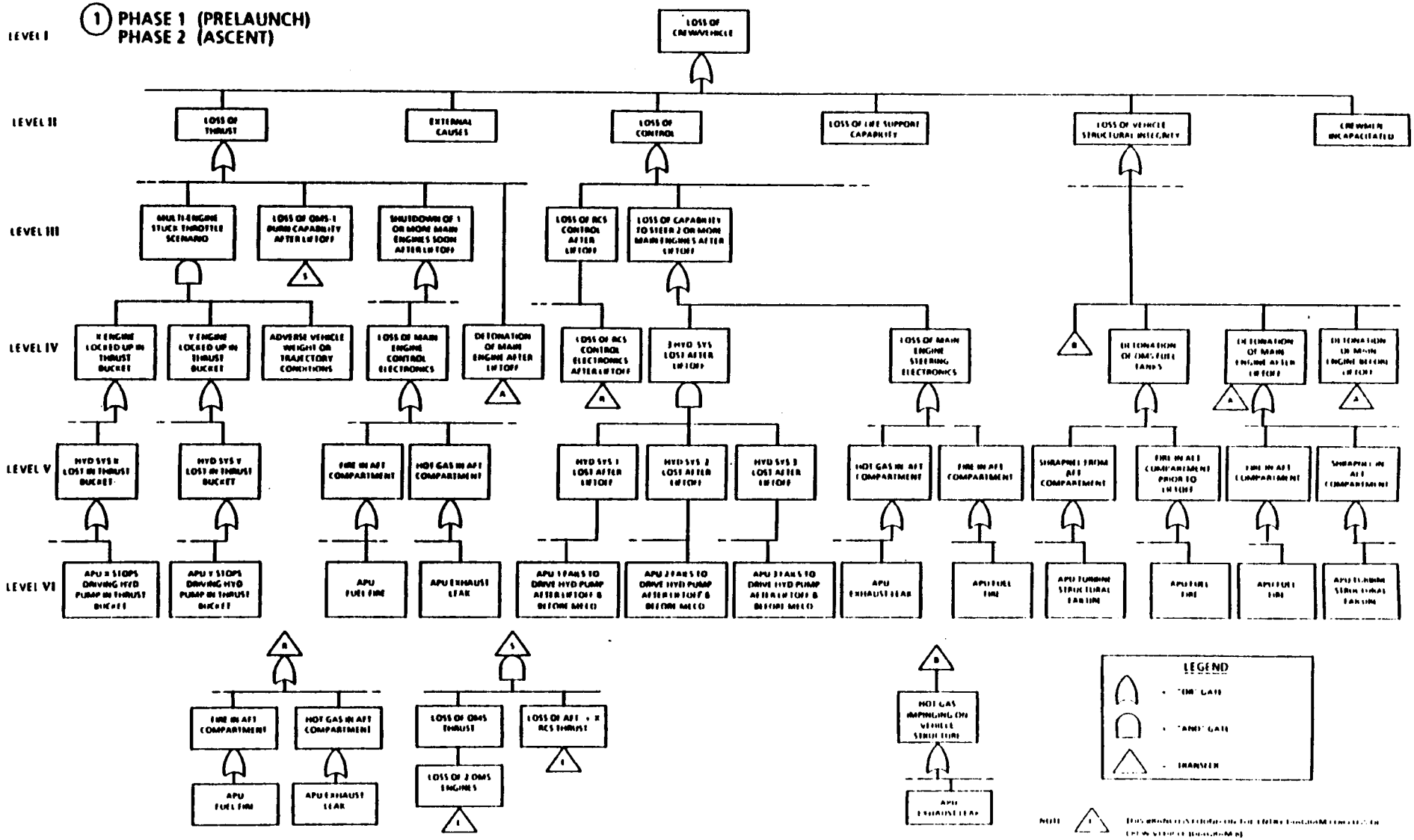


Figure 5-5 MASTER LOGIC DIAGRAM

d. Spurious overspeed or underspeed shutdown (APU only)
e. Other failures leading to permanent shutdown of APU or HPU

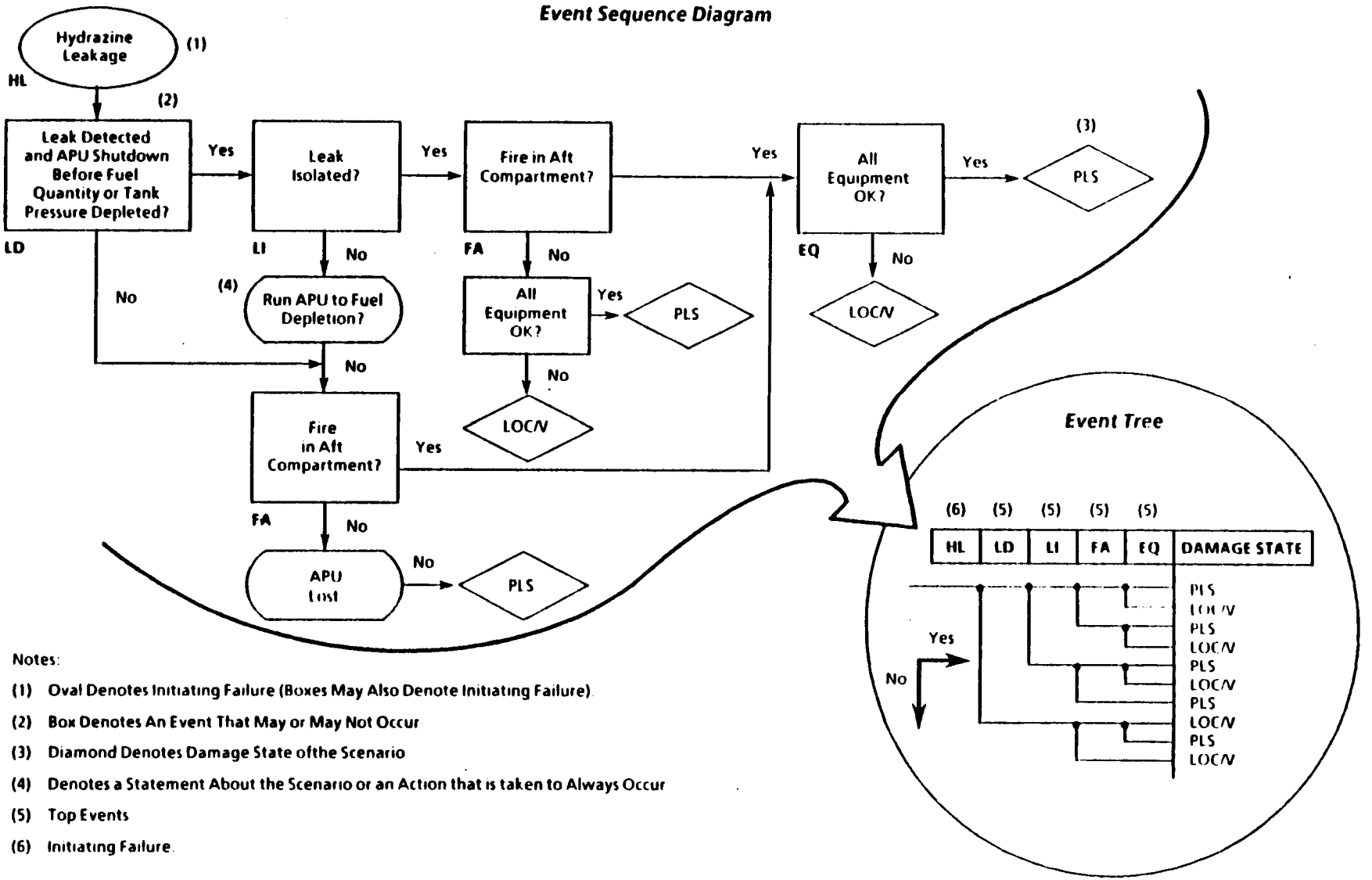
Included in hydrazine leaks are those that cause hydrazine to enter the aft compartment, go overboard, or enter the solenoid cavity of solenoid valves.

Once the initiating events are thus defined the next step is to define the set of possible scenarios emanating from each. For this purpose two further diagrammatic devices are used: Event Sequence Diagrams (ESD) and Event Trees (ET).

5.7.2 Event Sequence Diagrams

Event Sequence Diagrams are flow charts that diagram the initial failures, subsequent independent events and cascading events that could occur to form a scenario. The ESD graphically presents the flow of all reasonable combinations of events; i.e., all reasonable scenarios. It associates each scenario with a damage state. The example event sequence diagram of Figure 5-6 shows a diagram of boxes and lines. The words in each box may be interpreted as a question asking if the event occurs. Horizontal lines leading from left to right between boxes indicate a "yes" answer (Y in Figure 5-6) to the question. The next event to the right, therefore, would follow a successful event of the left box. Vertical lines indicate a "no" answer to the question. The next event down, therefore, would follow a failure event in the top box. A path of lines and boxes from the initiating failure to and including a damage state is called a scenario.

This study identified and structured scenarios that incorporated three types of propagating (dependent) failures. The first type is called a "functional interaction." In this type, the first piece of equipment to fail (e.g., a driver for the APU secondary fuel control valve) causes the second piece of equipment to stop working (e.g., the secondary valve) because the second piece depends on the first piece to function; i.e., the driver provides electric power that keeps the secondary valve open. The second type is called a "spatial interaction." In this type, a second equipment failure occurs by virtue of the first equipment failure because of the spatial proximity of the two pieces of equipment. For example, the second APU can fail by virtue of a leakage and fire from another APU. The third type of dependent failure is called a "common cause" failure. In this case, two or more pieces of nearly identical equipment



Notes:

(1) Oval Denotes Initiating Failure (Boxes May Also Denote Initiating Failure)

(2) Box Denotes An Event That May or May Not Occur

(3) Diamond Denotes Damage State ofthe Scenario

(4) Denotes a Statement About the Scenario or an Action that is taken to Always Occur

(5) Top Events

(6) Initiating Failure.

Figure 5-6 SIMPLIFIED ESD AND ASSOCIATED EVENT TREE

fail nearly at the same time (e.g., during the same mission) because of an identified defect, mechanism, or cause common to both. For example, fuel pumps can leak hydrazine in any or all APUs during the same mission because the shaft seals provide a common weak spot. Such occurrences are correlated because of the single cause and should not be treated as independent, uncorrelated occurrences.

5.7.3 Event Trees

Although an event sequence diagram contains virtually all the information needed to adequately depict scenarios, it is not helpful for answering questions about the likelihood of scenarios. In order to do this, an event sequence diagram is converted to an event tree. As shown in Figure 5-6, the events along the top of the tree correspond to the boxes (i.e., failure categories) in an event sequence diagram. Sometimes these "top events" represent multiple boxes in the event sequence diagram. An event tree is amenable to computerized quantification of the likelihood of the scenarios. Each path from "HL" to a damage state in the event tree of Figure 5-6 is a scenario.

Below each top event in the event tree there are one or more nodes, or branch points. Each node represents a decision about the occurrence or non-occurrence of its associated top event in that particular scenario, and is associated with a likelihood. The likelihood of occurrence of that top event in each scenario (i.e., for each node below the top event) depends on the sequence of events that come before in the scenario -- these likelihoods are "conditional" likelihoods. The likelihood gives the fraction of time that each of the two branches at that node is followed. We therefore refer to the conditional likelihoods of the nodes of the event tree as "split fractions".

5.8 MULTISTAGE MODELING

The operating configuration of the APU and the Shuttle changeover the duration of a mission, and the scenarios leading to damage states change during the mission. Before launch the APU and HPU start and run briefly. Scenarios during this time would lead to launch scrub or, much less frequently, to loss of crew or vehicle. During ascent, APU and HPU scenarios would be characterized by routine failure and would lead to aborts, Primary Landing Site (PLS), or LOC/V. In orbit, APUs do not run except for a brief period for Flight Control System (FCS) checkout. Scenarios are

dominated by standby failures such as leakages, heater failures, and thermostat failures. Damage states are typically PLS entry, with a remote chance of LOC/V caused by APU problems. During entry, the APUs are started and run. During the lower part of the entry, the flow of air into the compartment containing the APUs creates a chance of leakage-induced fires. During entry, therefore, this additional failure mode must be modeled along with those failures that could occur during ascent.

Since both scenarios and damage states change with each phase of the mission, event sequence diagrams are developed for each phase. In some cases, event trees are also developed for each phase. In this study we found that four event sequence diagrams could be approximated by two stages, "Stage A" and "Stage B", as shown in Figure 5-7. The damage state of Stage A, which begins at APU start prelaunch and continues through APU shutdown after ascent, provides the initial conditions for Stage B. For example, a leakage may occur during Stage A which, in accordance with flight rules, requires that an APU be declared lost and a PLS entry occur. Stage B begins with the presumption that one APU is leaking and the mission time for which the scenarios are quantified is that of a curtailed mission representative of a PLS entry rather than that of a full mission.

Each stage is represented by one or more event trees, as indicated in Figure 5-8.

Multistage modeling allows us to identify failures that contribute to the risk profile of a particular part of the mission, provide risk profiles for each stage of the mission, identify scenarios that would span the entire mission (i.e., one APU fails on ascent and one APU fails on descent), and provide the risk profile of the entire mission.

5.9 DETERMINATION OF SPLIT FRACTIONS

Each node in an event tree requires a split fraction. These split fractions are determined directly or by constructing a logic model for the node to support development of the split fraction. We use the probability of frequency format described earlier to express our state of knowledge about the split fractions. If the top event at a node is simple enough or if sufficient data exists at the node level, then the probability distribution for the split fraction is estimated directly. When the top event at a node represents a complex system, a detailed model of the system is required to break the system down into its

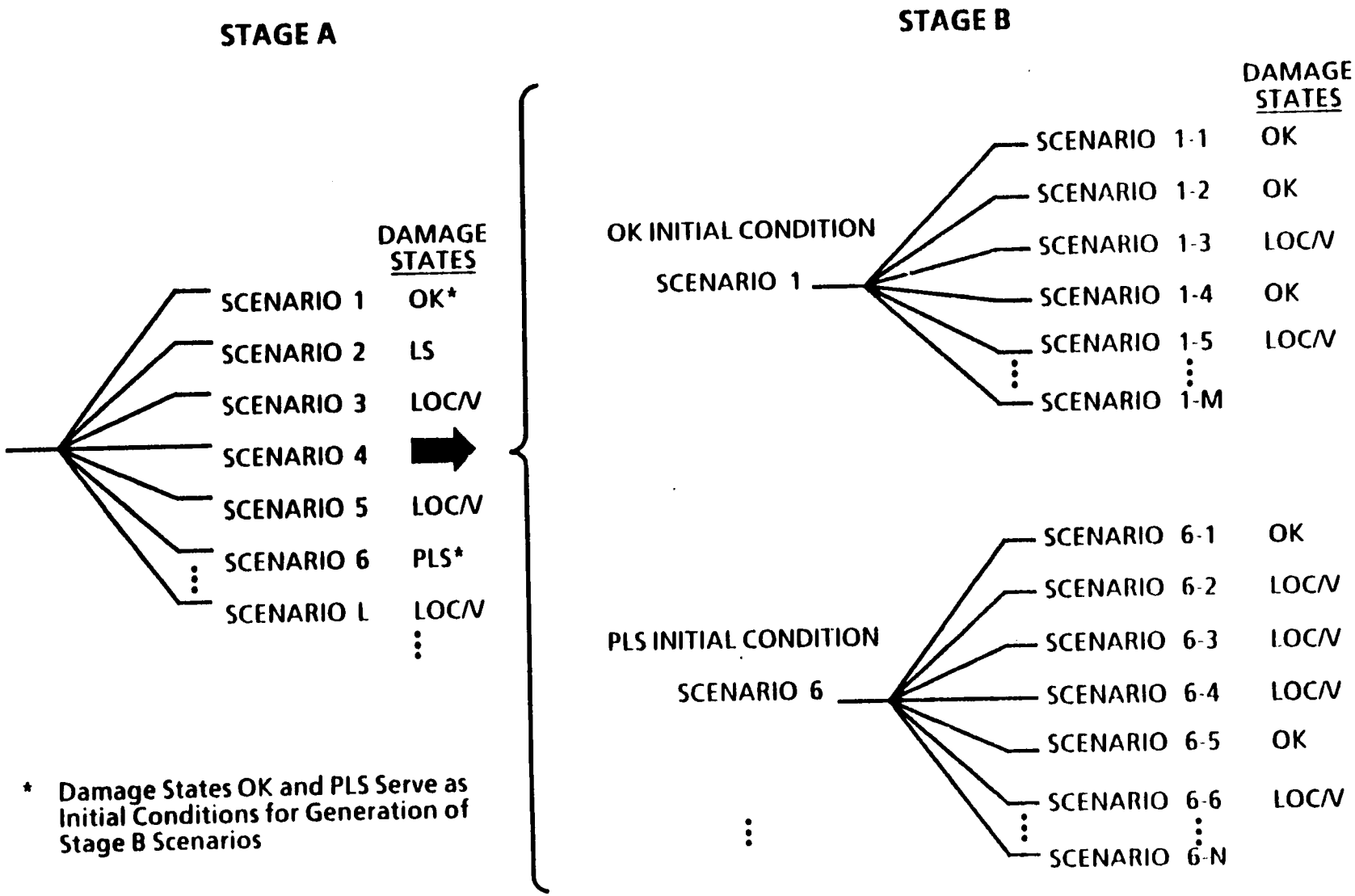


Figure 5-7 MULTISTAGE MODELING

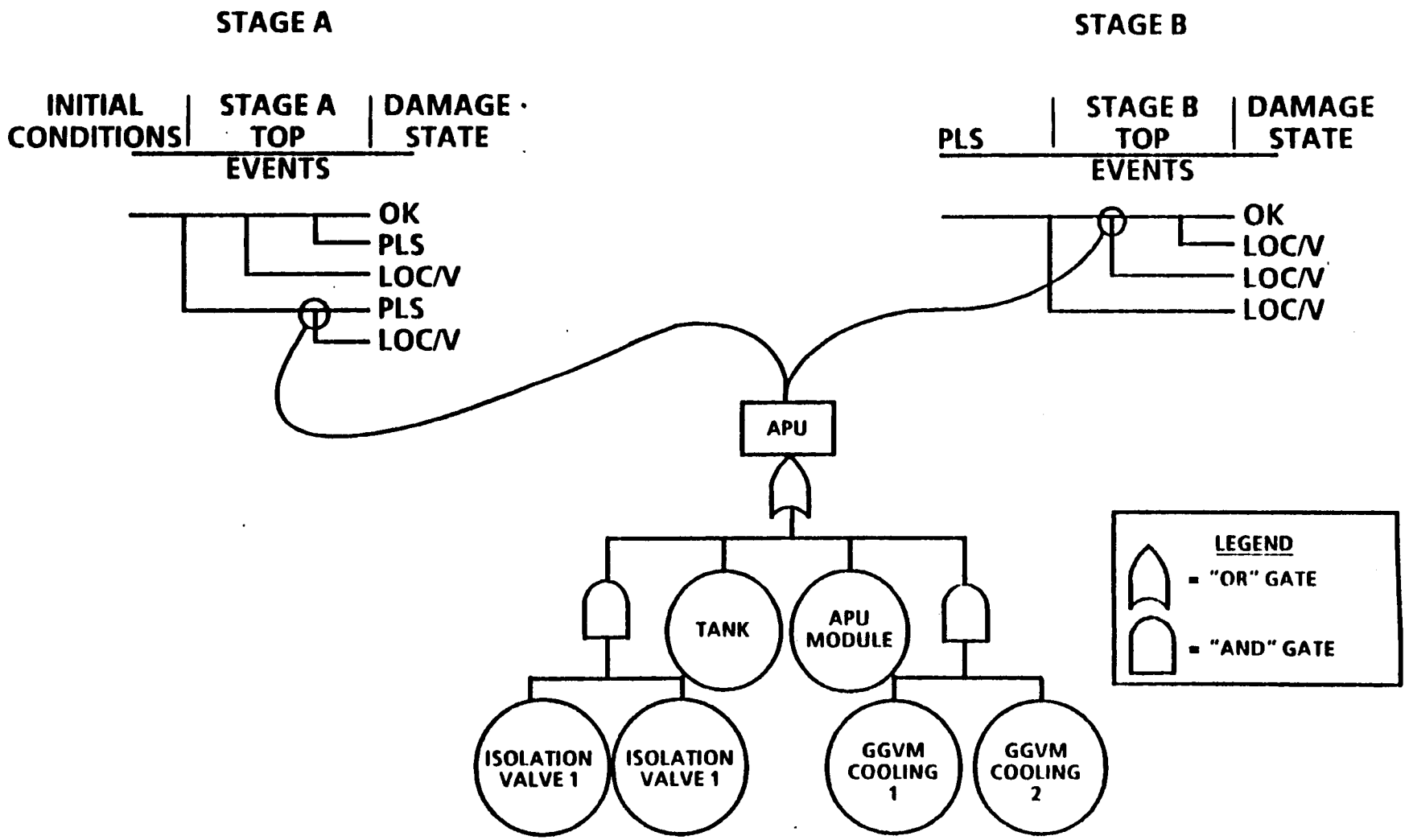


Figure 5-8 RELATIONSHIP OF SPLIT FRACTION MODELS TO EVENT TREES

component parts. This model defines how failures and successes of component parts (called basic events in the language of PRA) affect the failure and success of the top event. Several traditional methods are available for this. Fault Tree analysis is one of the more prominent ones, and is the one used in this analysis. Figure 5-8 indicates this by pointing out that a fault tree dealing with certain parts of the APU is associated with a node.

5.9.1 Fault Trees

The basic concept in fault tree analysis is to find out about a complex unit, for which we have little information, by looking at component parts about which we have much more information. Therefore, a fault tree is developed down to the level at which statistical failure and success data may be used to obtain frequencies of the basic events. Basic events are denoted by circles in Figure 5-8. We do not develop a basic event for every conceivable failure mode at a subcomponent level if statistical data exists at the higher component level.

The parameters that we wish to know about with respect to the basic event are called "running failure rate" and "demand failure rate." A running failure rate is defined as the number of failures of a component per unit time. It may represent a component that is operating or one on standby. A demand failure rate is the number of failures of a component per demand on it to actuate, energize, start or stop. For example, items such as solenoid valves usually are characterized by both parameters: a demand failure rate when the valve is first called upon to open and a running failure rate as it operates.

These parameters are multiplied by either the duration of operation (for running failure rate) or the number of demands (for demand failure rate) to obtain an "unavailability". These unavailabilities are combined, as defined by the gates in a fault tree, to obtain the split fraction for the top event at the node.

In general, the frequencies of basic events like split fractions are expressed as probability distributions. These distributions express our state of knowledge about the frequency of each basic event. They are developed by applying whatever analysis, calculations, experience, relevant testing, and engineering judgment is available.

5.9.2 Bayes' Theorem

Bayes' Theorem is a fundamental law of logical inference. It provides a mechanism for updating probability distributions which express our current state of knowledge in order to incorporate additional knowledge. Thus, if actual flight data or hot fire test data are available in addition to a previously developed frequency distribution for a basic event or a top event, they can be combined by a "statistical inference" process using Bayes' Theorem (References 100 and 106). The Bayesian approach is capable of taking into account both engineering judgment about the event frequency and empirical data such as the actual number of failures that were observed during operation of the APU.

5.9.3 Expert Opinion

Section 5.5 introduced the notion that the format for quantitative expression of knowledge is a probability distribution. Using this format, the PRA team's state of knowledge about the frequency of each event is expressed as a probability curve. The curves are based on the total body of evidence, data, experience, analysis, and information that is available. Included in this total body of evidence are the engineering judgments of systems experts. This differs from "formal" or statistical evidence, which is generally given in terms of so many failures out of so many tries or hours. Both formal and informal evidence are ultimately combined, through Bayes' theorem, to arrive at the final state of knowledge probability curves.

The question arises as to how the experts' judgments are elicited and quantified. In cases where we have lots of statistical evidence, expert knowledge is not an important issue. However, it is often the case that informal evidence is a necessary supplement to sparse data. In some cases, it may be all that is available. In the latter case, the elicitation and quantification process must be done with some care and structuring. The following five part process has proven effective and was used for this PRA.

a. Motivating the experts - explain the importance of the assessment, its confidentiality, and the fact that information (not commitments or predictions) is the goal.

b. Structuring the discussion - define the question to be answered about the parameter of interest, verify that the question can be answered, define the units or scale for

answering the question, and explicitly define the inherent assumptions in the question.

c. Preconditioning the experts - informal discussion of the parameter of interest to detect biases and induce the expert to reveal his true judgments.

d. Encoding - ask questions to encode the experts' judgment.

e. Verifying - construct the probability distribution and verify that the experts believe it is valid.

In this project, a research step occurred before the expert opinion group was convened. Written questions were formulated during the evolving scenario identification and structuring process. Some of these questions had to do with certain phenomena initiated by an APU failure that could potentially contribute to cascading of damage in the aft compartment. Examples of these questions are:

a. Under what conditions can hydrazine leakage cause fire in the aft compartment?

b. What is the potential damage done by a fire?

c. What are the conditions leading to turbine rotor failure? What is the energy of the fragments? What is the spray pattern? What is the potential for containment?

d. What damage can be caused by uncontained shrapnel and the accompanying release of hydrazine?

The systems experts performed the necessary research and analysis to answer these questions. The answers were documented to serve as a basis for the development of conditional probability distributions.

In preparation for the meeting to elicit expert opinion, a detailed set of specific scenarios and required probabilities were defined. Where possible these were reviewed by the systems experts before the meeting. The moderator began the meeting by introducing the purpose of the discussion, methodology of PRA, and the role of the systems experts.

The moderator then began the discussion of the first scenario. He made sure that everyone in the room understood this scenario exactly and the physical phenomena it is designed to represent.

He made sure similarly that each parameter in this scenario (mainly the split fractions) was thoroughly understood. Then, focusing on one parameter at a time, he asked the experts to discuss the evidence and attempt to quantify this evidence in terms of probabilities of the occurrence of the scenario. For example, the moderator described a scenario in which both control valves failed in the open position causing a turbine runaway and turbine disc fragmentation. He then asked the team what would happen and what was the likelihood of the fragments being contained.

The object was to obtain a team consensus. Thus, individual members initially proposed different distributions, reflecting different interpretations and weighings of the evidence. However, with enough discussion, a single distribution was agreed on that represented the team's state of knowledge as a whole.

It is the moderator's job, of course, to manage this process so that all available knowledge is incorporated into the distribution. The results of the meeting, the definitions of the scenarios and the parameters, the specific evidence relevant to each, and the group's probability distributions were documented. This provided a basis for reflection, reassessment, and the collection of new evidence.

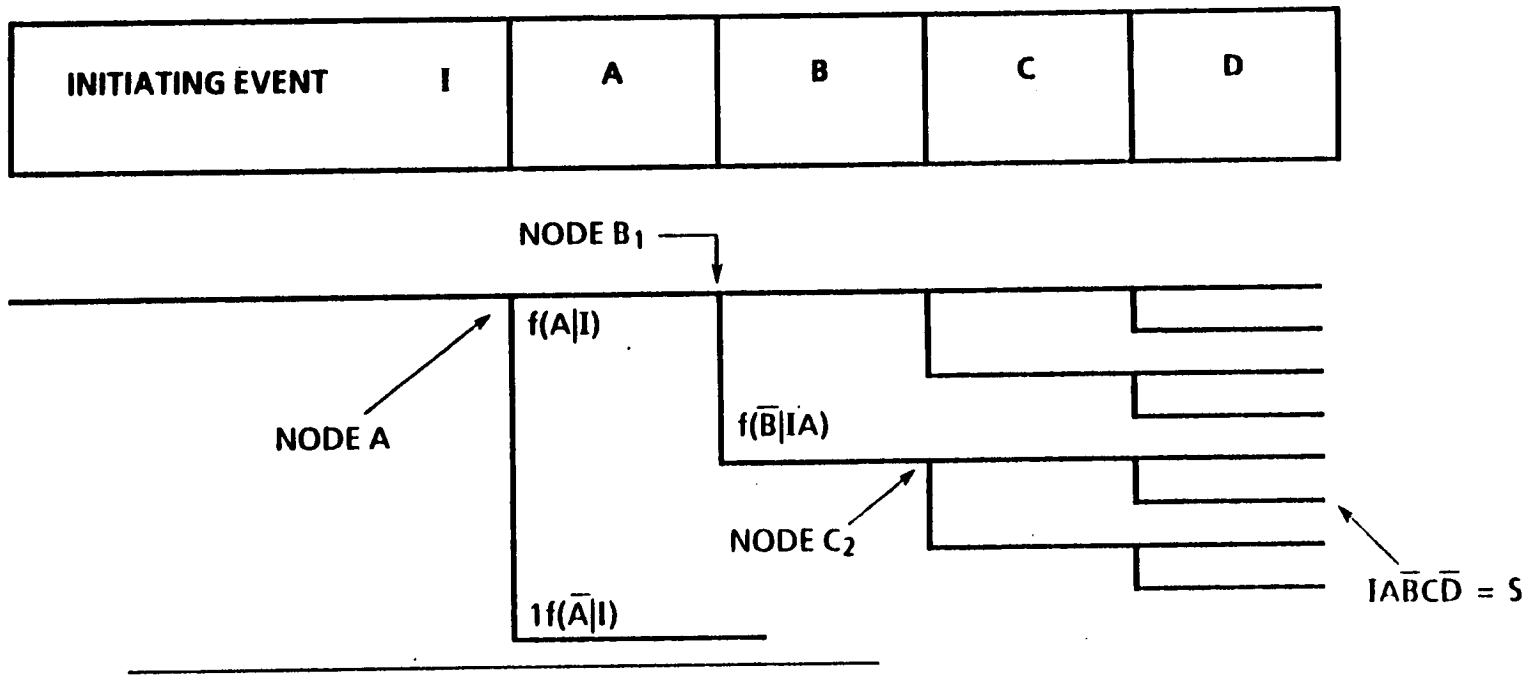
The outcome of this process was a set of probability distributions that represented the group's knowledge of the likelihood of the spatial interaction split fractions in the event trees.

5.10 QUANTIFYING SCENARIOS

The frequency of each path (scenario) in an event tree is obtained by multiplying the frequency of the initiating event (in occurrences per mission) by the "split fractions" at every node along the path.

In Figure 5-9, $\phi(I)$ is the frequency of initiating failure I. Out of all scenarios, starting at I, $f(A|I)$ is the fraction in which event A happens, given the initiating failure, I. The quantity, $1-f(A|I)$ is then the fraction in which A does not happen.

Our convention is that B means "not" B. Out of all scenarios in which I and A happen, $f(B|IA)$ is the fraction in which event B does not happen, and so on. Proceeding in this way, if the path S is I A B C D, as shown in the figure, then the frequency, $\phi(S)$, of this path is given by the equation in the lower left corner of Figure 5-9.



$$S = I\ A\ \bar{B}\ C\ \bar{D}$$

$$\Phi(S) = \Phi(I)f(A|I)f(\bar{B}|IA)f(C|IA\bar{B})f(\bar{D}|IA\bar{B}C)$$

Figure 5-9 EVENT TREE QUANTIFICATION

The process of quantifying scenario frequencies then is just the numerical evaluation of equations of this type.

In a multistage model the scenarios may be grouped according to their damage states. The ϕ(s)'s are then added to yield the frequency of each damage state. For example, the ϕ(s)'s of scenarios that lead to LOC/V are summed to give the total frequency of LOC/V.

A more accurate estimation of total LOC/V frequency is obtained for Stage B in a multistage model if the PLS damage state is divided into groups called damage bins. Each damage bin is characterized by a particular kind of damage to one or more APUs. For example, this study used three such bins. One characterized by an APU lost, one characterized by one or more APU's leaking, and one characterized by one APU lost and one leaking. Of course, a bin in which everything is OK is also defined.

The frequency of each bin is the sum of the frequencies of its constituent scenarios. Each bin serves as an initial condition to the next stage of the model.

The frequency of LOC/V of Stage B for this study is then a combination of the contributions of the four bins (three damage bins and the OK bin) that were the output of Stage A. If we define ϕ_B as the frequency of LOC/V for Stage B and ϕ^A(Bin i) as the frequency of Bin i from Stage A, then

$$\phi_B\ (\text{LOC/V}) = \sum_{i=1}^{4} \phi^A\ (\text{Bin i}) \sum_{j=1}^{L} \phi_j{}^B\ (\text{LOC/V}|\text{Bin i})$$

where

$\phi_j{}^B$ (LOC/V|Bin i) is the frequency of scenario j from a total of L scenarios that lead to LOC/V, given Bin i as an initial condition.

The total LOC/V frequency is the summation of ϕ_A (LOC/V) and ϕ_B (LOC/V).

5.11 RISK DIAGNOSIS

Having assembled the risk profile per Sections 5.1 through 5.10, it remains to interpret the risk curves and determine the contributions to risk. Figure 5-10 illustrates this process. A similar figure would apply to each damage state.

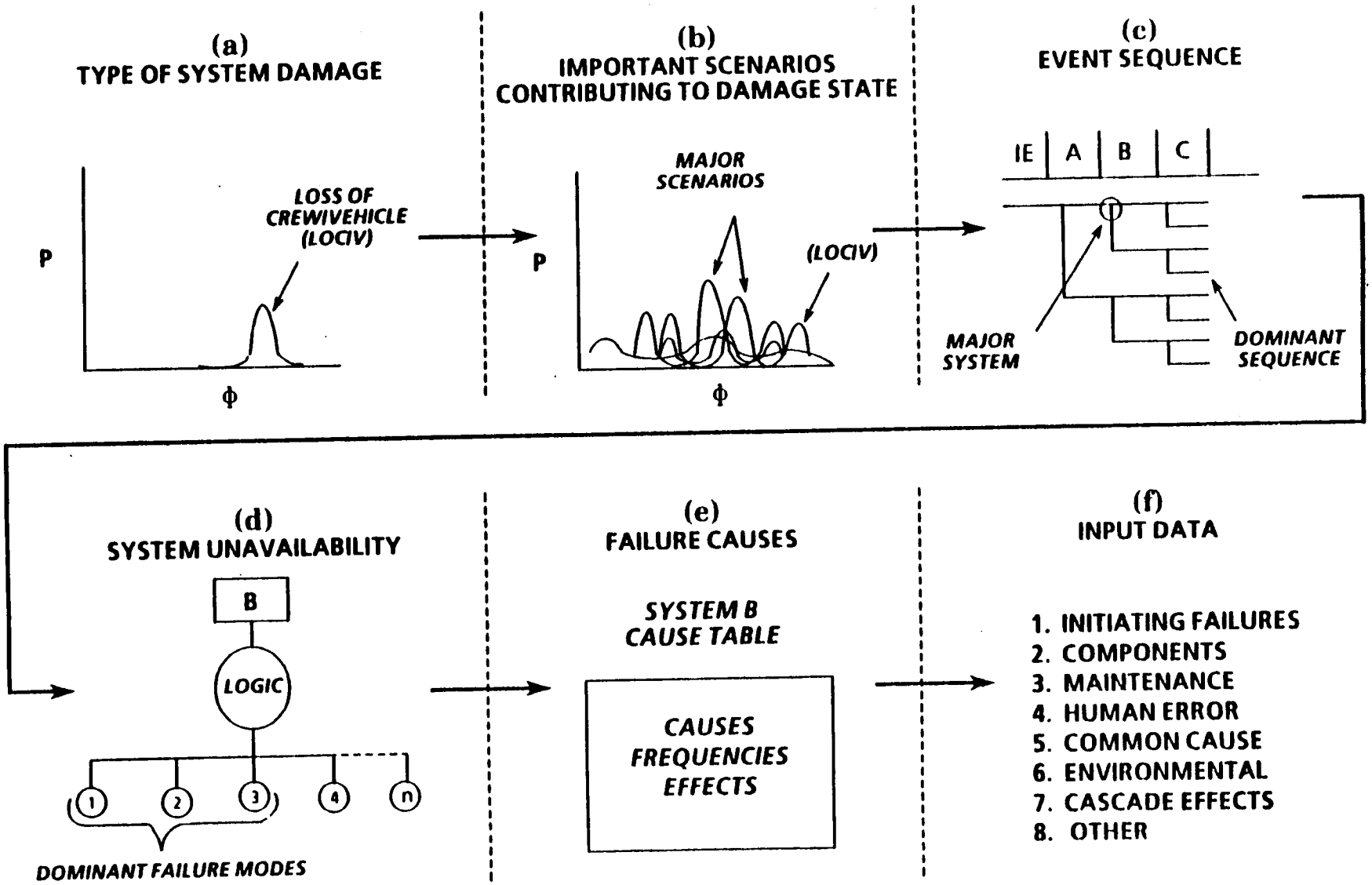


Figure 5-10 RISK DIAGNOSIS

The LOC/V risk profile itself, (Figure 5-10a) provides a great deal of information. We know that the risk is not as great as the space to the right of the curve and not as low as the space to the left of the curve. We expect it to be about where the "hump" of the curve is. We have, therefore, bounded the possibilities and told the decision maker how certain we are of the risk.

Furthermore we can identify the risk profiles of the individual scenarios that are the most important contributors to the total risk profile (Figure 5-10b). Scenarios that are not the most important contributors to the total risk profile should receive less priority and less attention. That is, scenarios that have frequencies toward the left tail of the risk profile should not receive immediate attention. Identification of scenarios as important or unimportant contributors to a damage state is possible because an event tree unambiguously associates each scenario with a damage state.

The use of event trees also allows easy identification of the top events that contribute to each high-risk scenario (Figure 5-10c). To find which components of the APU or HPU that are most important to each top event, the split fraction model is investigated (Figure 5-10d). This is facilitated by a cause table (Figure 5-10e) which delineates in ranked order from most frequency to least frequency, the individual components and contributions of components that contribute to the top event. The fractional contribution of each combination of components or individual component to the top event in a particular sequence is derived from this table. More depth of information about why a component has a particular failure rate is found in the data analysis (Figure 5-10f).

Components of high ranking that contribute to important scenarios should receive the most attention for possible corrective actions. Components that are ranked low in any important scenarios or do not appear in any important scenarios (no matter how high the ranking) should receive lower priority.

In this way the PRA results help establish the allocation of resources for effective risk management.

5.12 SUMMARY OF PRA METHODOLOGY

The previous ten sections discussed the PRA methodology employed in the APU/HPU risk assessment. This section summarizes this methodology in terms of a procedure shown in Figure 5-11. The 14 steps of the procedure are listed as shown.

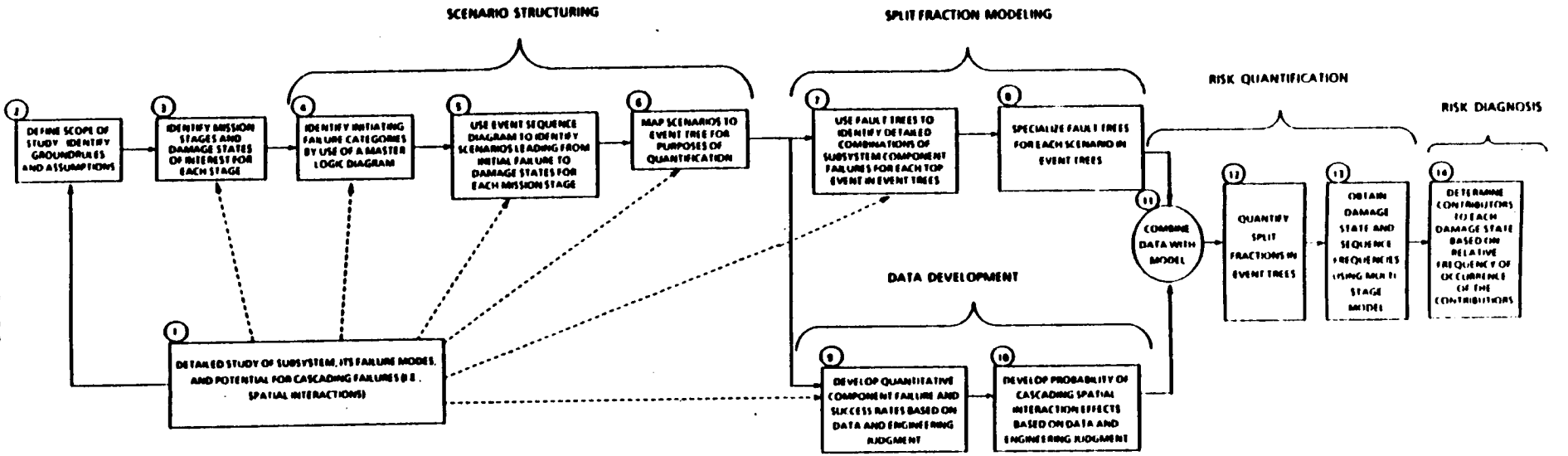


Figure 5-11 PROCEDURE FOR APU/HPU QUANTITATIVE RISK ASSESSMENT

Step 1: Study System

A detailed study of the system forms the basis of the rest of the PRA. This study includes such aspects as system failure modes, modes of operation, interaction with the ground controllers, interaction with and dependencies on other systems, failure history, maintenance, testing, design changes, refurbishment, environmental conditions when operating and when not, and surveillance and inspection activities.

Step 2: Define Scope

As with any other analysis or evaluation, the scope of effort (what is to be included and what is to be excluded) and the guiding groundrules and assumptions are identified. Minor changes to these are acceptable as the project progresses when more is learned about the system that is under assessment.

Step 3: Damage State and Mission Stage Identification

A key element in defining the work to be done for the rest of the PRA is identifying the damage states of interest and defining the mission stages to be analyzed. This is not considered part of Step 2 because considerable technical work must be done in order to establish an appropriate definition of mission stages.

Steps 4, 5, & 6 Scenario Structuring

The development of initiating failure categories, event sequence diagrams and event trees that identify scenarios leading to damage states was described in Sections 5.7 and 5.8.

Steps 7 & 8 Split Fraction Modeling

The use of fault trees to model the top events and the development of scenario-dependent split fraction models were discussed in Section 5.9.

Steps 9 and 10 Data Development

This study developed data for three types of events. The first type (Step 9) was for random equipment failure for each APU (or HPU). The second type (Step 9) was for common cause failure of two APUs (or HPUs) together. The third type of data (Step 10) was for cascading effects associated with a failure that by virtue of its proximity to other components could cause other components to fail. Such events are called spatial interaction events in this study. They result from phenonema such as fires, hydrazine decomposition, hydrazine chemical attack, other chemical reactions, hot exhaust gas, and shrapnel from turbine rotor failure. Section 5.10 described the methodology of data development and of determination of the values of the split fractions.

Steps 11, 12, & 13 Risk Quantification

Combining data with the model, developing the split fractions from fault trees and quantifying the multistage event tree model was described in Sections 5.8, 5.9, and 5.10. The result of Step 13 is the risk profile for each damage state.

Step 14 Risk Diagnosis

The procedure and usefulness of disassembling the results to find the constituent contributors to the risk profile was described in Section 5.11.

6.0 AUXILIARY POWER UNIT (APU) SCENARIO PRESENTATION

For purposes of this analysis, APU operations were divided into five mission phases (prelaunch, ascent, orbit, entry, and post landing), as shown in Figure 6.0-1.

The model was developed using five mission phases; however, it was concluded that quantification could be accomplished using only two, as shown in Figure 6.0-1, in order to reduce model complexity. Stage A extends from APU prelaunch start-up to APU post-ascent shutdown. Stage B extends from the end of Stage A to APU post landing shutdown. The periods prior to APU startup pre-launch, and after APU shutdown post landing were omitted from the analysis due to APU non-operation.

In the subsections below, the methodology described in Section 5.0 is traced step-by-step through an analysis of the APU Sub-system. The results of this analysis provide the framework or model, which can then be evaluated using the failure frequency data described in Section 7.0.

Section 6.1 details the ultimate damage states selected for the analysis. Section 6.2 details the Master Logic Diagrams (MLDs) developed to show how APU-related initial failure categories can lead to these damage states.

The event sequence diagrams are presented in Section 6.3. These are flow diagrams illustrating the scenarios leading to different damage states as a consequence of various categories of APU fail-ures. The APU failure categories and different damage states developed in the event sequence diagrams provide the framework for development of the event trees, presented in Section 6.4.

The event trees establish the decision points (called nodes) for which specific probabilities (called split fractions) must be determined in order to arrive at overall probabilities for the ultimate damage states. The event trees are similar to decision diagrams -- each decision point must be answered by a "yes/no" question. Each path through the event tree results in either a damage state or a state of no damage, based on the cumulative effect of all failures in that path.

Determination of each event tree decision point, or split fraction, depends on a logical combination of events, which is expressed in the form of a fault tree. Development of these fault trees, or split fraction models, is presented in Section 6.5.

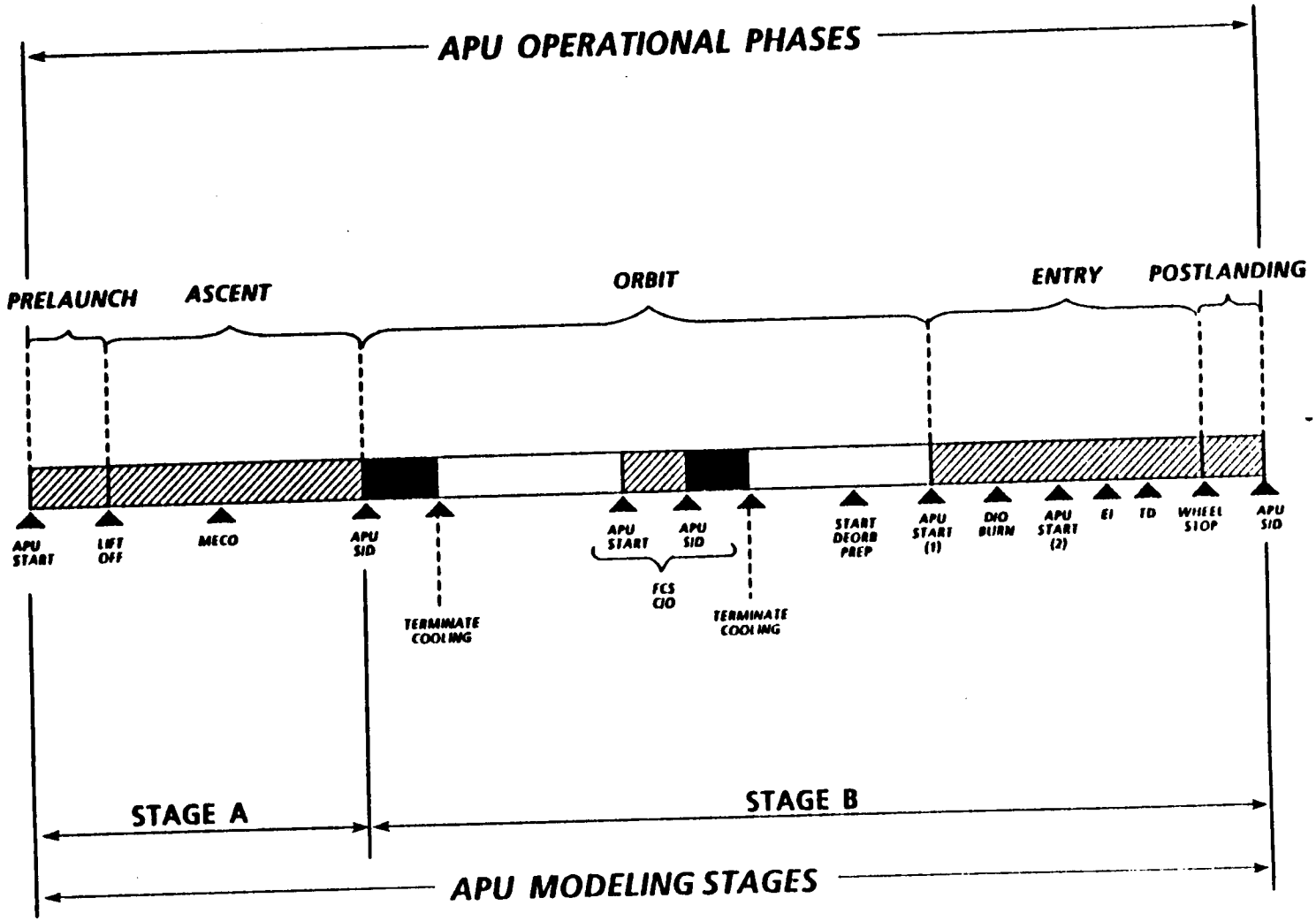


Figure 6-1. APU Operational Phases and Modeling Stages

Section 6.6 deals with the analysis of a special class of events called Spatial Interaction Events (SIEs). These are events by which a failing APU can cause damage to other APUs or to other vital equipment in the Orbiter aft compartment. The mechanisms of such occurrence might be shrapnel, fire, chemical attack, and hot gas impingement.

6.1 DAMAGE STATES

A damage state is the outcome of a scenario. A damage state is usually an undesired event selected because of a need to understand its frequency of occurrence.

The ultimate damage states selected for this study were not peculiar to the APU or the HPU under study, but were of a broad category which would encompass any of the Space Shuttle's subsystems. In addition, the damage states were selected to be consistent with the NASA Failure Mode and Effects Analysis (FMEA) as defined in NSTS 22206 (Reference 29). The ultimate damage states selected were:

a. Loss of crew and/or vehicle
b. Loss of mission

Loss of mission implies that the ability to perform all or a substantial portion of the payload-related activities was lost. However, this study did not address any particular payload. Loss of crew/vehicle is self-explanatory.

These damage states were examined for each of the five mission phases (defined for the analysis as prelaunch, ascent, orbit, entry, and post landing) to determine which damage states were applicable during each of the phases. The results are presented in Table 6.1-1.

Loss of mission was not judged to be a viable damage state for the entry and post landing phases.

Once the damage states for the phases were defined, the next step in the study was to develop a set of Master Logic Diagrams (MLDs) using the ultimate damage states as the Top Events. This process is discussed in Subsection 6.2.

Table 6.1-1

DAMAGE STATE APPLICABILITY

DAMAGE STATE	SPACE SHUTTLE MISSION PHASE				
	PRELAUNCH (1)	ASCENT (2)	ORBIT (3)	ENTRY (4)	POST LANDING (5)
Loss of Crew/ Vehicle	X	X	X	X	X
Loss of Mission	X Launch Scrub	X Intact Abort First Day PLS Entry	X Enter ASAP Next PLS Entry Minimum Duration Flight	N/A	N/A

6.2 MASTER LOGIC DIAGRAM DEVELOPMENT

6.2.1 General Development Process

With a set of ultimate damage states established for each mission phase, the next step was to determine if and how failures initiated in the APU system could contribute to these damage states. The MLD served to guide and document this thought process. Appendix B6.2 contains the MLDs developed for this study.

The ultimate damage states established for each mission phase represent the "top events" of the MLD for that phase. The approach taken was to develop the second level of each diagram in the form of broad general categories, rather than immediately focusing on the APUs. This "top down" approach keeps the analyst open to the possibility of unanticipated failure effects involving the APUs. It also allows the diagrams to serve as a general framework for analysis of other Space Shuttle systems. Just below the top event is the "second level" which comprises six general Shuttle functions whose failure would cause the top event. Some of these Shuttle functions were not developed further, as there appeared to be no relationship between the APU and those events.

The third level of the MLD identifies more specific Shuttle functions that depend, in part, on APUs. Succeeding levels extend this breakdown into ever more specific Shuttle functions, until specific APU system failures begin to appear in the diagram at levels 6 and below. In some of the simpler diagrams, APU failures appear earlier.

Many MLDs were developed that dealt with physical processes about which there is some uncertainty. These physical processes are related, in some way, to the top events. All such points of uncertain dependency were noted, and documented in the form of technical issues to be resolved. Completion of the final analysis depended on resolution of these issues by the best means available. This involved in-house analysis, a data search for technical references, and reliance on expert opinion.

MLDs can be developed to any level of detail desired, down to the smallest, and seemingly most insignificant part, to show possible failure paths that lead to the top event. The purpose of the MLDs, however, was not to delineate all failure modes that could cause the top events. Their purpose was to identify broad categories of initial failures, as discussed in Section 5, from which to begin the the more detailed identification of scenarios and the delineation of failure modes (in the fault trees) associated with the scenarios.

The completed MLDs served as a reference for the next step in the analysis, the development of Event Sequence Diagrams, as well as serving as a continuing reference source through the ensuing analysis process. Their importance in the PRA process should not be underestimated.

6.2.2 MLD Descriptions

As a general rule, an MLD was developed for each damage state defined for each mission phase. The intact abort damage state for ascent (Phase 2) was further subdivided into specific abort modes, and an MLD was developed for each. This served to clarify the contribution of APU failures to ascent abort modes.

The MLDs, as developed, are provided in Appendix B6.2. They are outlined in Table 6.2-1 and discussed individually below.

Table 6.2-1

MLD DEFINITIONS

MLD	DAMAGE STATE	MISSION PHASE	DESCRIPTION
1	Loss of Crew/ Vehicle	Phases 1 and 2	Prelaunch and Ascent
2	Loss of Mission	Phase 2	Return To Launch Site (RTLS) (Ascent)
3	Loss of Mission	Phase 2	Transatlantic Abort Landing (TAL) (Ascent)
4	Loss of Mission	Phase 2	Abort Once Around (AOA) (Ascent)
5	Loss of Mission	Phase 1	Launch Scrub (Prelaunch)
6	Loss of Crew/ Vehicle	Phase 3	Orbit
7	Loss of Mission	Phase 3	Orbit
8	Loss of Crew/ Vehicle	Phases 4 and 5	Entry and Post Landing

MLD 1 - Loss of Crew/Vehicle - Phases 1 and 2

MLD #1 (Appendix B6.2-1) depicts how APU failures can lead to loss of crew and vehicle during the prelaunch and ascent phases. The overall functional effects of APU failures contributing to loss of crew and vehicle were determined to fit into three broad categories: (1) loss of thrust; (2) loss of control; and (3) loss of vehicle structural integrity. Of these three, only loss of vehicle structural integrity applies to the prelaunch time-frame. All three categories apply to the ascent phase.

For the prelaunch phase, loss of crew/vehicle scenarios involve high high energy detonations of equipment in or near the aft compartment, such as the Orbital Maneuvering System (OMS) propellant tanks. One source of such a detonation could be shrapnel from an APU turbine coming apart, or a fire from an APU fuel leak. There may be other possible sources of OMS tank detonation, but this study was only concerned with those possibilities emanating from the APU. During ascent, the high-energy detonation failure modes still apply, and other failure effects leading to loss of crew and vehicle become possible. Included were: (1) Loss of multiple hydraulic systems due to multiple APU failures. This is shown in the MLD as loss of three hydraulic systems. As a conservative groundrule, this was later changed to require loss of only two, should the failure occur prior to Main Engine Cut Off (MECO); (2) Loss of critical electronics due to APU exhaust leaks or due to a fire resulting from APU fuel leaks. Fire was later determined not to be credible during the prelaunch and ascent phases due to the prelaunch aft compartment nitrogen purge; (3) Two engines unable to throttle up after the "thrust bucket" due to APUs failing during this critical period. Ascent performance margins are also a factor here.

MLD 2 - Loss of Mission, RTLS - Phase 2

MLD #2 (Appendix B6.2-2) shows how failures of one or more APUs can lead to an RTLS abort. Two scenarios are established. The first involves loss of thrust during the initial part of ascent, within which an RTLS can be accomplished (i.e., before "Negative Return"). The operational effect of one APU shutting down during ascent is the inability to change the thrust level (i.e., throttle setting) of a main engine. Should one APU shut down during the "thrust bucket" main engine throttling, (generally 65% of full throttle), the reduction of total thrust available to the launch vehicle can lead to an RTLS abort. As was shown in MLD #1, this is also dependent upon vehicle ascent performance margins for the

particular mission involved. The second scenario involves the impending (predicted) loss of critical systems. In this case, the Mission Control Center (MCC) invokes an RTLS abort in an effort to return the vehicle to the launch area because of the impending loss of two or three hydraulic systems due to impending failures of two or three APUs. Examples of impending failures of APUs are large fuel leaks or fuel tank pressurant gas leaks.

MLD 3 - Loss of Mission, TAL - Phase 2

This MLD (Appendix B6.2-3) is similar to the RTLS MLD (MLD 2) discussed above, except that the MCC abort mode invoked is a Transatlantic Abort Landing. In the case of the "stuck throttle" scenario, this means that for one engine's thrust set to the "thrust bucket" thrust level as a result of an APU failure, vehicle performance margins for this particular mission allow a TAL to be achieved rather than an RTLS.

In the case of the impending APU failure scenario, more time is available before the two or three hydraulic systems are lost than was the case in MLD #2; i.e., the leaks are slower, allowing a TAL to be achieved rather than an RTLS abort.

The TAL abort mode is considered safer and, therefore, more desirable than the RTLS abort mode. However, because of the flight path, the time before landing is longer. The flight rules call for invoking the most desirable abort mode that the predicted time to failure will allow.

MLD 4 - Loss of Mission, AOA - Phase 2

The only viable scenario in this MLD (Appendix B6.2-4) is an Abort Once Around invoked by the MCC to return the vehicle before two or three hydraulic systems are lost. This is similar to the TAL and RTLS scenarios discussed above. However, in this case, the impending loss of the hydraulic systems allows time for a 90 minute AOA in preference to a less desirable TAL.

MLD 5 - Loss of Mission, Launch Scrub - Phase 1

This MLD (Appendix B6.2-5) displays ways that APU failures or anomalies can result in a launch scrub by violating the Space Shuttle Launch Commit Criteria (LCC). Any of the APUs can shut down, resulting in violation of the hydraulic pressure criteria

and an automatic launch scrub. An APU may also suffer a performance degradation, which violates one of the APU performance redlines and results in a manual launch scrub. Another possibility is excessive use of APU fuel due to lengthy launch holds. These launch holds could be caused by problems with APUs, or by problems with any other launch vehicle or ground launch system.

MLD 6 - Loss of Crew/Vehicle - Phase 3

Failures on orbit can lead directly to loss of crew and vehicle, or eliminate a function that is necessary for safe entry and landing. Most APU-caused failures fall into the latter category. MLD 6 (Appendix B6.2-6) shows direct loss of vehicle resulting from loss of control, or from high-energy detonations during orbit. Also shown are failures that jeopardize safe entry and landing. Included in this category is the loss of thrust necessary for the deorbit burn (branch J is shown on MLD #8) due to failures of the OMS and the Reaction Control System (RCS) backward-firing (+X) jets. The diagram postulates damage to these systems due to APU hot exhaust leaks or APU high energy release. The high energy release category includes energetic shrapnel from the APU turbine or gearbox. These apply during the Flight Control System (FCS) checkout run only. It was later determined that the gearbox is not a credible source of such high-energy shrapnel.

Other failures that affect entry and landing fall under the category of loss of control. This includes loss of OMS/RCS control and loss of aerosurface control. APU failures that can lead to these conditions include hot exhaust leaks that can damage electronics, fluid tanks or fluid lines, and APU fuel leaks which can lead to fires during entry. A fuel fire is not credible on orbit due to the lack of ambient oxygen.

The "loss of vehicle structural integrity" category postulates an explosion of an OMS or RCS fuel or oxidizer tank due to APU hot gas leaks or shrapnel.

MLD 7 - Loss of Mission - Phase 3

The Loss of Mission while on orbit can involve either a critical situation requiring entry as soon as possible, a loss of redundancy requiring entry at the next Primary Landing Site (PLS) opportunity, or a loss of instrumentation requiring a Minimum Duration Flight (MDF). As can be seen in MLD #7 (Appendix B6.2-7), various APU failures can contribute to these situations.

The impending failures that result in the need to enter as soon as possible include impending loss of all three hydraulic systems due to fuel tank leaks or fuel pressurant gas leaks. The objective in this situation is to effect a landing before the malfunctioning systems are totally lost. The same type of APU failures, if they affect only one or two hydraulic systems, will result in a decision to deorbit at the next PLS opportunity. This is to avoid a prolonged orbit stay with critical system redundancy lost.

The declaration of an MDF considered here is the result of instrumentation failures that effect insight into the status of the APUs. It does not involve direct failures of the APUs themselves.

MLD 8 - Loss of Crew/Vehicle - Phases 4 and 5

This MLD (Appendix B6.2-8) depicts how APU failures can lead to loss of crew/vehicle during the entry and post landing phases. The overall functional effects of APU failures leading to loss of crew/vehicle were determined to fit into three broad categories: (1) loss of OMS/RCS deorbit thrust; (2) loss of control; i.e., OMS/RCS control, aerosurface control, or braking/steering rollout control; and (3) loss of vehicle structural integrity.

All three categories apply to the entry phase. Loss of thrust no longer applies after the deorbit OMS burn, and loss of control no longer applies after Wheel Stop (WS). After WS only high energy detonations caused by APU-generated shrapnel, fire, or hot exhaust leaks can lead to loss of vehicle. APU failures after shutdown were not considered in this study.

The "loss of thrust" category of entry failures is identical to that discussed for MLD #6. It involves APU-caused high energy shrapnel or hot gas leaks which damage the OMS and RCS systems.

The "Loss of Control" category is also similar to that discussed under MLD #6, but with the additional possibility of APU fuel leaks causing destructive fires in the aft compartment. Other additions to this category include loss of landing gear deploy before touchdown, and loss of braking and steering before wheel stop. This is assumed to result in loss of crew and/or vehicle. The steering and braking systems depend on the Orbiter's hydraulic systems, and are thus vulnerable to APU failures. The landing gear deploy system, however, has a pyrotechnic system as a backup to the hydraulic system.

The MLD also postulates damage to the vehicle structure due to an APU fuel tank rupture, or an OMS/RCS fuel or oxidizer tank explosion caused by APU shrapnel, hot gas leaks, or fuel fires.

6.3 EVENT SEQUENCE DIAGRAMS

Event Sequence Diagrams (ESDs) illustrate sequences of events leading from initial failure categories, defined by the master logic diagrams, to damage states. They tell how an initial failure (i.e., failure mode) causes a damage state (an effect). When quantified by the use of event and fault trees, the scenarios and the events within the scenarios can be ranked with respect to their importance to a damage state such as loss of crew/vehicle.

6.3.1 Interpretation of the ESDs

The ESDs were developed representing five mission phases in four stages as follows:

a. Stage 1 represents the prelaunch and ascent phases, and includes the time from APU start at TIG-5 minutes to APU shutdown after the OMS-1 burn. The duration of this stage was taken to be approximately 18 minutes.

b. Stage 2 represents the orbit phase, and includes the time from APU shutdown on orbit to APU start, 5 minutes before the deorbit burn. The duration of this stage was assumed to be about 5 days.

c. Stage 3 represents entry, descent, and landing phases, and includes the time from APU start before the deorbit burn to wheelstop. The duration of this stage was taken to be about 50 minutes.

d. Stage 4 includes the time from wheelstop to crew egress, during about 10 minutes of which the APU continues to run.

The ESDs we developed solely from the perspective of APU performance during the mission. Interfacing systems and scenarios that couple performance margins of other systems with the APU were considered out of scope. For example, coupling the scenarios of HPU failures with APU failures was not attempted in this study.

It should be pointed out that the ESDs discussed below model the APU mission in four stages, rather than the two stages ultimately employed for the final event tree modeling. The ESD development process provided APU system insight, which allowed subsequent model simplification without significant loss of modeling accuracy.

The thought process employed in the development of the ESDs, as discussed below, is more important than the specific model stage in which the scenarios reside.

The boxes in an ESD ask questions about the occurrence (or non-occurrence) of a category of events. For example, the question in Appendix B6.3-1, "Hydraulic System OK?", may be viewed as asking a a large number of questions. Each question would refer to a component in the hydraulic system. For example, one might ask if the pump itself is OK. ESDs illustrate the overall flow of events that lead from an initial APU failure to shuttle damage states such as LOC/V and PLS entry. They are not meant to illustrate the detailed logic that is involved in determining combinations of failure modes that lead to APU failure. This is achieved in the split fraction models described in Section 6.5.

6.3.1.1 Interpretation of Initial Failure Categories

The questions relating to the initial failure categories are found in the boxes across the top of the ESD. The categories are phrased as questions such that a successful event (i.e., no initial failure) receives a "yes" answer to the question and a horizontal line is then followed to the next event. For example, the initial failure categories of equipment failure, turbine overspeed, fuel leakage, and exhaust gas leak are represented in Appendix B6.3-1 as follows:

a. No permanent APU failures? (equipment failures)
b. No recoverable APU failures? (equipment failures)
c. Turbine speed control OK? (turbine overspeed)
d. Fuel boundary remains intact? (fuel leak)
e. Exhaust gas boundary remains intact? (exhaust gas leak)

The question "hydraulic system OK?" is also asked, even though the hydraulic system is out of the scope of this PRA, to demonstrate how an ESD can diagram the interdependencies between subsystems and include sequences of events that cross subsystem boundaries.

A line pointing downward from an initial failure category that an initial failure has occurred (i.e., a "no" answer to the question).

A sequence of boxes and lines that follow the arrows from initial failure to a damage state is called a scenario. A success of the APU occurs when, according to the principles of scenario structuring described in Section 5, all the answers to the questions across the top (see Appendix B6.3-1) are "yes". Since the boxes across the top represent a complete set of initiating failure categories, then in the absence of initiating failures the APU must have operated successfully. Any scenario that has a vertical (down) line must, therefore, be less than completely successful. The actual "damage" of the scenario depends on the number and type of subsequent failures and the timing of these failures. The ESD explicitly shows cascading failures associated with spatial interactions as well as functional dependencies and independent failures.

6.3.1.2 Diagramming Dependencies in an ESD

An example of a functional dependency is shown in the sequence initiated by a failure of the hydraulic system. The failure mode is one that causes a hydraulic pump seizure before an underspeed shutdown can occur. This situation could potentially be caused by a sudden large rupture of a hydraulic fluid line. Should a seizure of the hydraulic pump occur, the kinetic energy of the system could possibly cause a rupture of the APU turbine rotor. This is represented by the question "APU turbine intact?" in Appendix B6.3-1. Thus the APU turbine functionally depends on avoidance of catastophic hydraulic pump seizure. Of course a more obvious functional dependency is that hydraulic system pump operation depends on APU operation.

An example of a scenario that includes cascading damage is shown if the APU turbine is not intact. A negative answer to the question "APU turbine intact?" means that the turbine rotor has come apart and the pieces have not been contained within the turbine housing. In that situation, the APU has failed and hydrazine has escaped into the aft compartment. The questions then concern whether the leak was isolated (say by secondary valve or isolation valve closure), whether there is sufficient oxygen in the aft compartment to support combustion, and whether the other conditions necessary for a fire are present.

If a fire cannot occur, the ESD recognizes that damage in the aft compartment may be caused by shrapnel from the turbine. Other causes of damage in the aft compartment may be from detonation of an APU resulting from the heating effects of the decomposition reaction of hydrazine with materials that act as a catalyst,

hydrazine reaction with electrical insulation causing open circuits or hot shorts in "flight critical equipment", and even effects of impingement of hot gas from exhaust duct leakage on flight critical equipment or APU circuitry. The term "flight critical equipment" is defined for this study to be any component or groups of components that are not part of the APU or HPU and whose failure directly causes a LOC/V in conjunction with failures in the scenario. If a fire can occur, then it is also recognized as a phenomenon that could cause the failure of other equipment in the aft compartment. More detailed discussions of phenomena relating to cascading damage are provided in Section 6.6.

6.3.1.3 Modeling Spatial Interaction Events in an ESD

Spatial interaction events (SIE) denote potential failures of equipment by virtue of their spatial proximity to phenomena such as fires, shrapnel, and hydrazine reactions that tend to cause cascading damage.

The spatial interaction phenomena considered in this study are as follows:

a. Hydrazine reaction with materials in the aft compartment causing deterioration of either wire insulation or other material in the aft compartment following hydrazine leakage.

b. Exothermic hydrazine decomposition reaction in an oxygen poor environment following hydrazine leakage.

c. Fire in the aft compartment caused by hydrazine combustion following hydrazine leakage.

d. Shrapnel caused by turbine rotor failure at either normal speed or turbine runaway conditions.

e. Detonations caused by compression of hydrazine bubbles, leakage into solenoid cavities of the fuel isolation or control valves, hydrazine overheating from fires, stuck-on heaters, or hydrazine decomposition reactions, hot restarts without gas generator cooling, and APU starts with gas generator catalyst bed temperature or pressure too low.

(f) Leakage of hot gas into the aft compartment caused by exhaust duct failure.

The ESD also recognizes that certain failures may cascade and cause other failures. For example, shrapnel generation and detonations will often cause hydrazine leakage into the aft compartment which, in turn, could result in either a fire or decomposition reaction which, in turn, could cause another detonation, etc. A more detailed discussion of the damage potential of these events is found in Section 6.6.

Below the SIE in Appendix B6.3-1 is a triangle with a Greek or English character printed within. This denotes a transfer to another place in the ESD that has another triangle with the same character within. The ESD for spatial interaction events is found on page 2 of Appendix B6.3-1. This diagram asks questions concerning the number of APUs that have failed and whether flight critical equipment has failed as a result of the phenomena contributing to spatial interactions.

Page 2 of Appendix B6.3-1 first asks if spatial interaction has failed flight critical equipment. Then it asks if two APUs have failed as a result of the initial failure and the spatial interaction. The model assumes a LOC/V if either occurs. Finally, the ESD asks if two, one or no APUs have failed as a result of the initial failure, spatial interaction, and potential independent failure of another APU.

6.3.1.4 Permanent/Recoverable Failures: Interpreting the Flight Rules

Page 2 of Appendix B6.3-1 indicates that the damage state LOC/V would occur if two APUs failed during ascent. Flight rules require that certain APU malfunctions would cause the Mission Control Center (MCC) to declare an APU to be lost for the remainder of the mission, unless it was needed to provide a second APU for landing. These malfunctions are called "recoverable failures" (RF) to distinguish them from equipment failures that inherently incapacitate the APU in such a way that it cannot be recovered during the mission. The latter failures are called "permanent failures" (PF).

A fundamental groundrule for this study was that permanent failures of two APUs any time during the mission except after wheelstop would be considered a LOC/V.

The examples given so far show how an ESD diagrams functional dependencies, cascading damage, and spatial interactions. Independent failures are diagrammed in a similar manner. Although the combination of two or more failures occurring independently is probably of lower frequency than dependent failures, the ESD recognizes their potential. The PRA assesses the frequency of the scenarios by the use of event trees, split fraction models and failure history data later in the study.

Suppose, for example, that an APU is declared lost by flight rules because of a spurious shutdown. That same APU could also be leaking hydrazine. Appendix B6.3-1 represents a declared lost APU by a vertical line under the box with the question: "no recoverable APU failures?". The "L" transfer then leads to the next question, which is about whether the hydrazine fuel boundary remains intact. A leakage in this scenario (one that follows a spurious shutdown but with no other failures) would be a second failure of the APU, occurring independently; that is, not caused by or related to the spurious shutdown.

All scenarios in the APU ESDs ask if hydrazine leakage, or exhaust gas leakage, or both can occur. This recognizes that virtually any APU malfunction or failure can also be accompanied by the initial failure categories of hydrazine and exhaust gas leakage.

The ESDs account for the three APUs in the orbiter and they diagram scenarios in which failures can occur in more than one APU during the same mission. The shadow boxes of the initial failure categories across the top of Appendix B6.3-1 are the diagrammatic devices used to illustrate this. The diagram is read left to right for each APU.

In summary, ESDs are capable of illustrating scenarios that include failures, malfunctions, flight rule considerations, multiple sub-systems, dependent events, cascading damage, spatial interactions, human actions, and damage states for each stage of the mission. The remainder of Section 6.3 describes the events found in the APU ESDs for Stage 1, Stage 2, Stage 3, and Stage 4. Since, as discussed above, hydraulic system failures were included for illustrative purposes only, the following discussion will not include hydraulic system-initiated scenarios.

6.3.2 Stage 1: Prelaunch and Ascent (Mission Phases 1 and 2)

The ESD in Appendix B6.3-1 covers the mission between 5 minutes before liftoff when the APU starts prelaunch, and when the APU shuts down following the OMS-1 orbital insertion burn.

6.3.2.1 Scenarios Initiated by Permanent APU Failures

This initiating failure category includes a number of failures of APU equipment that are not recoverable during the mission. These would include, for example, failure to start the APU, failures of pump, valves, turbine, and gearbox to continue running, lube oil system plugging, fuel line plugging, and underspeed shutdown. It would also include failure to successfully shut down an APU after MECO. A complete description of all initiating failures included in the model of this category is presented in Section 6.5.2. This category does not include hydrazine leakages to the aft compartment or into valve solenoid cavities. It does not include turbine runaway events and events that would cause MCC to declare an APU lost when it is still potentially operable.

Two specific pieces of equipment, the gearbox and the turbine, have been singled out for additional attention in the diagram because certain failure modes of these components could potentially lead to spatial interaction events. The following describes the scenarios in Appendix B6.3-5 that are beneath the box with the question: "No permanent failures?".

The next event beneath this category asks if the gearbox is OK. This event includes all failure modes of the gearbox. A negative answer to this question could mean that the gearbox has failed in a way that could cause rapid seizure of the turbine shaft. Therefore, the question: "APU turbine remains intact?" is asked. A negative answer means that the gearbox failure may (or may not) have caused an energetic failure of the turbine rotor with subsequent escape of the pieces from the APU housing. If the gearbox is OK, then the ESD asks about independent turbine failure at normal turbine speed. If the APU turbine remains intact, then the diagram shows that a permanent failure (PF) has occurred and transfers to questions about leakage.

If the turbine does not remain intact, the same questions related to cascading failure phenomena and spatial interaction events as those described in Sections 6.3.1.2 and 6.3.1.3 become relevant in order to describe the various sequences of events that could arise from turbine failure. Tracing through the ESD from page 1 of Appendix B6.3-1 to page 2 of that figure and B6.3-2, the diagram recognizes that, indeed, further damage might not occur to other APUs and flight critical equipment, leaving only the initial failure of an APU. It is also recognized that subsequent failures occurring as a consequence of shrapnel or leaking hydrazine could lead to a LOC/V.

6.3.2.2 Scenarios Initiated by Recoverable APU Failures

This initiating failure category includes those APU malfunctions that are included in the flight rules as reasons for MCC to declare an APU lost, but also leaves the APU potentially operable should a second APU be required for landing. This category excludes hydrazine leakages; those have been assigned their own initial failure category. The recoverable failure category includes the following malfunctions:

a. Underspeed or overspeed shutdowns that can be unambiguously identified as spurious. That is, they are caused by electrical or instrument malfunction that causes the APU controller to close the secondary control valve in an otherwise successfully operating APU.

b. Gas generator bed temperature cannot be maintained above 70°F for an APU start.

c. The lube oil outlet pressure is greater than 150 psia during APU operation.

d. The pressure drop between the gearbox and the lube oil outlet is less than 20 psi during APU operation.

e. The lube oil outlet temperature is greater than 375°F or the gearbox bearing temperature is greater than 400°F.

f. Turbine speed cannot be maintained between 95% and 121% while running.

g. Gearbox pressure is less than 2 psia before APU start.

None of these malfunctions have been singled out as a credible precursor to spatial interaction events; therefore, the ESD transfers to questions about leakage.

6.3.2.3 Scenarios Initiated by Turbine Speed Control Failure Category

This initial failure category includes all failures that cause an overspeed of the APU turbine. The combinations of control valve, controller, electric power and other failures contributing to turbine overspeed are in the split fraction models described in Section 6.5.2.1.

In general, it appears that both the primary and secondary control valves must fail in the open position to cause an overspeed. Closure of the isolation valves is not sufficient to prevent an overspeed because enough hydrazine is present downstream of these valves to continue powering the turbine. It also appears that a single failure of the secondary valve stuck in mid position will not cause an overspeed because most of the fuel is directed back to the pump inlet. It was determined that a failure of the primary valve seat such that the seat dislodges and keeps the secondary valve from closing is first, highly unlikely, and second, more likely to block the flow path than to cause an underspeed shutdown than to cause an overspeed. Therefore, this event was included in the assessment of fuel line plugging as part of the permanent failure category.

Should an overspeed condition occur, then an APU overspeed trip can prevent catastrophic turbine runaway. This is questioned in the box "overspeed trip avoids runaway?". If the answer is positive, then the ESD asks about fuel leakages that are independent of the overspeed event. If overspeed trip is not successful, then the turbine speed would be expected to reach over 136,000 rpm in about 200 milliseconds. At this speed, the APU turbine is unlikely to remain intact. The expected event is that the turbine rotor would come apart in a small number (e.g., three) of pieces and the pieces would not be contained by the containment ring, nor by the turbine housing itself. Shrapnel would enter the aft compartment accompanied by hydrazine which would escape the APU through the holes created by the pieces of turbine rotor. The shrapnel tends to spray in a pattern that subtends a 30° arc centered on the turbine wheel plane of rotation.

Some of the shrapnel could be energetic enough to puncture the large cryogenic liquid oxygen and liquid hydrogen lines that are within the spray pattern of the turbine shrapnel. If the outer shell and inner lining of these fuel lines are punctured, the results expected are overpressurization of the aft compartment because of the vaporization process or the explosive chemical reaction of oxygen and hydrogen causing a loss of structural integrity to the vehicle. Shrapnel could also be sufficiently energetic to damage flight critical electrical/ electronic equipment in the aft compartment, other compartment-mounted equipment, as well as the APU fuel tanks. Shrapnel penetration of the OMS deck is also possible.

Hydrazine leakage would not be expected to cause a fire in the aft compartment during ascent because the compartment is purged with nitrogen and low atmospheric oxygen conditions are quickly attained as the shuttle gains altitude. However, hydrazine is capable of a chemical reaction that tends to strip Kapton electrical insulation from wires. The potential for LOC/V dramatically increases if a hydrazine fuel tank is punctured or the leak in the failed APU cannot be isolated. These potential scenarios have been summarized on the ESD at the bottom of Appendices B6.3-1 and B6.3-2, and described in Sections 6.3.1.2 and 6.3.1.3 above. More detailed discussion about individual phenomena is presented in Section 6.6.

6.3.2.4 Scenarios Initiated by Hydrazine Leakage

This initial failure category includes hydrazine leakage from any part of the APU into the aft compartment, into the fuel pump seal drain line, and into the isolation valve or control valve solenoid cavities. The situation in which hydrazine contaminates and causes blockage of lube oil is included within the permanent failure category. Scenarios resulting from hydrazine leakage follow a negative answer to the question: "Fuel boundary remains intact?". They are summarized on page 3 of Appendix B6.3-1 and described below.

If the leaking APU has not itself failed; i.e., a negative response to the question "Leaking APU failed from other cause?", the ESD asks if any other APU has failed. It does this because flight rules indicate that different responses are required if an APU has already failed. If no other APU has failed (the expected situation), then the question "Leak detected and APU shutdown before fuel quantity and tank pressure depleted?" is asked. Negative answers to this question include the following scenarios:

a. Leak is not detected and APU fuel quantity is depleted or tank pressure drops below 70 psi before APU is shut down. This represents a permanent failure of an APU and would probably release a great deal of hydrazine into the aft compartment.

b. Leak is detected but the leak is so large that the fuel quantity is depleted or tank pressure drops below 70 psi before MECO (flight rules do not allow an APU to be shut down before MECO for a fuel leak). This represents a permanent failure of an APU and would probably also release a great deal of hydrazine into the aft compartment.

c. Hydrazine leaks into one of the valve solenoid cavities, decomposes, causes a pressure increase inside the valve and eventually ruptures the valve. If this occurs in an isolation valve, the entire contents of the fuel tank could be dumped into the aft compartment. This would certainly be a permanent failure of an APU with a substantial chance of damaging flight critical equipment or a second APU. If the rupture occurs in one of the control valves, then the APU would be failed, but the amount of hydrazine released into the aft compartment would be limited unless an isolation valve also failed to close. An underspeed shutdown of the APU would command the isolation valves to close.

Positive answers to the question; "Leak detected and APU shutdown before fuel quantity and tank pressure quantity and tank pressure depleted?" include the following scenario: The leak is detected and the APU is shutdown post-MECO with sufficient fuel and tank pressure to complete the mission. In this situation, the ESD asks if the leak is successfully isolated. This question refers to two situations. A leak downstream of the isolation valves will be isolated only if both isolation valves close. A leak upstream of the isolation valves cannot be isolated. An isolated leak is treated as a recoverable failure (RF). A leak that cannot be isolated is a permanent failure. If no other APU has failed, then flight rules require that the APU be restarted and run to fuel depletion. If another APU has failed, then this requirement is waived so that the leaking APU may be available for landing.

If the answer to the question: "Other APU already failed?" is affirmative, then there are fewer options and fewer scenarios than discussed above. In this situation, there is one APU failed and one leaking. Flight rules direct either a landing at the next PLS opportunity, if the leaking APU can support the required run time, or an intact abort if the leaking APU can support only a limited duration of flight. If the answer to the question: "Remaining fuel quantity sufficient to support landing?" is negative, then a LOC/V would result.

If the answer to the question: "Leaking APU failed from other cause?" is affirmative, then only questions concerning the potential of spatial interactions need to be asked because the leaking APU has failed.

All leak scenarios shown on page 3 in Appendix B6.3-1 lead to questions about the potential for fire. These questions are asked to complete the qualitative development of scenarios even though

their likelihood of occurrence is negligible during ascent owing to nitrogen purging of the aft compartment. After the questions concerning fire, the ESD asks questions about the spatial interaction events that were described in Sections 6.3.1.2 and 6.3.1.3 above.

6.3.2.5 Scenarios Initiated by Exhaust Gas Leakage

This category includes failures in the exhaust gas duct or turbine housing that allow hot gas to flow into the aft compartment.

Damage to APUs and flight critical equipment may be caused in two ways. First, hot gas impingement on electronic equipment may cause component failures. Second, a very large leak could potentially overpressurize the aft compartment and lead to sidewall or bulkhead failure or hydrogen detonation. Section 6.6 discusses these phenomena in more detail.

Since exhaust gas leakage itself does not inherently cause failure of an APU, the ESD models all potential scenarios from this initial failure category as spatial interaction events on page 2 of Appendix B6.3-1. These have been described in Section 6.3.1.3.

6.3.2.6 Defining the Damage States for Prelaunch and Ascent

Page 4 of Appendix B6.3-1 is reached after scenarios for all three APUs have been checked. This is indicated by the transfer triangle the letters AD within. The objective of this part of the ESD is to determine the appropriate damage state that should be assigned to the previous sequences of events covering the three APUs. If any failures occur or any redlines are violated before launch, then the scenario would be associated with a launch scrub. If an APU fails after launch (a yes answer to "Has liftoff occurred?"), then questions regarding the time or altitude become relevant for determining the damage state. If a failure occurs any time during ascent except in the "thrust bucket", the appropriate action is for the shuttle to continue to orbit, deploy any deployable payloads, and enter at the next primary landing site opportunity. This is termed "PLS" in the ESD. An APU failure in the thrust bucket has been assumed to result in an intact abort.

Sequences of events that lead to one APU failed and one impending APU failure (e.g. leaking hydrazine into the aft compartment), are assumed to lead to a PLS if the impending failure is not

projected to occur before wheelstop. If, in the estimation of MCC, the impending failure will not support a PLS, then an intact abort is the assumed damage state. These assumptions are consistent with the stated mission flight rules. The type of abort called by the MCC depends on the altitude and flight performance margins at that point in the mission. The possible options are abort to orbit, abort once around, return to launch site, or transatlantic abort landing. Of course, an impending failure that will not support either a PLS or an intact abort is actually a permanent failure and, when coupled with another failure, is assumed to lead to a LOC/V. A spurious shutdown of an APU before MECO was assumed to have the same effect as a permanent failure when determining damage states. If no APU failures occur but instrumentation supporting APU telemetry has failed, then the flight rules direct the MCC to declare a minimum duration flight. The success or failure of such instrumentation was beyond the scope of this study's quantitative assessment.

6.3.3 Stage 2: Orbit (Mission Phase 3)

The ESD presented in Appendix B6.3-2 describes APU related scenarios on orbit in terms of three time intervals:

a. After APU shutdown and before FCS checkout page 1 of Appendix B6.3-2. The APU is not operating but must perform heating and cooling functions, and maintain system integrity.

b. During FCS checkout (page 2 of Appendix B6.3-2), one APU is run for about 3 to 10 minutes in order to provide power to check out the hydraulically-actuated aerosurfaces in preparation for entry.

c. After FCS checkout (page 4 of Appendix B6.3-2), the APU is not operating but must perform heating and cooling functions and maintain system integrity.

6.3.3.1 Scenarios Initiated by Failure of a Fuel Isolation Valve to De-energize

Should a fuel isolation valve fail to de-energize after APU shutdown, the crew follows Flight Rule 10-11C. If power is not removed from the valve solenoid within about 20 minutes, a local detonation of stagnant hydrazine may occur due to overheating. The crew restarts the APU and attempts two underspeed shutdowns

to close the valves. If the valves do not de-energize after the second attempted underspeed shutdown, the APU is allowed to continue running until fuel depletion.

The ESD models this situation by first asking: "Hot restart without detonation?". A negative response to this question indicates that either the hot restart was not attempted soon enough or a hot restart led to a detonation. The latter can occur if the injector cooling system failed to adequately cool the gas generator injector nozzle so that hydrazine detonated upon contact with the hot injector. In this situation, the ESD recognizes the potential spatial interaction events caused by the hydrazine decompostion in the aft compartment and shrapnel from the detonation. These spatial interaction events are shown on page 6 of Appendix B6.3-2, and are same as those in Appendix B6.3-1 except that the potential for fire is not shown for orbit.

A successful hot restart without detonation leads to the question: "Underspeed shutdown closes valves?". A positive answer means that the APU is OK and the ESD then asks about the next potential initial failure. A negative answer leads to a series of questions concerning possible failures of the APU while it is running to fuel depletion. A running APU does not allow local hydrazine heatup because of the heat transport afforded by flowing hydrazine. However, any running APU is always subject to the same initial failure categories. Therefore, the initial failure mode found on page 1 of Appendix B6.3-2 that follows "Run APU to fuel depletion" is similar to that of ascent shown on page 1 of Appendix B6.3-1. Should the APU shutdown at any time before fuel is depleted, a detonation is assumed to have occurred and the spatial interaction questions are asked. A detonation was not assumed for hydrazine or exhaust gas leakages.

6.3.3.2 Scenarios Initiated by Hydrazine Overheating After Shutdown

Heat from the hot portions of the APU; (e.g., the injector, gas generator, or turbine) tends to flow toward the fuel pump and gas generator valves via thermal conduction because convective heat transfer does not occur on orbit in the aft compartment and heat transfer away from the APU by radiation is a slow process. The stagnant hydrazine in the fuel pump or GGVM may rise to above the decomposition temperature, resulting in the formation of bubbles. The fuel pump/GGVM cooling system was designed to maintain temperatures in these parts of the APU below 200°F. Tests show that this temperature is reached about 30 minutes after APU shutdown in orbit.

The question: "Hydrazine does not overheat after shutdown?" is answered affirmatively if the fuel pump/GGVM cooling system operates successfully. In that case, the ESD leads to questions about other initial failure categories. If cooling fails, then the question: "Overheating does not cause detonation?" is asked. An affirmative answer means that detonation has not occurred and the failure is considered recoverable.

There is a possibility of detonation if the APU is started while hydrazine temperatures are above 200°. If the hydrazine is allowed to cool to below 200°F before start, no detonations are expected.

An APU with a failed fuel pump/GGVM cooling system is considered recoverable if needed during entry, descent and landing.

If the answer to the question: "Overheating does not cause detonation" is negative, then the spatial interaction questions are asked with consideration to detonation, shrapnel, hydrazine decomposition, and chemical attack.

6.3.3.3 Scenarios Initiated by Overcooling After Shutdown

Heating of the APU fuel lines, water lines, lube oil lines and gas generator are provided during orbit to maintain hydrazine, oil, and water above minimum acceptable levels. Gas Generator heating is required to assure an acceptable temperature for APU startup. Failure to maintain water temperature in the fuel pump/GGVM cooling system above freezing is considered to be a failure mode of the GGVM and fuel pump cooling system and is included in the failures discussed in the previous section. Flight rules call for the APU to be considered lost under the following conditions:

a. Fuel tank or fuel line temperature less than or equal to 35°F
b. Fuel pump temperature less than or equal to 35°F
c. Lube oil temperature less than or equal to 0°F
d. GGVM temperature less than or equal to 35°F

Hydrazine freezes at 35°F. If a portion of the APU has frozen, and subsequently heats up, local uneven thawing could cause a line rupture (hydrazine expands when thawing). Lube oil loses its fluidity at 0°F and an APU start at low temperatures could cause gear bearings to overheat. However, these failures are believed to be recoverable if a second APU is absolutely needed to avoid landing with a single APU. They are not considered to be causes of spatial interaction events.

6.3.3.4 Scenarios Initiated by Hydrazine Leakage Before FCS Checkout

Fire scenarios are not relevant for hydrazine leakage on orbit. The other hydrazine related phenomena discussed in Sections 6.3.1.2, 6.3.1.3, 6.3.2.4, and 6.6 are relevant to orbit. Unlike ascent, however, an APU with an isolatable leak could be restarted and run to fuel depletion if no other APUs have failed.

If leakage occurred and was detected before APU shutdown during ascent, then the ability to isolate the leak is assessed soon after APU shutdown. If the leak can be isolated, and sufficient fuel and tank pressure remain to complete a landing, then the APU is considered recoverable. Otherwise, the APU is considered permanently failed. In either case, the APU is considered lost and the flight rules require a landing at the next PLS opportunity. Spatial Interaction event questions are asked to complete the scenario.

If the leak is not isolatable, then the question; "APU fuel quantity and tank pressure can support start and landing?" is asked. A landing at the next PLS opportunity is required by flight rules. If the fuel is insufficient and this is the first APU to exhibit a permanent or recoverable failure, the APU will be started, and run to fuel depletion. If another APU has already been lost, then the ESD leads to the spatial interaction questions on page 6 of Appendix B6.3-2. If the fuel is sufficient and another APU has been declared lost, the APU will not be restarted, but thermal conditioning in preparation to support entry and landing will occur. Spatial interaction questions are asked following all unisolatable leaks.

Unisolatable APU leakage occurring after APU shutdown while in orbit is described in the ESD, with the same scenarios as described above for unisolatable leaks occurring before APU shutdown. After APU shutdown, leaks that occur downstream of the isolation valves would release only a limited amount of hydrazine. In fact, the leak may even seal itself until entry. Scenarios initiated by these isolatable leaks are treated in the Stage 3 ESD.

An APU with unisolatable leaks, and that cannot support landing is restarted and run to fuel depletion if no other APU has been declared lost. This may involve a hot restart so the question "hot restart without detonation?" is asked at the bottom of page 1 of Appendix B6.3-2. This question involves failure of the injector cooling system. Failures of an APU that would cause a spurious

start of the APU while the injectors are still hot are also included in this question and in the subsequent questions on pages 5 and 6 of Appendix B6.3-2.

The sequences of events related to failures during APU operation while running to fuel depletion are presented on page 5 of Appendix B6.3-2. They are similar to the Stage 1 sequences with the following exceptions:

a. Recoverable failures are irrelevant.

b. All sequences lead to questions concerning spatial interactions. The outcome of spatial interaction questions is either LOC/V or one APU permanently failed.

c. Questions about fires are not asked, but the potential for hydrazine to remain frozen in the aft compartment and either combust or decompose to cause further damage during descent is recognized.

6.3.3.5 Scenarios During FCS Checkout

FCS checkout is performed if no APU has failed or been declared lost up to that time in the mission. Page 2 of Appendix B6.3-2 shows the scenarios related to FCS checkout. Shadow boxes are not shown because only one APU is used for FCS checkout.

If the running APU fails, then the ESD questions whether it also exhibits a leak. An isolated leak would release a limited amount of hydrazine into the aft compartment. An unisolated leak would be a much larger threat to flight critical equipment or a second APU during descent.

If the running APU exhibits a recoverable failure or does not fail at all, then the ESD asks: "fuel boundary remains intact?". Page 3 of Appendix B6.3-2 shows the leakage scenarios. If the leak is severe enough that fuel quantity or tank pressure can no longer support a start and landing, then the APU is considered permanently failed and the ESD refers to possible subsequent failures associated with spatial interactions. If the leak is small enough that fuel quantity and tank pressure remain sufficient after APU shutdown and the leak is isolated, then the failure is recoverable and spatial interaction questions are asked. If the leak is not isolated, the APU is restarted and run to fuel depletion. Questions about hot restart without detonation and subsequent potential spatial interactions are then asked.

6.3.3.6 Scenarios Following FCS Checkout

The APU used for FCS checkout must successfully shut down, cool down, and maintain fluid system temperatures above minimums. The other APUs must continue to maintain temperatures above minimums before and during FCS checkout. Scenarios associated with these functions are shown on page 4 of Appendix B6.3-2, and are essentially identical to those shown on page 1 of that ESD.

6.3.3.7 Defining Damage States for Orbit

A negative response to the question on page 1 of Appendix B6.3-2, "no APUs failed or declared lost by mission rules?" indicates that FCS checkout will not be performed and the portion of the ESD labeled "deorbit discriminator" is entered. The deorbit discriminator is also entered from page 4 of Appendix B6.3-2 after scenarios that deal with the post-FCS checkout time interval. The deorbit discriminator is found on page 7 of Appendix B6.3-2, and defines the damage states for each scenario in Stage 2. If one APU is lost either permanently or by flight rules, a landing at the next PLS opportunity is assumed. If two APUs are permanently failed, a LOC/V is assumed. If all APUs are OK, but the MCC loses the ability to monitor APU status more than 72 hours prior to deorbit, then a minimum duration flight is declared. If loss of ability to monitor APU status occurs within 72 hours of orbit, the mission proceeds normally. Otherwise, all three APUs are considered OK to support entry.

6.3.4 Stage 3: Entry, Descent, Landing to Wheelstop (Mission Phase 4)

Appendix B6.3-3 describes scenarios associated with the time interval from APU start at deorbit TIG-5 minutes to wheelstop.

The scenarios are presented in terms of failures to start the APUs after orbit (page 1 of Appendix B6.3-3) and failures during APU operation (pages 2 through 5 of Appendix B6.3-3).

6.3.4.1 Scenarios Involving Readiness of APUs to Start

These scenarios arise largely from flight rules 10-23, 10-24, and 10-28, and from the Entry Checklist (JSC-18540). Normally, one APU will be started at deorbit TIG-5 and the remaining two at 13 minutes before Entry Interface (EI-13). Flight rules,

however, provide for different start times for various APU failures. These are summarized as notes 1, 2, and 3 on page 1 of Appendix B6.3-3. The following discussion applies to page 1 of Appendix B6.3-3. An affirmative answer to the question; "2 or 3 APUs ready for start?" means that the flight rule-enforced delays apply to no more than one APU. The ESD then asks if the first attempted start of an APU at TIG-5 is successful. If it is, then the ESD asks if at least one other is ready to start at EI-13. The start failures at EI-13 are modeled as part of the questions on pages 2 and 3 of the ESD.

A negative answer to the question "2 or 3 APUs ready for start?" implies that either all APUs are delayed due to flight rules or two APUs are delayed. A delay of all APUs is indicated by a negative answer to the question; "1 APU ready for start?". In this situation, the ESD asks if APUs are ready to start at EI-13. It is assumed that at least two APUs would be started before TAEM to support landing. A positive answer to the question "1 APU ready for start?" is followed by a question about whether the APU is successfully started using all available start techniques.

An affirmative answer to the question; "2 or 3 APUs ready for start?" is followed by the question of whether the first APU to attempt start does so successfully. If the APU starts, then the other two start attempts are made at EI-13. If the first APU to attempt starting fails, then the ESD asks if the second APU to attempt start does so successfully. If this one also fails to start, then alternate start techniques are employed in an attempt to provide at least one operable APU before the deorbit burn. If both APUs still do not start, the ESD points out that flight rules recommend a one orbit delay to decide on a work-around. Flight rules do not provide guidance on the course of action to be taken if a one orbit delay fails to provide a work-around. Therefore, the ESD conservatively assumes that a LOC/V would result if a work-around cannot be found for at least one APU. If one APU is successfully started and one has failed, the ESD recognizes that the running APU would operate with a depressurized hydraulic system until EI-13.

This diagram and the accompanying notes 1,2, and 3 model the number of APUs that have successfully started at TIG-5 and the number to be started at EI-13 or Terminal Area Energy Management (TAEM). The start and run failure-initiated scenarios are presented on pages 2 through 5 of Appendix B6.3-3 and described below.

6.3.4.2 Start and Run Failure Scenarios

The initial failure categories for Stage 3 are identical to those of Stage 1. With the exception of the hydrazine leakage initial failure category, the subsequent scenarios are also essentially identical. These have been described in Sections 6.3.2.1, 6.3.2.2, 6.3.2.3, and 6.3.2.5. The scenarios during this stage are influenced, however, by flight rules that do not apply to ascent or orbit. For example, if one APU has failed before or fails during descent, the remaining two APUs will operate at high speed starting at TAEM and automatic shutdown will be inhibited during the remainder of descent and landing. Furthermore, hot restarts will be attempted during descent to assure two APUs operating before TAEM. This consideration is shown on page 2 of Appendix B6.3-3. Should the answer to the question "2 or more APUs operate OK?" be negative, then the questions: "start recoverable APU before TAEM ?" and "recovered APU runs OK?" are asked. A negative response to either question would result in a LOC/V according to the groundrules of this study.

Hydrazine leakage scenarios are described below and are presented on page 3 of Appendix B6.3-3.

6.3.4.3 Hydrazine Leakage Scenarios in Stage 3

This initial failure category includes hydrazine leakage from any part of the APU into the aft compartment, the fuel pump seal drain line, and the isolation valve or control valve solenoid cavities. The situation in which hydrazine contaminates and causes blockage of lube oil flow is included within the permanent failure category. The scenarios also include the situation in which a leak may have developed on orbit but is not detected until entry. Such situations are modeled as a leak that is detected before blackout. Scenarios resulting from hydrazine leakage follow a negative answer to the question; "fuel boundary remains intact?".

Many leakage locations allow hydrazine to be released into the aft compartment during entry. The potential for fire as the shuttle descends becomes quite an important consideration for determining the consequences of hydrazine leakage. Furthermore, certain materials in the aft compartment such as Kapton electrical wire insulation are vulnerable to chemical attack by hydrazine.

If the leaking APU has not itself failed; i.e., a negative response to the question "leaking APU failed from other cause?", the ESD asks if the leak was detected before blackout. If so, and

there are no previous APU failures, then the flight rules indicate that the APU would be shut down. If the leak is isolated and the remaining fuel quantity and tank pressure are sufficient to support landing, then the APU is potentially recoverable at TAEM. Recovery would be attempted, however, only if a second APU is needed for landing.

A negative response to the question "fuel quantity and tank pressure sufficient to support landing?", includes the following situations:

a. A severe leak such that insufficient fuel remains to support landing.

b. Hydrazine leaks into one of the solenoid cavities, decomposes, causes a pressure increase inside the valve, and eventually ruptures the valve. If this occurs in an isolation valve, the entire contents of the fuel tank could be dumped into the compartment. This would certainly be a permanent failure of an APU, with a substantial chance of damaging flight critical equipment or a second APU. If the rupture occurs in one of the control valves, then the APU would be failed, but the amount of hydrazine released would be limited unless an isolation valve also failed to close. An underspeed shutdown of the APU would command the isolation valves to close.

If a leak is not isolated by shutting down the APU and the remaining fuel quantity and tank pressure are judged by MCC to be insufficient to support landing, then the APU would be hot restarted and run to fuel depletion. The potential for detonation exists if the injector cooling fails or a spurious APU start occurs without sufficient injector cooling. If the APU cannot be restarted, it is considered to be permanently failed. Running an APU with an unisolatable leak to fuel depletion limits the amount of hydrazine available to cause damage in the aft compartment. Therefore, the inability to do this results in a higher potential for loss of a second APU or flight critical equipment.

An APU with an unisolatable leak that is judged able to support landing is not required to be restarted. Since it appears that relatively small leaks can allow enough hydrazine accumulation in the aft compartment to cause a damaging fire, this course of action increases the chance of loss of flight critical equipment or additional APUs. Flight rules indicate that any time an

unisolatable leak causes the tank pressure to reach the minimum start pressure (100 psia), the APU is to be started so that it is available to support landing.

The ESD shows different scenarios for the situation in which a leak is detected before blackout but an APU has previously failed or been declared lost. The leaking APU would not be shut down. The rationale given in the flight rules is to avoid risking a start failure and, thereby, having to land with a single APU. Even though the chance of fire might be greater than if the APU is shut down, the flight rules indicate that this is preferable to the chance of failing to start the leaking APU and attempting a landing with only one operating APU. The results of this study (see Section 8) suggest that the conditional probability of a fire that damages a second APU or flight critical equipment, given a leak, is far greater than the probability of failing to start an APU. Therefore, this flight rule may, in fact, increase the risk of LOC/V in the situation of one APU lost and one leaking.

Leaks that occur at lower altitudes and after blackout are treated differently by flight rules than those that occur before blackout. Leaks from the seal cavity with no previous APU failures require that the leaking APU be shut down. If an APU has previously failed, then the leaking APU would not be shut down. Leaks into the aft compartment do not require the APU to be shut down. If the answer to the question "leaking APU failed from other cause?" is affirmative, then only questions concerning the potential of fire and other spatial interactions need to be asked.

All leak scenarios shown on page 3 of Appendix B6.3-3 lead to questions about the potential for fire in the aft compartment. After the questions concerning fire, the ESD asks questions about the spatial interactive events. These are shown on page 4 of Appendix B6.3-3 and are identical to the questions asked on page 2 of Appendix B6.3-1 and described in Sections 6.3.1.2 and 6.3.1.3.

6.3.4.4 Defining Damage States for Stage 3

The damage states relevant for Stage 3 are LOC/V and OK. A scenario's damage state depends on the number of APUs failed and the timing of those failures. Page 5 of Appendix B6.3-3 diagrams the logic used to define the damage states.

Two APUs lost before touchdown is considered by the model to result in a LOC/V. If only APU number 1 is lost, then nosewheel

steering is lost, but the crew can successfully steer by differential braking. If no more than one APU is lost, the model results in a successful mission.

If APU number 3 and APU number 1 are lost or if APU number 3 and APU number 2 are lost before wheelstop, the model assumes a successful mission with one half normal braking power. If all three APUs are lost before wheelstop but after touchdown, the model assumes a LOC/V caused by inability to brake and steer.

6.3.5 Stage 4: Wheelstop to Crew Egress (Mission Phase 5)

The APU normally runs for a short time (approximately 10 to 20 minutes) after wheelstop. However, if an APU is leaking the APUs are shutdown as soon as possible after wheelstop. The crew remains with the vehicle for up to about 40 minutes after APU shutdown. Appendix B6.3-4 shows the ESD for this stage. Only those scenarios that can cause a catastrophic event such that the Orbiter explodes or is consumed by fire are of concern in this stage. Failures of APUs cannot cause loss of crew or vehicle, unless the failures lead to such a catastrophic event. This stage, therefore, is included for illustration only. Quantification of such scenarios is beyond the scope of this study. The initial failure categories are shown across the top of Appendix B6.3-4. They are as follows:

a. Failure of APU turbine to remain intact -- this includes all failures that could generate shrapnel from the APU turbine.

b. Leakage of hydrazine during and after APU shutdown -- this includes all hydrazine leaks that could potentially lead to catastrophic fire.

c. Exhaust gas leaks -- this includes all large exhaust gas leaks that could potentially cause overheating and detonation of hydrazine within an APU.

d. Hydrazine overheating after APU shutdown -- this includes scenarios in which leakage causes a fire which, in turn, causes a detonation and events, such as failure to deenergize an isolation valve, that lead to a detonation of hydrazine without previous hydrazine leakage.

Following failure of an APU turbine to remain intact, the ESD questions whether shrapnel is contained, whether a fire occurs and whether either one could cause catastophic Orbiter damage. A "yes" to the last question results in a LOC/V. Otherwise, the APUs are considered to have completed their mission. Examples of scenarios that would be catastrophic are:

a. Explosion of fuel/oxidizer in the OMS or RCS propellant tanks after being punctured by shrapnel

b. Detonation of hydrazine in the APU fuel tanks leading to a fire that destroys the aft fuselage

c. Fire caused by leaking hydrazine that overheats the fuel/oxidizer in the OMS or RCS propellant tanks

Following leakage of hydrazine, the ESD questions the occurrence of a fire and whether the fire causes catastrophic damage.

Following an exhaust gas leak, the ESD questions if the hot gas caused a detonation, whether the detonation resulted in a fire, and whether the fire caused catastrophic damage.

Following overheating and detonation of hydrazine after APU shutdown, the ESD questions if the detonation and fuel leak resulted in a fire, and if the fire caused catastrophic damage.

6.3.6 Summary

Section 6.3 has discussed the event sequence diagrams used to develop and illustrate scenarios that begin with initial failures of the APU and eventually lead to one of five damage states. The damage states are OK, launch scrub, intact abort, enter at next PLS opportunity, and LOC/V. A typical Shuttle mission was divided into four stages for the purpose of modeling with ESDs. The modeling stages are prelaunch and ascent, orbit, entry through wheelstop, and wheelstop through crew egress.

Although ESDs are useful for the development and communication of scenarios, they are not adequate for quantifying the risk of the APU. Event trees and split fraction models are used for this and are discussed in the next two sections.

6.4 APU EVENT TREE DEVELOPMENT

The ESDs presented in the previous section were developed to clearly describe the sequential flow of events for APU-initiated scenarios that could lead to LOC/V, launch scrub, intact abort, land at next primary landing site opportunity, or a successful mission.

Event trees were developed from the ESDs to facilitate quantification because established computer programs were available for obtaining frequencies of scenarios expressed in the form of event trees. Because quantification is the goal of an event tree, the top events need not have a one-to-one correspondence with the boxes in the event sequence diagrams, and the top events need not be shown from left to right in their expected order of occurrence. Instead, the top events can represent an individual box in an ESD, a group of boxes in an ESD, or a breakdown of an individual box. The order of the event tree top events was established to best capture the inter-event dependencies and facilitate the development of scenario-dependent split fractions.

The construction of event trees, particularly in a multi-stage model as described in Section 5, depends on the analysts' skill and experience, knowledge of the data, and knowledge of the split fraction models. The objective is to best utilize the available data to obtain an accurate estimate of the frequency of each scenario.

6.4.1 Two-Stage Event Tree Model

Section 6.3 includes descriptions of the potential scenarios during the time frame from 5 minutes before launch (i.e., APU start) to APU shutdown after wheelstop. It was found that two event tree stages, called Stage A and Stage B, could adequately serve as a framework for quantification of these scenarios.

Stage A served as a quantitative framework for those scenarios characteristic of the time from 5 minutes before launch to APU shutdown after the OMS-1 orbit insertion burn. This event tree includes start failures, failures to continue running after start, recoverable failures, and failures to successfully close the fuel tank isolation valves upon APU shutdown.

Stage B served as a quantitative framework for those scenarios characteristic of orbit, entry, and landing through APU shutdown.

It includes start failures, failures to continue running after start, recoverable failures, and attempts to recover APUs. Combining the ESDs from orbit, entry/landing, and post wheelstop does not compromise the accuracy of the estimates of the damage state fractions. The ability to identify whether certain failures occurred in orbit or during entry/landing is lost. However, for the purposes of this study, this is not considered to be a significant loss.

The quantification of Stage A results in determination of the fraction of ascents that end in each damage state. The quantification of Stage B results in determination of the fraction of flights that end in each damage state.

The Stage A Event Tree (Appendix B6.4-1) consists of the initial event, which is the attempted start of the APUs in the Orbiter, followed by 21 top events, and ends with the damage state of each sequence. The damage state is shown in Appendix B6.4-1 as an "x" below one of the following: loss of crew or vehicle (LV), launch scrub (LS), intact abort (IA), or land at next primary landing site (PLS). Also shown is a summary of the number of APUs leaking (the number below NL), the number of spurious shutdowns (the number below NS), the number of permanent failures (the number below NF), and whether the scenario must be continued in the next stage (an X under EL). Taken together, a line of Xs and numbers at the end of a sequence in the event tree is called a damage vector. Each sequence is associated with a damage vector. Two or more sequences may have the same damage vector. A transfer in the tree (e.g., XFR1) means that the dotted line is to be replaced by a previously defined group of sequences. For example, the dotted lines that end with XFR1 is to be replaced by the group of sequences and associated damage vectors to the right of the "X1" mark beneath top event "BA". A transfer is not used unless both the sequence of events and the associated damage vector are appropriate to replace the dotted line. A legend is provided on the first page of Appendix B6.4-1, Appendix B6.4-2, and Appendix B6.4-3, that describes the top event designators and damage state designators for Stage A and Stage B Event Trees.

In the general case of a two-stage model, each damage vector serves not only as the end state of Stage A but as an initial condition of Stage B. An initial condition defines the failures that begin each Stage B quantification. In general, a Stage B event tree must be quantified for each Stage A damage vector. The fraction of each Stage A damage vector (which is the same as the fraction of its associated sequence) serves as the frequency of the initial event for Stage B. That is, the fraction of

missions ending in each Stage B sequence is multiplied by the same factor, namely, the damage state fraction that serves as the initial condition for the event tree.

In most applications of a two-stage model, and this was no exception, many damage vectors have nearly the same impact on the Stage B model. Many of the damage vectors lead to quantification of Stage B with essentially the same initial failures. This suggests that many damage vectors can be grouped together in what are called "damage bins" and the frequencies of the grouped damage vectors can be summed to obtain the total damage bin frequency. The Stage B Event Tree, therefore, need only be quantified for each damage bin rather than for each damage vector.

The damage bin is characterized by a set of failures that serves as initial conditions for Stage B and by a fraction of ascents that lead to the particular bin. Having accepted the notion of "binning", it was also recognized that certain damage vectors have low frequency of occurrence and may conservatively be represented by a damage bin with a much larger frequency of occurrence. In this case the word "conservative" means that the status of the APUs as characterized by the damage bin is worse than the low frequency damage vector that it is grouped with. In this application the following damage bins have been defined.

a. All damage vectors with an "x" under LV were grouped into a bin for loss of crew or vehicle.

b. All damage vectors with an "x" under LS were grouped into a bin for launch scrub.

c. All damage vectors with an "x" under IA were grouped into a bin for intact abort.

All damage vectors with an "x" under PL were grouped into three bins representing three groups of APU damage having similar effects on the ability to land at the next primary landing site opportunity. These three bins were as follows:

d. Damage vectors with one APU lost

e. Damage vectors with one APU leaking

f. Damage vectors with one APU lost and one APU leaking

All damage vectors with no failures were grouped into an "OK" bin.

The first three bins above need not serve as initial conditions for Stage B because loss of crew or vehicle, launch scrub, and intact abort are the end states of interest. It is also of interest, however, to assess the chance that Stage A sequences which have been declared as PLS or were OK end in loss of crew or vehicle. Therefore, the last four damage bins (three for PLS and one for OK) serve as initial conditions for Stage B. Scenarios exhibiting spurious shutdowns were grouped with bins 4, 5, or 6 depending on the scenario. A detailed description of the binning logic is shown in Table 6.4.1.

Damage bin number 7 served as the initial condition for the Stage B Event Tree called Stage B7. Damage bin number 4 served as the initial condition for the Stage B Event Tree called Stage B4. The Stage B7 Event Tree is shown in Appendix 6.4-2 and the Stage B4 Event Tree in Appendix 6.4-3. These illustrate how the initial conditions affected the number and variety of sequences during Stage B. Only two damage bins were required to define the end states of Stage B. These were loss of crew or vehicle (LV) and OK.

6.4.2 Stage A Event Tree

The Stage A Event Tree is shown in Appendix 6.4-1. It models the time period from APU start before launch to APU shutdown after the OMS-1 orbital insertion burn.

6.4.2.1 Relationship of ESD to Stage A Event Tree

Table 6.4.2 presents a summary description of each top event in the Stage A Event Tree (refer to Appendix B6.4-1 for the event tree itself). Table 6.4.3 relates each top event in the Stage A Event Tree to one or more ESD questions.

6.4.2.2 Construction of the Stage A Event Tree

The assumptions, groundrules and approximations used to construct the tree were as follows:

a. APU failure was defined as the inability to power its associated hydraulic pump to the extent necessary to maintain adequate hydraulic pressure at the expected hydraulic demand.

b. Two APU failures lead to loss of crew or vehicle (LV).

TABLE 6.4.1

DAMAGE BIN ASSIGNMENTS-STAGE A

Number of APUs That Exhibit:			Bin Number			
Permanent Failure	Leakage	Spurious Shutdown	4	5	6	7
0	0	0				X
0	0	1	X			
0	0	2	X			
0	1	0		X		
0	1	1	X			
0	1	2	X			
0	2	0		X		
0	2	1		X		
0	3	0		X		
1	0	0	X			
1	0	1	X			
1	1	0			X	
1	1	1			X	
1	2	0			X	

Notes:

1. Three spurious shutdowns or one permanent failure and two spurious shutdowns were conservatively assumed to be LOC/V

TABLE 6.4.2

TOP EVENT DEFINITIONS -- APU EVENT TREE - STAGE A*

Event	Definition
IE	Demand for APU Start
HY	Hydraulic System Failure**
TA	Turbine Overspeed
PA	Equipment Failure of One APU After it Starts
DA	Failure of the Second APU After it Starts
CA	Failure of the Second APU or Failure of Flight Critical Equipment Owing to Spatial Interactions Initiated by Failure of the First APU
HA	Failure of One APU Owing to Exhaust Gas Leak
GA	Failure of Flight Critical Equipment or the Second APU Owing to Exhaust Gas Leak
L1	Leakage of Hydrazine From APU 1
L2	Leakage of Hydrazine From APU 2
L3	Leakage of Hydrazine From APU 3
FA	Failure of Flight Critical Equipment or Two APUs Owing to Spatial Interactions Initiated by Hydrazine Leakage
C1	Hydrazine Leakage Causes Failure of APU 1 Given That Two APUS Have Not Failed
C2	Hydrazine Leakage Causes Failure of APU 2 Given That Two APUs Have Not Failed

TABLE 6.4.2 (Concluded)

TOP EVENT DEFINITIONS -- APU EVENT TREE - STAGE A

Event	Definition
C3	Hydrazine Leakage Causes Failure of APU 3 Given That Two APUs Have Not Failed
S1	Spurious Shutdown of APU 1
S2	Spurious Shutdown of APU 2
S3	Spurious Shutdown of APU 3
BA	Failure of One or Two APUs Upon Start or While Running Before Launch
EA	Failure Occurs in the Thrust Bucket
MA	Failure Occurs After MECO
IA	Intact Abort Called by MCC

---

* Stage A Event Tree is Shown in Appendix B6.4-1.

** This top event is included to show how an event tree can include scenarios that cross subsystem boundaries. Quantitative evaluation of the hydraulic system is out-of-scope.

TABLE 6.4.3

RELATIONSHIP OF STAGE A EVENT

TREE TOP EVENTS TO APU ESD 1 - PRELAUNCH AND ASCENT*

Event	Questions from Appendix B6.3-1 & Table 6.4.2
HY	"Hydraulic System OK" and All Boxes Beneath that Question
TA, DA	"Turbine Speed Control OK" and All Boxes Beneath that Question
PA, DA	"No Permanent APU Failures " and All Boxes Beneath that Question This event also includes the question "Fuel Isolation Valves Close Within 10 Minutes After APU Shutdown" and All Boxes Beneath it in Appendix B6.3-2
CA	All questions following "SIE". They include: "SIE Does Not Fail Flight Critical Equipment" "SIE and Initial Failure Does Nct Cause Two APUs to Fail" "SIE and Initial Failure Does Not Cause the Second APU to Fail With One Already Failed" the Above Questions Relate to Spatial Interactions that Follow Failures Involving Shrapnel.
HA, GA	"Exhaust Gas Boundary Remains Intact" and All Spatial Interaction Questions Beneath It. The Spatial Interaction Questions Now Refer Only to the Damage Potentially Caused by Exhaust Gas Release.
L1, L2, L3	"Fuel Boundaries Remain Intact"
FA	"Sufficient Oxygen for Fire in Aft Compartment" "Fire in Aft Compartment" and All Questions Following "SIE". The Spatial Interaction Questions Now Refer to the Damage of Flight Critical Equipment or APUs Potentially Caused by Hydrazine in the Aft Compartment.
C1, C2, C3	"Remaining Fuel Quantity Sufficient to Support Landing" "Leak Isolated"

TABLE 6.4.3 (Concluded)

Event	Questions from Appendix B6.3-1 & Table 6.4.2
	"Leak Detected and APU Shutdown Before Fuel Quantity and Tank Pressure Depleted"
	"Sufficient Oxygen For Fire in Aft Compartment"
	"Fire in Aft Compartment"
	All Questions Following "SIE". These Spatial Interaction Questions Now Refer to Damage of an Individual APU Potentially Caused by Hydrazine in the Aft Compartment
S1, S2, S3	"No Recoverable Failures"
	Spurious Shutdowns and Isolatable Leaks Were Modeled as Recoverable Failures
BA	The Question "Has Liftoff Occurred" and Questions Below It
	This Top Event Determines the Fraction of Each Scenario That Occurs Before or After Launch. It is Used to Decide on Whether the Scenario Ends in Launch Scrub or LOC/V.
MA	This Top Event Does Not Appear on an ESD. It Was Added to the Event Tree to Distinguish Failures After MECO That Would Not Contribute to Intact Aborts.
EA	"Has Thrust Bucket Started?"
	"Has Thrust Bucket Ended?"
IA	"Second APU/Hydraulics Loss Impending"
	"Will Failing APU/Hydraulics Not Support PLS?"
	"Will Failing APU/Hydraulics Not Support Intact Abort?"

---

* Stage A Event Tree is Shown in Appendix B6.4-1.

c. All failures except leakage and spurious shutdown have been modeled as permanent or nonrecoverable.

d. The event tree was quantified from APU start (Liftoff minus 5 minutes) to APU shutdown on orbit. Failure of a fuel tank isolation valve to close upon attempted shutdown was conservatively modeled as a permanent failure.

e. A large hydrazine leak was defined as a leak for which the APU would deplete all usable fuel before the end of the flight.

f. Any modeled failure of any APU that occurred before launch was assumed to lead to launch scrub, with one exception. Shrapnel and hydrazine-generated failures of flight critical equipment from turbine overspeed were conservatively assumed to result in loss of crew or vehicle, even if they occurred on the pad.

g. With one exception, the APUs were assumed to be identical and spatially symmetrical to each other so that frequencies and consequences were independent of which APU had failed. This allowed APU 3 to be assigned as the failed APU with no loss of generality or quantitative accuracy when the failures under TA, PA, or HA occur. The exception was leakage. The conditional probability of failing APU 3 given a leak in APU 1 or APU 2 or both (top event C3) was lower than the conditional probability of failing APU 1 or 2, given a leak in either or both of these APUs. Similarly, the conditional probability of failing APU 1 or 2 due to a leak in APU 3 (top events C1 and C2) was much lower than the conditional probability of APU 3 failing itself.

h. The possibility of two APUs failing independently in the same flight from turbine overspeed was not modeled because the frequency of this sequence was much smaller than the frequency of sequences leading to loss of crew or vehicle that involve one turbine overspeed with other failures.

i. The frequency of failure of a running APU before launch is approximated by a function of the ratio of time it runs before launch to the total time from five minutes before lift-off to APU shutdown. All start failures were modeled as occurring before launch.

j. The APUs were modeled as if each one had its own auto shutdown inhibit switch (a post-51L modification).

k. Two spurious shutdowns or a permanent failure and a spurious shutdown were assumed to result in loss of crew or vehicle if they occurred before MECO. However, if one occurred after the spurious shutdown was treated as a recoverable failure for entry/landing. Sequences involving three spurious shutdowns or one permanent failure and two spurious shutdowns were not explicitly shown in the event tree because of the extremely small chance of occurrence.

l. An APU exhibiting a malfunction which by Flight Rules would cause MCC to declare it lost was assumed to operate until after MECO.

m. Hot restarts were not modeled in Stage A since they must occur after APU shutdown post-MECO.

n. If the same APU exhibits both a spurious shutdown and a hydrazine leak, the damage vector shows it as a hydrazine leak. This was a conservative assignment because of the relatively high conditional probability of cascading damage, given a leaking APU during descent. The net affect on the quantitative results is small because a leaking APU will not be used during Stage B unless another APU fails.

o. The frequency of failures occurring after MECO was modeled as a function of the ratio of the time from MECO to APU shutdown to the total Stage A time.

p. Any APU failure or spurious shutdown that occurred in the thrust bucket was assumed to lead to an intact abort. The frequency of a failure occurring in the thrust bucket was modeled as a function of the ratio of the time in the thrust bucket to the total Stage A time.

q. Any APU exhibiting a failure or a spurious shutdown can also exhibit a hydrazine leak.

6.4.3 Description of Stage A Top Events

A summary description of each top event and its relationship to the rest of the Stage A Event Tree is provided in this section. The detailed model that provides the basis for assessing the frequency of occurrence of each top event split fraction is provided in Section 6.5. The data required to quantify these models is described in Section 7.

Top Event HY: Hydraulic System Failure

This event was included as an illustration of how an event tree can include scenarios that cross subsystem boundaries. A failure of HY implies that its associated APU is useless. The event tree, therefore, treats HY failure as if an APU has failed.

Top Event TA: Turbine Overspeed

This event occurs if both the primary and secondary fuel control valves fail in the open position while the APU is operating and the overspeed trip fails to close the secondary valve. Closure of the fuel tank isolation valves following an overspeed trip may not prevent turbine runaway and shrapnel caused by turbine runaway. The hydrazine quantity downstream of the isolation valves may be sufficient, given the presence of bubbles or effective suction by the APU fuel pump to allow the turbine to reach breakup speed.

Mechanical, electrical and controller causes of turbine overspeed were included. Turbine overspeed implies that the APU has failed. It was then appropriate to ask if the resulting shrapnel and hydrazine escape could have caused a second APU or other flight critical equipment in the aft compartment (i.e., top event CA) to fail. The tree also asks if another APU could have failed independently from the turbine overspeed either by equipment failure (e.g., top event DA) or by leakages. Occurrence of this event after launch and in the absence of other failures leads to a PLS entry unless it occurs in the thrust bucket. In that case, it leads to an intact abort.

Top Event PA: APU Equipment Failure After APU Start

This event occurs if any equipment failure or failures combine to prevent an APU from providing sufficient power to its hydraulic pump as defined above. For example, this event includes break-up of the turbine rotor at normal speed. However, this event excludes turbine overspeed, leakages, spurious shutdowns, and start failures. This top event does not include failures caused by erroneous commands from sources external to the APU (e.g., from the crew or MCC). These failures are outside the scope of this study. The combinatorial failures included in this top event are described in detail in Section 6.5. Occurrence of this event after launch and in the absence of other failures leads to a PLS entry unless it occurs in the thrust bucket. In that case, the event leads to an intact abort.

Top Event DA: Failure of Second APU After APU Start

This event asks if either PA or TA has occurred. It includes failure of a second APU given that one APU has failed. The same combinations of equipment failures that contribute to PA are also relevant here. Occurrence of this event after launch leads to loss of crew and vehicle.

Top Event CA: Spatial Interaction Failure of Second APU or Flight Critical Equipment

This event includes failure of a second APU or flight critical equipment due to shrapnel or hydrazine induced cascading damage. It considers the possibility that shrapnel and hydrazine leakage could be produced by turbine rotor break-up, either in an over-speed or normal speed condition. The sequence of events involving both TA and CA, then, would lead to loss of crew and vehicle from turbine shrapnel or leaking hydrazine. The sequence of events involving both PA and CA would be caused by one of the failures included in the PA split fraction model, namely, turbine rotor break-up. The subsequent events are identical to those for TA and PA, but with a different frequency.

Top Event HA: Exhaust Gas Leakage Fails One APU

This event includes the possibility that exhaust gas leakage can fail an APU. Occurrence of this event after launch and in the absence of other failures leads to a PLS entry unless it occurs in the thrust bucket. In that case, the event leads to an intact abort.

Top Event GB: Exhaust Gas Leakage Fails Second APU

This event includes the possibility that exhaust gas leakage fails a second APU given that one APU is known to have failed from exhaust gas leakage or from other causes. Occurrence of this event after launch leads to loss of crew and vehicle.

Top Event L1: Hydrazine Leakage in APU 1

This event includes leakages of hydrazine into the aft compartment from anywhere in APU 1.

Top Event L2: Hydrazine Leakage in APU 2

This event includes leakages of hydrazine into the aft compartment from anywhere in APU 2.

Top Event L3: Hydrazine Leakage in APU 3

This event includes leakages of hydrazine into the aft compartment from anywhere in APU 3.

The event tree structure involving L1, L2, and L3 includes all combinations of APUs leaking individually or together in the same mission. After the questions about leakage, it was appropriate to ask about potential cascading damage caused by free hydrazine in the aft compartment. Occurrence of any detected leakage would cause mission control to declare that APU lost and lead to a PLS entry, according to Flight Rules.

Top Event FA: Leakage-Induced Failure of Two APUs or Flight Critical Equipment

This event includes those spatial interactions stemming from the presence of hydrazine in the aft compartment that could cause failure of at least two APUs or other flight critical equipment. In the scenarios in which one APU has already failed, this event includes failure of a second APU or flight critical equipment. Occurrence of this event after launch leads to loss of crew and vehicle.

Top Event C1: Leakage Induced Failure of APU 1

This event includes spatial interaction induced failure of APU 1 from the presence of hydrazine in the aft compartment, given that two APUs have not already failed. Occurrence of this event after launch and in the absence of other failures leads to a PLS entry, unless it occurs in the thrust bucket. In that case, it leads to an intact abort.

Top Event C2: Leakage-Induced Failure of APU 2

This event includes spatial interaction induced failure of APU 2 from the presence of hydrazine in the aft compartment, given that two APUs have not already failed. Occurrence of this event after launch and in the absence of other failures leads to a PLS entry unless it occurs in the thrust bucket. In that case, it leads to an intact abort.

Top Event C3: Leakage-Induced Failure of APU 3

This event includes spatial interaction induced failure of APU 3 from the presence of hydrazine in the aft compartment, given that

two APUs have not already failed. Occurrence of this event after launch and in the absence of other failures leads to a PLS entry unless it occurs in the thrust bucket. In that case, it leads to an intact abort.

In any sequence, including a leaking APU, C1, C2, and C3 are asked in order to account for the possibility that leakage from one APU could fail another APU. Although the leakages themselves (occurrence of L1, L2, or L3) are potentially recoverable if needed to support landing, the additional occurrence of C1, C2, or C3 implies a permanent, non-recoverable failure.

Top Events S1, S2, and S3: Spurious Shutdown

This event includes equipment failures of APU 1 (S1), APU 2 (S2), or APU 3 (S3) that cause a spurious shutdown of the affected APU. For example, MPU 1 failing high could cause the controller to sense an overspeed and shut down the APU. It was assumed that this condition can be identified during orbit, so that the APU could be started if needed to have two operating APUs during descent. Should any such shutdown occur in the thrust bucket, an intact abort occurs. Should a spurious shutdown occur before or after MECO, a PLS entry is assumed. Should two shutdowns before MECO, a loss of crew and vehicle results.

Top Event BA: Failure Occurs Before Launch

This event includes all combinations of start failures of any or all APUs. It also includes that fraction of running failures of any or all APUs that occur before launch. Occurrence of this event leads to a launch scrub.

Top Event EA: Failure Occurs in the Thrust Bucket

This event includes those failures that occur in the thrust bucket and is assumed to lead to an intact abort. It was quantified as a function of the ratio of time in the thrust bucket to the total Stage A time.

Top Event MA: Failure Occurs after MECO

This event includes those failures that occur after MECO. This is a significant time because the APUs are not needed for throttling functions after the main engines have shut down. They are, however, needed for a TVC during the MPS dump, not considered as a safety critical event for this study. Any recoverable or permanent APU failure occurring after MECO leads to a PLS entry.

Top Event IA: Intact Abort Called by MCC

If one APU has failed and another was leaking before MECO, the flight rules provide for the MCC to make a decision as to the ability of the leaking APU to support a landing. If the APU leak is large enough so that the APU will not support a landing at the next primary landing site opportunity, then the MCC may declare an intact abort to allow the shuttle to return as soon as possible. Occurrence of this event leads to an intact abort in the event tree.

6.4.4 Stage B Event Trees

The Stage B Event Trees are shown in Appendices B6.4-2 and B6.4-3. They model the time from APU shutdown after the orbital insertion burn to APU shutdown after wheelstop.

6.4.4.1 Relationship of ESD to Stage B Event Trees

Table 6.4.4 presents a summary description of each top event in the Stage B Event Trees (refer to Appendices B6.4-2 and B6.4-3 for the event trees themselves). Table 6.4.5 relates each top event in the Stage B Event Trees to one or more ESD questions.

6.4.4.2 Construction of the Stage B Event Trees

The Stage B7 Event Tree (Appendix B6.4-2) was initiated by the OK damage bin described in Section 6.4.1 (also called Impact Vector 1). It must represent scenarios consisting of up to two APU failures in order to result in the LOC/V damage state. The Stage B4 Event Tree (Appendix B6.4-3) was initiated by damage bin No. 4, described in Section 6.4.1 (also called Impact Vector 2), which consists of Stage A scenarios ending with one APU failed. The Stage B4 Event Tree is far simpler because we need only represent scenarios consisting of no APU failures or one APU failure in order to result in the LOC/V damage state.

Accuracy and completeness of the modeling and quantification effort in those areas of the study that can potentially contribute most to the risk are important. Standard practice in multi-stage modeling is to estimate the potential contribution to the total mission risk from each Stage A damage bin. This allows the allocation of the study resources (e.g., manpower, time, and money)

to those areas that are estimated to be the most important contributors to the total mission risk.

It was determined for this study that Stage B Event Trees for damage bins 5 and 6 need not be developed because of their extremely low frequency of occurrence. That is, the resources required to develop event trees and split fraction models, and to perform quantification for bins 5 and 6 would be wasted because these bins could, at most, contribute less than one percent of the total frequency of loss of crew or vehicle for the total flight.

In view of this, it was decided to allocate resources to the detailed analysis of the top 99% of the potential total mission risk. However, the contribution of damage bins 5 and 6 are not neglected. They were conservatively assumed to lead to loss of crew or vehicle when all of the contributors to the LOC/V state for the entire flight were added up. This is standard practice for PRA.

The assumptions, groundrules and approximations used to construct the Stage B trees are as follows:

a. APU failure is defined as the inability to power its associated hydraulic pump to the extent necessary to maintain adequate hydraulic pressure at expected hydraulic demand.

TABLE 6.4.4

TOP EVENT DEFINITIONS - APU EVENT TREE - STAGE B*

Event	Definition
IE	Damage Bin From Stage A
SS	One APU Fails to Start
DS	Second APU Fails to Start
TB	Turbine Overspeed
PB	Equipment Failure of One APU After it Starts
DB	Failure of the Second APU After it Starts
CB	Failure of the Second APU or Failure of Flight Critical Equipment Owing to Spatial Interactions Initiated by Failure of the First APU
HB	Failure of one APU Due to Exhaust Gas Leak, or GGVM Detonation
GB	Failure of Flight Critical Equipment or the Second APU Due to Exhaust Gas Leak, or Valve Detonation
M1	Leakage of Hydrazine from APU 1
M2	Leakage of Hydrazine from APU 2
M3	Leakage of Hydrazine from APU 3
FB	Failure of Flight Critical Equipment or Two APUs Due to Spatial Interactions Initiated by Hydrazine Leakage
D1	Hydrazine Leakage Causes Failure of APU 1 Given that Two APUs Have Not Failed
D2	Hydrazine Leakage Causes Failure of APU 2 Given that Two APUs Have Not Failed
D3	Hydrazine Leakage Causes Failure of APU 3 Given that Two APUs Have Not Failed

TABLE 6.4.4 (Concluded)

Event	Definition
R1	Leak in APU 1 Before EI-13 or into Pump Seal Cavity
R2	Leak in APU 2 Before EI-13 or into Pump Seal Cavity
R2	Leak in APU 3 Before EI-13 or into Pump Seal Cavity
T1	Spurious Shutdown of APU 1
T2	Spurious Shutdown of APU 2
T3	Spurious Shutdown of APU 3
TE	Failure of at Least One APU After TAEM-3.5 Minutes
PW	Failure of at Least One APU After Wheelstop
RE	Failure to Recover APU When Needed For Landing
SB	Uninhibited Spurious Shutdown of at Least One APU (Applies Only for Impact Vector Two)

---

* Stage B Event Trees are Shown in Appendices B6.4-2 and B6.4-3.

TABLE 6.4.5

RELATIONSHIP OF STAGE B EVENT TREE TOP EVENTS TO APU ESDS 2, 3, AND 4 -- ORBIT AND ENTRY/DESCENT/LANDING*

Event	Questions From Appendices B6.3-2 Through B6.3-4
SS, DS	"No Permanent APU Failures" This Box Represents Both Start and Run Failures. None of the Start Failures were Identified as Potentially Leading To Spatial Interaction Events. Start Failures were Separated from Run Failures to Accurately Quantify Failures Which Could Not Occur After Wheelstop.
TB, DB	"Turbine Speed Control OK" and all Boxes Beneath this Question
PB, DB	"No Permanent APU Failures" and all Boxes Beneath this Question "Hydrazine Does Not Overheat After Shutdown" "Overheating Does Not Cause Detonation" "Temperature Stays Above Minimum for Hydrazine, Lube Oil, and Gas Generator"
CB	"Sufficient Oxygen for Fire in AFT Compartment" "Unisolated Leak" "Fire in AFT Compartment" All Questions Following "SIE". They Include: "SIE Does Not Fail Flight Critical Equipment" "SIE End Initial Failure Does Not Cause Two APUs to Fail" "SIE and Initial Failure Does Not Cause the Second APU to Fail With One Already Failed" The Above Questions Relate to Spatial Interactions that Follow Failures Involving Shrapnel

TABLE 6.4.5 (Continued)

Event	Questions From Appendices B6.3-2 Through B6.3-4
HB, GB	"Exhaust Gas Boundary Remains Intact" and all Spatial Interaction Questions Beneath it. The Spatial Interaction Questions Refer to the Damage Potentially Caused by Exhaust Gas Release
	"Fuel Bound Areas Remain Intact" and all Spatial Interaction Questions Beneath it. The Spatial Interaction Questions Refer to the Damage Potentially Caused by Hydrazine in the Aft Compartment.
M1, M2, M3	"Fuel Boundaries Remain Intact"
	"Hydrazine Boundary Remains Intact"'
FB	All Questions Beneath "Hydrazine Boundary Remains Intact" in Appendix B6.3-2
	All Questions Beneath "Fuel Boundary Remains Intact" in Appendix B6.3-3
	All Questions Following "SIE". The Spatial Interaction Questions now Refer to Damage of Flight Critical Equipment or APUs Potentially Caused by Hydrazine in the Aft Compartment
D1, D2, D3	"APU Fuel Quantity and Tank Pressure can Support Start and Landing"
	"Leak Isolated"
	"Hot Restart Without Detonation" and all Questions that Follow it
	"Remaining Fuel Quantity and Tank Pressure Sufficient to Support Landing"
	"Tank Pressure Sufficient for Restart"
	"Sufficient Oxygen to Support Fire"
	"Fire in Aft Compartment"

TABLE 6.4.5 (Concluded)

Event	Questions From Appendices B6.3-2 Through B6.3-4
	All Questions Following "SIE". These Spatial Interaction Questions now Refer to the Damage Potentially Caused by Hydrazine in the Aft Compartment to an Individual APU.
R1, R2, R3	"No Seal Cavity Leak" and Questions Below it in Appendix B6.3-3
	"Leak Detected Before Blackout" and Questions to the Right of it in Appendix B6.3-3
T1, T2, T3	"No Recoverable Failures"
	Spurious Shutdowns and Isolatable Leaks were Modeled as Recoverable Failures
TE, RE	"Start Recoverable APU Before TAEM"
	"Recovered APU Operates OK"
PW	"Has Wheelstop Occurred"

---

* Stage B Event Trees are Shown in Appendices B6.4-2 and B6.4-3.

b. Two APU failures lead to loss of crew or vehicle (LV).

c. All failures except spurious shutdown and detected leakages are modeled as permanent (non-recoverable).

d. The event tree, split fraction models and quantification reflect the following Flight Rules (Reference 39) wherever applicable: 10-19, 10-20, 10-22, 10-23, 10-24, 10-25, 10-27, 10-28, 10-29, 10-31, and 10-36.

e. A "large" hydrazine leak is defined as a leak for which the APU would deplete all usable fuel before the end of the mission.

f. APU failures that occurred after wheelstop were modeled. However, the frequency of these failures leading to LOC/V is believed to be negligible and is not quantified.

g. With one exception, the APUs are assumed to be identical and spatially symmetrical to each other so that frequencies and consequences are independent of which APU has failed. This allowed APU 3 to be assigned as the failed APU with no loss of generality or quantitative accuracy when the failures under TA, PA, or HA occur. The exception was leakage. The conditional probability of failing APU 3, given a leak in APU 1 or APU 2 or both (top event C3) was lower than the conditional probability of failing APU 1 or 2, given a leak in either or both of these APUs. Similarly, the conditional probability of failing either APU 1 or 2 due to a leak in APU 3 (Top Events C1 and C2) is much lower than the conditional probability of APU 3 failing itself.

h. The possibility of two APUs failing independently in the same mission from turbine overspeed is not modeled because the frequency of this sequence is much smaller than the frequency of sequences leading to loss of crew or vehicle that involves one turbine overspeed with other failures.

i. A spurious shutdown that occurs later than 3.5 minutes before TAEM was assumed to be non-recoverable in time to support the remainder of the mission.

j. The APUs were modeled as if each one had its own auto shutdown inhibit switch (a post-51L modification).

k. Any APU exhibiting a malfunction which by Flight Rules would cause the MCC to declare it lost on orbit was assumed to be started, if needed, at EI-13. Recoverable failures occurring after TIG-5 minutes are assumed to be restartable, if needed, at TAEM-3.5 minutes. Spurious shutdowns that occurred during ascent or during FCS checkout are assumed to be started, if needed, at EI-13, with auto shutdown inhibit in effect.

l. Hot restarts are modeled in Stage B and include failure of the injector cooling system and the potential for detonation if injector cooling fails.

m. Any failed APU can also exhibit a hydrazine leak. The potential spatial interactions from that leak were included in the model.

n. Automatic shutdown is assumed to be inhibited (unless the circuit fails) for any attempted restart or any start of an APU with another having already failed.

o. One APU which suffers a spurious shutdown during Stage B with no other failed APUs will not be restarted. Three normally recoverable failures occurring before wheelstop are considered loss of crew and vehicle. This is because the second and third failures would have to occur in spite of auto shutdown being inhibited, and would thus be irrecoverable.

p. Hydrazine overheating due to loss of fuel pump/GGVM cooling is judged to be an insignificant contributor to risk. This cooling system is employed only in certain abort cases whose considerations are outside the scope of this study and, therefore, is not quantified.

q. Stage B split fraction models were quantified independently of Stage A. This means that independent failures of redundant components that occurred in a single APU in Stage A are treated as not failed at the start of Stage B. This is considered an acceptable simplification because the ascent phase (Stage A) represents less than 1% of the total mission time during which these failures could possibly occur.

r. Small leakages are treated as being undetectable during stage B. However, the model does provide for shutdown of an APU whose pump seal was leaking before blackout. The model provides for failing an APU as a result of a leak into the

solenoid cavities or as a result of an unisolatable external leak. For all other leaks, a running APU is conservatively modeled as continuing to run without being shut down or restarted. This treatment is consistent with the experience of STS-9 when the leak is not detected until too late to shutdown the APUs.

6.4.5 Description of Stage B Top Events

A summary description of each top event and its relationship to the rest of the Stage B Event Tree is provided in this section. The detailed model that provides the basis for assessing the frequency of occurrence of each top event split fraction is provided in Section 6.5. The data required to quantify these models is described in Section 7.

Top Events SS and DS: APUs Fail to Start

These events included all start failures of APUs either at deorbit TIG-5 minutes or at EI-13 minutes. Event SS represents failure of one APU to start; event DS represents failure of a second or third APU to start, given that one APU has already failed. These failures are malfunctions that occur from APU equipment failures occurring at start attempt. These failures cannot be recovered. Therefore, the occurrence of DS implies loss of crew and vehicle. The occurrence of SS implies that one APU is lost for Stage B and that the failure of one more APU would cause loss of crew and vehicle.

Top Event TB: Turbine Overspeed

This event occurs if both the primary and secondary fuel control valves fail in the open position while the APU is operating and the overspeed trip fails to close the secondary valve. Occurrence of this event after a previous APU failure would not require failure of the overspeed trip because the auto shutdown function would have been inhibited. Closure of the fuel tank isolation valves following an overspeed trip may not prevent turbine runaway and shrapnel caused by turbine runaway. The quantity of hydrazine downstream of the isolation valves may be sufficient given the presence of bubbles or effective suction by the APU fuel pump to allow the turbine to reach breakup speed.

Mechanical, electrical, and controller causes of turbine overspeed were included. Turbine overspeed implies that the APU has failed. It was then appropriate to ask if the resulting shrapnel

and hydrazine escape could have caused a second APU or other flight critical equipment (i.e., top event CB) to fail. The tree also asks if another APU could have failed independently from the turbine overspeed either by equipment failure (e.g., top event DB) or by leakages. Occurrence of this event leads to failure of one APU and to a release of hydrazine into the aft compartment. Failure of another APU as a consequence of the shrapnel and hydrazine release is treated in event CB.

Top Event PB: APU Equipment Failure After APU Start

This event occurs if any equipment failure or failures combine to prevent an APU from providing sufficient power to its hydraulic pump as defined above. For example, this event includes break-up of the turbine rotor at normal speed, and heater failures. Heater failures were quantified for the orbit period. This event does exclude, however, turbine overspeed, leakages, spurious shutdowns, and start failures. This top event does not include failures caused by erroneous commands from sources external to the APU (e.g., from the crew or the MCC). These failures are outside the scope of this study. The combinatorial failures included in this top event are described in detail in Section 6.5. Occurrence of this event leads to failure of one APU. If turbine break up has occurred, shrapnel- and hydrazine-related spatial interaction events are accounted for in event CB.

Top Event DB: Failure of Second APU After APU Start

This event is asked if either PB or TB has occurred. It includes failure of a second APU given that one APU is known to have failed.

The same combination of equipment failures that contribute to PB are also relevant here. Occurrence of this event after launch leads to LOC/V.

Top Event CB: Spatial Interaction Failure of Second APU or Flight Critical Equipment

This event includes failure of a second APU or flight critical equipment due to shrapnel or hydrazine-induced propagating damage. It considers the possibility that shrapnel and hydrazine leakage could be produced by turbine rotor break-up, either in an over-speed or normal speed condition. The sequence of events involving both TB and CB, then, would lead to LOC/V from turbine shrapnel or leaking hydrazine. The sequence of events involving both PB and CB would be caused by one of the failures included in the PB split fraction model, namely, turbine rotor breakup. The subsequent

events are identical to those for TB and PB, but with a different frequency.

Top Event HB: Exhaust Gas Leakage or Detonation of GGVM

This event includes the possibility that exhaust gas leakage can fail an APU. It also includes the possibility that hydrazine leaks into the solenoid cavity of one of the fuel control valves, autodecomposes, and ruptures the valve cover such that hydrazine escapes into the aft compartment. A large hole is conservatively assumed to be formed and the APU is assumed to be lost.

Top Event GB: Exhaust Gas Leakage or Detonation of Isolation Valve

This event includes the possibility that exhaust gas leakage fails a second APU given that one APU is known to have failed from exhaust gas leakage or from other causes. It also includes the possibility that hydrazine leaks into the solenoid cavity of one of the fuel tank isolation valves, autodecomposes, and ruptures the valve cover such that hydrazine escapes into the aft compartment. This leakage is assumed to be unisolatable and large. It allows the contents of the fuel tank to enter the aft compartment. The conditional probability of failing another APU or flight critical equipment with the contents of the fuel tank emptied into the aft compartment was so large that this event has been assigned to the loss of crew or vehicle damage state.

Top Event M1: Hydrazine Leakage in APU 1

This event includes leakages of hydrazine into the aft compartment from anywhere in APU 1, except those leakages covered in HB and GB above, and those from the fuel pump seal into the drain line.

Top Event M2: Hydrazine Leakage in APU 2

This event includes leakages of hydrazine into the aft compartment from anywhere in APU 2, except those leakages covered in HB and GB above, and those from the fuel pump seal into the drain line.

Top Event M3: Hydrazine Leakage in APU 3

This event includes leakages of hydrazine into the aft compartment from anywhere in APU 3, except those leakages covered in HB and GB above.

The event tree structure involving M1, M2, and M3 includes all combinations of APUs leaking individually or together in the same mission. After the questions about leakage, it was appropriate to ask about potential cascading damage caused by hydrazine release. Leakage was quantified from the end of Stage A through APU shutdown, including orbit.

Top Event FB: Leakage Induced Failure of Two APUs or Flight Critical Equipment

This event includes those spatial interactions stemming from the presence of hydrazine in the aft compartment that could cause failure of at least two APUs or other flight critical equipment. For scenarios in which one APU has already failed, this event includes failure of a second APU or flight critical equipment. Occurrence of this event before wheelstop leads to loss of crew and vehicle.

Top Event D1: Leakage Induced Failure of APU 1

This event includes spatial interaction induced failure of APU 1 from the presence of hydrazine in the aft compartment, given that two APUs have not already failed.

Top Event D2: Leakage Induced Failure of APU 2

This event includes spatial interaction induced failure of APU 2 from the presence of hydrazine in the aft compartment, given that two APUs have not already failed.

Top Event D3: Leakage Induced Failure of APU 3

This event includes spatial interaction induced failure of APU 3 from the presence of hydrazine in the aft compartment, given that two APUs have not already failed.

In any sequence in which any APU is leaking, D1, D2, and D3 are asked in order to account for the potential of leakage from one APU failing another APU. Although the leakages themselves (occurrence of M1, M2, or M3) are potentially recoverable if needed to support landing, the additional occurrence of D1, D2, or D3 implies a permanent, non-recoverable failure.

Top Events R1, R2, R3: Seal Cavity Leaks

These events include the fraction of leakages that occur before EI-13, and those that occur through the fuel pump seal into the

seal drain line for APU 1 (R1), APU 2 (R2), and APU 3 (R3). Should any of these types of leakages be detected in the absence of an APU failure, Flight Rules indicate that the leaking APU would be shut down, and restarted only if needed for landing. The model assumes that such restarts are made at TAEM-3.5 minutes. Should these events occur during a scenario that includes a previous failure of an APU, then the model assumes that the leading APU will continue to operate.

Top Events T1, T2, and T3: Spurious Shutdown

This event includes equipment failures of APU 1 (T1), APU 2 (T2), or APU 3 (T3) that would cause a spurious shutdown of the affected APU. For example, MPU 1 failing high could cause the controller to sense an overspeed and shut down the APU. If one APU has exhibited a spurious shutdown and no other APUs have failed or have been declared lost, then the model assumes that the APU experiencing the spurious shutdown is not restarted because it is not needed. If the spurious shutdown occurs after TAEM-3.5 minutes, then the APU is considered lost. Otherwise, the APU will be recovered at TAEM-3.5 minutes. If a scenario includes two spurious shutdowns before TAEM-3.5 minutes, one (the second shutdown that occurred) represents a permanent failure because auto shutdown would have been inhibited after the first APU failed. The model assumes that recovery of the APU that failed first is attempted at TAEM-3.5 minutes.

Top Event TE: Failure Occurs After TAEM-3.5 Minutes

This event includes the fraction of all APU failures that occur after TAEM-3.5 minutes. All such failures are assumed to be non-recoverable. Two such failures, including spurious shutdowns, are assumed to lead to loss of crew and vehicle. This time was selected because analysis groundrules dictate that two APUs are required for TAEM and the approach and landing phases of entry. The 3.5 minute margin accounts for the injector cooling hot re-start procedure required to restart a previously shut down APU. The model conservatively ignores the APU cool down procedure.

Top Event PW: Failure Occurs after Wheelstop

This event includes those failures that occur after wheelstop. This is significant because the APUs are no longer needed after wheelstop; APU failures cannot cause a loss of crew or vehicle unless the failure causes a catastrophic explosion or fire. All APU failures that occur after wheelstop have been modeled.

However, the frequency of failure is believed to be negligible. Therefore, they do not contribute to the risk of loss of crew or vehicle.

Top Event RE: Failure to Recover APU

Event RE asks if an APU that had been shut down by MCC call or had experienced a spurious shutdown during entry was successfully restarted. It includes failure of injector cooling with subsequent potential for detonation of the APU. Occurrence of this event leads to a loss of crew and vehicle. The fact that the restart was attempted indicates that the APU was needed to support landing.

6.5 SPLIT FRACTION MODEL DEVELOPMENT

6.5.1 Principles of Model Development

A guiding principle for the modeling and computational effort was to place more emphasis and detail in those aspects of the model that promised to be important to risk. This meant, for example, that many scenarios involving large numbers of failure occurrences would not be important because of their low associated probabilities. Such scenarios could be quickly estimated by a preliminary analysis using a general knowledge of the model and the basic event data. It was not difficult, for example, to estimate the order of magnitude of the total LOC/V frequency from a knowledge of the event tree, APU design, and the failure history database without going through the formal computer analysis. However, in some cases knowledge to make such initial assessments was not available until late in the study. It was necessary to include such events in the analysis. One of the most prominent examples is the case of consequential permanent failures resulting from exhaust gas leaks. Exhaust gas leaks were identified in the master logic diagrams as an initiating failure and were, therefore, included in the event trees. Their frequency of occurrence and the conditional probability of consequential failure of an APU were not assessed until well after the event trees had been completed and while the split fraction models were under development. Their contribution to risk was found to be negligibly small (less than 0.1 per cent of the total LOC/V frequency). The exhaust leak models are, therefore, more complex than necessary.

In developing the interrelated event tree and fault tree models, it was also necessary to strike a balance in modeling complexity between these two types of logic trees. This was an iterative process that began by developing a simple first-cut event tree and its associated fault trees. The fault trees were found to be too complex to be analyzed easily. This led to a more complex event tree, and the associated fault trees were found to be much more reasonable. This iterative process was continued until a reasonable balance was achieved.

The fault tree analysts also had to be aware of the data analysis because, as discussed in the Study Methodology Section (Section 5), it is pointless to model components at a level below that for which data exists. Furthermore, the availability of data in a particular form influences the way the fault tree analyst chooses to express the basic events. The process of split fraction modeling is iterative and highly interactive with the event tree development and data analysis processes.

As indicated in Section 6.4, the event tree for APU Stage A is a logic diagram that shows the various admissible combinations of top event occurrences and nonoccurrences that constitute the various scenarios to be analyzed. In order to compute the scenario occurrence frequencies, it is first necessary to compute the appropriate split fractions for the top events appearing in each scenario. In some cases, these split fractions are single numbers determined from all available evidence, as described in Section 5. In other cases, the top events represent a substantial part of the APU, and the corresponding split fractions were computed from fault tree analyses. The paragraphs that follow describe the fault trees that were developed for calculating the split fractions for the event tree top events. The outcome of the split fraction models, when evaluated by the data for the basic events, is a set of split fraction Cause Tables as described in Section 5 and as shown in the Quantitative Results Section (Section 8).

6.5.2 General Groundrules and Assumptions

Before describing the fault trees, it is appropriate to describe some general ground rules, assumptions, and analysis considerations that are fundamental to all of the fault trees. One of the assumptions concerns the asymmetry in APU physical locations. The main area in which this consideration might be significant is in spatial interactions -- that is, in the area of cascading

failure of an APU following the failure of some other APU. It was decided to simplify the analysis by assuming that the APUs are symmetrical with respect to physical location. That is, all APUs are assumed to be co-located together in the aft compartment in the same way that APU 1 and APU 2 are co-located. This is a conservative assumption. Because of this assumption, there is no uniqueness to the names of the APUs. Thus, if an unidentified, unnamed APU fails in conjunction with one of the top events in the event tree (call that Event E1), then that failed APU can be "named" APU 3 without any loss of generality. The actual name of that failed APU is of no importance in determining probabilities.

Consider now some other top event (call it E2) that appears to the right of event E1 in the event tree. Fault tree models can now be constructed for event E2 in which the failed APU 3 does not appear. This represents a great simplification in the modeling process.

Another simplifying assumption is that the failure of either isolation valve to close for APU shutdown is a permanent failure. This represents a slight conservatism with respect to the potential recovery procedures allowed in Flight Rule 10-11C, but it greatly simplifies the analysis process. Were it to have been found that this failure mode yielded a significant contribution to LOC/V, then the models could have been changed to reflect the recovery process allowed in the flight rules and the calculations revised to show the effect.

6.5.3 Treatment of Exhaust Duct Leakage

After some preliminary modeling and quantification of exhaust duct leakage, it was concluded that exhaust duct leakage would be a negligible contributor to loss of crew or vehicle. The reasons for this are as follows:

a. The frequency of occurrence of exhaust duct leakage either from shrapnel or from random failure is very low (approximately one occurrence in one hundred thousand hours of APU operation).

b. Exhaust duct leakage does not constitute loss of the APU.

c. The probability of failure of an APU or of flight critical equipment in the aft compartment as a consequence of exhaust gas impingement is quite low (between one in one hundred and one in one thousand per leak).

d. Therefore, it was expected that a LOC/V due to exhaust gas leak would occur approximately once in ten million missions.

Rather than produce a detailed quantification for such a remote occurrence, the effort was simplified and the frequency of all scenarios associated with exhaust duct leaks was assessed as negligible, even though a detailed model had already been developed.

6.5.4 Treatment of Dependencies in the Split Fraction Models

Prior experience shows that common cause failures tend to be important risk contributors because multiple failures can occur as a result of a single failure condition common to two or more units. Usually this is at a substantially higher probability than that associated with multiple independent failures. Hence, it was important to include such potential contributors wherever they were indicated by the recorded APU and HPU failure history databases.

In most cases the fault trees are intended to provide probabilistic results that serve directly as the split fractions for their associated top events. In some cases, however, the fault trees provide intermediate results that must be combined with other models to obtain the required top event split fractions. For example, two consecutive top events in the event tree in Figure 6.4.1 are labeled PA and DA. PA represents the event in which one or more APUs have a permanent failure, while DA represents the event in which at least two APUs fail given that at least one has failed. The fault tree for PA yields the associated split fraction directly. However, the fault tree for DA yields the probability of at least two APU failures. To obtain the split fraction for the DA event, divide the DA result by the PA result, thereby giving the probability of two or more APU failures given that one or more failures are known to have occurred. This type of analysis also applies to the top events HA and GA in that same event tree.

6.5.5 Treatment of Order of Occurrence in the Models

Event trees are simply logic diagrams that indicate what specific combinations of events occur and do not occur; such trees do not ordinarily convey any information as to the order in which events occur. Thus, the fault tree models have to be carefully constructed to account for order, when order is of concern. For example, in the Stage A event tree shown in Figure 6.4.1, there

are top events labeled TA and DA. TA accounts for the potential for a turbine runaway, and DA accounts for the possibility of a second independent permanent failure of an APU. Since the TA event appears first in the event tree, the fault tree for it models the potential for a runaway of one out of three APUs.

The DA event must then consider the implications of the order in which the two events occur. If the TA event occurs first (which is taken to occur with a probability of 50%), then the TA analysis based on one APU failing out of three is correct, and the DA fault tree must consider the potential for one APU to fail out of two APUs (because the third APU, which is named APU 3, has already failed by runaway). However, if DA occurs first (with a probability of 50%), then the DA fault tree must be based on one out of three failing, and the TA fault tree should be based on one out of two. Since the TA analysis is already based on one out of three, a correction factor must be included in the DA fault tree to correct from the 1-out-of-3 TA analysis to the proper 1-out-of-2 basis needed for TA in this case. In summary, some complexity is added to the fault trees to accurately account for the order in which top events in the event tree could occur. Such correction factors will be found below in a number of the fault trees, and the "secondary" fault trees needed to cover the 1-out-of-2 case for TA (and other such top events) are also presented below. The specific TA/DA case mentioned here is discussed with the appropriate fault trees below.

6.5.6 Nomenclature

A special naming convention has been used in all of the fault trees. The first two characters of the event names are the same as the two characters in the top event for which the fault tree was developed. For the basic events, the third and fourth characters identify the type of component being modeled, and the fifth character identifies the particular failure mode. For the gates, the third, fourth, and fifth characters identify the level of the gate in the fault tree and distinguish gates at each level. The last (sixth) character is 1, 2, or 3 to identify the specific APU in which the component or gate resides. If the last character is a 0, then it identifies a generic component or gate -- that is, something (such as a common cause failure) not associated with any specific APU.

To simplify the general appearance of the fault trees, they are shown in full only for APU 1. That detailed development is shown as a transfer with a label of the form XY1. The other two APUs are then represented as transfers in with labels of the form XY2

and XY3. In those subtrees, all gates and basic events in the subtree XY1 that end with a 1 are converted to a 2 or a 3 for the corresponding subtrees XY2 and XY3, respectively.

The paragraphs that follow are divided into two main parts -- one for the APU Stage A analysis, and one for the APU Stage B analysis.

6.5.7 Stage A Analysis

Top Event TA: Turbine Overspeed

The first top event in the Stage A Event Tree shown in Figure 6.4.1 is TA. This event represents a specific type of APU permanent failure -- namely, one involving turbine runaway, where failures cause the turbine speed to increase above normal operating levels and the overspeed protection system fails to shut the turbine down. This particular failure mode has been separated from all of the other permanent failures because of the high potential for consequential failure of other APUs or flight-critical equipment due to the high-energy shrapnel generated by the overspeed.

The fault trees developed for TA are shown in Appendix B6.5-1 and B6.5-2. The first fault tree (labeled TA) covers the model for the case of one runaway out of three APUs, while the second (labeled TA-D) models the case of one runaway out of two APUs. The second fault tree is provided to support top events to the right in the event tree where the order in which events occur is a consideration.

Both fault trees model runaway in terms of having both the primary and secondary control valves failing open, together with failure of the overspeed protection system to shut down the APU and prevent the runaway condition. The numerical result computed from fault tree TA directly yields the requisite split fraction for the top event TA in the event tree.

Top Event PA: Equipment Failure of 1 APU After it Starts

The second top event in the Stage A Event Tree shown in Figure 6.4-1 is PA. This event represents all but two contributors to the permanent failure of at least one of the three APUs. The two exceptions are (1) the turbine runaway failures covered by TA, and (2) the start failures, which are more conveniently analyzed in the Top Event BA (the failures occurring before lift-off and contributing to launch scrub).

The fault trees developed for PA are provided in Appendices B6.5-3 and B6.5-4. The first fault tree (labeled PA) models the permanent failure of at least one out of three APUs, while the second one (labeled PA-T) models the permanent failure of at least one out of two APUs. This second fault tree is provided to support top events to the right of event PA in the event tree where the order in which events occurs is a consideration.

Both PA fault trees model permanent failures in terms of the following primary failure modes:

a. Fuel line blockage
b. Fuel pump failure
c. Low fuel tank pressure
d. Turbine fails to run
e. Turbine wheel shutdown failure
f. Gearbox fails to run
g. Gas generator run failure
h. Fuel tank isolation valves fail closed
i. Fuel depleted after shutdown
j. Common cause failure of lube oil circulation due to contamination

The numerical result computed from Fault Tree PA directly yields the requisite split fraction for the Top Event PA in the event tree.

Top Event DA: Failure of a Second APU After it Starts

The third top event in the Stage A Event Tree is DA. This event represents all but two contributors to the permanent failure of at least two of the three APUs, where the two exceptions are (1) the turbine runaway failures covered by TA, and (2) the start failures, which are more conveniently analyzed in the Top Event BA (the failures occurring before lift off and contributing to launch scrub). The only difference between this event and the event PA is that DA accounts for at least two out of three APUs failing, while PA accounts for at least one out of three APUs failing.

In the event tree, the PA event represents the probability of an independent permanent failure occurring in at least one APU, and the DA event represents the probability of an independent permanent failure occurring in at least two APUs given that at least one is known to have occurred. The scenario in which PA occurs and DA does not occur represents the case in which exactly

one APU has an independent permanent failure. The scenario in which both PA and DA occur represents the case in which two or more APUs have independent permanent failures. When the TA event occurs in the event tree, only the DA event is questioned with regard to the occurrence of a second permanent failure as a result of an independent cause. In this case, it is not addressed via Event PA. This is simply an analysis convention that was adopted for convenience; this situation could just as well have been addressed by using PA.

The fault trees developed for DA are shown in Appendices B6.5-5 through B6.5-7. Appendix B6.5-5 is the fault tree DA1 that applies to the first (uppermost) node for DA in the event tree and models the permanent failure of at least two out of three APUs. Appendix B6.5-6 is the Fault Tree DA2 that applies to the second (lower) node for DA in the event tree. This models the second permanent failure that occurs in conjunction with the turbine runaway failure modeled by the TA event, and the fault tree is in the same basic form as the PA Fault Tree. The Fault Tree DAT in Appendix B6.5-7 models the case of two permanent failures out of two APUs, which is provided to support top events to the right of event DA in the event tree where the order in which events occur is a consideration.

The fault tree for DA2 in Appendix B6.5-6 is the first illustration of the logic required to account for the order in which events occur, as discussed in Section 6.5.1. If event TA occurs first, then the TA 1-out-of-3 fault tree model is correct, and the DA logic must consider 1-out-of-2 failure logic. This situation is shown on the right side of the diagram in Appendix B6.5-6. If, on the other hand, DA occurs first, then the TA 1-out-of-3 logic must be corrected to 1-out-of-2 logic, and the correct logic for DA is 1-out-of-3. This situation is shown on the left side of that diagram. The correction factor represented by the basic event DATCF0 is the ratio of the result from the TA-D tree to that from the TA tree.

All of the fault trees needed for the DA event model permanent failures in terms of the following primary failure modes:

a. Fuel line blockage
b. Fuel pump failure
c. Low fuel tank pressure
d. Turbine fails to run
e. Turbine wheel shutdown failure
f. Gearbox fails to run
g. Gas generator run failure

h. Fuel tank isolation valves fail closed
i. Fuel depleted after shutdown through a gearbox shaft seal
j. Common cause failure of lube oil circulation due to contamination

The numerical result from Fault Tree DA1 in Appendix B6.5-5 must be divided by the numerical result from Fault Tree PA to obtain the split fraction needed for node 1 for the event DA; this split fraction is the conditional probability of two or more permanent failures given that one or more permanent failures have occurred. The numerical result computed from Fault Tree DA2 in Appendix B6.5-6 directly yields the requisite split fraction for node 2 of Top Event DA in the event tree.

Top Event CA: Failure of a Second APU or Flight Critical Equipment Due to Failure of the First APU

The fourth top event in the Stage A Event Tree is CA. This event represents the consequential permanent failure of flight critical equipment or of at least one APU following the permanent failure of one other APU.

The CA fault tree is shown in Appendices B6.5-8 and B6.5-9. Appendix B6.5-8 is the Fault Tree CA1 that applies to the first (uppermost) node for CA in the event tree and models the consequential failure of flight critical equipment or of at least one other APU following the nonrunaway permanent failure of one APU (from Event PA). Appendix B6.5-9 is the Fault Tree CA2 that applies to the second (lower) node for CA in the event tree. This models the consequential permanent failure of flight critical equipment or of at least one other APU following a turbine runaway failure (from Event TA). Separate fault trees are required because the potential for consequential failure following a turbine runaway is higher than that for other forms of permanent failure. The numerical results computed from both Fault Trees CA1 and CA2 directly yield the requisite split fractions for nodes 1 and 2 of Top Event CA in the event tree.

Top Event HA: Failure of One APU Due to Exhaust Gas Leak

The fifth top event in the Stage A Event Tree is HA. This event represents the failure of at least one APU as a consequence of an exhaust gas leak in at least one APU. The model is based on the realization that the potential for a non-leaking APU to fail is extremely remote. Thus, the model only accounts for failures of APUs that are themselves experiencing hot gas leaks. This is also a very low frequency, as described earlier.

The fault trees developed for HA are shown in Appendices B6.5-10 and B6.5-11. The first fault tree, HA1, models the permanent failure of at least one out of three APUs as a consequence of exhaust gas leaks, while the second, labeled HAT, models the permanent failure of at least one out of two APUs as a consequence of exhaust gas leaks. This second fault tree is provided to support top events to the right of event HA in the event tree where the order in which events occurs is a consideration.

The numerical result computed from Fault Tree HA1 directly yields the requisite split fraction for the Top Event HA in the event tree.

Top Event GA: Failure of a Second APU or Flight-Critical Equipment Due to Exhaust Gas Leak

The sixth top event in the Stage A Event Tree is GA. This event represents the failure of at least two APUs as a consequence of exhaust gas leaks in at least two APUs, given that at least one APU is known to have failed as a consequence of a hot gas leak. The model is based on the realization that the potential for a non-leaking APU to fail is extremely remote. Thus, the model only accounts for failures of APUs that are themselves experiencing hot gas leaks.

The fault trees developed for GA are shown in Appendices B6.5-12 through B6.5-16. Appendices B6.5-12 through B6.5-15 show four different fault trees. The numerical results computed from the four fault trees are used in the same manner, as described above, for event DA to provide the requisite split fractions for the four nodes of Top Event GA in the event tree. The Fault Tree GAT shown in Appendix B6.5-16 is used in the same manner as described above for Fault Tree DAT for event DA.

Top Events L1, L2, L3: Leakage of Hydrazine From APU 1, 2, or 3

The seventh, eighth, and ninth top events in the Stage A Event Tree shown in Figure 6.4.A are Lk, where k can be 1, 2, or 3. This event represents the independent occurrence of a fuel leak in APU k. Rather than consider the logic for these three top events in terms of a fault tree or a set of three fault trees, it was much simpler to express the logic in terms of a simple event tree as a means of representing the probability values needed for the various combinations of leakage occurrences. Event Tree LK is shown in Appendix B6.5-17. The split fraction to be used for each node for each top event is shown at that

node. Lambda represents the failure rate with which independent leakage occurs, and "t" is the time interval of interest over which the leak can occur. Beta represents a common cause factor, which is a measure of the conditional probability that a second APU has a fuel leak given that one is already known to be leaking. Lambda and beta can both be derived from the Shuttle flight history data, as discussed in Section 7.0.

An important characteristic of the split fraction formulas given for the various nodes in Appendix B6.5-17 is that the scenario probabilities shown for all scenarios involving exactly one leaking leaking APU are all identical. The same is true for the scenarios with exactly two leaking APUs. Also, the sum of the probabilities for all eight scenarios is exactly one.

Using the leakage split fractions listed is simply a matter of matching the nodes in that figure with the corresponding nodes in the event tree in Figure 6.4.1. That is, the split fraction P21 for node 1 of the event L2 is matched to all nodes in the event tree for which L2 occurs when L1 does not occur. Likewise, the split fraction P22 for node 2 of the event L2 is matched to all nodes in the event tree for which L1 does occur. A similar approach is used for the nodes for L3.

Top Event FA: Failure of Flight-Critical Equipment Due to Hydrazine Leakage

The tenth top event in the Stage A Event Tree is FA. This event represents the permanent failure of flight critical equipment as a direct consequence of a fuel leak in one or more APUs. No fault tree was constructed for this event since the requisite split fraction is simply one number that depends only on the specific leakage conditions for the scenario being analyzed. The development of those single split fractions is discussed in Section 7.0.

Top Events C1, C2, C3: Failure of 1 APU Due to Hydrazine Leakage

The eleventh, twelfth, and thirteenth top events in the Stage A Event Tree are Ck, where k can be 1, 2, or 3. This event represents the consequential failure of APU k due to a fuel leak in one of the APUs (the leak can be in APU k, in some other APU, or in some combination of both -- the specific condition depending entirely on the particular event tree scenario being analyzed).

A generic fault tree applicable to all of the Ck event tree nodes is presented in Appendix B6.5-18. The numerical result computed

from Fault Tree Ck directly yields the requisite split fraction for the appropriate nodes of Top Event Ck in the event tree.

Top Events S1, S2, S3: Spurious Shutdown of APU 1, 2, or 3

The fourteenth, fifteenth, and sixteenth top events in the Stage A Event Tree are Sk, where k can be 1, 2, or 3. This event represents a specific type of APU recoverable failure -- namely, one involving a spurious overspeed or underspeed trip of the turbine in APU k. This condition causes an immediate, automatic shutdown of the affected APU, but that APU can be recovered during Stage B by setting the associated automatic over/underspeed control switch to the inhibit position. This particular failure mode has been separated from all of the other recoverable failures because of the immediate, automatic loss of the affected APU (recoverable failures from fuel leakage do not result in immediate, automatic shutdown of the affected APU).

The generic fault tree developed for Sk is shown in Appendix B6.5-19. This diagram, like others described previously, takes event occurrence order into account in those scenarios in which some other failure is identified as occurring in conjunction with the spurious overspeed or underspeed trip. If the other failure occurred first (with 50% probability), then the occurrence of the spurious trip requires a failure of the inhibit circuitry. If the spurious trip is first, then the inhibit circuitry is considered not to have been activated. The basic event DARAT0 provides the necessary factor for correcting the probability obtained from the other event in the event tree, in the same manner as described previously. The numerical result computed from Fault Tree Sk directly yields the requisite split fraction for the Top Event Sk in the event tree.

Top Event BA: Failure of One or Two APUs Before Launch

The seventeenth top event in the Stage A Event Tree is BA. This event represents a correction factor to distinguish between failures occurring before and after lift-off. The prior events in the event tree account for all run failures, regardless of the time at which they occur while the APUs are running. Failures occurring before lift-off ordinarily result in launch scrub, while failures occurring afterward can result in a variety of damage states, depending on their severity.

The fault tree developed for BA is presented in Appendices B6.5-20 and B6.5-21. Two trees are shown: one (labeled BA0 in Appendix B6.5-20) that applies only to the first node for the BA event in

the event tree and the other (labeled BAn in Appendix B6.5-21) that applies to all other nodes. The BA0 fault tree accounts for all start failures which are not otherwise taken into account in the fault trees developed for all other top events in the event tree. Start failures, of course, all occur before lift-off and are, therefore, prelaunch failures that ordinarily lead to launch scrub. Such failures are not considered elsewhere in the event tree logic. The BAn fault tree accounts for the start failures and the proportion of run time that constitutes the pre-lift-off period. This is a simple time ratio--the ratio of pre-launch run time to the total Stage A run time. The pre-launch run time is 5 minutes, while the post-launch Stage A run time is 13 minutes, yielding a ratio of R = 5/18 for scenarios in which one APU has failed. The ratio becomes $2R - R^2$ for scenarios in which two APUs have failed. The numerical result computed from Fault Tree BA directly yields the requisite split fraction for Top Event BA in the event tree.

Top Events EA, MA: Failure Occurs in Thrust Bucket, and Failure Occurs After MECO

The eighteenth and nineteenth top events in the event tree are EA and MA. These events identify failures that occur in the thrust bucket (EA) and post MECO (MA). These are, like the event BA, simply time ratios. The event EA is the ratio of time in the thrust bucket to the total Stage A run time. The time in the thrust bucket is about 0.5 minutes, and the total Stage A run time is 18 minutes. This gives a ratio of 0.5/18, or 0.028, for the numerical value of the split fraction for the event EA. The run time following MECO is approximately 5 minutes, which gives a ratio of 5/18, or 0.28, for the numerical value of the split fraction for event MA.

Top Event IA: Intact Abort Called by MCC

The last top event in the event tree is IA. This event identifies failures that, in the judgment of ground personnel and the flight crew, cannot support landing at the first PLS, thereby resulting in an intact abort. This is a judgment call made by MCC at the time that the failure occurs. It is beyond the scope of this study to evaluate in-flight decisions made by MCC. Therefore, a conservative (50 - 50) chance that this event would lead to an intact abort was assigned. Although this may be conservative, it does not significantly affect the overall frequency of intact aborts, which is dominated by failure in the thrust bucket.

6.5.8 Stage B Analysis

As discussed in Section 6.4.1, the analysis of the Stage A Event Tree leads to quite a few damage vectors. However, these damage vectors were combined into four damage bins that form the initial conditions for the analysis of Stage B. These four initial conditions for the Stage B analysis are defined in Table 6.4.1.

The Stage B Event Trees were developed for damage bins 4 and 7, as discussed in Section 6.4. Each damage bin constitutes the initial condition for a Stage B quantification. Each event tree has potentially different split fraction models that form the basis for quantifying that event tree.

Before discussing the individual initial conditions, it is appropriate to discuss certain considerations that apply to all of the initial conditions. In many cases, the fault trees needed for the Stage B analyses are the same or very nearly the same as the corresponding fault trees for Stage A. In all such cases, the primary emphasis in the discussions that follow is to identify the differences between the fault trees for those two stages. The recovery Event (RE) at the end of the Stage B Event Trees refers to recovery from failures that occur during Stage B; recovery from Stage A failures is taken into account in the fault trees in a manner consistent with the flight rules. In Stage A, start failures were included in the Event BA as a basis for identifying launch scrub conditions. In Stage B, all start failures are taken into account at the beginning of the event trees, in Top Events SS and DS. Start and run failures were separated so that the time ratios used in events like TE and PW could be applied solely to probabilities that are time-based, with no demand failures involved. Since the PB and DB Events account for all run failures for the full duration of Stage B, there is no need to include run failure considerations in the fault trees for the RE Event; only failures to restart on demand (if required) need be considered in RE. For initial conditions other than Bin 7 (also called Impact Vector 1), the Stage B analysis is begun with at least one APU failure (either permanent or recoverable) having occurred during Stage A. Under such circumstances, the over/underspeed auto trip switch would have been set to inhibit automatic shutdown. This means that spurious conditions which would otherwise cause an automatic shutdown of the affected APU (such as MPU 1 failing high or low) would be inhibited and, thereby, prevent shutdown from occurring. However, if there is a failure of the inhibit circuitry, then such a condition can still cause a spurious shutdown. In this

case, such a shutdown is a permanent failure because there is no way to inhibit the faulty signal. Such contributions to permanent failure have been included in the SB Fault Tree. One final comment about the analysis of Impact Vector 1. For all scenarios involving Mk (fuel leak) and Tk (spurious automatic shutdown), the analysis has been simplified by conservatively assuming that the leak occurs first, which means that the spurious trip is a permanent failure.

6.5.8.1 Initial Condition 7 (Impact Vector 1)

Based on the discussion in Section 6.4, initial condition 7 (from Damage Bin 7) is defined as follows:

All three APUs successful at the end of Stage A

The fault trees developed to support the associated event tree in Appendix B6.4-2 for this initial condition are discussed below. This initial condition is referred to in the fault tree diagrams as Impact Vector 1.

Top Event SS: One APU Fails to Start

The first top event in the Stage B Event Tree is SS. This event represents a specific type of APU permanent failure -- namely, failure of one or more APUs to start on demand. This particular failure mode had to be separated from the run failures covered by Top Events PB and DB so that the time ratios used in Top Events TE and PW would be applied only to run-time failures and not to a combination of run-time and demand failures.

The fault tree developed for SS is shown in Appendix B6.5-22. This diagram is essentially the same as the one developed for the start failures in the Top Event BA for Stage A, with a few exceptions as described below. In Stage A, any kind of failure of the primary valve was considered grounds for scrubbing the mission, including cases in which the primary valve fails open. In Stage B, however, such conditions (the valve failing open) would not cause start failure because the secondary valve would begin cycling and take over control of fuel flow.

The other change was to remove the basic event in which the secondary valve leaks before APU startup. If that happens, fuel leaks into the gas generator and causes it to heat up. In that case, the APU is not started because of the danger of fuel

detonation. In Stage A, that leads to launch scrub. In Stage B that simply delays startup of the APU until the injector spray system can cool the temperature down to an acceptable level. Thus, this would not be a failure unless another.APU fails and either the injector spray cooling system fails or the APU fails to start for some other reason. This third-order failure scenario was judged to be of too low a probability to be of any practical concern and was removed from the analysis.

The numerical result computed from the Fault Tree SS directly yields the requisite split fraction for the Top Event SS in the event tree.

Top Event DS: Second APU Fails to Start

The second top event in the Stage B Event Tree is DS. This event represents a specific type of APU permanent failure -- namely, failure of two or more APUs to start on demand. This particular top event is used in conjunction with the top Event SS to be able to distinguish between cases in which only one start failure occurs versus cases in which two or more failures occur.

The fault tree developed for DS is shown in Appendix B6.5-23. This diagram is essentially the same as the one developed for Top Event SS except that the simple OR gate for the top event has been changed to a 2-out-of-3 gate. All other aspects of the fault tree are exactly the same.

The numerical result computed from the Fault Tree DS must be divided by the numerical result from Fault Tree SS to obtain the split fraction needed for the Top Event DS; this split fraction is the conditional probability of two or more start failures, given that one or more start failures are known to have occurred.

Top Event TB: Turbine Overspeed

The third top event in the Stage B Event Tree is TB. This event represents a specific type of APU permanent failure--namely, one involving turbine runaway, where failures cause the turbine speed to increase above normal operating levels and the overspeed protective system fails to shut the turbine down. This particular failure mode has been separated from all of the other permanent failures because of the high potential for consequential failure of flight-critical equipment or other APUs due to the high-energy shrapnel and subsequent hydrazine release generated by the overspeed.

The fault trees developed for TB are presented in Appendices B6.5-24 through B6.5-26. Appendix B6.5-24 presents the fault tree (labeled TB1) that applies to the first (uppermost) node for TB in the event tree and models a turbine runaway failure of at least one out of three APUs. Appendix B6.5-25 presents the fault tree (labeled TB2) that applies to the second (lower) node for TB in the event tree. This models a turbine runaway failure that occurs after an APU start failure (Event SS). The fault tree in Appendix B6.5-26 models the case of one turbine runaway out of two APUs, which is provided to support top events to the right of Event TB in the event tree where the order in which events occur is a consideration.

The fault trees in Appendices B6.5-24 through B6.5-26 are identical to the corresponding fault trees developed for Stage A. The fault tree in Appendix B6.5-25 is identical to that in Appendix B6.5-26. The numerical results computed from Fault Tree TB directly yield the requisite split fractions for the two nodes of Top Event TB in the event tree.

Top Event PB: Equipment Failure of One APU After Start

The fourth top event in the Stage B Event Tree is PB. This event represents all but four contributors to the failure of at least one of the three APUs, where the four exceptions are: (1) the turbine runaway failures covered by TB, (2) the start failures, which are analyzed in Top Event SS, (3) leakage events, and (4) spurious shutdowns.

The fault trees developed for PB are presented in Appendices B6.5-27 and B6.5-28. The first fault tree (labeled PB) models the permanent failure of at least one out of three APUs, while the second one (labeled PB-T) models the permanent failure of at least one out of two APUs. This second fault tree is provided to support top events to the right of Event PB in the event tree where the order in which events occurs is a consideration.

The fault trees developed for the PB Top Event are essentially the same as those developed for Stage A. The major exception to this is the portion added to account for failures occurring during the on-orbit portion of the mission. These failures include heaters that fail on and heaters that fail off. The fault tree also includes fuel and lube oil leaks and the inadvertent hot restart of an APU.

The numerical result computed from Fault Tree PB directly yields the requisite split fraction for the Top Event PB in the event tree.

Top Event DB: Failure of Second APU After Start

The fifth top event in the Stage B Event Tree is DB. This event represents all but four contributors to the permanent failure of at least two of the three APUs, where the four exceptions are as identified for Top Event PB. The only difference between this event and the Event PB is that DB accounts for at least two out of three APUs failing, while PB accounts for at least one out of three APUs failing.

In the event tree, the PB Event represents the probability of an independent permanent failure occurring in at least one APU, and the DB Event represents the probability of an independent permanent failure occurring in at least two APUs, given that at least one is known to have occurred. The scenario in which PB occurs and DB does not occur represents the case in which exactly one APU has an independent permanent failure. The scenario in which both PB and DB occur represents the case in which two or more APUs have independent permanent failures. When either the SS or the TB Event occurs in the event tree, only the DB Event is questioned with regard to the occurrence of a second permanent failure as a result of an independent cause; that is, this case is not addressed via Event PB. This is simply an analysis convention that was adopted for convenience; this situation could just as well have been addressed by using PB.

In the above paragraph, the term "independent" refers to independence with respect to other top events in the event tree. That is, it is not intended to preclude the potential occurrence of common cause failures within the context of the PB and DB analyses themselves. It simply means that the PB and DB permanent failures have been modeled such that they are independent of other top events.

The fault trees developed for DB are shown in Appendices B6.5-29 through B6.5-32. Appendix B6.5-29 presents a fault tree (labeled DB1) that applies to the first (uppermost) node for DB in the event tree and models the permanent failure of at least two out of three APUs. Appendix B6.5-30 presents a fault tree (labeled DB2) that applies to the second (middle) node for DB in the event tree. This models the second permanent failure that occurs in conjunction with the turbine runaway failure modeled by the TB Event, and the fault tree is in the same basic form as the PB Fault Tree. Appendix B6.5-31 presents a fault tree (labeled DB3) that applies to the third (bottom) node for DB in the event tree and models the second permanent failure that occurs following a start failure in another APU. This fault tree is very similar

to that shown in Appendix B6.5-30, except that the other failure (failure to start) is definitely known to have occurred first, and this knowledge simplifies the model. The fault tree in Appendix B6.5-32 models the case of two permanent failures out of two APUs, which is provided to support top events to the right of Event DB in the event tree where the order in which events occur is a consideration.

The fault tree for DB2 is another illustration of the logic required to account for the order in which events occur, as discussed in Section 6.5.1. If Event TB occurs first, then the TB 1-out-of-3 fault tree model is correct, and the DB logic must consider 1-out-of-2 failure logic. This situation is shown on the right side of the diagram in Appendix B6.5-25. If, on the other hand, DB occurs first, then the TB 1-out-of-3 logic must be corrected to 1-out-of-2 logic, and the correct logic for DB is 1-out-of-3. This situation is shown on the left side of that figure. The correction factor represented by the Basic Event DBTCF0 is the ratio of the result from the TB-D Tree to that from the TB Tree.

The fault trees developed for the DB Top Event are essentially the same as those developed for Stage A. The only exception to this is the adaptation needed to address the added node for the case in which a start failure (via Top Event SS) occurs first, and this fault tree is very similar to the DB2 Fault Tree. Since the DB Fault Tree depends on the subtrees for each separate APU in the PB Event, it follows that the DB Event also automatically includes the on-orbit additions described above for the PB Event.

The numerical result from Fault Tree DB1 must be divided by the numerical result from Fault Tree PB to obtain the split fraction needed for Node 1 for the Event DB; this split fraction is the conditional probability of two or more permanent failures given that one or more permanent failures are known to have occurred. The numerical result computed from Fault Trees DB2 and DB3 directly yield the requisite split fractions for Nodes 2 and 3 of Top Event DB in the event tree.

Top Event CB: Failure of the Second APU or Failure of Flight Critical Equipment Initiated By Failure of the First APU

The sixth top event in the Stage B Event Tree is CB. This event represents the consequential permanent failure of flight critical equipment or at least one APU following the permanent failure of one other APU.

The CB Fault Tree is presented in Appendices B6.5-33 through B6.5 35. Appendix B6.5-33 presents a fault tree (labeled CB1) that applies to the first (uppermost) node for CB in the event tree and models the consequential failure of flight critical equipment or of at least one other APU following turbine break-up of one APU at normal speed (Event PB). Appendix B6.5-34 presents a fault tree (labeled CB2) that applies to the second (middle) node for CB in the event tree. This models the consequential permanent failure of flight critical equipment or at least one other APU following a turbine runaway failure (Event TB). Appendix B6.5-35 presents a fault tree (labeled CB3) that applies to the third (lowest) node for CB in the event tree and models the consequential failure of flight critical equipment or at least one other APU following permanent start failure of one APU (Event SS). Separate fault trees are required for the various nodes because the potential for consequential failure following a turbine runaway is higher than for permanent failures taken into account in the PB Event, and the probability of consequential failure following start failures is assessed to be negligibly small. The numerical results computed from the CB Fault Trees directly yield the requisite split fractions for Nodes 1 through 3 of Top Event CB in the event tree.

Top Event HB: Failure of One APU Due To Exhaust Gas Leak or GGVM Detonation

The seventh top event in the Stage B Event Tree is HB. This event represents the failure of at least one APU as a consequence of an exhaust gas leak in at least one APU, or as a consequence of external fuel leakage produced by a detonation resulting from fuel leaking into the solenoid cavity of either GGVM valve.

The model for the first part is exactly the same as that developed for Stage A. The second part was not included in the Stage A analysis because it was judged to be a very low likelihood event during that part of the mission because of its very short duration. It would take time for the fuel to leak into the solenoid cavity and for the subsequent fuel decomposition and detonation to occur. For Stage B, however, it has a higher likelihood of occurrence because of the longer duration--most particularly during the long on-orbit period. Because of the knowledge acquired concerning the very low likelihood of failure as a consequence of exhaust gas leaks, it became clear that Event HB is dominated by the solenoid detonation event.

There are two classes of solenoid detonation events that can occur. One involves the GGVM; the other, the isolation valves. In the case of the GGVM, the consequential external fuel leakage

is smaller (because of closed isolation valves) and is much more apt to result in failure of only the leaking APU. In the case of the isolation valves, the consequential external fuel leakage is much more massive (coming directly from the fuel tank because of the inability to isolate the leak) and is expected to fail more than just the leaking APU. Based on these considerations, it seemed reasonable to cover the GGVM case in the Event HB, which addresses single APU failures, and to include the isolation valve case in Event GB, which covers multiple APU failures.

The fault trees developed for HB are presented in Appendices B6.5-36 through B6.5-40. Appendix B6.5-36 presents a Fault Tree (labeled HB1) that applies to the first (uppermost) node for HB in the event tree and models the permanent failure of at least one out of three APUs as the primary consequence of an external fuel leak caused by detonation in the GGVM as a result of fuel leakage into one of the two solenoid cavities.

Appendix B6.5-37 presents a fault tree (labeled HB2) that applies to the second node for HB in the event tree. This models, in conjunction with another permanent failure (from Event PB), the permanent failure of a second APU as the primary consequence of an external fuel leak caused by detonation in the GGVM because of fuel leakage into one of the two solenoid cavities.

Appendix B6.5-38 presents a fault tree (labeled HB3) that applies to the third node for HB in the event tree and models, in conjunction with a turbine runaway failure (from Event TB), the permanent failure of a second APU as the primary consequence of an external fuel leak caused by detonation in the GGVM because of fuel leakage into one of the two solenoid cavities.

Appendix B6.5-39 presents a fault tree (labeled HB4) that applies to the fourth node for HB in the event tree. This models, in conjunction with a permanent start failure of one APU (from Event SS), the permanent failure of a second APU as the primary consequence of an external fuel leak caused by detonation in the GGVM because of fuel leakage into one of the two solenoid cavities.

Separate fault trees are required for the various nodes to properly account for the order correction factors. The exhaust-gas-leak portions of the event trees are exactly the same as those developed for Stage A. The new fuel-leak portions simply identify the ways in which fuel can leak into the solenoid cavities and account for the resultant potential for detonation.

The numerical results computed from the HB Fault Trees directly yield the requisite split fractions for the various nodes for the HB Event.

Top Event GB: Failure of Flight Critical Equipment or Second APU Due to Exhaust Gas Leak or Valve Detonation

The eighth top event in the Stage B Event Tree is GB. This event represents the failure of at least two APUs as a consequence of an exhaust gas leak in at least two APUs, or as a consequence of massive external fuel leakage produced by a detonation resulting from fuel leaking into the solenoid cavity of one of the isolation valves in an APU.

The model for the first part is exactly the same as that developed for Stage A. The second part was not included in the Stage A analysis because it was judged to be a very low likelihood event during that part of the mission because of its very short duration. It would take time for the fuel to leak into the solenoid cavity and for the subsequent fuel decomposition and detonation to occur. For Stage B, however, it has a higher likelihood of occurrence because of the longer duration of the on-orbit period. Because of the knowledge acquired concerning the very low likelihood of failure as a consequence of exhaust gas leaks, it became clear that Event GB is dominated by the solenoid detonation event.

As discussed for the HB Event, there are two classes of solenoid detonation events that can occur. One involves the GGVM, the other the isolation valves. In the case of the GGVM, the consequential external fuel leakage is smaller and is much more apt to result in failure of only the leaking APU. In the case of the isolation valves, the consequential external fuel leakage is much more massive (coming directly from the fuel tank) and is expected to fail more than just the leaking APU. For scenarios involving both the HB and GB Events, those two events can most reasonably be treated as separate, independent events. That is, the numerical result from the GB quantification directly provides the requisite split fraction for the Top Event GB in the event tree (which is considered acceptable because the exhaust gas leak probabilities are so very small with respect to the solenoid detonation considerations).

The fault trees developed for GB are presented in Appendices B6.5-41 through B6.5-46. Appendices B6.5-41 through B6.5-45 present five different fault trees to support scenarios involving no other failures to the left of it in the event tree and Events HB, PB, TB, and SS. These fault trees are very similar to those developed for

the Event HB. The numerical results computed from those five fault trees provide the requisite split fractions for the five nodes of Top Event GB in the event tree. No conditional probabilities are computed as was done in the Stage A analysis. The Fault Tree GB-T presented in Appendix B6.5-46 is used in the same basic manner as described above for Fault Tree DB-T for Event DB.

Top Events M1, M2, M3: Hydrazine Leakage from APU 1, 2, or 3

The ninth, tenth, and eleventh top events in the Stage B Event Tree presented in Figure 6.4.2 are Mk, where k can be 1, 2, or 3. This event was analyzed in exactly the same manner as was done for Stage A, and the event tree used for representing the requisite split fractions is shown in Appendix B6.5-47. To use the leakage split fractions listed in that appendix, it is simply a matter of matching those nodes in that figure with the corresponding nodes in the event tree in Figure 6.4.2. The Split Fraction P21 for Node 1 of the Event M2 is matched to all nodes in the event tree for which M2 occurs when M1 does not occur. Likewise, the Split Fraction P22 for Node 2 of the Event M2 is matched to all nodes in the event tree for which M1 does occur. A similar approach is used for the nodes for M3.

Top Event FB: Failure of Flight Critical Equipment Due to Spatial Interaction Initiated by Hydrazine Leakage

The twelfth top event in the Stage B Event Tree is FB. This event represents the permanent failure of flight critical equipment as a direct consequence of a fuel leak in one or more APUs. No fault tree was constructed for this event since the requisite split fraction is simply one number that depends only on the specific leakage conditions for the scenario being analyzed. The development of those single split fractions is discussed in Section 7.0.

Top Events D1, D2, D3: Hydrazine Leakage Causes Failure of APU 1, 2, or 3 Given That Two APUs Have Not Failed

The thirteenth, fourteenth, and fifteenth top events in the Stage B Event Tree are Dk, where k can be 1, 2, or 3. This event represents the consequential failure of APU k due to a fuel leak in one of the APUs. The leak can be in APU k, in some other APU, or in some combination of both. The specific condition depends entirely on the particular event tree scenario being analyzed.

A generic fault tree applicable to all of the Dk Event Tree nodes is presented in Appendix B6.5-48. This fault tree is exactly the same as that developed for the Stage A analysis.

Top Events R1, R2, R3: Leak in APU 1, 2, or 3 Before EI-13 or Into Pump Seal Cavity

The sixteenth, seventeenth, and eighteenth top events in the Stage B Event Tree are Rk, where k can be 1, 2, or 3. This event represents the shutdown of an APU because of a small fuel leak. Included in this category are all pump seal leaks. Also included are small leaks that occur before EI and are detected. The generic fault tree for this event is presented in Appendix B6.5-49. The probability that a leak occurs before EI given that a leak has occurred is taken to be a time ratio:

$$\frac{T_{EI} - T_{TIG-5}}{T_{SD} - T_{TIG-5}} \qquad \text{(SD = SHUTDOWN)}$$

This fraction is conservative (small) in that it is based on the time TIG-5 rather than some average of the start times from TIG-5 to EI-13. The value of this fraction is 25/66, or 0.38.

Top Events T1, T2, T3: Spurious Shutdown of APU 1, 2, or 3

The nineteenth, twentieth, and twenty-first top events in the Stage B Event Tree are Tk, where k can be 1, 2, or 3. This event represents an APU recoverable failure involving a spurious overspeed or underspeed trip of the turbine in APU k. This condition causes an immediate, automatic shutdown of the affected APU, but that APU can normally be recovered later during Stage B by setting the associated automatic shutdown switch to the inhibit position. This particular failure mode has been separated from all of the other recoverable failures because of the immediate, automatic loss of the affected APU.

The generic fault tree developed for Tk is shown in Appendix B6.5-50. This fault tree is essentially the same as that developed for the Stage A analysis.

Top Events TE, PW: Failure of at Least One APU After TAEM-3.5 Minutes; Failure of at Least One APU After Wheelstop

The twenty-second and twenty-third top events in the event tree are TE and PW. These events identify failures that occur during TAEM (TE) and post wheelstop (PW).

The split fractions for the TE Event simply involve time ratios. The specific manner in which the ratio is used depends on the specific scenario being analyzed. The fundamental probability (a time ratio) is defined as follows:

$$P_1 = \frac{T_{SD} - T_{TAEM-3.5}}{T_{SD} - T_{EI-13}} \qquad (SD = SHUTDOWN)$$

Based on this formula, the following expressions can be used to calculate the split fractions for the associated scenario conditions:

P_1 . . . . . 1 of 1 fails after TAEM
$2P_1 - P_1^2$ . . 1 of 2 fails after TAEM
P_1 . . . . . 2 of 2 fail after TAEM

The above estimates are conservative (high) in that they are based on EI-13 in the denominator instead of some average value between TIG-5 and EI-13. The value of the fundamental probability is taken to be 20.5/54, or 0.38.

In the case of PW, a simple time ratio can be used for scenarios having APUs failing for causes other than fuel leaks, while a more complex formulation is needed for scenarios involving fuel leaks. A simple time ratio is not adequate in the case of fuel leakage because of the time delay inherent in accumulating sufficient hydrazine in the aft compartment to cause damage given the onset of a leak. For cases involving a simple time ratio, the following fundamental probabilities are defined:

$$P_T = \frac{T_{SD} - T_{WS}}{T_{SD} - T_{TAEM-3.5}} \quad \text{. . . for failures occurring after TAEM-3.5}$$

$$P_F = \frac{T_{SD} - T_{WS}}{T_{SD} - T_{TIG-5}} \quad \text{. . . for all other failures}$$

Based on these formulas, the following expressions are used to calculate the split fractions for the associated scenario conditions:

P_T . . . . . 1 of 1 event that occurs after TAEM-3.5 also occurs after wheelstop

$2P_T - P_T^2$ . . 1 of 2 events that occurs after TAEM-3.5 also occurs after wheelstop

P_T^2 . . . . . 2 of 2 events that occur after TAEM-3.5 also occur after wheelstop

P_F . . . . . 1 of 1 event occurs after wheelstop

$2P_F - P_F^2$ . . 1 of 2 events occurs after wheelstop

P_F^2 . . . . . 2 of 2 events occur after wheelstop

The value of P_T is 10/20.5, or 0.49. The value of P_F is 10/66, or 0.15.

For cases requiring the more complex formulation (that is, when fuel leakage is involved), their bases can be described using the diagram presented in Appendix B6.5-51. The horizontal scale is a non-linear time scale. The vertical scale at the right indicates the total amount of fuel leaked, while the scale at the left indicates the total amount of leaking fuel accumulated in the aft compartment. The shaded region labeled T in the center represents uncertainty in the threshold amount of fuel required in the aft compartment to support combustion. Line L1 indicates a leak occurring on-orbit. In orbit, the vent doors are open, so leaking fuel can exit the aft compartment. It is not until after the vent doors are closed for deorbit that fuel can begin to accumulate in the aft compartment, as indicated by line A1. Line A1 intersects threshold region T at some point between TAEM and wheelstop, indicating that a fire would be expected to begin before wheelstop. Line A2 shows a leak occurring after EI. Hydrazine begins to accumulate in the aft compartment immediately. That line intersects the threshold region T after wheelstop, indicating that a fire is expected to be delayed until after wheelstop.

From this overview perspective, the PW split fraction is computed as follows:

$$\frac{T_O + T_{TAEM-3.5} - T_{TIG-5}}{T_O + T_{SD} - T_{TIG-5}} \times P_{WDWS} +$$

$$\frac{T_{SD} - T_{TAEM-3.5}}{T_O + T_{SD} - T_{TIG-5}} \times \frac{T_{SD} - T_{WS} + T_{BU}}{T_{SD} - T_{TAEM-3.5}}$$

The coefficient of PWDWS is the fraction of the total Stage B time that occurs before TAEM-3.5. PWDWS is the conditional probability that damage from a fuel leak occurs after wheelstop, given that the leak occurs before TAEM-3.5. The value for this probability was evaluated from the distribution presented in Appendix B6.5-52. This distribution was developed from a review of the leakage data in the database. The point estimate (mean) from this distribution is 0.7. In the second term, the first ratio represents the fraction of the total Stage B time that occurs after TAEM-3.5. The second ratio represents the fraction of the post-TAEM-3.5 time that a leak occurs late enough to permit the build-up delay of the fuel in the aft compartment to delay the consequential damage until some time after wheelstop. This build-up time, T_{BU}, was assessed to be about 4 minutes, based on an evaluation of available leakage information in the database.

Top Event RE: Failure to Recover APU When Needed For Landing

The last top event in the event tree is RE. This event covers failure to recover APUs that failed during Stage B. This includes failure to restart and detonation at restart. Run failures are covered by the PB and DB Events, and consequential failures due to fuel leaks are covered by the Dk Events.

Although there is one basic fault tree, there are three variations of it, based on the specific scenario being analyzed. These three forms are presented in Appendices B6.5-53 through B6.5-55; one for the case of small fuel leaks (REL), one for the case of a spurious shutdown (RES), and one for scenarios involving both a spurious shutdown and a small fuel leak (RELS).

6.5.8.2 Initial Condition 4 (Impact Vector 2)

Based on the discussion in Section 6.4, initial condition 4 (from damage bin 4) is defined as follows:

One APU permanently failed and one APU spurious shutdown during Stage A

The split fraction models discussed below support the event tree in Appendix B6.4-3 that was developed for this initial condition. The fault tree diagrams refer to this initial condition as Impact Vector 2.

Top Event DS: Second APU Fails to Start

The first top event in the Stage B Event Tree is DS. This event represents a specific type of APU permanent failure -- namely, failure of a second APU because of failure to start on demand.

The fault tree developed for DS is presented in Appendix B6.5-56. This diagram is essentially the same as the one developed for the start failures in the Top Event SS for Stage B, initial condition 7 (Impact Vector 1). The only difference from that model is that the top gate is based on 1-out-of-2 logic, rather than the 1-out-of-3 logic used for Impact Vector 1.

The numerical result computed from the Fault Tree DS directly yields the requisite split fraction for the Top Event SS in the event tree.

Top Event TB: Turbine Overspeed

The second top event in the Stage B Event Tree is TB. This event represents a specific type of APU permanent failure -- namely, one involving turbine runaway, where failures cause the turbine speed to increase above normal operating levels and the overspeed protection system fails to shut the turbine down.

The fault tree developed for TB is presented in Appendix B6.5-57. This model is essentially the same as that developed for Event TB for Stage B, Impact Vector 1. The only difference is that the top gate has 1-out-of-2 logic instead of the 1-out-of-3 logic used for Impact Vector 1. The numerical result computed from Fault Tree TB directly yields the requisite split fraction for the Top Event TB in the event tree.

Top Event DB: Failure of the Second APU After It Starts

The third top event in the Stage B Event Tree is DB. The fault tree developed for DB is presented in Appendix B6.5-58. This model is essentially the same as that developed for Event PB for Stage B, Impact Vector 1. The only difference is that the top gate has 1-out-of-2 logic instead of the 1-out-of-3 logic used for Impact Vector 1. The numerical result computed from Fault Tree DB directly yields the requisite split fraction for the Top Event TB in the event tree.

Top Event SB: Uninhibited Spurious Shutdown of at Least One APU

The fourth top event in the Stage B Event Tree is SB. This event represents a variation on a specific type of APU failure -- namely, one involving a spurious overspeed or underspeed trip of the turbine in APU k. While this condition causes an immediate, automatic shutdown of the affected APU, its effects for Impact Vector 2 in Stage B are quite different from those for Impact Vector 1 in Stage B. For Impact Vector 1, the automatic trip circuitry can subsequently be manually set to the inhibit position so that the APU can be started at a later time. For Impact Vector 2, however, that inhibit selection was made before any of the APUs were started for the entry phase of the mission. Thus, if a spurious shutdown occurs anyway, it means that the inhibit circuitry was not functioning properly and that the APU cannot be restarted. This instance of a spurious shutdown represents a permanent failure.

The fault tree developed for SB is presented in Appendix B6.5-59. This fault tree is similar to the fault tree for Tk in the analysis for Impact Vector 1, except that it has been changed to account for failure of the inhibit circuitry. The numerical result computed from Fault Tree SB directly yields the requisite split fraction for the Top Event SB in the event tree.

Top Event HB: Failure of One APU Due to Exhaust Gas Leak or GGVM Detonation

The fifth top event in the Stage B Event Tree is HB1. This model is essentially the same as that developed for Event HB for Stage B, Impact Vector 1. The only difference is that all failures of APU 3 have been deleted from the model. The numerical result computed from Fault Tree HB1 directly yields the requisite split fraction for the Top Event HB in the event tree.

Top Event GB: Failure of Flight Critical Equipment or a Second APU Due to Exhaust Gas Leak or Valve Detonation

The sixth top event in the Stage B Event Tree is GB0. This model is essentially the same as that developed for Event GB for Stage B, Impact Vector 1. The only difference is that hot gas leak of APU 3 (the name assigned to the APU that failed during Stage A) cannot occur, and that basic event has been deleted from the fault tree. However, since fuel can still leak into the solenoid cavities in the isolation valves of the failed APU, that basic event has been retained. The numerical result computed from

Fault Tree GB0 directly yields the requisite split fraction for the Top Event GB in the event tree.

Top Events M1, M2, M3: Hydrazine Leakage from APU 1, 2, or 3

The seventh, eighth, and ninth top events in the Stage B Event Tree are Mk, where k can be 1, 2, or 3. This event was analyzed in exactly the same manner as was done for Stage B, Impact Vector 1, and the event tree depicting all admissible states is presented in Appendix B6.5-62.

Top Event FB: Failure of Flight Critical Equipment Due to Spatial Interactions Initiated by Hydrazine Leakage

The tenth top event in the Stage B Event Tree is FB. This event represents the permanent failure of flight critical equipment as a direct consequence of a fuel leak in one or more APUs. No fault tree was constructed for this event since the requisite split fraction is simply one number that depends only on the specific leakage conditions for the scenario being analyzed. The development of those single split fractions is discussed in Section 7.

Top Event PW: Failure of at Least One APU After Wheelstop

The eleventh top event in the event tree is PW. This event is analyzed in exactly the same manner as discussed in the preceding TE and PW Events for Stage B, Impact Vector 1 (Initial Condition 7).

6.5.8.3 Initial Conditions 5 and 6 (Impact Vectors 3 and 4)

As discussed in Sections 6.4 and 8, the maximum possible collective contribution of both of these initial conditions to LOC/V is of the order of 1 per cent or less. Neither of these conditions can possibly make a dominant contribution to the risk of loss of crew or vehicle. Since little significant additional knowledge or insights can be gained by analyzing either of these two initial conditions, there is no need to develop the event trees or fault trees associated with either of these initial conditions, and no such trees are presented.

6.6 SPATIAL INTERACTIVE EVENTS (SIEs)

An SIE is a propagating failure within a system or a cascading failure into another system that results from an initiating

failure or condition by virtue of close proximity. To be an SIE, a consequential failure must also be initiated by means of a physical interactive mechanism such as hot gas or shrapnel that results from failure of or degraded operation of the system. Thus, a detonation of fuel in one APU Gas Generator Valve Module (GGVM) because of an exhaust leak in another APU is a spatial interactive event, whereas loss of an APU because of a secondary fuel valve failure to the closed position in the GGVM is not.

The split fraction representing an SIE is modeled as a conditional probability distribution as described in Section 5.4. The SIE split fractions discussed in this analysis are a subset of the set of all split fractions defined by the node points on the APU event trees.

Three types of SIEs have been identified as significant for this study. They are (1) events related to APU turbine breakup, (2) events related to APU fuel (hydrazine) leakage, and (3) events related to hot exhaust gas leakage. The impact of an SIE depends in some cases on the flight phase in which it occurs. In these cases, the conditional probability distributions modeling the split fraction will vary from one phase to the next. The three categories of SIEs are discussed in the paragraphs below.

6.6.1 Events Related to APU Turbine Breakup

The SIEs resulting from APU turbine breakup are those in which turbine fragments directly damage other APUs or flight critical equipment, or in which fuel leaking from the damaged APU then damages other equipment. Leaking fuel can cause contact corrosion, flames from decomposition, or flames from combustion. SIEs initiated by fuel leakage are discussed in 6.6.2. SIEs initiated by turbine fragments are reflected in the conditional probability distributions defined in Section 7.6.1, and are discussed below.

Turbine breakup can occur while the APU is operating in its normal design speed range or during an uncontrolled overspeed. A breakup at normal speed would result from installation of a seriously flawed turbine or from the propagation to critical size of a minute crack that was not detected in pre-installation inspection. Data to develop these failure frequencies are presented in Section 7.6. A breakup at overspeed would result when both fuel control valves fail to close on command. This could result from a failure in the valves themselves or in the APU controller. Data to develop these component failure frequencies are presented in Section 7.5.

The effects of an SIE initiated by turbine breakup depend on the energy level of the uncontained fragments, the likelihood of a fragment striking a piece of critical equipment, and the vulnerability of that equipment to damage. The energy level of the uncontained fragments is determined by the speed at which the turbine breaks up and by the energy absorbed in breaking out of the APU housing. Uncontained fragments from turbine breakup at normal speeds would, therefore, have significantly lower energy levels than fragments from an overspeed breakup. The APU housing design is a factor as well. The containment ring on the HPU is 26% larger than that on the APU. For this reason, the energy levels of uncontained fragments from the APU are significantly higher than those from the HPU.

Determining the likelihood of a fragment striking a piece of critical equipment is a complex analytical task, but for which Monte Carlo-based techniques have been developed. The aft compartment is extremely crowded with not only APU fuel lines and tanks, but with LH_2 and LO_2 feedlines, avionics bays, hydraulic lines and numerous wiring harnesses. The probability distribution to describe this likeli-hood was, therefore, based on all available knowledge including test and analytical data and was developed subjectively, using the process described in Sections 5.8 and 7.6.

The vulnerability of equipment to damage is determined by the fragility of the equipment compared to the possible energy levels of the fragments.

Shrapnel may be generated by means other than turbine breakup, such as APU fuel detonation in a fuel line or from a gearbox failure. These possibilities were also evaluated and were not considered significant.

6.6.2 Events Related to APU Fuel Leakage

The SIEs that result from APU fuel leakage are those in which fuel leaking from an APU damages flight critical equipment or an APU. SIEs associated with APU fuel leakage are reflected in the conditional probability distributions defined in Section 7.6.2. Values assigned to the split fractions are also discussed in Section 7.6 below.

6-96

6-97

Missing in Original

BHealy

Another potential source of detonation is the APU fuel pump seal. If the carbon face of this seal were to be damaged and allow metal to rub against metal, then high temperatures or sparks would be produced, causing hydrazine detonation within the fuel pump. This event occurred once during testing of an APU.

The two scenarios described below may produce conditions leading to hydrazine detonation upon restarting a leaking APU.

Scenario 1:

Condition: An APU fuel leak occurs between the closed fuel isolation valve and the fuel pump; the hydrazine in the connecting fuel line leaks away leaving only hydrazine vapor or a vacuum.

Result: When the fuel isolation valve is opened just prior to restarting the APU, the fuel will surge along the line and compress the hydrazine vapor, perhaps causing detonation. Even if no vapor remains in the fuel line, the action of the hydrazine accelerating into the line past the fuel isolation valve could introduce vapor bubbles into the fuel stream and the water hammer effect, which occurs when the fuel reaches the fuel pump, could cause detonation (Reference 95).

Scenario 2:

Condition: Hydrazine leaks into the solenoid cavity of a fuel isolation valve or gas generator control valve.

Result: A failure of the valve by means of (1) detonation of the hydrazine induced by the catalytic action of some material contained within the cavity, such as nickel plated iron, (2) electrical shorting of the coil, or (3) detonation caused by a spark. If the valve does not fail immediately, then later when the APU is restarted, the hydrazine may have removed enough electrical insulation to cause either a spark followed by hydrazine detonation or simply electrically short the coil (Reference 90).

6.6.3 Events Related to Hot APU Exhaust Gas Leakage

The SIEs that result from hot APU exhaust gas leakage are those in which leaking hot APU exhaust gas damages flight critical equipment or an APU.

6.6.3.1 High Pressure Hot APU Exhaust Gas Leakage

It may be possible for high pressure/high temperature gas to escape from the APU gas generator to the general environment by means of a narrow channel connecting the gas generator to a high pressure transducer. Gas within the gas generator has a design temperature of 1700°F, and a pressure of 1300 psia (Reference 33). The gas is expected to cool somewhat by passage through the access channel.

Because of the leak location, only the leaking APU could possibly be damaged by high pressure hot APU exhaust gas leakage. Hot gas may damage the APU wiring insulation. This insulation is Teflon wrapped with Kapton tape, and may be destroyed by sustained exposure to temperatures of 500°F or above. The possibility is considered remote and, as a simplifying assumption in this study, the probability was considered negligible.

6.6.3.2 Low Pressure Hot APU Exhaust Gas Leakage

As shown in Reference 84, an APU gas generator leak into the APU exhaust duct can produce exhaust gas temperatures as great as 1600°F without starving the APU turbine due to the loss of hot gas flow. The APU exhaust duct, constructed of Inconel 600, is qualified for a temperature of 1160°F at sea level and 1000°F in space (Reference 103).

Reference 98 shows that Inconel 600 suffers a fairly rapid decay in strength at temperatures above 1200°F. It may be possible that exposure of the APU exhaust duct to high temperatures resulting from a gas generator leak, in combination with APU vibration levels, could eventually lead to exhaust duct failure. However, there is some confidence that the duct would survive at least one flight in this condition without failure. It should be noted that no testing has been done to verify this opinion.

The prime contractor currently recommends shutting down an APU that shows a high exhaust temperature indicative of a gas generator leak. However, NASA-JSC has eliminated exhaust gas temperature as an indicator for APU shutdown due to the unreliability of the APU's Exhaust Gas Temperature (EGT) transducers and to the availability of other indicators of APU health (Reference 26). NASA-JSC also believes that the possibility

of exhaust duct failure due to a gas generator leak is remote (Reference 43). Again, the probability was considered negligible as a simplifying assumption in this study.

Avionics Bay Damage

The APU exhaust plume consists of a mixture of N_2, H_2. and NH_3 gas at an exhaust duct exit temperature of between 900°F and 1160°F. At the exit points of any exhaust leak into the aft compartment, the temperature will be no greater than 1160°F.

The three aft avionics bays are located on the lower part of the 1307 bulkhead, below the APUs. The configuration of the APU exhaust ducts is such that few exhaust leak locations would result in a leak plume being directed onto the exterior of one of the avionics bays at close range. A leak of the APU 1 exhaust duct in the worst possible location could result in the leak plume impinging on the upper surface of Avionics Bay 4 at a distance of about 6 feet. For other exhaust leak locations, the direct line distance to the nearest avionics bay is 13 feet or more.

Reference 85 indicates that for the APU exhaust plume at sea level conditions, the temperature at an axial distance from the nozzle exit of 6 feet is less than 400°F. The temperature at an axial distance of 13 feet is approximately 200°F. It is very unlikely that any APU exhaust leak would direct more than a small portion of the total exhaust gas flow, resulting in even lower temperatures at comparable distances from an exhaust leak. It should also be noted that the APU exhaust pressure is less than 10 Pounds per Square Inch (psi), meaning that an exhaust leak into the aft compartment is a diffused cloud of hot gas rather than a directed jet of hot gas.

Yet another mitigating factor is that the avionics equipment in question is enclosed within an aluminum honeycomb box (the avionics bay itself) covered by a one inch thick insulation blanket, and is cooled by freon circulating through cold plates.

In view of the above considerations, the chances of damage to avionics bay electronics equipment due to direct effects of an APU exhaust leak are considered negligible for the purposes of this study.

APU Damage

Damage to electrical wiring in the immediate vicinity of the exhaust duct is a credible event, particularly wiring for the APU itself. The wiring insulation is Teflon with Kapton tape wrapping, which is destroyed by sustained exposure to temperatures of 500°F or above. Temperatures in this range are possible due to an exhaust leak, but are still unlikely as they require a substantial portion of the APU exhaust plume to be diverted into the aft compartment.

It appears that the elbow joints of the exhaust duct or the APU to exhaust duct seal are somewhat more susceptible to leaks. In either case, the wiring susceptible to damage from the leak is the wiring of the leaking APU. Thus, there may be a small probability of loss of an APU with an exhaust leak, and a much smaller probability of loss of one APU due to another APU's exhaust leak. The latter applies to APUs 1 and 2 only; APU 3 is 10 feet away from the nearest other APU exhaust duct. The probability of these events was considered negligibly small for this study.

Another effect to consider is the effect of the leaking APU exhaust on fluid lines of another shut down APU. The extreme consequence of this could be detonation of fuel in the lines. Periods of potential exposure of a stagnant fuel line in one APU to another APU's leaking exhaust are limited to about 5 minutes during Flight Control System (FCS) checkout and about 20 minutes during entry. Rough calculations indicate possible detonation during the entry timeframe if a high pressure, focused jet of APU 1 exhaust impinges on APU 2 fuel lines before APU 2 start, or vice-versa. As concluded earlier, such a high pressure, focused jet is of negligible probability.

Orbiter Aft Compartment Overpressurization

A possible Orbiter damage scenario is overpressurization of the aft compartment due to the accumulation of exhaust gas in the compartment during the period of entry, before the vent doors open at Mach 2.4. The vent doors are closed at the Software Major Mode (MM304) transition (EI-5 minutes), so exhaust gas accumulation can begin at this point. The exhaust gas pressure is approximately 10 psi in space, and only 0.3 psid pressure is required to cause structural failure to the aft compartment.

Calculations show that a leak rate of ≈10% of the total exhaust gas flow, starting at MM 304 [Entry Interface (EI)], is required to cause damage to the aft compartment structure before the vent doors open. Such a leak rate would require a large hole in the duct and a mechanism for diverting the flow out of the hole. This event is also considered to be of negligible probability.

APU Exhaust Gas Ignition or Explosion

Yet another possible source of severe damage to the vehicle is ignition of hydrogen accumulated in the aft compartment due to an APU exhaust leak. This is not a concern during ascent or orbit, because there is insufficient oxygen to support combustion. It could be a concern during entry below 60,000 feet, where sufficient oxygen exists to support combustion. Because of the extremely low likelihood of significant gas leakage into aft compartment, and the considerations mentioned above, this failure event is considered to be of negligible probability.

7.0 APU DATA DEVELOPMENT

This section describes in detail the process used to collect and evaluate the failure data for the APU, and also the process used to develop probability distributions for component failure rates from this data.

A few comments concerning probability distribution are appropriate at this point. Probability distributions are used in this context to reflect the fact that component failure rates are uncertain. The use of probability distributions provides a complete description of our state of knowledge about the failure rates of the equipment in question, including any sources of variability among similar components. By contrast, use of a single number, called a point estimate, would tend to imply a degree of exactness that is not justified by the data.

It is important to bear in mind that the existence of uncertainty about component failure rates does not imply that the results are inaccurate or that they reflect a state of ignorance on the part of the analysts. Rather, uncertainty arises from a number of sources:

a. The relatively small amount of data that is available on many components

b. The possibility of missing data (e.g., failures that are not captured by the data collection process)

c. Decisions about whether incipient failures should be treated as failures in the data analysis

d. Estimation of the applicable exposure data (e.g., the total number of hours that a component operated)

e. The application of data from one situation (e.g., checkout) to other situations such as actual flights

f. The assumption that failure rates are constant over time

g. Differences in component reliability from one mission to another (e.g., due to differences in refurbishment)

h. Differences in component reliability from one APU to another, or between similar components in the same APU

i. The extrapolation of failure rate estimates developed for other applications (e.g., aircraft) to the Space Shuttle

j. The environmental factors that should be used in adjusting failure rate estimates from one application to another

The approach used in this study to describe and quantify such uncertainties is the Bayesian theory of probability. In this approach, each basic event frequency is described by a probability distribution specifying the various possible values for that frequency and the likelihood of each. The Bayesian approach is capable of taking into account both engineering judgment about the event frequency, and also empirical data such as the actual number of failures that were observed during operation of the APU.

In particular, a prior probability distribution is specified to reflect all the available information on similar components in other applications, as tempered by engineering judgment. This distribution is generally then updated with the observed APU data to yield a revised (i.e., posterior) distribution. In other cases, the posterior distribution is simply set equal to the prior distribution, and no update is performed. This is done in cases where little relevant information is available from other sources. The available APU data is therefore used to develop the prior distribution instead of to update it. In addition, no update is performed in cases where no APU data is available for use in the update; e.g., in modeling certain types of emergency demands that have not occurred during the operating experience of the APUs to date.

The use of judgment is in keeping with the Bayesian theory of probability, and the judgment of an analysis group that is knowledgeable about equipment reliability is a valid form of evidence for use in formulating distributions. Experience has shown that the judgment of experienced analysts is often remarkably close to actual data when the two have been compared. For example, several studies of component reliability have found expert estimates of component failure rates to be typically within a factor of two to four from the observed failure rates.

Section 7.1 describes the raw data sources from which APU failure data was obtained. These sources include such documents as corrective action reports, anomaly reports, and so on. For most spatial interaction events (SIEs), virtually no empirical data was available. Therefore, judgmental distributions were developed for

the frequencies of these events (e.g., the likelihood of damaging an adjacent APU as the result of a turbine overspeed). The process used for developing SIE distributions is described in Section 5.8 and the resulting judgmental distributions are described in Section 7.6. These distributions were based on extensive knowledge of such events, and also on a number of analytical studies performed specifically in support of this PRA.

Section 7.3 presents tables summarizing the raw data that was discussed in Section 7.1. These tables served as the basis for the data analysis. However, several adjustments were made to the information in these tables. The guidelines and criteria that were used to categorize the data according to component type and failure mode, and also the criteria used for determining which events (e.g., incipient failures) that would be considered non-failures in this study are described in Section 7.4.

In general, the criteria specified in Section 7.4 are fairly conservative. Conservative in this study means erring on the side of overestimating the frequency of events. For example, grouping several similar components into a single category for purposes of data analysis can result in narrower uncertainty bounds, by increasing the amount of data available for use in estimating failure rates. Therefore, in this study, such grouping was generally done only when the components in question were virtually identical (e.g., for identical components on different APUs, or for the two isolation valves on each APU).

The reason for this approach was to avoid inadvertently attributing inapplicable data to particular components, since otherwise an inappropriate failure rate distribution could result. To give some indication of the kinds of problems that can result from inappropriate grouping of components, consider an example involving two distinct types of components. If one type of component fails once every 100 hours and the second type fails three times every 100 hours, then grouping the data for these two components would give an average failure rate of twice every 100 hours, which is not appropriate for either type of component. Treating the two types of components separately, as was done in this study, gives slightly broader but more accurate distributions for the component failure rates.

Section 7.5 presents the actual prior and posterior distributions that were developed for the categories of component failures specified in Section 7.4. The sources of data used to update the distributions for the various failure rates are indicated. The Bayesian analysis that was used to develop the posterior

7-4

Missing in Original

B. Healy

a. TEST - Development, Qual, Acceptance

b. SIMILARITY - Parts nearly alike; built to same specifications, same usage, same manufacturer

c. ANALYSIS - Analytical evaluation; e.g., large parts/systems not lending themselves to tests of such things as expected launch vibrations

d. OBSERVATION - Actual use of components in flight or in similar space environment

For example, test and checkout failure data was compiled as determined from prelaunch FRFs, Hot Fires, and Confidence Runs which may be compared to acceptance tests. Similarly, electrical component failure rates and mechanical device failure rate data were obtained from established historical sources, References 97 and 99, respectively, which parallel certification by similarity. Along the same lines, analysis was employed during the development of the probability distributions for the SIEs. The flight time accumulated for many of the APU components, without failure, is in keeping with certification by observation.

Three broad types of data were required: (1) exposure data indicating how long the various APU components had operated; (2) data indicating how many failures of each given component had occurred over the corresponding exposure period; and (3) the failure modes that were observed.

It was obvious that utilizing Qualification Test (Qual) data would not produce reasonable failure rates. The failures associated with the Qual test program phase would likely represent flaws in the early design or manufacturing process. These failures would not necessarily be indicative of the final flight or production components or of later refinements in the manufacturing process.

An exception to the use of Qual test data was made in the development of the Spatial Interactive Events (SIE). There was no other available source of information from which to draw conclusions about unlikely, but catastrophic, occurrences such as an APU turbine wheel failing in overspeed.

The Acceptance Test (ATP) phase was the next level of component development for which data was known to be available. This data was considered to be of value in tracking failures from the time of contractor component, or system delivery, to end-of-life.

However, several difficulties were encountered that made it necessary to exclude the ATP data entirely. They were: (1) the lack of information on actual design changes resulting from ATP failures, (2) the inability to screen out facility failures and anomalies caused by facility or test setups, (3) the lack of time and funding available in this study to assure that the failures observed and documented in the ATP data were representative of the flight configuration.

Launch checkout and flight data were selected as the most meaningful data to support this analysis. This data represents the APU system in the flight configuration and flight environment. Moreover, it was judged that any valid failure modes identified in Qual or Acceptance tests, and not corrected, would be reflected in flight failure rates, thus reducing the effect of not including data from these development categories.

Several sources of launch checkout and flight data were found to be available and accessible during the study time frame and are described below. With the exception of one source, this data existed in paper form only. The exception, the APU Subsystem Manager's database, was a computer resident file with no hard copy printout available.

These sources were utilized to develop failure histories, and flight histories dating from 1 January 1981 through flight #24, which landed on 18 January 1986. Other sources such as NASA/ contractor test reports and discussions with knowledgeable personnel were used primarily as an information base to assist in the development of probability distributions for the Spatial Interactive Events.

The information from all sources was analyzed using a specific set of criteria necessary to track APU failures. The data was assembled into computer files according to the criteria established. For example, it was necessary to track APU serial numbers, dash numbers, flight numbers, and flight dates to prevent duplicating failure and anomaly entries.

The salient information needed to develop flight failure rates and mission timing sequences was compiled as a basis for developing model input data. The individual data sources and their use in this study are provided and discussed below.

a. Johnson Spacecraft Center (JSC) Orbiter Full Problem Report (FPR) (Reference 28)

b. Shuttle Flight Data and In-flight Anomaly List (References 31 and 32)

c. JSC Mission Reports, Missions 1 thru 23 (References 1 through 24)

d. The National Aeronautics and Space Administration (NASA) APU Subsystem Manager's Database

e. Study and test reports from NASA and contractor sources and published technical documents

The FPR, the Shuttle Flight Data and In-flight Anomaly List, the JSC Mission Reports and the study and test reports existed only in paper form. The remaining source, the Subsystem Manager's database, was resident in a Model 870 VAX computer located in Building 13 at JSC. These sources support various NASA functions, and as a result, differed as to format and data content. The salient information from each of the data sources was added to a personal computer (PC) data base program that provided edit, sort, search, and print capability. Conflicts found throughout the review and data compiling process required resolution before a coherent set of data could be developed. The individual sources are discussed in the following paragraphs.

7.1.1 JSC Orbiter Full Problem Report

The FPR was utilized as a prime source of APU failure data. Each record in this document contained various types of information such as Corrective Action Report (CAR) numbers, APU serial numbers, dates of failures, part numbers, and problem descriptions, which were invaluable in tracking and comparing failures from different sources. Also included were failure modes as well as analysis and resolution comments. The following data fields were utilized to develop a computer data file needed to compile the relevant data for the study:

	DATA FIELD	DESCRIPTION
a.	Page Reference	FPR page number
b.	Test Op	Test operation (FLT, CKO, ATP, QUAL)
c.	Failure Mode	Hardware failure
d.	Report Number	CAR number assigned to failure
e.	Part Name	Hardware Name
f.	Part Number	Hardware Number
g.	Serial Number	APU serial number

h.	Date Detected	Date anomaly first reported
i.	Problem Description	Anomaly description
j.	Analysis & Resolution	Recommendations made to correct condition causing failure

One major data element was the report or CAR number. This "common" number allowed failure correlations between JSC Mission Reports and the Shuttle Flight Data and In-flight Anomaly List.

Based on the ground rules established in paragraph 7.1, only Flight (FLT) and Checkout (CKO) records were selected for use in this study.

Appropriate information from the FPR records was entered into the PC database and sorted into FLT and CKO files. The FPR data could then then be compared with data from other sources to assure that failures were logged only once. By careful review, the first four data sources discussed in Paragraph 7.1 were combined into one data file to produce the Raw Data Tables as described in Section 7.3.

7.1.2 Shuttle Flight Data and In-Flight Anomaly List

The Shuttle Flight Data and In-flight Anomaly List is a historical report of flight related information. It also includes in-flight anomalies and references to problems encountered during the STS missions.

The report is divided into two sections. The first section, entitled "Shuttle Flight Data," provided the following mission-related information:

a. APU serial and dash number
b. APU position
c. Launch and launch scrub dates
d. Initial altitude and inclination
e. Flight sequence number, flight, and Orbiter number
f. Solid Rocket Booster (SRB) Separation time
g. Thrust bucket throttle times
h. Main Engine Cut-off (MECO) time
i. Other flight related data

The second section, entitled "Shuttle In-flight Anomaly List", provided a list of significant anomalies that occurred on STS missions. The anomalies of interest for this study were for the Auxiliary Power Unit under a Work Unit Code (WUC) designator V46. The type of information gathered was a brief description of the

anomaly, the STS flight problem number and/or the CAR number associated with the anomaly.

APU failure data from these two sections were combined to make up an "APU Flight" and "APU In-flight Anomaly" data file similar to that used to compile the FPR data. This data file was used as one of the four data sources from which comparisons were made prior to the development of the Final Data Tables. The flight related portions of the data base, such as SRB separation time and thrust bucket throttle time, were used to develop a "Study" mission data-base, combining mission sequence, flight, and Orbiter tail numbers from the JSC Mission Reports.

7.1.3 The NASA Subsystem Manager's Database

This data source consists of three separate historical data files containing information from Flights 1 thru 24, and is maintained by the NASA APU Subsystem Manager (SSM). The three files are entitled: (1) Flite 2, (2) Operational History, and (3) Hardware. Only data files 1 and 2 were used for the APU study.

The Flite 2 data file is essentially a compilation of APU anomalies tracked by the SSM. The data fields included were:

a. APU position and serial number
b. Mission ID (STS Reference)
c. Anomaly date
d. Component name
e. Vehicle number
f. Anomaly phase and description
g. Action taken

The Flite 2 data file assisted in determining which specific APU component (e.g., fuel pump, gas generator, relief valve) had failed when the FPR data only listed the anomaly or failure as an APU without regard to a part number.

The Operational History data file provided APU run times by APU position and serial number. The data fields included were:

a. APU Position and Serial Number
b. Run Time Event (FRF, STS Flight, Launch scrub, etc.)
c. Flight Date (Date of Run Time Event)
d. Run Time in Decimal Minutes
e. Pre/Post FLT Test (FLT or Test Time)

This file provided the APU run times associated with Flight Readiness Firings (FRF), Launch Scrubs, Confidence Runs (CR) and Checkout Operations at Kennedy Space Center (KSC), and Checkout at the Sundstrand facility.

These run times were divided into three categories: (1) Flight (FLT), (2) Checkout (CKO), and (3) Not Applicable (N/A). The flight run time corresponded to APU operation during past missions. The checkout time corresponded to APU CRs, Hot fires, FRFs, and APU operation during launch scrubs. All Sundstrand run times were classified "N/A", as there was no means to determine the test configuration. A Sundstrand test configuration, for example, might not include a flight-qualified controller or the APU flight-type tank, lines and isolation valves. The test setups most likely would not have included all of the flight instrumentation. In other words, an accumulation of APU system component operating times could not reliably be determined. Failure rates of individual components comprising the APU were considered outside the scope of this study.

The data was sorted to provide run times in the different categories, and was compared with the APU flight run times as obtained from the JSC Mission Reports (See 7.1.4). The CKO run times were accumulated separately, to be used in conjunction with checkout failures as obtained from the FPR data in determining checkout failure rates.

7.1.4 JSC Mission Reports

The JSC Mission Reports were used to obtain mission related data. These reports were also used as references when mission information obtained from other data sources required further clarification.

The mission reports proved to be very valuable during the course of this study. They were utilized to determine:

a. Lift-off (L/O) time
b. APU run times for ascent, orbit, and entry
c. Time of entry interface (EI)
d. Blackout end
e. Terminal area energy management (TAEM)
f. Touchdown (TD)

g. Wheelstop (WS)
h. APU deactivation time

It was necessary to accumulate APU run times by flight phases to determine the variation in run time during these periods. Since the SSM's Operational History file did not separate these times into the needed phases (ascent, orbit, and entry), the JSC Mission Reports were used as the baseline source of APU on/off/duration run times for the study. The total APU run times from the SSM's database were compared to those obtained from the JSC Mission Reports, and less than a 1% difference was noted. Therefore, it was concluded that the APU run times extracted from the mission reports would be adequate for use in the development of the mission-related database as shown in Appendix B7.3.

7.1.5 Study Reports, Test Results, & Personal Communications

Some of the failure modes under consideration during this study have a very low likelihood of occurrence. Directly applicable test data does not exist for some failure modes; e.g., some catastrophic SIEs. In order to estimate these likelihoods, information from a large number of study and test reports from NASA and contractor sources and other technical publications was utilized.

Valuable information used to supplement the written reports was obtained through telecons with various knowledgeable people in specialized fields at JSC and other locations. It was discovered during the study that tests were in progress at White Sands Proving Grounds on the properties of Hydrazine and its effect on certain materials. The results of these tests may have had an influence on some of the hydrazine use during this study. However, the results were not available for consideration and application for this study.

7.2 SPATIAL INTERACTIVE EVENT DATA

This section presents the APU SIE split fraction distributions in the format used for entry into the PRA model. Table 7.2-1 presents the data relevant to ascent and Table 7.2-2 presents the data relevant to entry. These distributions and the information supporting their development are presented individually in Section 7.6 and are presented here for clarity and convenience.

TABLE 7.2-1

SPATIAL INTERACTIVE EVENT APU ASCENT DISTRIBUTIONS

BASIC EVENT	FAILURES	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
CA2F1	Turbine Failure Given Primary and Secondary Valves Fail Open	8.5000E-01	6.2178E-01	8.5994E-01	9.5879E-01
CA2F3	Uncontained Shrapnel Produced Given Turbine Overspeed Failure	1.	1.	1.	1.
CA1F3N	Uncontained Shrapnel Produced Given Turbine Failure at Normal Speed	9.0909E-01	7.8177E-01	9.1423E-01	9.6951E-01
CA2F5	Failure of 2nd APU or FCE Given Shrapnel Due to Turbine Overspeed Failure	9.0909E-01	6.4760E-01	9.3178E-01	9.9452E-01
CA2F5N	Failure of 2nd APU or FCE Given Shrapnel Due to Turbine Failure at Normal Speed	5.0000E-01	5.7092E-02	4.8035E-01	8.7311E-01
L12F7	Hydrazine Leak Given Uncontained Shrapnel From Another APU	1.2281E-01	4.7878E-02	1.1573E-01	1.9052E-01
C1CQF	APU Failure Given a Small Leak in that APU	2.0000E-01	2.0609E-02	1.7205E-01	3.9875E-01
C12F13	APU Failure Given a Small Leak in Another APU	1.6140E-02	1.9024E-03	9.7847E-03	4.8681E-02
FA2F15	Failure of 2 APUs or FCE Given a Small Leak in One of Them	5.4250E-03	6.6215E-05	4.2513E-03	1.2040E-02
FA1F17	Failure of 2 APUs or FCE Given Small Leaks in at Least 2 APUs	8.0800E-03	1.9280E-03	6.2260E-06	1.9587E-02

TABLE 7.2-2

SPATIAL INTERACTIVE EVENT APU ENTRY DISTRIBUTIONS

BASIC EVENT	FAILURES	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
CA2F1	Turbine Failure Given Primary and Secondary Valves Fail Open	8.5000E-01	6.2178E-01	8.5994E-01	9.5879E-01
CA2F3	Uncontained Shrapnel Produced Given Turbine Overspeed Failure	1.	1.	1.	1.
CA1F3N	Uncontained Shrapnel Produced Given Turbine Failure at Normal Speed	9.0909E-01	7.8177E-01	9.1423E-01	9.6951E-01
CBF5	Failure of 2nd APU or FCE Given Shrapnel Due to Turbine Overspeed Failure	8.8889E-01	7.1035E-01	8.9738E-01	9.7025E-01
CBF5N	Failure of 2nd APU or FCE Given Shrapnel Due to Turbine Failure at Normal Speed	4.0000E-01	1.2654E-02	3.4938E-01	8.2442E-01
L12F7	Hydrazine Leak Given Uncontained Shrapnel From Another APU	1.2281E-01	4.7878E-02	1.15736-01	1.9052E-01
DKF12	APU Failure Given a Small Leak in That APU	6.3107E-01	3.1976E-01	6.3017E-01	8.3266E-01
DKF13	APU Failure Given a Small Leak in Another APU	4.3636E-01	1.6333E-01	4.2281E-01	6.5338E-01
FBF15	Failure of 2 APUs or FCE Given a Small Leak in One of Them	4.4872E-01	2.0926E-01	4.3845E-01	6.31836-01
FBF17	Failure of 2 APUs or FCE Given Small Leaks in at Least 2 APUs	7.9439E-01	5.0294E-01	8.0532E-01	9.4251E-01

7.3 RAW DATA TABLE DEVELOPMENT

This section summarizes the vast amount of data collected to support two basic needs of the study: (1) determination of observed APU failure frequencies, and (2) establishment of a typical mission time reference from which probabilities of occurrence could be calculated. One example of the latter was the need to determine the variation in Entry Interface (EI) times to obtain the average time for the start of two APUs during entry.

There were three sources of failure frequencies: (1) actual flight experience, (2) failure rates based on similarity data from accepted sources, and (3) failure rates derived from engineering judgment, supported by limited historical data.

A commercial software database program was utilized to compile, manipulate and format the data for sorting and printing. Two separate databases were developed from the sources discussed in the previous paragraphs: a failure history database and a mission event database. These databases are discussed in paragraphs 7.3.1 and 7.3.2. The failure rates of electrical items are described in paragraph 7.3.3.

7.3.1 Failure History Database and Output

The Failure History database was developed to compile flight failures and checkout failures from the sources identified previously. This database consists of (1) the APU Flight Failure data file, and (2) the APU Checkout Failure data file.

The Flight Failure Data Tables (Appendix B7.3-1) represent records created from the APU Flight Failure Data file. The data fields are categorized as (1) the mission sequence number and mission ID number which define the mission on which the failure was cited; (2) the APU position, serial number, and dash number; (3) the component part number and name of the failed hardware; (4) the failure mode and problem description which provide descriptive information; and (5) a resolution and additional comments for each failure. The data fields such as problem number, JSC document number, CAR number, Boeing page number, and source code are used only as reference material. The "source code key" can be used as reference to identify the source of the information contained in the record.

The Checkout Failure Data Tables (Appendix B7.3-1) represent records from the APU Checkout Failure data file. The data fields of interest are: (1) the planned mission date and the STS mission ID number; (2) the APU position, serial number, and APU dash number; (3) the vehicle number; (4) the component part number and nomenclature of the failed hardware; (5) the failure mode and operational phase during which the failure occurred (anomaly phase); (6) problem description and comments that define the failure and subsequent resolution; (7) the date the failure was cited; and (8) the CAR number and Boeing page number which provide a reference to the information source.

The data was sorted according to part number/name to display the failure modes and number of failures per component observed in the historical data file. The next step in the data development process was to categorize the data as discussed in paragraph 7.4.

7.3.2 Mission Related Database and Output

Early in the course of the study, it was thought that "flight" run times of the APU's should be tracked separately from the ground based "checkout" times. Two database files were generated to track and accumulate this information.

The APU flight run times were taken from the JSC Mission Reports for flights 1 through 23, since the reports listed the times by mission phase. However, the mission reports did not list "check-out" run times. The SSM's database listed these times of interest as Confidence Runs (CR), Flight Readiness Firings (FRF), Launch Aborts (LA), and Hot Fires. This data included flight run times but was not divided into mission phases. Therefore, it was decided to use the SSM's data for the prime source of APU checkout run time (CKO) and the JSC Mission Reports for the flight (FLT) run time. Subsequent comparison of the flight run times between the two sources indicated a difference of less than 1%.

Appendix B7.3-2 shows the APU flight run times by STS Mission and mission phase. The total run time for all APUs was calculated to be 6,258.96 minutes.

Appendix B7.3-2, pages 7 through 9, shows the checkout run times, calculated to be 331.19 minutes. The sum of flight and checkout run times, 6,590.15 minutes, was the basis for calculating component failure rates for an operating APU.

During the orbit period, when an APU is not operating, certain failure scenarios are still valid. Leaks can occur or heaters can fail "on" or "off". Appendix B7.3-2, pages 1 and 2, shows the accumulation of all mission times from APU start to APU shutdown. This value of 3,671.1367 hours represents the exposure time of a single APU to events such as leakage. The total exposure time used in this study was three times this value plus the time accumulated during checkout, for a total of 11,018.9299 hours. This represents the total exposure time of a flight-configured APU to a leakage environment.

Additional mission related data is shown in Appendix B7.3-2, page 15, including mission timing parameters such as EI, TAEM, Touch-down (TD), and Wheelstop (WS). Appendix B7.3-2, page 16, shows additional ascent mission related data.

7.3.3 Treatment of Electrical Components

The APU electronic controller was treated as a "black box". Controller failures, as found in the flight history data, could be tracked only to the point that a problem required removal and replacement of the controller itself. Excessive effort and time would have been required to determine from the vendor what individual component(s) within the box had caused the problem. Therefore, failure rates were estimated for the box itself, rather than for components within the box. References 71 and 74 were the source for development of the basic controller failure rates, along with information gained from Reference 86.

There are electrical components external to the controller for which failure rates were required. These components include switches, diodes, hybrid drivers, and Remote Power Controllers (RPC). The available flight history data did not reveal any failures of these components in the APU system. In cases such as this, other means can be employed to estimate failure rates. MIL-HDBK-217D (Reference 97) and NPRD3 (Reference 99) were utilized to estimate failure rates of electrical components.

The MIL-HDBK-217D provides the raw input data for determining failure rates of electrical components external to the APU controller. Fault trees (Reference 71) were developed to depict the failure scenario between the components and the end items of concern; e.g., the isolation valves. The result of this analysis was used as one input to the development of probability distributions for the failure rate of electrical components in

the risk model. Development of the probability distributions is discussed in Sections 7.4 and 7.5.

7.4 FAILURE HISTORY DATA CATEGORIZATION

A number of guidelines and criteria were established for the APU data categorization task. They are discussed below.

1. Failures occurring before January 1, 1981, were omitted from the data base on the grounds that the APU was still undergoing design development prior to that time.

2. Failures occurring during qualification tests (QUAL) and acceptance tests (ATP) were not included in the database for this project. These tests were thought to be largely inapplicable, on the basis that bench tests of individual components or subassemblies might not reflect the actual operation of a completed APU. In addition, since these tests are often performed early in the process of readying an APU for flight, they detect many types of failures that would not be expected during an actual flight.

3. Failures occurring both during checkout tests (CKO) and during actual flights (FLT) were included in the database. It was recognized that some types of checkout failures might not be expected to occur during flight. However, it was decided to include checkout data in the APU database. In particular, checkout tests occur far enough along in the process of readying an APU for flight that they were judged to reasonably reflect the condition of APUs during flight.

4. All checkout failures were carefully reviewed to determine whether they would actually be applicable to flight situations. In particular, an attempt was made to include only those checkout failures that occurred during hot firing of an APU (as opposed to bench tests of individual components, helium leak tests, and so on). However, it was not always possible to make this determination from the available data. When in doubt, checkout failures were conservatively included in the database.

5. Failures reported as having been detected during refurbishment were not included in the data base unless it seemed likely that they actually occurred during a previous flight. The purpose of this ground rule was to avoid the inclusion

of maintenance and refurbishment errors that were successfully detected and resolved before the completion of the refurbishment process.

6. Failures arising from maintenance or refurbishment problems were included in the data base if they were detected during flights or hot firings (i.e., if they were not successfully resolved before the completion of the refurbishment process).

7. Incipient failures (e.g., lube oil contamination or turbine blade cracking) were included in the data base only if their consequences were judged to be of sufficient likelihood and severity to be worth modeling. Examples of the types of incipient failures excluded under this criterion are: (1) unusually high gearbox heat retention that did not result in excessive gearbox temperature, (2) unexpected high vibration that did not exceed the redline level, and (3) valve cover leaks that did not result in valve failure.

8. A similar guideline was applied to components operating slightly outside of their intended specifications. Such problems were included in the database for the APU risk assessment only if they resulted in component failure, interfered with a vital function, or violated established flight rule limits. According to this rule, for example, problems resulting in turbine speeds below 80% or above 129% would have been considered failures. Problems resulting in a fluctuating turbine speed that nonetheless remained within the above limits would not have been considered failures.

9. Failures of noncritical components (e.g., temperature transducers or redundant valves) were included in the database if situations could be identified where these components would be important. For example, failures of the injector cooling system were included even though the system is not used during normal operation, since it is required for hot restart of an APU.

10. Failures of some components that do not appear in our APU model were nonetheless included in the database. This was done if it was judged that the failure rates for these components would be substantially the same as the failure rates for other components that were being modeled. For example, all pressure transducer failures were included in the database, even though only the gearbox pressure trans-

ducer was actually modeled. Grouping similar components in this manner resulted in narrower uncertainty bounds for certain components, by increasing the amount of data available for use in estimating failure rates.

11. Data for components that are significantly different in design and/or operation were not grouped. For example, data for the isolation valves was analyzed separately from data for the gas generator valves, since the gas generator valves experience pulsing operation. Analyzing such components separately ensures that large amounts of inapplicable data were not attributed to any particular component.

12. Even data for very similar components was not grouped if the components in question have different failure modes. For example, even though the primary and secondary fuel control are of virtually identical design, the primary valve is normally open while the secondary valve is normally closed. Therefore, data for these two valves was generally analyzed separately.

13. The adoption of corrective actions in response to particular failures was evaluated on a case-by-case basis to determine whether the action in question would actually be effective in preventing a recurrence of the problem. For example, major design changes such as the removal or addition of a valve would definitely be taken into account. However, for many corrective actions (e.g., improved cleanliness procedures), it was not possible to determine with a high degree of confidence that they would actually be successful in preventing a recurrence of the problem. Therefore, a more detailed review of corrective actions may prove worthwhile for those failures that are found to be dominant contributors to the total risk of APU failure.

Based on the guidelines and criteria established above, distributions were developed for the frequencies of various types of components and component failure modes. The components used for the APU ascent and descent models are specified in Table 7.4-1.

TABLE 7.4-1

COMPONENT CATEGORIES CONSIDERED IN THE APU MODEL

COMPONENT CATEGORY	FAILURES	SPECIFIC COMPONENT(S)
Bypass valve	Fails to open on demand	Fuel pump bypass valve
	Fails to close on demand	Fuel pump bypass valve
Solenoid valve	Fails to open on demand	Isolation valves
		Secondary valve
		GN2 repressurization valve
		Injector cooling valves
	Fails to close on demand	Isolation valves
		Primary valve
		Secondary valve
	Fails closed while pulsing	Primary valve
		Secondary valve
	Fails open while pulsing	Primary valve
		Secondary valve
	Leaks on closing	Isolation valves
		Secondary valve
	Leaks while closed	Isolation valves
		Secondary valve
	Leaks into solenoid cavity	Primary valve
		Secondary valve
		Isolation valves

TABLE 7.4-1 (Continued)

COMPONENT CATEGORY	FAILURES	SPECIFIC COMPONENT(S)
	Transfers closed (i.e., plugs)	Isolation valves Injector cooling valves
Valve driver	Fails on or off	Secondary valve driver Isolation valve driver
	Fails at start-up	Isolation valve driver
Fixed displ. pump	Fails while operating	Fuel pump Lube oil pump
	Fails at start-up	Fuel pump Lube oil pump
	Leaks	Fuel pump seal
Turbine	Fails while operating	N/A
	Fails at start-up	N/A
	Generates shrapnel/overspeed	N/A
	Generates shrapnel/normal spd.	N/A
Gearbox	Needs repressurization	N/A
	Fails while operating	N/A
	Fails at start-up	N/A
Gas generator	Fails while operating	N/A
	Fails at start-up	N/A
Tank or bottle	Leaks	Fuel tank (GN2 side) GN2 bottle

TABLE 7.4-1 (Continued)

COMPONENT CATEGORY	FAILURES	SPECIFIC COMPONENT(S)
Diaphragm	Leaks	Fuel tank diaphragm Accumulator diaphragm Water tank diaphragm
Fuel system	Leaks	Single APU Multiple APUs
Water System	Leaks	Injector cooling system
Hot gas exh. duct	Leaks	N/A
Filter	Plugs	Fuel inline filter Fuel pump filter
Lube oil system	Plugs	Single APU Multiple APUs
Electric power	Fails while operating	Power to isolation valve Power to primary valve Power to secondary valve
	Fails at start-up	Power to isolation valve Power to primary valve Power to secondary valve
Switch	Transfers open	Isolation valve switch Heater switches
	Transfers closed	Inhibit switch Start/run switch Heater switches Controller power switch

TABLE 7.4-1 (Continued)

COMPONENT CATEGORY	FAILURES	SPECIFIC COMPONENT(S)
	Fails to open on demand	Isolation valve switch Heater switches Controller power switch
	Fails to close on demand	Isolation valve switch Heater switches
	Transfers to wrong position	Start/run/override switch
	Transfer open, common cause	Multi-pole switches
Controller	Fails on at start-up	Primary valve controller Over/underspeed controller
	Fails off at start-up	Primary valve controller Secondary valve controller
	Fails on demand	Override controller
	No signal while operating	Inhibit circuit Shutdown controller Primary valve controller Secondary valve controller Gearbox press. controller
	Spur. signal while operating	Secondary valve controller Primary valve controller Gearbox press. controller Shutdown controller

TABLE 7.4-1 (Concluded)

COMPONENT CATEGORY	FAILURES	SPECIFIC COMPONENT(S)
Pressure transducer	Fails high	Gearbox press. transducer
	Fails low	Gearbox press. transducer
MPU	Fails high while operating	MPUs 1, 2, and 3
	Fails low while operating	MPUs 1, 2, and 3
	Fails high at start-up	MPUs 1, 2, and 3
	Fails low at start-up	MPUs 1, 2, and 3
	Fails mid-range while operating	MPU 1
Control power RPC	Fails on	N/A
Inhibit circuit	Internal short	Inhibit circuit diode
Heater	Fails off	Heater 1/2
		Heater 3/23
		Heater 4/5
		Heater 10/17
		Heater 13
		Heater 14/15
		Heater 111/112
		Heater 116/117
		Lube oil heater
	Fails off, common cause	Heaters 13A and 13B
		Lube oil heaters A and B
	Fails on	Heater 10/17
		Heater 14/15
		Heater 111/112
		Heater 116/117

7.5 FAILURE RATES

Once the data has been categorized as a basis for determining the components and failure modes for which failure rate distributions will be needed, the next step is to specify prior distributions for those failure rates. After that, one must specify the relevant data for each component failure mode (i.e., the number of observed APU component failures and the number of operating hours and/or demands to which each component was subject). Finally, the data must be combined with the prior distributions to yield posterior distributions. The results of these three steps are presented in the sections below.

7.5.1 Development of Prior Distributions

A number of sources were used as background information in developing prior distributions. These include the Nonelectronic Parts Reliability Data (NPRD) handbook, prepared by the Rome Air Development Center; MIL-HDBK-217D (used for electronic components); the Reliability Engineering Data Series report on Failure Mechanisms, prepared by the Avco Corporation; NASA operating life limits for the APU; and the engineering judgment of the analysis team (based on previous risk assessments and data analyses).

In many cases, adjustments to the information obtained from these sources were needed. For example, many of the failure rate estimates obtained from NPRD were for components in aircraft or ground-based environments rather than missile environments. Environmental adjustment factors were judged to be a reasonable way to account for many of these differences; factors for this purpose were obtained from the Avco Failure Mechanisms report. In addition, all the failure rate estimates in NPRD are presented on a per-hour basis (H), while many of the failure rates for the APU risk study were needed on a per-demand basis (D). In such cases, the number of demands per hour in a typical application was estimated as a basis for converting the failure rate to the desired units.

In a few cases, estimates were not available from sources such as NPRD or MIL-HDBK-217D, and the judgment of the analysis team provided little guidance for the development of prior distributions. In such cases, observed APU failure experience was used in the development of the prior distribution. These distributions were not subsequently updated, since the relevant data had already been incorporated into the prior.

Finally, after the initial assessment of prior distributions, the distributions for similar components or related failure modes were compared with each other as a reasonableness check. For example, the failure rates for different types of rotating equipment (e.g., the turbine, pumps, and gearbox) were compared to assure that they were roughly comparable, and that the assigned failure rates were consistent with engineering knowledge, such as the differing speeds at which the various types of equipment operate. Similarly, the rates of leaks from pump seals, tanks, and diaphragms were compared to ensure that the more vulnerable components were assigned the higher leak rates.

This type of comparison was intended to assure that the various failure rates reflected the correct relative ranking. The comparison process, which was especially important since many of the prior distributions were based on different data sources and/or different applications, did result in the adjustment of several distributions to correspond more closely with what the analysis team considered realistic for application to the Space Shuttle.

Table 7.5-1 presents the prior distributions that resulted from this process. For each distribution, the table contains the category of components to which the distribution applies, the relevant failure mode or modes, the 5th and 95th percentiles of the prior distribution, and the sources used in developing that prior distribution. Engineering judgment is nearly always used in the development of distributions, because there is rarely enough data to unambiguously specify a distribution.

Virtually all the prior distributions were assumed to be lognormal in form, as is common practice in PRAs. For these distributions, the medians can be found as the geometric mean of their 5th and 95th percentiles. The only exception to the assumption of lognormality is the conditional frequency of leaks in the fuel systems of additional APUs, given that one APU is leaking. Because the 95th percentile of this frequency was quite high, a lognormal distribution would not have been reasonable; in particular, it would have allowed conditional probabilities of leaks to be significantly greater than 1.0. Therefore, a beta distribution was used for this parameter instead of a lognormal distribution.

7.5.2 Specification of Failure Data

Once prior distributions have been developed for each category of components and each failure mode, the next step is to specify the relevant data for each category (i.e., the number of observed component failures of each type, and the number of operating hours (H) and/or demands (D) to which each component was subject, which is referred to as exposure data).

The estimation of exposure data is a difficult process. It requires determination of whether the relevant failure mode is likely to occur over time or on a per-demand basis; whether the failure mode can occur at any time or only when the APU is operating; and whether a failure would likely be detected if one occurred. For example, failures of some types of redundant components may not be detectable during normal APU operation.

As an illustration, the relevant exposure data for failure of the APU fuel pump to run was taken to be 110 hours -- the total amount of run time accumulated on all APUs to date during flight and checkout (CKO) hot firings. For failures of passive components (e.g., tank leaks), the relevant exposure data was taken to be 11,019 hours. This is based on the total amount of run time plus on-orbit time accumulated on all APUs to date during flights, and also the small amount of run time involved in CKO hot firings. Finally, for demand-based failures, the number of demands experienced by a typical component during flights and hot firings was calculated to be 217. This total assumes that the component in question experiences exactly one demand during each firing of an APU, and is made up of several contributions:

a. Two demands (one during ascent and one during descent) for each of three APUs on 24 missions, for a total of 144 demands

b. One additional demand for a single APU on each of the 24 missions (for the on-orbit checkout run), for a total of 24 demands

c. One demand for a single APU during each of the 46 CKO hot firings, for a total of 46 demands

d. One demand for each of the three APUs during the confidence run (prior to the first flight), for a total of three demands

Care must be taken in applying these values to particular components, however, to assure that they are applicable. For example, the exposure data for isolation valves opening or closing on demand was taken to be 434 demands instead of 217 demands, since there are two isolation valves in each APU. Similarly, the exposure data for the GGVM secondary valve leaking after successful closure was taken to be only 10,909 hours instead of 11,019 hours, because the secondary valve would have been open during the 110 hours of actual APU operation and thus could not have leaked during that time. As a final example, it was assumed that there was effectively no exposure data for loss of the automatic shutdown signal from the APU controller, since a failure leading to loss of the shutdown signal would most likely have gone undetected unless a shutdown became necessary during flight.

Table 7.5-2 presents the prior distribution and the failure and exposure data for each basic event included in the analysis. As can be seen from that table, the prior distributions for some events were not updated and were used directly as posterior distributions, because all relevant failure data for those events had already been used in developing the priors. For reference purposes, Table 7.5-3 provides descriptions of the actual failures indicated in Table 7.5-2. This provides a complete description of the information that was input to the Bayesian updating process.

7.5.3 Development of Posterior Distributions

The Bayesian updating process was performed using the RISKMAN 4 computer software on a desktop personal computer. The results of this process are shown in Table 7.5-4. This table shows the mean frequency for each basic event (based on the posterior distribution obtained from the Bayesian update), and also the 5th, 50th and 95th percentiles.

In using the distributions in this table, one must keep in mind that the two isolation valves in the APU are assumed to have identical distributions for each failure mode, as are the three MPUs. Thus, for example, the frequencies of the basic events BAM2H and BAM3H (MPUs two and three, respectively, fail high at start) are described by the distribution shown in Table 7.5-4 for the basic event BAM1H (MPU one fails high at start). Similarly, the frequency of the basic event BAVBO (isolation valve B fails to open on demand) is described by the distribution for BAVAO (isolation valve A fails to open on demand).

As discussed in Section 7.0, the Bayesian analysis used to develop the distributions shown in Table 7.5-4 automatically assigns the appropriate weights to the observed data and the prior distribution, respectively, based on the relative strength of the two types of evidence in each particular situation. For example, when a great deal of empirical data is available, the data will tend to dominate the posterior. Similarly, when relatively little empirical data is available, the posterior distribution will tend to resemble the prior distribution; in this case, the data is simply not strong enough to override the information contained in the prior distribution.

For most of the basic events shown in Table 7.5-4, relatively little failure data was available -- at most one or two observed failures, and often none. Therefore, most of the posterior distributions look fairly similar to the priors on which they were based. However, a general trend can be seen. In cases where no failures were observed, the posterior is slightly lower than the prior. This is a result of the Bayesian inference process, and is intuitively reasonable. This effect is greatest when the prior distribution extends to include fairly high failure rates, which are inconsistent with the lack of observed failures. Similarly, in cases where one or more failures were actually observed, the posterior distribution is generally slightly higher than the prior distribution. With the small amounts of exposure data available for most components, even a single failure is often sufficient to suggest that the failure rate might be higher than is indicated by the prior distribution.

The frequencies of a few basic events were described by point estimates instead of distributions, usually on the basis that their frequencies were negligible or were known very precisely. Most of these events were considered to be negligible for the purposes of this study, and were therefore assigned frequencies of zero. The events in this category included the following:

a. Spurious activation of the isolation valve automatic shutdown signal (basic events PACRA and PACRB during operation, and BACRA and BACRB at start-up). This failure mode is considered extremely unlikely.

b. A number of APU start failures, which were considered extremely unlikely: BAFTN (GN2 leakage into the fuel tank at start); BAGGS (failure of the gas generator); BALFB and BAPFB (plugging of the inline fuel filter and the fuel pump filter); and BARVO (inadvertent opening of the fuel pump relief valve).

c. Common cause failure of two or more APUs due to causes other than lube oil blockage (basic event DAOCC). The frequency of other common cause failure modes was considered to be dominated by the frequency of lube oil plugging.

d. Common cause failure of both fuel control valves in the open position (basic event TACCF). This is considered much less likely than independent failure of both valves due to mechanical and/or control problems because one of the valves fails in the open position upon loss of power and the other one fails closed. The detached valve seat single point failure is likewise considered to be of very low probability.

e. Gearbox failure due to loss of lube oil: basic events PALLL for a lube oil line leak and PAGBL for a gross gearbox leak. The frequency of these failure modes was considered to be dominated by the frequency of smaller leaks resulting in repressurization, as modeled by basic event PAAGL.

f. Basic event PAHSP (high speed operation selected during ascent). High speed operation would not be manually selected by the shuttle crew during the ascent phase, unless at least one APU had shut down.

g. Valve leakage after closure at the end of the ascent phase (PAVAZ and PAVBZ for the isolation valves, and PASVZ for the secondary valve). Fuel depletion due to valve leakage after closure is modeled in Stage A (ascent), but is quantified in Stage B (orbit).

h. Failure of the water spray boiler (basic event PAWSB). The water spray boiler is out of scope for this analysis, and is included in the fault trees only for completeness.

Additional events that were assigned point estimates other than zero are as follows:

a. Basic event DARAT. This is a correction factor reflecting the fact that if a spurious shutdown occurs, only two APUs instead of three may be subject to turbine overspeed and other failure modes. This basic event was conservatively assigned a value of 1.0, which is equivalent to ignoring the correction factor.

b. Basic event PAOSK. Successful functioning of the overspeed shutdown circuitry and successful closure of the secondary valve. This event was assigned a likelihood of 1.0 in the PA and PB fault trees because the chance of failure is extremely small; a value of 1.0 is a highly accurate approximation of the probability of success.

c. The likelihood that automatic shutdown is enabled (basic event SAPEQ). The frequency of this condition is assumed to be 1.0 in cases where no other APU failures have occurred, since automatic shutdown would not be disabled in the absence of a failed APU.

d. An order correction factor (basic event PALKF) for the conditional probability that a gearbox leak occurs subsequent to the failure of a component needed to respond to the leakage (e.g., the GN2 valve). This order correction factor was assumed to equal 0.5.

e. Order correction factors for the sequencing of spurious shutdowns and other APU failures. The likelihood that the spurious shutdown would have occurred first (basic event SASSD) was assumed to equal 0.5. The likelihood of the other failure occurring first (basic event SAOFO) was taken to be one minus the frequency of SASSD (i.e., also equal to 0.5).

f. The conditional probability that a fuel system leak occurs upstream of the isolation valves (basic event CIUSL). This was estimated to equal 0.3, based on a ratio of the frequency of tank leaks to the total frequency of all fuel system leaks.

g. The conditional probability that a fuel system leak occurs downstream of the isolation valves, but upstream of the secondary valve (basic event CIDSL). This was estimated to equal 0.5 based on the locations of the observed fuel system leaks to date.

TABLE 7.5-1

PRIOR DISTRIBUTIONS

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED *
			5TH PERCENTILE	95TH PERCENTILE	
VBPD	Bypass valves	Fail to open or close on demand	$2x10^{-5}$/D	$3x10^{-3}$/D	NPRD, ENVF, DMD/HR
VSNC	Solenoid valves (non-H_2O systems)	Fail to close on demand	$8x10^{-5}$/D	$7x10^{-3}$/D	SACS
VSNO	Solenoid valves (non-H_2O systems)	Fail to open on demand	$8x10^{-5}$/D	$7x10^{-3}$/D	SACS
VSND	Solenoid valves (non-H_2O systems)	Fail to reseat properly when closed	$8x10^{-5}$/D	$7x10^{-3}$/D	SACS
VSNL	Solenoid valves (non-H_2O systems)	Leak	$1x10^{-6}$/H	$1x10^{-4}$/H	NPRD
VSNR	Solenoid valves (non-H_2O systems)	Fail open or closed while pulsing	$1x10^{-4}$/H	$1x10^{-2}$/H	NASOL

---

* Key to Sources

AVCO - AVCO Corporation
CWOD - Comparison With Other Distributions
D - Demand
DMD/HR - Demands Per Hour
ENVF - Environmental Factor
H - Hour
MIL - MIL-HDBK-217D
NASOL - NASA Operating Life Limit
NPRD - Nonelectronics Parts Reliability Data
OBSD - Observed Data
SACS - Shuttle APU Containment Study (Reference 25)

TABLE 7.5-1 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED *
			5TH PERCENTILE	95TH PERCENTILE	
VSNT	Solenoid valves (non-H_2O systems)	Plug while open or transfer closed	$5x10^{-8}$/H	$4x10^{-6}$/H	SACS
CKTR	Controller board	Fail to operate or spurious signal	$1x10^{-6}$/H	$1x10^{-3}$/H	MIL, NPRD, ENVF
TSPR	MPU (magnetic speed sensor)	Read high or low	$5x10^{-5}$/H	$5x10^{-3}$/H	NPRD, ENVF
TPRH	Press. transducer	Read high or low	$2x10^{-5}$/H	$3x10^{-3}$/H	NPRD, ENVF
SLLK	Pump seal	Leak	$5x10^{-6}$/H	$1x10^{-3}$/H	NPRD, ENVF, CWOD
PVLK	Tank/press. vessel	Leak	$3x10^{-7}$/H	$3x10^{-5}$/H	NPRD, CWOD
FTDB	Diaphragm	Leak	$1x10^{-6}$/H	$1x10^{-4}$/H	AVCO, ENVF
ACLK	Gearbox	Loss of pressure	$5x10^{-6}$/H	$1x10^{-3}$/H	NPRD, CWOD
PFXR	Fixed displ. pump	Fail to run	$3x10^{-6}$/H	$3x10^{-4}$/H	NPRD, ENVF, CWOD
FLLP	Lube oil filter	Plugging	$1x10^{-4}$/H	$1x10^{-2}$/H	OBSD
FTLK	Fuel/water system	Leak	1x10-5/H	1x10-3/H	OBSD
FTL2	Fuel System	Leak in 2nd APU given 1 APU leaking	$2x10^{-2}$/H	$5x10^{-1}$/H	OBSD

TABLE 7.5-1 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	PARAMETERS OF PRIOR DISTRIBUTION 95TH PERCENTILE	SOURCES USED *
SWIO	Switch	Fail to open on demand	$3x10^{-6}$/D	$3x10^{-4}$/D	NPRD, ENVF, DMD/HR
SWOP	Switch	Transfer open	$4x10^{-7}$/H	$2x10^{-5}$/H	NPRD, OBSD
SWCC	Multi-pole switch	Both trains transfer open by common cause	$4x10^{-9}$/H	$2x10^{-7}$/H	CWOD
GGNR	Gas generator	Fail to run	$1x10^{-6}$/H	$7x10^{-4}$/H	NPRD, ENVF
THLK	Hot gas exh. duct	Leak	$1x10^{-6}$/H	$1x10^{-4}$/H	NRPD, ENFV
TBNR	Gas turbine	Fail to run	$3x10^{-5}$/H	$3x10^{-3}$/H	NPRD, ENVF
SWCL	Switch	Transfer closed	$1x10^{-7}$/H	$6x10^{-6}$/H	NPRD, OBSD
SWIC	Switch	Fail to close on demand	$1x10^{-5}$/D	$1x10^{-3}$/D	NPRD, ENVF
DRON	Driver	Fail on or off while operating	$1x10^{-6}$/H	$1x10^{-3}$/H	MIL, OBSD
DRST	Driver	Fail on demand	$3x10^{-7}$/D	$3x10^{-5}$/D	MIL, OBSD, DMD/HR
FFPL	Fuel in line fltr	Plugging	$3x10^{-7}$/H	$3x10^{-5}$/H	NPRD, ENVF
FPPL	Fuel pump filter	Plugging	$3x10^{-6}$/H	$1x10^{-3}$/H	NPRD, ENVF
GQDL	Fuel tank GN2 quick disconnect	Leak	$2x10^{-6}$/H	$2x10^{-4}$/H	NPRD, ENVF

TABLE 7.5-1 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED *
			5TH PERCENTILE	95TH PERCENTILE	
RPIM	Gearbox	Persistent leak given a leak	$1x10^{-3}$/D	$1x10^{-1}$/D	OBSD
IS02	Isolation valves	Transfer closed due to common cause	$1x10^{-6}$/H	$1x10^{-4}$/H	CWOD
EPSF	Iso. valves power supply	Single train fails off	$1x10^{-6}$/H	$2x10^{-4}$/H	MIL
EPDF	GGVM power supply	Two trains fail off**	$1x10^{-6}$/H	$1x10^{-4}$/H	MIL
GBXR	Gearbox	Fail to run	$1x10^{-6}$/H	$1x10^{-4}$/H	CWOD
CCLO	Lube oil	Plug in 2nd APU given 1 APU plugged	$1x10^{-2}$/D	$2x10^{-1}$/D	OBSD
PFXS	Pump	Fail to start	$1x10^{-7}$/D	$5x10^{-5}$/D	OBSD
TBNS	Turbine	Fail to start	$1x10^{-7}$/D	$5x10^{-5}$/D	OBSD
GBXS	Gearbox	Fail to start	$1x10^{-7}$/D	$5x10^{-5}$/D	OBSD
PFXS	Pump	Fail to start	$1x10^{-7}$/D	$5x10^{-5}$/D	OBSD
TBNS	Turbine	Fail to	$1x10^{-7}$/D	$5x10^{-5}$/D	OBSD
GBXS	Gearbox	Fail	$1x10^{-7}$/D	$5x10^{-5}$/D	OBSD

** 2 indep. power supplies or 1 swi

TABLE 7.5-1 (Concluded)

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED *
			5TH PERCENTILE	95TH PERCENTILE	
EPSS	Isolation valve electric power	Fail to start on demand	$1x10^{-5}$/D	$3x10^{-3}$/D	CWOD
EPDS	Secondary valve electric power	Fail to start on demand	$2x10^{-5}$/D	$6x10^{-3}$/D	CWOD
CKTS	Controller	Fail to start on demand	$1x10^{-6}$/D	$1x10^{-3}$/D	SACS
MPUS	MPU	Fail to start on demand	$5x10^{-5}$/D	$5x10^{-3}$/D	CWOD
VSWO	Solenoid valves (inj. cooling system)	Fail to open on demand	$4x10^{-4}$/D	$4x10^{-2}$/D	OBSD
VSWK	Solenoid valves (inj. cooling system)	Plug due to contamination	$1x10^{-7}$/H	$3x10^{-5}$/H	CWOD
HTOF	Heater	Fail off	$1x10^{-5}$/H	$1x10^{-3}$/H	NPRD, ENVF,
HTON	Heater	Fail off	$1x10^{-5}$/H	$1x10^{-3}$/H	NPRD, ENVF,
HTCC	Heater	2 trains fail by common cause	$1x10^{-6}$/H	$3x10^{-4}$/H	CWOD
GGLK	GGVM valve	Hydrazine leak into solenoid cavity	$3x10^{-7}$/H	$1x10^{-4}$/H	OBSD
ISLK	Isolation valve	Hydrazine leak into solenoid cavity	$3x10^{-8}$/H	$1x10^{-5}$/H	CWOD

TABLE 7.5-2

PRIOR DISTRIBUTIONS AND OBSERVED DATA FOR APU BASIC EVENTS

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION		BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
	5TH PERCENTILE	95TH PERCENTILE					
VBPD	$2x10^{-5}/D$	$3x10^{-3}/D$	BABVO	Fuel bypass vlv.	Fail to open on demand	0	217 D
			BABVC	Fuel bypass vlv.	Fail to open on demand	0	217 D
VSNC	$8x10^{-5}/D$	$7x10^{-3}/D$	PASVC	Secondary valve	Fail to cls. on demand	1	217 D
			BAPVC	Primary valve	Fail to cls. on demand	0	217 D
			PAVAC	Iso. valve A/B	Fail to cls. on demand	0	434 D
VSNO	$8x10^{-5}/D$	$7x10^{-3}/D$	BAVAO	Iso. valve A/B	Fail to open on demand	0	434 D
			PANVO	GN2 valve	Fail to open on demand	0	9 D
			BASVO	Secondary valve	Fail to open on demand	0	217 D
VNBD	$8x10^{-5}/D$	$7x10^{-3}/D$	PAVAL	Iso. valve A/B	Leak when closing	0	434 D
			BASVL	Secondary valve	Leak at startup (because of previous closure)	1	217 D

Key to abbreviations:

D	- Demand	H	- Hour	Iso.	- Isolation	Sec.	- Secondary
Elec.	- Electrical	Htr.	- Heater	Press.	- Pressure	Trans.	- Transducer
GB	Gearbox	Inj.	- Injector	Prim.	- Primary	Vlv.	- Valve

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
			PASVL	Secondary valve	Leak when closing	1	217 D
VSNL	$1x10^{-6}$/H	$1x10^{-4}$/H	PAVAZ	Iso. valve A/B	Leak after closing	0	21,818 H
			PASVZ	Secondary valve	Leak after closing	0	10,909 H
			PANVL	GN2 valve	Leak after closing	0	11,019 H
VSNR	$1x10^{-4}$/H	$1x10^{-2}$/H	PAPVE	Primary valve	Fail open when pulsing	0	110 H
			PAPVD	Primary valve	Fail closed when pulsing	1	110 H
			TASVE	Secondary valve	Fail open when pulsing	0	0 H
			PASVD	Secondary valve	Fail closed when pulsing	0	0 H
VSNT	$5x10^{-8}$/H	$4x10^{-6}$/H	PAVAK	Iso. valve A/B	Plugged while open	0	0 H
VSWK	$1X10^{-7}$/H	$3X10^{-5}$/H	RBWVK	Inj.cooling vlv.	Plug while open	0	0 H
VSWO	$4x10^{-4}$/D	$4x10^{-2}$/D	RBWVO	Inj.cooling vlv.	Fail to open on demand	0	0 D
ISLK	$3x10^{-8}$/H	$1x10^{-5}$/H	GBACO	Isolation valve	Leak into solenoid cavity	0	22,038 H
GGLK	$3x10^{-7}$/H	$1x10^{-4}$/H	HBPCO	GGVM valve	Leak into solenoid cavity	0	22,038 H
CKTR	$1x10^{-6}$/H	$1x10^{-4}$/H	SAICF	Inhibit circuit	Fail to inhibit	0	0 H
			BASVL	Secondary valve	Leak at startup (because of previous closure)	1	217 D

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
			TASDS	Shutdown controller	Loss of signal	0	0 H
			PASVU	Sec. controller	Fail on	0	0 H
			PAPVQ	Prim. controller	Loss of signal	0	110 H
			PAPVU	Prim. controller	Fail on	0	110 H
			PASVQ	Sec. controller	Loss of signal	0	110 H
			PAPCH	GB press. controller	Loss of signal	0	110 H
			PAPCL	GB press. controller	Fail on	1	110 H
			SASVS	Shutdown controller	Fail on	0	110 H
TSPR	$5x10^{-5}$/H	$5x10^{-3}$/H	TAM1L	MPU 1/2/3	Fail low	1	220 H
			TAM1M	MPU 1	Fail midrange	0	0 H
			SAM1H	MPU 1/2/3	Fail high	0	330 H
TPRH	$2x10^{-5}$/H	$3x10^{-3}$/H	PAPTH	GB press. trans.	Fail high	2	807 H
			PAPTL	GB press. trans.	Fail low	0	477 H
SLLK	$5x10^{-6}$/H	$1x10^{-3}$/H	PAFPL	Pump seal	Leak	7	11,019 H

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
PVLK	$3x10^{-7}$/H	$3x10^{-5}$/H	PAFNL	Fuel tank	Nitrogen leak	0	11,019 H
			PANBL	GN2 bottle	Nitrogen leak	0	11,019 H
FTDB	$1x10^{-6}$/H	$1x10^{-4}$/H	PAFDL	Fuel tank diaphragm	Leak	0	11,019 H
			PAACI	Accumulator diaghragm	Leak	0	22,038 H
			RBWDL	Inj. cooling tank diaphragm	Leak	0	10,909 H
ACLK	$5x10^{-6}$/H	$1x10^{-3}$/H	PAAGL	Gearbox	Repress.	6	11,019 H
PFXR	$3x10^{-6}$/H	$3x10^{-4}$/H	PAFPR	Fuel pump	Fail to run	0	110 H
			PALPR	Lube oil pump	Fail to run	0	110 H
FLLP	$1x10^{-4}$/H	$1x10^{-2}$/H	PALOF	Lube oil system	Loss of flow	3	110 H*
FTLK	$1x10^{-5}$/H	$1x10^{-3}$/H	LALK1	Fuel system	Leak	4	11,019 H*
			RBWLL	Inj. cooling system	Leak	0	10,909 H

---

* Prior distribution not updated, observed data already incorporated.

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
FTL2	$2x10^{-2}$/H	$5x10^{-1}$/H	LALK2	Fuel system	Leak in 2nd APU given 1 is leaking	2	4 D*
SWCC	$4x10^{-9}$/H	$2x10^{-7}$/H	PBCS1	Fuel system heater switch	Both poles transfer open by common cause	0	10,909 H*
			PBCS4	Lube oil heater switch	Both poles transfer open by common cause	0	10,909 H*
SWIO	$3x10^{-6}$/D	$3x10^{-4}$/D	PASAO	Iso.vlv. switch	Fail to open	0	434 D
			PBTAO	Heater switch	Fail to open on demand	0	72 D
			PBCPO	Controller pwr. switch	Fail to open on demand	0	217 D
SWOP	$4x10^{-7}$/H	$2x10^{-5}$/H	PASAF	Iso.vlv. switch	Transfer open	0	0 H
			PBBSO	Fuel system htr. switches	Transfer open	0	21,818 H
			PBHBS	Lube oil heater switch	Transfer open	0	10,909 H
GGNR	$1x10^{-6}$/H	$7x10^{-4}$/H	PAGGR	Gas generator	Fail to run	0	110 H

---

* Prior distribution not updated, observed data already incorporated.

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
THLK	$1x10^{-6}$/H	$1x10^{-4}$/H	HAHGL	Hot gas exhaust duct	Leak	0	110 H
TBNR	$3x10^{-5}$/H	$3x10^{-3}$/H	PATBR	Turbine	Fail to run	0	110 H
SWIC	$1x10^{-5}$/	$1x10^{-3}$/D	BASAC	Iso.vlv.switch	Fail to close	0	434 D
			PBHBC	Lube oil htr.sw.	Fail to close on demand	0	0 D
			PBTBC	Fuel sys.htr.sw.	Fail to close on demand	0	11 D
SWCL	$1x10^{-7}$/H	$6x10^{-6}$/H	TAISC	Inhibit switch	Transfer closed	0	0 H
			PBCRS	Start/run sw.	Transfer closed	0	10,909 H
			PBCPS	Cntrlr.pwr.sw.	Transfer closed	0	10,909 H
			RBSWF	Start/run switch	Transfer to start from override position	0	0 H
			PBASC	Heater switch	Transfer closed	0	0 H
GBXR	$1x10^{-6}$/H	$1x10^{-4}$/H	PAGBD	Gearbox	Fail to run	0	110 H
CCLO	$1x10^{-2}$/D	$2x10^{-1}$/D	DALCC	Lube oil system	Block in 2nd APU given 1 blocked	2	3 D*

---

* Prior distribution not updated, observed data already incorporated.

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
PFXS	$1x10^{-7}$/D	$5x10^{-5}$/D	BAFPS	Fuel pump	Fail to start	0	217 D
			BALPS	Lube oil pump	Fail to start	0	217 D
TBNS	$1x10^{-7}$/D	$5x10^{-5}$/D	BATBS	Turbine	Fail to start	0	217 D
GBXS	$1x10^{-7}$/D	$5x10^{-5}$/D	BAGBD	Gearbox	Fail to start	0	217 D
EPDS	$1x10^{-5}$/D	$3x10^{-3}$/D	BAIVP	Iso. valve elec. power	Fail to start	0	217 D
EPSS	$2x10^{-5}$/D	$6x10^{-3}$/D	BASVP	Sec. valve elec. power	Fail to start	0	217 D
			PBPVP	Prim. valve elec. power	Fail to start	0	217 D
CKTS	$1x10^{-6}$/D	$1x10^{-3}$/D	BAPVQ	Prim. valve controller	Fail on at start	0	217 D
			BASVQ	Sec. valve controller	Fail to start	0	217 D
			PBPVH	Prim. valve controller	Fail off at start	0	217 D
			RBCRT	Override controller	Delay too short	0	0 D
			TBSVS	Over/underspeed controller	Fail on at start	0	217 D

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
TSPS	$5x10^{-5}$/D	$5x10^{-3}$/D	BAM1H	MPU	Fail high at start	0	651 D
			BAM1L	MPU	Fail low at start	0	217 D
DRON	$1x10^{-6}$/H	$1x10^{-3}$/H	TASDO	Sec. vlv. driver	Fail on	0	0 H
			PADRO	Iso. vlv. driver	Fail on	0	220 H
			PBRP	Cntrlr. pwr. RPC	Fail on	0	10,909 H
FFPL	$3x10^{-7}$/H	$3x10^{-5}$/H	PALFB	Fuel in line filter	Blocked	0	110 H
FPPL	$3x10^{-6}$/H	$1x10^{-3}$/H	PAPFB	Fuel pump filter	Blocked	0	110 H
GQDL	$2x10^{-6}$/H	$2x10^{-4}$/H	PANLQ	Fuel tnk GN2 line quick disconnect	Leak	0	11,019 H
RPIM	$1x10^{-3}$/D	$1x10^{-1}$/D	PAGND	Gearbox	Severe leak given a leak	0	6 D*
ISO2	$1x10^{-6}$/H	$1x10^{-4}$/H	PAFCC	Iso. valves	Common cause transfer closed	0	110 H
EPSF	$1x10^{-6}$/H	$1x10^{-4}$/H	PAVAP	Iso.vlv.elec.pwr.	Fail off	0	220 H
EPDF	$1x10^{-6}$/H	$2x10^{-4}$/H	PASVP	Sec.vlv.elec.pwr.	Fail off	0	110 H

---

* Prior distribution not updated, observed data already incorporated.

TABLE 7.5-2 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	PARAMETERS OF PRIOR DISTRIBUTION 95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
			PAPVP	Primary valve electric power	Fail off	0	110 H
DRON	$1x10^{-6}$/H	$1x10^{-3}$/H	PACRA	Iso. vlv. driver	Fail off	0	0 H
DRST	$3x10^{-7}$/D	$3x10^{-5}$/D	RBPKD	Inhibit circuit diode	Internal short	0	0 D
			BACRA	Iso. vlv. driver	Fail off start	0	0 D
HTOF	$1x10^{-5}$/H	$1x10^{-3}$/H	RBA9Q	Heater 3/23	Fail off	1	10,909 H
			RBABQ	Heater 4/5	Fail off	0	10,909 H
			RBA7Q	Heater 1/2	Fail off	0	10,909 H
			PBA5Q	Heater 13	Fail off	1	10,909 H
			PBA4Q	Heater 10/17	Fail off	0	10,909 H
			PBA3Q	Heater 111/117	Fail off	3	10,909 H
			PBA2Q	Heater 116/117	Fail off	6	10,909 H
			PBA1Q	Heater 14/15	Fail off	0	10,909 H
			PBHAQ	Lube oil heater	Fail off	0	19,909 H
HTCC	$1x10^{-6}$/H	$3x10^{-4}$/H	PBLHC	Lube oil heaters	Fail by common cause	0	10,909 H
			PBFHC	Heater 13A/B	Fail by common cause	1	10,909 H

TABLE 7.5-2 (Concluded)

PRIOR DISTRIBUTION DESIGNATOR	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXPOSURE DATA
HTON	$1x10^{-5}$/H	$1x10^{-3}$/H	PBA4U	Heater 10/17	Fail on	1	10,909 H
			PBA3U	Heater 111/112	Fail on	0	10,909 H
			PBA2U	Heater 116/117	Fail on	0	10,909 H
			PBA1U	Heater 14/15	Fail on	0	10,909 H

TABLE 7.5-3

APU COMPONENT FAILURE DESCRIPTIONS

BOEING PAGE NO	CAR NO	DATE	FLT NO	APU NO	COMP. GROUP	BASIC EVENT	DESCRIPTION
187	AC8511-01	08/06/84	41B	3	VSNC	PASVC	GGVM shut off valve leaking at a rate of 248 scim due to a broken poppet valve seat
N/A*	N/A	04/12/81	1CR	3	VSNL	BASVL PASVL	GGVM shutoff valve allowed fuel to leak into the system, caused gas generator bed temperature to exceed start limits
426	07F010-01	06/18/83	7	3	VSNR	PAPVD	Underspeed shutdown due to an immense quantity of contamination in the GGVM
196	AC8914-01	11/01/84	41G	1	CKTR	PAPCL	Gearbox press. measurement read low due to bad signal conditioner in APU controller
113	AC0055-01	07/24/81	1	2	TSPR	TAM1L	MPU #2 was inopr.; MPU resis. measured opn
N/A*	N/A	11/20/83	9	2	TPRH	PAPTH	Gearbox GN2 pressure went off scale high, but later returned to normal
431	11F007-01	02/03/84	41B	3	TPRH	PAPTH	Gas gen. press. trans. read 100 psia high
102	AB9197-01	04/01/81	1	1	SLLK	PAFPL	Exam. of catch bottle revealed excess leakage from fuel pump seal (20 cc in 10 min.)
102	AB9197-01	04/01/81	1	2	SLLK	PAFPL	Exam. of catch bottle revealed excess leakage from fuel pump seal (45 cc in 10 min.)

---

* Data obtained from the APU subsystem manager database.

TABLE 7.5-3 (Continued)

BOEING PAGE NO	CAR NO	DATE	FLT NO	APU NO	COMP. GROUP	BASIC EVENT	DESCRIPTION
102	AB9197-01	04/01/81	1	3	SLLK	PAFPL	Exam. of catch bottle revealed excess leakage from fuel pump seal (11 cc in 10 min.)
124	AC0905-01	11/07/81	2	1	SLLK	PAFPL	Exam. of catch bottle revealed 41 cc hydrazine after 7.35 min. of operation
N/A*	N/A	04/04/83	6	1	SLLK	PAFPL	Examination of the seal cavity drain system revealed a small amount of seal leakage
N/A*	N/A	04/04/83	6	2	SLLK	PAFPL	Seal cavity drain was found plugged after flight readiness firing
N/A*	N/A	11/11/82	5	3	SLLK	PAFPL	Leak rate to seal cavity drain was 0.289 cc per min.; hydrazine leaking around fuel pump temp. transducer
181	AC8266-01	06/18/84	41D	1	ACLK	PAAGL	Gearbox leaked GN2 at rate of 4.8 psid in 24 hours
181	AC8266-01	06/18/84	41D	3	ACLK	PAAGL	Gearbox leaked GN2 at rate of 7.0.psid in 24 hours; 5 psi press. drop between gearbox and seal cavity drain was not maintained
N/A*	N/A	04/04/83	6	1	ACLK	PAAGL	Low gearbox press. caused activation of GN2 repressurization system on two occasions
N/A*	N/A	06/18/83	7	1	ACLK	PAAGL	GN2 repress. of gearbox occurred twice
N/A*	N/A	06/18/83	7	3	ACLK	PAAGL	GN2 repress. of gearbox occurred once

---

* Data obtained from the APU subsystem manager database.

TABLE 7.5-3 (Continued)

BOEING PAGE NO.	CAR NO.	DATE	FLT NO.	APU NO.	COMP. GROUP	BASIC EVENT	DESCRIPTION
N/A*	N/A	08/30/83	8	1	ACLK	PAAGL	GN2 repress. of gearbox occurred twice
123	AC0878-01F	11/04/81	2	1	FLLP	PALOF	High outlet press. (100 psia) in gearbox lube system; plugged filter caused by fuel contamination
123	AC0878-01F	11/04/81	2	3	FLLP	PALOF	High outlet press. (100 psia) in gearbox lube system; plugged filter caused by fuel contamination
422	04F010-01	07/01/82	4	3	FLLP	PALOF	High lube oil press. indicative of plugged filter during first 3 min. of flight; at 9 min. lube oil press. again rose to approx. 100 psia and continued that level until shutdown
428	09F012-01	11/28/83	9	1	FTLK	LALK1	Hydrazine leakage from cracked fuel injector tubes resulting in fire and explosion
429	09F013-01	11/28/83	9	2	FTLK	LALK1	Hydrazine leakage from cracked fuel injector tubes resulting in fire and explosion
N/A*	N/A	04/12/81	1CR	1	FTLK	LALK1	Ext. leakage from fuel pump cover
N/A*	N/A	04/12/81	1CR	2	FTLK	LALK1	Ext. leakage at fuel pump inlet fitting
414	01F013-01	04/12/81	1	2	HTCC	PBFHC	Gas gen. bed htr.elements "A" & "B" failed off due to leak of argon gas (heat trans. material) through a bad weld

---

* Data obtained from the APU subsystem manager database.

TABLE 7.5-3 (Continued)

BOEING PAGE NO.	CAR NO.	DATE	FLT NO.	APU NO.	COMP. GROUP	BASIC EVENT	DESCRIPTION
425	07F005-01	06/18/83	7	2	HTOF	PBA2Q	Fuel service line temp. fell below lower FDA limit due to thermostat contamination
N/A*	07F026-01	06/18/83	7	3	HTOF	RBA9Q	Thermostat for water injection cooling line heater "A" failed
N/A*	N/A	06/18/83	7	3	HTOF	PBA3Q	Thermostat on seal cavity drain line failed due to contamination; heater "B" failed off
N/A*	N/A	08/30/83	8	2	HTOF	PBA2Q	Fuel service line heater "B" failed off, causing line temperature to drop to 41°F
434	11F016-01	02/03/84	41B	2	HTOF	PBA5Q	Gas generator/fuel pump heater system "A" failed off due to a broken wire in the thermal switch circuitry
N/A*	N/A	10/05/84	41G	2	HTOF	PBA3Q	Fuel pump seal cavity drain heater "A" failed off
435	24F011-01	04/29/85	51B	1	HTON	PBA4U	Fuel bypass line heater "B" failed on; with increasing temp., thermal switch contact resistance increased gradually, in lieu of normal snap action
436	24F012-01	04/29/85	51B	3	HTOF	PBA3Q	Seal cavity drain line heater "3A" failed off due to contamination of therm. 5132A
438	30F014-01	11/06/85	61A	1	HTOF	PBA2Q	Fuel tank isol. valve temp.low when on "A" heater due to insulation damage and improper taping of the heater

---

* Data obtained from the APU subsystem manager database.

TABLE 7.5-3 (Concluded)

BOEING PAGE NO.	CAR NO.	DATE	FLT NO.	APU NO.	COMP. GROUP	BASIC EVENT	DESCRIPTION
439	32F006-01	01/12/86	61C	1	HTOF	PBA2Q	Thermal insulation not properly installed, causing isolation valve temp. to drop
439	32F006-01	01/12/86	61C	3	HTOF	PBA2Q	Thermal insulation not properly installed, causing isolation valve temp. to drop
440	32F008-01	01/12/86	61C	3	HTOF	PBA2Q	Fuel line system "B" heater failed (thermostats 534B and 539B)

TABLE 7.5-4

APU DATA ANALYSIS RESULTS

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
BABVO	Bypass Valve Fails To Open On Demand	4.6890E-04	1.6904E-05	1.7302E-04	1.2761E-03
BABVC	Bypass Valve Fails On Demand	4.6890E-04	1.690E-05	1.7302E-04	1.2761E-03
PASVC	Secondary Valve Fails To Close On Demand	2.6314E-03	2.3053E-04	1.5042E-03	7.4968E-03
BAPVC	Primary Valve Fails To Close On Demand	9.6016E-04	5.0318E-05	4.4838E-04	2.6847E-03
PAVAC	Isolation Valve Fails To Close On Demand	7.2792E-04	4.5426E-05	3.7203E-04	1.8789E-03
BAVAO	Isolation Valve Fails To Open On Demand	7.2791E-04	4.5426E-05	3.7203E-04	1.8789E-03
PANVO	*GN2 Repress. Vlv. Fails To Open On Demand	1.7635E-03	7.4374E-05	7.1606E-04	6.2313E-03
BASVO	Secondary Valve Fails To Open On Demand	9.6016E-04	5.0318E-05	4.4838E-04	2.6847E-03
PAVAL	Isolation Valve Leaks When Closing	7.2792E-04	4.5426E-05	3.7203E-04	1.8789E-03
BASVL	Secondary Valve Leaks At Start	2.6314E-03	2.3053E-04	1.5042E-03	7.4968E-03
PASVL	Secondary Valve Leaks After Closing	2.6314E-03	2.3053E-04	1.5042E-03	7.4968E-03
PAVAZ	Isolation Valve Leaks After Closing	1.1447E-05	5.9427E-07	5.4357E-06	3.2473E-05
PASVZ	Secondary Valve Leaks After Closing	1.4806E-05	6.8792E-07	6.5132E-06	4.0612E-05

---

* This failure rate was multiplied by 1.5 in the split fraction equations, to reflect the fact that repressurization was required twice instead of once in about half of the observed instances of gearbox leakage, for an average of 1.5 demands per leak.

TABLE 7.5-4 (Continued)

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
PANVL	GN2 Repress. Valve Leaks After Closing	1.4757E-05	6.8458E-07	6.4975E-06	4.0524E-05
TASVE	Secondary Valve Fails Open When Pulsing	2.6639E-03	9.3338E-05	9.6978E-04	9.6813E-03
PAPVE	Primary Valve Fails Open When Pulsing	1.4766E-03	6.8516E-05	6.5002E-04	4.0539E-03
PAPVD	Primary Valve Fails Closed When Pulsing	4.4805E-03	3.4939E-04	2.4035E-03	1.2253E-02
PASVD	Secondary Valve Fails Closed When Pulsing	2.6639E-03	9.3338E-05	9.6978E-04	9.6813E-03
PAVAK	Isol. Vlv. Plugs (Due To Contamination) When Open	1.0859E-06	4.6805E-08	4.3431E-07	3.8749E-06
RBWVK	Water System Valve Plugs While Open	1.1E-05	4.7E-07	4.3E-06	3.9E-05
RBWVO	Water System Vlv. Fails To Open On Demand	1.1E-02	3.7E-04	3.9E-03	3.9E-02
GBACO	Hydrazine Leak Into Solenoid Cavity Of Isolation Valve	1.8E-06	2.7E-08	4.2E-07	5.8E-06
HBPCO	Hydrazine Leak Into Solenoid Cavity Of GGVM Valve	8.0E-06	1.7E-07	2.7E-06	2.5E-05
SAICF	Inhibit Circuit Fails To Inhibit	2.6639E-05	9.3338E-07	9.6979E-06	9.6813E-05
TASDS	Shutdown Controller Loss of Signal	2.6639E-05	9.3338E-07	9.6978E-06	9.6813E-05
PASVU	Secondary Controller Fails On	2.6639E-05	8.6765E-07	8.5191E-06	8.1431E-05
PAPVQ	Primary Controller Loss Of Signal	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05
PAPVU	Primary Controller Fails On	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05

TABLE 7.5-4 (Continued)

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
PASVQ	Secondary Controller Loss Of Signal	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05
PAPCH	Gearbox Press. Controller Loss Of Signal	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05
PAPCL	Gearbox Press. Controller Fails On	1.4652E-04	5.8627E-06	5.4499E-05	4.9157E-04
SASVS	Shutdown Controller Fails On	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05
RBCRT	Override Cntrlr. Fails On Demand (Delay Too Short)	2.9E-04	9.1E-07	3.0E-05	9.7E-04
PBPVH	Prim. Valve Cntrlr. Fails Off On Demand (Valve Open)	1.5E-04	8.9E-07	2.3E-05	5.1E-04
TBSVS	Over/Underspeed Cntrlr. Fails On At Start	1.5E-04	8.9E-07	2.3E-05	5.1E-04
TAM1L	Magnetic Pickup Unit (MPU) Fails Low	2.2403E-03	1.7470E-04	1.2017E-03	6.1266E-03
TAM1M	MPU Fails Midrange	1.3320E-03	4.6669E-05	4.8489E-04	4.8406E-03
SAM1H	MPU Fails High	6.3906E-04	3.0873E-05	2.9074E-04	1.8189E-03
PAPTH	Gearbox Pressure Transducer Fails High	1.6729E-03	2.5920E-04	9.8931E-04	3.8727E-03
PAPTL	Gearbox Pressure Transducer Fails Low	3.5948E-04	1.2250E-05	1.4535E-04	1.0499E-03
PAFPL	Fuel Pump Seal Leak	5.2791E-04	2.0301E-04	3.6891E-04	6.8469E-04
PAFNL	Fuel Tank Leak, GN2 Side	6.0394E-06	2.7224E-07	2.3493E-06	1.8356E-05
PANBL	GN2 Bottle Leak	6.0394E-06	2.7224E-07	2.3492E-06	1.8356E-05
PAFDL	Fuel Tank Diaphragm Leak	1.4757E-05	6.8458E-07	6.4975E-06	4.0524E-05

TABLE 7.5-4 (Continued)

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
PAACI	Accumulator Diaphragm Leak	1.1400E-05	5.9340E-07	5.4213E-06	3.2309E-05
RBWLL	Water System Leak	5.2E-05	4.3E-06	2.8E-05	1.4E-04
RBWDL	Water Tank Diaphragm Leak	1.5E-05	6.8E-07	6.5E-06	4.1E-05
PAAGL	Gearbox Leak	4.5644E-04	1.5593E-04	3.2410E-04	6.5549E-04
PAFPR	Fuel Pump Fails To Run	7.6853E-05	2.7910E-06	2.8867E-05	2.7967E-04
PALPR	Lube Oil Pump Fails To Run	7.6853E-05	2.7910E-06	2.8867E-05	2.7967E-04
PALOF	Lube Oil System Loss Of Flow	2.6639E-03	9.3338E-05	9.6979E-04	9.6813E-03
LALK1	Fuel System Leak	2.6639E-04	9.3338E-06	9.6979E-05	9.6813E-04
LALK2	Fuel Sys.Leak In 2nd APU, Given 1 Leaking	2.4138E-01	2.0825E-02	2.0717E-01	4.8795E-01
PBRPC	Controller Power RPC Fails On	2.5E-05	4.0E-07	8.2E-06	7.1E-05
RBPKD	Internal Short Across Inhibit Circuit Diode (On Demand)	8.0E-06	2.8E-07	2.9E-06	2.9E-05
BACRA	*Isolation Vlv. Driver Fails Off On Demand	8.0E-06	2.8E-07	2.9E-06	2.9E-05
PACRA	Isol. Vlv. Driver Fails Off While Running	2.9E-04	9.1E-07	3.0E-05	9.7E-04
RBA9Q	Train A Or B/Water Heater 3/23 Fails Off	1.0E-04	1.4E-05	7.0E-05	2.3E-04

---

* This failure rate was multiplied by 3 in the split fraction equations, to reflect the fact that the isolation valves have 3 drivers in series.

TABLE 7.5-4 (Continued)

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
RBA8Q	Train A Or B/Water Heater 4/5 Fails Off	5.2E-05	4.3E-06	2.8E-05	1.4E-04
RBA7Q	Train A Or B/Water Heater 1/2 Fails Off	5.2E-05	4.3E-06	2.8E-05	1.4E-04
PBA5Q	Train A Or B Of Heater 13 Fails Off	1.0E-04	1.4E-05	7.0E-05	2.3E-04
PBA4Q	Train A Or B Of Heater 10/17 Fails Off	5.2E-05	4.3E-06	2.8E-05	1.4E-04
PBA3Q	Train A Or B Of Heater 111/112 Fails Off	2.4E-04	6.1E-05	1.8E-04	4.1E-04
PBA2Q	Train A Or B Of Heater 116/117 Fails Off	4.6E-04	1.7E-04	3.5E-04	6.8E-04
PBA1Q	Train A Or B Of Heater 14/15 Fails Off	5.2E-05	4.3E-06	2.8E-05	1.4E-04
PBHAQ	Train A Or B Of Lube Oil Heater Fails Off	5.2E-05	4.3E-06	2.8E-05	1.4E-04
PBFHC	Both Trains of Heater 13 Fail Off By Common Cause	6.5E-05	4.6E-06	3.6E-05	1.5E-04
PBLHC	Both Lube Oil Heater Trains Fail Off By Common Cause	2.1E-05	5.3E-07	7.8E-06	5.7E-05
PBA4U	Train A Or B Of Heater 10/17 Fails On	1.0E-04	1.5E-05	7.0E-05	2.3E-04
PBA3U	Train A Or B Of Heater 111/112 Fails On	5.2E-05	4.3E-06	2.8E-05	1.4E-04
PBA2U	Train A Or B Of Heater 116/117 Fails On	5.2E-05	4.3E-06	2.8E-05	1.4E-04
PBA1U	Train A Or B Of Heater 14/15 Fails On	5.2E-05	4.3E-06	2.8E-05	1.4E-04
PBBSO	Train A Or B Heater Switch Transfers Open	4.5E-06	3.6E-07	2.2E-06	1.3E-05
PBTBC	Heater Switch Fails To Close On Demand	2.6E-04	9.3E-06	9.7E-05	9.6E-04

TABLE 7.5-4 (Continued)

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
PBTAO	Heater Switch Fails To Open On Demand	7.8E-05	2.8E-06	2.9E-05	2.8E-04
PBASC	Heater Switch Transfers Closed	1.7E-06	9.4E-08	7.5E-07	5.8E-06
PBHBC	Lube Oil Heater Switch Fails To Close	2.7E-04	9.3E-06	9.7E-05	9.7E-04
PBCS1	Fuel System Heater Switch - Both Poles Transfer Open	5.7E-08	3.8E-09	2.8E-08	1.9E-07
PBCS4	Lube Oil System Heater Switch -- Both Poles Transfer Open	5.7E-08	3.8E-09	2.8E-08	1.9E-07
PBHBS	Lube Oil Heater Switch Transfers Open	5.0E-06	3.7E-07	2.4E-06	1.4E-05
RBSWF	Start/Run Switch Goes To Start Instead Of Override	1.7E-06	9.4E-08	7.5E-07	5.8E-06
PBCRS	Start/Run Switch Transfers Closed	1.6E-06	9.3E-08	7.4E-07	5.5E-06
PBCPS	Controller Power Switch Transfers Closed	1.6E-06	9.3E-08	7.4E-07	5.5E-06
PBCPO	Cntrlr. Pwr. Sw. Fails To Open On Demand	7.4E-05	2.8E-06	2.9E-05	2.6E-04
PASAO	Isolation Valve Switch Fails To Open	6.9730E-05	2.7661E-06	2.7121E-05	2.1435E-04
PASAF	Isolation Valve Switch Transfers Open	2.8680E-04	1.7592E-05	1.2330E-04	8.3552E-04
PAGGR	Gas Generator Fails To Run	1.4355E-04	9.0197E-07	2.4673E-05	4.4286E-04
HAHGL	Hot Gas Exhaust Duct Leak	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05
PATBR	Turbine Fails To Run	6.0414E-04	2.7225E-05	2.3496E-04	1.8365E-03

TABLE 7.5-4 (Continued)

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
BASAC	Isolation Valve Switch Fails To Close	1.9019E-04	9.0084E-06	7.6141E-05	5.6335E-04
TAISC	Inhibit Switch Transfers Closed	8.4023E-05	4.6987E-06	3.7682E-05	2.9090E-04
PAGBD	Gearbox Fails To Run	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05
DALCC	Restricted Lube Oil Circulation In 2nd APU Given 1 APU Circulation Restricted	6.7699E-02	9.5419E-03	4.3823E-02	1.9497E-01
BAFPS	Fuel Pump Fails To Start	1.2777E-05	9.1386E-08	2.1384E-06	4.7024E-05
BALPS	Lube Oil Pump Fails To Start	1.2777E-05	9.1386E-08	2.1385E-06	4.7024E-05
BATBS	Turbine Fails To Start	1.2777E-05	9.1386E-08	2.1384E-06	4.7024E-05
BAGBD	Gearbox Fails To Start	1.2777E-05	9.1386E-08	2.1384E-06	4.7024E-05
PBPVP	Electric Power To Primary Valve Fails To Start On Demand	6.2E-04	1.3E-05	2.0E-04	1.9E-03
BAIVP	Elec. Pwr. To Isol. Valve Fails To Start	4.0290E-04	8.5825E-06	1.1849E-04	1.0918E-03
BASVP	Failure Of Electric Power (Or 1 of 2 Switches) To Secondary Valve	6.2071E-04	1.3293E-05	2.0452E-04	1.8790E-03
BAPVQ	Primary Valve Controller On At Start	1.5315E-04	8.8544E-07	2.3380E-05	5.1009E-04
BASVQ	Secondary Vlv. Cntlr. Fails Off At Start	1.5315E-04	8.8544E-07	2.3380E-05	5.1009E-04
BAM1H	MPU Fails High At Start	4.8201E-04	2.7854E-05	2.4075E-04	1.2683E-03
BAM1L	MPU Fails Low At Start	7.4092E-04	3.4467E-05	3.2596E-04	2.0316E-03

TABLE 7.5-4 (Concluded)

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
TASDO	Secondary Valve Driver Fails On	2.8670E-04	9.0961E-07	3.0235E-05	9.6910E-04
PADAO	Isolation Valve Driver Fails On	1.5270E-04	8.8520E-07	2.3261E-05	5.0836E-04
PALFB	Fuel Inline Filter Plugs	7.9593E-06	2.7992E-07	2.9070E-06	2.8935E-05
PAPFB	Fuel Pump Filter Plugs	2.0401E-04	2.7220E-06	5.0018E-05	6.5074E-04
PANLQ	Fuel Tank GN2 Line QD Leaks	2.2800E-05	1.1868E-06	1.0843E-05	6.4617E-05
PAGND	Severe Gearbox Leak (Given Gearbox Is Leaking)	2.6639E-02	9.3338E-04	9.6979E-03	9.6813E-02
PAFCC	Isolation Valves Transfer Closed Due To Common Cause	2.6284E-05	9.3234E-07	9.6723E-06	9.5611E-05
PAVAP	Failure Of Electric Power To An Isolation Valve	2.5944E-05	9.3132E-07	9.6471E-06	9.4414E-05
PASVP	Failure Of Electric Power (Or Switch) To Secondary Valves	4.9572E-05	9.2306E-07	1.3570E-05	1.8657E-04
PAPVP	Failure Of Electric Power (Or Switch) To Primary Valves	4.9572E-05	9.2306E-07	1.3570E-05	1.8657E-04

7.6 SPATIAL INTERACTIVE EVENT DATA DEVELOPMENT

Based on the discussion of Section 6.6, two types of spatial interactive events (SIEs) were identified as significant for development of probability distributions.

a. Events related to APU turbine breakup

b. Events related to APU fuel (hydrazine) leakage

Each SIE, to be a meaningful input to the PRA, must be defined as a conditional probability and described in the probability of frequency format. However, the frequencies associated with SIEs are less amenable to direct calculation than are those associated with component failures, for which failure history data is available. The approach to developing the probability distributions was to collect and analyze, to the greatest extent possible, all information relevant to the SIEs. Examples of available sources were drawings, test reports, formal and informal analyses, and telecons. Candidate probability distributions were then proposed using the assembled and analyzed data.

A group of systems experts, hereinafter referred to as the "Group", whose function was discussed in Section 5.10, was assembled to review the most significant SIEs and propose probability distributions as a group.

There were some instances where test data or analyses were available, but time constraints did not allow adequate melding of opinion and the available data. For those cases, the final probability distribution represents a judicious weighing of the two sets of inputs.

Table 7.6-1 presents the split fractions required for input into the APU PRA.

7.6.1 SIE Data Related to APU Turbine Breakup

The following paragraphs present the probability of frequency distributions developed to represent the conditional probabilities related to APU turbine breakup, and discuss the data that support these distributions.

TABLE 7.6-1

APU SPLIT FRACTIONS FOR SIEs

Name	Split Fraction
F1	Pr (APU Turbine Fail | Primary and Secondary Valves Fail Open)
F3	Pr (Uncontained Shrapnel | Turbine Breakup Due to Overspeed)
F3N	Pr (Uncontained Shrapnel | Turbine Breakup at Normal Speed)
F5	Pr (Failure of Second APU or Flight Control Equipment (FCE) | Shrapnel Due to Turbine Breakup at Overspeed)
F5N	Pr (Failure of Second APU or FCE | Shrapnel Due to Turbine Breakup at Normal Speed)
F7	Pr (Fuel Leak | Uncontained Shrapnel from Second APU)
F12	Pr (APU fail | Small Leak in That APU
F13	Pr (APU Fail | Small Leak in Another APU
F15	Pr (2 APUs or FCE Fail | Small Leak in One of the Two APUs
F17	Pr (2 APUs or FCE Fail | Small Leaks in at Least Two APUs

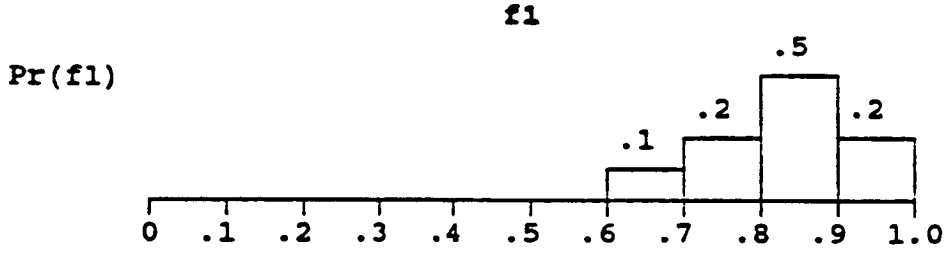
7.6.1.1 Probability of Turbine Breakup at Normal Speed

The probability of turbine breakup at normal speed was developed from military data (NPRD-3), Reference 99, as modified by environment factors appropriate to missile launches. This prior probability distribution is shown in the previous paragraph, Table 7.5-2. The actual failure history of APU turbines (zero failures in 110 hours) was then used as the likelihood to arrive at the posterior distribution also presented in the previous paragraph, Table 7.5-4, via the use of Bayes' Theorem. The information used for NPRD-3 is a compilation from diverse

small, high speed turbines used in military applications. The information did not provide the fraction of turbine failures which actually yielded turbine hub breakup. Therefore, a large uncertainty was assigned to the NPRD value to account for the applicability of the NPRD source to APU turbine breakup. The distribution used for this study was a log-normal with a 5^{th} percentile of 2.7×10^{-5} failure/hour and a 95^{th} percentile of 1.8×10^{-3} failure hour. This distribution was used in the evaluation of Top Events PA, PB and DB.

7.6.1.2 Probability of Turbine Breakup Due to Overspeed

The Group discussed the likelihood that a turbine breakup would result from an overspeed induced by failure of both the primary and secondary fuel control valves in the open position. If the valves fail open, a high speed shutdown should be commanded with automatic closing of the fuel isolation valves. This closing would limit the supply of fuel to the turbine and thus limit the peak rotation rate. It is not certain, however, that this closing will prevent breakup due to overspeed, since overspeed conditions are reached in approximately 300 milliseconds, and the fuel line downstream of the isolation valve contains sufficient hydrazine for 2 seconds of operation (about 7 pulses). In view of the above, the Group judged that if the fuel control valves fail open, there is a very high probability that the turbine will break up. This is expressed in the following discrete probability distribution.



Frequency of Occurrence (f1)

$Pr\ (f_1)$	.1	.2	.5	.2
f_1	.65	.75	.85	.95

This distribution was used in the evaluation of event tree Top Events CA and CB following occurrence of TA and TB respectively.

7.6.1.3 Probability of Uncontained APU Shrapnel as a Consequence of Turbine Breakup at Overspeed

The probability of having uncontained fragments as a result of a turbine breakup is determined by the expected breakup speed and by the ability of the APU structure to contain fragments at the expected energy levels.

There have been four incidents of turbine hub breakup during testing. These are shown in Table 7.6-2. In each case, breakup resulted from overspeed.

TABLE 7.6-2

TURBINE HUB BREAKUP DATA

Unit Test	Actual Breakup Speed
S/N 003 (Unnotched)	107,520 rpm (149.3%)
S/N 106 (Unnotched)	112,600 rpm (156.0%)
S/N 105 (Notched)	84,240 rpm (117%)
Rig Test (Drilled)	99,700 rpm (138.5%)

The data from three of the four turbine hub fragmentation incidents were utilized to estimate the turbine hub breakup likelihood as a function of turbine speed (Reference 61). The S/N 105 unit breakup speed was adjusted to estimate the unnotched breakup speed. The rig test data was not included since no information was available about the configuration or test conditions.

The results of this analysis of test data indicate that a mean turbine hub breakup speed of 108,000 rpm (150%) and a standard deviation of 4,267 rpm should be used in evaluating the effects of a turbine breakup due to overspeed. This analysis assumed that breakup speed is normally distributed and that unit S/N 105, as modified, is a valid data point for the analysis. It ignores the effect of life cycles on breakup speed.

Reference 25 presents calculations to estimate APU turbine overspeed required to burst the containment ring and produce shrapnel. Estimated speed for this event was 96,900 rpm or 134.6% of normal operating speed. Thus, the likelihood of APU fragments being uncontained is the likelihood that the fragmentation speed will exceed 96,900 rpm.

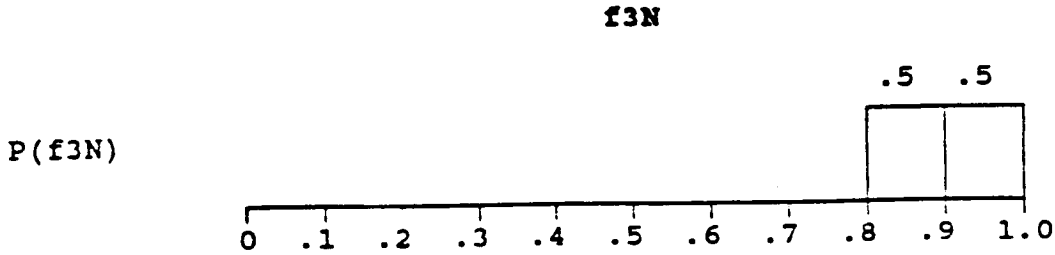
The group of systems experts discussed the information relating to the fragmentation incidents and agreed that a breakup due to an APU overspeed would certainly produce uncontained shrapnel, and therefore assigned:

P(f3)	1.0
f3	1.0

This value was used in the evaluation of event tree Top Events CA and CB following occurrence of TA and TB, respectively.

7.6.1.4 Probability of Uncontained APU Shrapnel as a Consequence of Turbine Breakup at Normal Speed

The information presented in paragraph 7.6.1.3 is also valid for assessing the effects of turbine breakup at normal speed. However, even though unit S/N 105 broke up at a speed below that required to burst the containment ring, fragments bypassed the containment ring and exited through the APU housing. This was attributed to the effects of notches in the turbine hub (Reference 96). The Group, in considering this failure, judged that any turbine that broke up at normal speed would have to be seriously flawed and, hence, assigned the following discrete probability distribution.



Frequency of Occurrence

P(f3N)	.50	.50
f3N	.85	.95

This distribution was used in evaluating event tree Top Events CA and CB following occurrence of PA and PB, respectively.

7.6.1.5 Probability of a Second APU or Flight Critical Equipment Failure as a Consequence of Uncontained Shrapnel from a Turbine Breakup at Overspeed

Given uncontained shrapnel from a turbine overspeed, the likelihood that this shrapnel would cause a second APU or flight critical equipment to fail is determined by three factors: the energy level of uncontained shrapnel, the likelihood of an uncontained fragment striking the equipment, and the vulnerability of the equipment.

The energy of the uncontained fragments can be estimated as the energy of the turbine hub fragments minus the minimum energy required to burst the containment ring. The energy of the turbine hub fragments was estimated by extending the calculations in Reference 25. It was assumed that the hub would break into three 120° segments, each weighing approximately 0.9 pounds. This breakup pattern is consistent with observed test failures (Reference 96).

Using the approach of Reference 25, the minimum energy required to burst the containment ring is calculated to be 19,359 lb-ft. The energy of APU turbine fragments and the energy of resulting uncontained fragments at various speeds are presented in Table 7.6-3.

TABLE 7.6-3

APU UNCONTAINED FRAGMENT ENERGIES

Oper. Speed (%)	W (rpm)	Fragment Energy (lb-ft)	Uncontained Frag.Energy (lb-ft)
100	72,000	10,688	0
110	79,200	12,932	0
120	86,400	15,390	0
130	93,600	18,063	0
140	100,800	20,948	1,589
150	108,000	24,048	4,689
160	115,200	27,361	8,002
170	122,400	30,888	11,529
180	129,600	34,629	15,270
190	136,800	38,584	19,225
200	144,000	42,752	23,393

The likelihood of an uncontained fragment striking a given piece of equipment must account for the fragment spray pattern and the location of the equipment in the aft compartment relative to the fragmentation source.

The fragment spray pattern that would result from an uncontained APU turbine fragmentation is difficult to define analytically because of the random nature of the particle paths, the lack of failure data and the complex APU containment ring geometry. Limited test data documentation, Reference 96, states that:

> "The pieces of the turbine wheel (hub) that were not contained by the [turbine] housing exited in a radial direction. In the S/N 106 burst, the section of wheel found in the aluminum heater panel exited within 15 ° of the true radial."

Based on this limited data, the possibility of fragments striking equipment at angles of at least 15° above or below the plane of the turbine wheel must be considered.

The expectation that the turbine will fragment into three 120° segments means that there is a 100% likelihood that any 120° arc of the x-y plane will contain one fragment. The likelihood of a given fragment direction within the 120° arc is uniformly distributed.

To assess the likelihood of a fragment striking a piece of equipment, a spatial analysis (Reference 61) was performed. This analysis considered the item's location above and below the plane of the turbine and its profile area. Table 7.6-4 lists equipment considered susceptible to being struck by APU fragments within ±15° of the turbine plane of rotation.

TABLE 7.6-4

POTENTIAL TARGETS OF APU TURBINE FRAGMENTS

EQUIPMENT	APU 1	APU 2	APU 3
LEFT OMS OXID TK	X	X	X
LEFT OMS FU TK		X	X
RT OMS OXID TK	X	X	X
RT OMS FU TK	X	X	
LEFT RCS OXID TK	X	X	X
RT RCS OXID TK	X	X	X
RT RCS FU TK		X	
APU 1 FU TK	X		X
APU 2 FU TK			X
APU 3 FU TK	X	X	X
AVIONICS BAY 4			X
AVIONICS BAY 5	X		
HYD RES 3	X	X	
APU 1 FU LINE	X	X	
APU 2 FU LINE	X	X	
APU 3 FU LINE			X
APU 1 LUBE LINE	X	X	
APU 2 LUBE LINE		X	
APU 3 LUBE LINE			X
APU 1 EXHST DUCT		X	
SYS 1 HYD LINE	X	X	X
SYS 2 HYD LINE	X	X	X
SYS 3 HYD LINE	X	X	X
SSME LO2 MANIF			
SSME 1 LO2 FDLINE	X	X	X
SSME 2 LO2 FDLINE			
SSME 3 LO2 FDLINE			
SSME LH2 MANIF	X		X
SSME 1 LH2 FDLINE	X	X	X
SSME 2 LH2 FDLINE	X	X	X
SSME 3 LH2 FDLINE			X
WIREBUNDLES	X	X	X

This table also lists "lines" and wirebundles that, because of their location, are considered potential targets. Because of their complex geometry, a subjective assessment of their susceptibility was performed instead of a quantitative spatial analysis.

Given the fragment spray pattern described above and the proximity of the APUs to the 1307 bulkhead and sidewalls, it must be considered that there is a very high likelihood than an uncontained fragment will strike either the bulkhead or a sidewall.

To assess the vulnerability of equipment, it is necessary to consider the penetration capability of the fragments relative to the characteristics of the target equipment. Reference 105 discusses the effects of fragmentation of jet engine turbines. The penetration capability of uncontained APU fragments was estimated by using the analysis approach of Reference 105 and the uncontained fragment energies presented in Table 7.6-3 above. All fragments were assumed to strike perpendicular to the surface. The penetration depth in common material for various overspeeds is shown in Table 7.6-5 below.

TABLE 7.6-5

PENETRATION CAPABILITY OF UNCONTAINED FRAGMENTS

Overspeed (%)	W (rpm)	Penetration Depth (Inches)		
		Al	Ti	Steel
130	93,600	0	0	0
140	100,800	0.36	0.16	0.14
150	108,000	0.61	0.27	0.25
160	115,200	0.80	0.37	0.32
170	122,400	0.96	0.44	0.39
180	129,600	1.11	0.51	0.45
190	136,800	1.24	0.57	0.50
200	144,000	1.37	0.68	0.55

Al = Aluminum Ti = Titanium

The physical dimensions of selected equipment installed in the aft compartment are presented in Table 7.6-6. As may be seen by comparing the data of Table 7.6-6 with those of Table 7.6-5, the theoretical penetration capability of uncontained fragments significantly exceeds the panel thickness of the critical equipment in Table 7.6-6, as well as portions of the 1307 bulkhead and aft compartment side walls.

TABLE 7.6-6

WALL THICKNESSES OF SELECTED EQUIPMENT

Equipment	Diameter (Inches)	Wall Thickness (Inches)	Material
Hydraulic Pressure Lines	1-1/4 to 1/4	.065 to .020	Titanium
Hydraulic Return Lines	7/8 to 1/4	.026 to .020	Titanium
MPS 17" LH2 Line	17	.040	Inconel 718
Vacuum Jacket		.025	CRES 321
MPS LH2 Manifold	--	.063	Inconel 718
Vacuum Jacket		.040	CRES 321
MPS 12" LH2 Line	12	.032	Inconel 718
Vacuum Jacket		.040	CRES 321
MPS 17" LO2 Line	17	.050	Inconel 718
Vacuum Jacket		.040*	CRES
MPS LO2 Manifold	--	.080	Inconel 718
Vacuum Jacket		Foam	CRES 321
MPS 12" LO2 Line	12	.050	Inconel 718
Vacuum Jacket		.040*	CRES 321
APU Fuel Lines	1/2	.025	Stnls Steel
APU GN2 Lines	3/8	.020	Stnls Steel
1307 Bulkhead Pnl	--	.050	Aluminum
Aft Comprt Sdwls	--	.136 to .070	Aluminum
OMS Deck Panels	--	.070 & .063	Aluminum
OMS Tanks	--	.0759	Titanium
Avionics Bays	--	1" Honeycomb	Aluminum
		.020 Facing Sh	Aluminum

*OV 102 only. LO2 lines are foam insulated on other vehicles.

In a discussion with a representative of the JSC Materials Technology Branch, some test results were obtained in which a 1 inch long cylindrical object was projected at a .05 inch thick panel similar to the 1307 bulkhead panels. The panel was penetrated by .5 lb. projectile traveling at 100 ft/sec. The energy of the projectile was 77.7 lb-ft, which is relatively small by comparison with the estimated energies for turbine wheel fragments in Table 7.6-3. These test results were not yet published at the time this study was conducted.

Based on the theoretical estimates and the limited amount of supporting test data, it must be concluded that all of the equipment items in Table 7.6-4 are vulnerable to being damaged if struck by uncontained fragments of an APU turbine hub. A comprehensive quantitative analysis pinpointing exact dimensions and impact angles is not within the scope and budget of this study.

In view of the significant number of critical equipment items subject to damage, and the complex geometry of the aft compartment, it must be concluded, for purposes of this PRA, that an uncontained turbine hub breakup has a very high probability of causing loss of a second APU or Flight Critical Equipment (FCE) and, consequently, crew and vehicle.

The likelihood of puncturing the External Tank is estimated to be zero. The centerline of the External Tank is parallel to the plane of rotation of the turbine. A particle on a trajectory 15° below the plane of turbine would have to penetrate a significant portion of the Orbiter to strike the External Tank, including the 1307 Bulkhead, the payload bay (and payloads) and finally, the Orbiter skin and tiles.

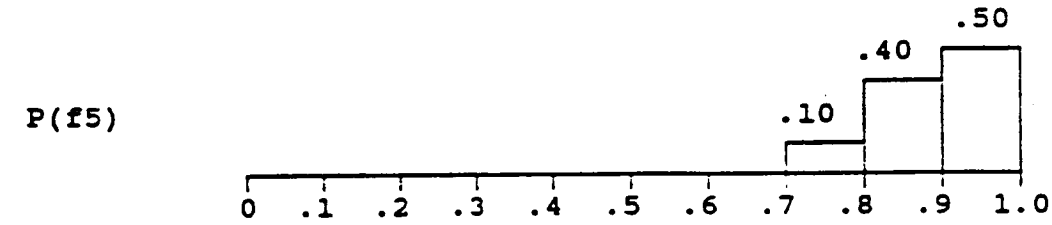
The Group discussed the likelihood that uncontained shrapnel from a turbine overspeed would cause a second APU or flight critical equipment to fail. In addition to failures caused by the shrapnel per se, the group's considerations included the failure of another APU or FCE as a result of the fuel leakage that would accompany the breakout of shrapnel.

It was recognized that the conditional probabilities would differ between ascent and descent. For example, during ascent the pre-launch nitrogen purge in the aft compartment precludes combustion from hydrazine sources. The main engine feedlines flowing large quantities of liquid oxygen and liquid hydrogen represent a severe threat if struck by shrapnel. However, during descent the main

engine feedlines are inert, but air not available during ascent, enters the aft compartment, providing an environment which will support combustion. This is relevant to the possibility of fire resulting from a hydrazine leak.

After considering the factors discussed in the initial paragraphs above, it was decided to use the following probability of frequency distributions for ascent and descent.

Ascent - f5

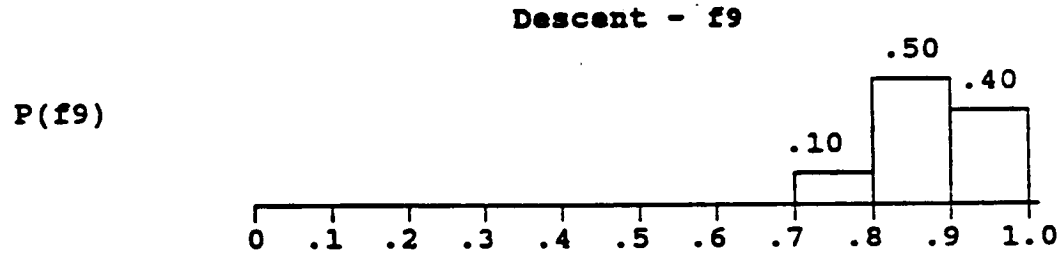


Frequency of Occurrence

P(f5)	.1	.4	.5
f5	.75	.85	.95

This distribution was used in the evaluation of Event Tree Top Event CA after the occurrence of TA.

Descent - f9



Frequency of Occurrence

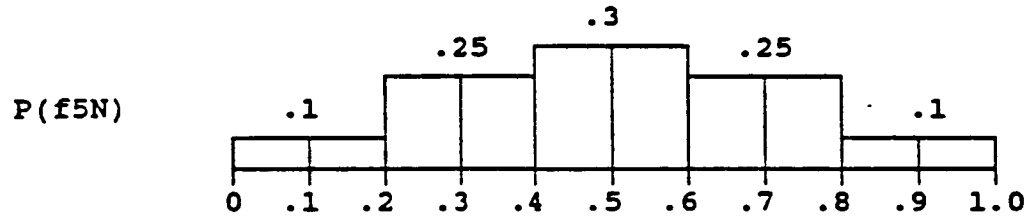
P(f9)	.1	.5	.4
f9	.75	.85	.95

This distribution was used in the evaluation of event tree Top Event CB after the occurrence of TB.

7.6.1.6 Probability of a Second APU or Flight Critical Equipment Failure as a Consequence of Uncontained Shrapnel from a Turbine Breakup at Normal Speed

The data from Table 7.6-3 above indicates that the energy from a breakup at normal speed would not be high enough to break the containment ring. However, as explained in Section 7.6.1.4, the Group, based on the S/N 105 test, judged that there was a high probability that shrapnel would bypass the containment ring and break through the APU housing. In considering this conditional probability, they also recognized that the shrapnel would be of a lower energy level and assigned the following distributions.

Ascent - f5N

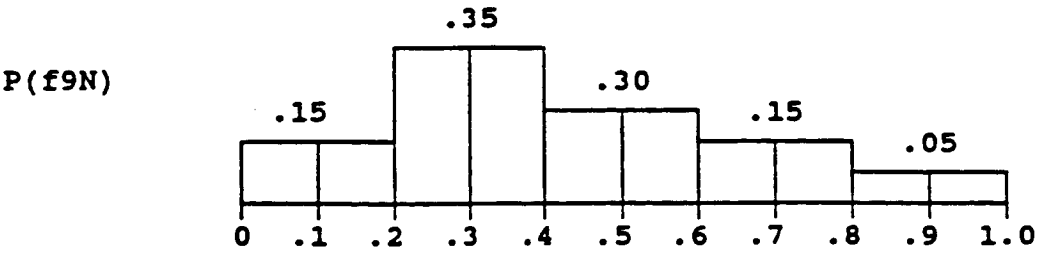


Frequency of Occurrence

P(f5N)	.1	.25	.3	.25	.1
f5N	.1	.3	.5	.7	.9

This distribution was used in the evaluation of Top Event CA after occurrence PA.

Descent - f9N



Frequency of Occurrence

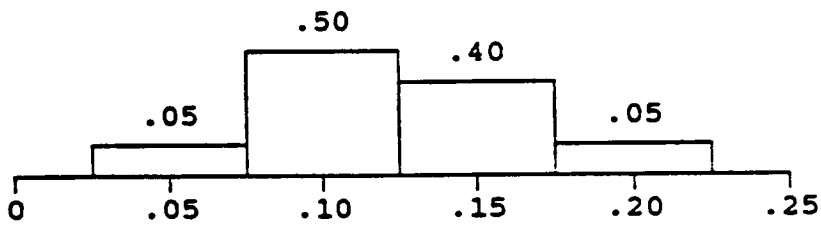
P(f9N)	.15	.35	.30	.15	.05
f9N	.1	.3	.5	.7	.9

This distribution was used in the evaluation of CB following the occurrence of PB.

7.6.1.7 Probability of a Hydrazine Leak as a Consequence of Uncontained Shrapnel From Another APU

The Group considered this conditional probability to include the possible effect of a fire which would certainly accompany a turbine breakup. STS-9 dramatically illustrated how a leak and fire from one APU can affect a second APU. Thus, while the probability of an APU being struck by a fragment is the same for ascent and descent, the likelihood of a fuel fire on descent makes damage more likely during that phase. The Group assigned the following probability distributions:

f7 - Ascent



Frequency of Occurrence

P(f7)	.05	.50	.40	.05
f7	.05	.10	.15	.20

This distribution was used in the evaluation of event tree Top Event FA after the occurrence of TA without the occurrence of CA.

No 7-74

In the event of a large hydrazine leak during entry, (e.g., the contents of an APU fuel tank leaks into the aft compartment) the experts surveyed believe that a large fire would result, leading to loss of the crew and vehicle.

APU fuel leakage may ultimately lead to hydrazine detonation. Hydrazine explodes when heated to a detonation temperature determined by the surface material in contact with the hydrazine. The detonation temperature may be achieved by heating the hydrazine or by adiabatically compressing hydrazine containing vapor bubbles.

Under adiabatic compression conditions, the threshold temperature limit for explosive decomposition of hydrazine was between 217°F and 195°F in containers made of CRES-321, Hastelloy-X, Haynes-25, CRES-316, CRES-347 and CRES-304L. These metals are listed in order of decreasing threshold temperature (Reference 92). Without compression, liquid hydrazine will explode at high temperature. Tests performed at the NASA White Sands Test Facility indicate that liquid hydrazine in a test chamber constructed of 304 stainless steel may explode at temperatures above about 445°F (Reference 88).

7.6.2.1 Probability of APU Failure Given a Small Fuel Leak in That APU

Several mechanisms contribute to the event of an APU failure given a small fuel leak in that APU. A small contribution to the frequency of this event arises from APU fuel leaking into the solenoid cavity of a fuel isolation valve or gas generator control valve and detonating, thereby interrupting usage of the valve. A second small contributor to this event is leakage by means of breakage of the carbon face of an APU fuel pump seal, allowing the hydrazine to detonate because of metal rubbing against metal, and thereby causing the fuel pump to fail.

Aside from fire, two additional mechanisms are relevant to hydrazine leakage into the aft compartment. These are: (1) stripping of Kapton electrical wiring insulation leading to loss of GGVM control, and (2) hydrazine decomposition initiated by some catalyst in the environment. Hydrazine is known to dissolve Kapton. However, the Group could not agree as to whether the APU Kapton wiring insulation would be removed in the time interval (about 8 minutes) between APU startup and attaining an altitude at which hydrazine cannot exist as a liquid. With regard to hydrazine decomposition, it is known that catalysts

exist which cause hydrazine to decompose at room temperature. An example of such a reaction is taken from Reference 91.

> "When two or three drops of hydrazine were dropped onto a layer of ferric oxide . . . at the temperature of the laboratory . . . in a nitrogen atmosphere, sparking occurred, and the oxide became red hot, but flame did not appear . . ."

Again the Group differed in their opinions regarding the possible presence of such a catalyst in the Orbiter aft compartment.

After consideration of the opinions offered, the following assignment was made for the distribution associated with APU failure given a small fuel leak in that APU during ascent:

Pr(f12A)	.15	.35	.35	.15
f12A)	.05	.15	.25	.35

This distribution was used in the evaluation of event tree Top Events C1, C2 and C3 when no APUs had failed, and in the evaluation of FA if an APU had previously failed.

Considering the increased risk due to fire on descent, the following assignment was made for the split fraction associated with APU failure given a small fuel leak in that APU during descent:

Pr(f12D)	.1	.2	.3	.25	.10	.05
f12D	.4	.5	.6	.7	.8	.9

This distribution was used in the evaluation of event tree Top Events D1, D2, and D3 when no APUs had failed or in the evaluation of FB if an APU had previously failed.

7.6.2.2 Probability of APU Failure Given a Small Fuel Leak in Another APU

The probability of APU failure given a small fuel leak in another APU was agreed by the Group to be much less during ascent than the probability of APU failure given a small fuel leak in that APU. Internal fuel leakage in another APU was considered to pose a reduced risk since the resulting detonation could produce, at most, low energy shrapnel.

8.0 QUANTITATIVE RESULTS OF THE APU PRA

The PRA model was constructed from the top down. The analysis started with the major functions of the shuttle, loss of which would cause loss of mission or loss of crew and vehicle. This failure logic was documented in the Master Logic Diagrams. Those diagrams were developed to the level of initial failure categories of the APU that could lead to the damage states LOC/V, intact abort, PLS, or launch scrub. By means of event sequence diagrams, all significant scenarios that could lead from an initial failure to one of the damage states were defined and described. The event trees and split fraction models provided further detail of the scenarios in a form that was also quantifiable. The level of detail was commensurate with the data collected from various sources throughout NASA, and was generally at a component or subcomponent level.

Quantification, in contrast to model development, is performed from the bottom up. Probability distributions that reflect actuarial information about the APU, analysis, maintenance procedures, and engineering judgment were developed for each component, subcomponent, and event in the model. The minimal cut sets of the split fraction models were obtained and the appropriate probability distribution assigned to each basic event in the cut sets. The RISKMAN software permitted the development of algebraic equations representing each split fraction and use of the assigned probability distributions to obtain the numerical value of each split fraction in the APU event tree. Another module of RISKMAN combined the split fractions to obtain the frequency of each scenario. Since each scenario was associated with a damage state (or the OK state), scenario frequencies were summed, as shown in Section 5, to obtain the total damage state frequency.

The results of this study are presented in terms of probability distributions and the risk contributions that make up those distributions. The probability distributions are discussed in terms of the following:

a. Prelaunch and ascent (Stage A) risk profiles for each damage state and the interpretation of the profiles

b. Entire flight (Stages A and B combined) risk profiles for each damage state and the interpretation of the profiles

The risk contributors are discussed in terms of the following:

a. Description of failure scenarios in order of their importance to the risk profiles

b. Description of APU component failure modes in order of their importance to the risk profiles

8.1 RISK PROFILES

8.1.1 Risk Profiles for Stage A: Prelaunch and Ascent

The probability distributions shown in Figure 8-1 represent the study conclusions about (1) the frequency with which APU failures would result in loss of crew or vehicle, (2) the frequency of flights in which APU failures would result in launch scrub, and (3) the frequency with which APU failures would result in intact aborts during ascent. The time employed in the determination of (1) and (3) above includes the period from lift-off to APU shut-down after the OMS-1 burn. The time employed in the determination of (2) includes the period from prelaunch APU start to lift-off. The frequency of launch scrubs includes only failures which prevent APU start and those which prevent continued APU operation. Those failure modes which represent only a violation of launch commit criteria were omitted due to limited time and resources, in order to simplify the model. The failure modes and failure scenarios contributing to these risk curves are presented in Tables 8-1 through 8-8, and are discussed later. Figure 8-2 shows all three probability distributions plotted on a common scale.

A great deal of information is contained in these distributions even without looking further into what scenarios contribute most to them. The results show that the range of possible frequencies of LOC/V during ascent lies between 1 in 250 and 1 in 100,000 flights. That is, one should not expect an LOC/V before 250 flights, but LOC/V is almost certain within 100,000 flights. We are 90% confident that the frequency with which APUs would cause loss of crew or vehicle during ascent lies between 1 in about 42,000 flights (5th percentile) and 1 in about 1,400 flights (95th percentile). The median frequency of occurrence is 1 in about 9600 flights (50th percentile), and the average frequency of occurrence is 1 in about 3800 flights (mean).

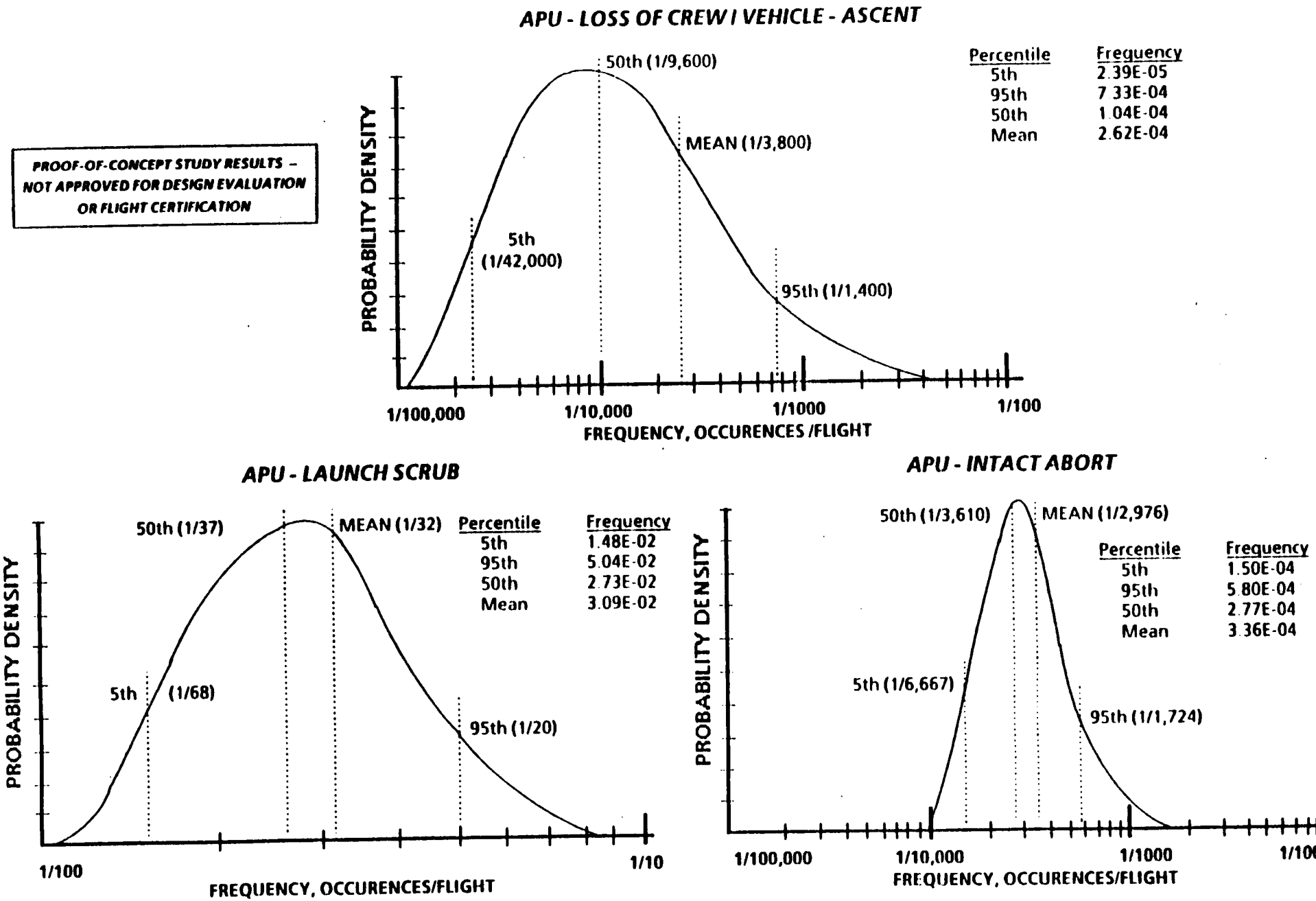


Figure 8-1. Probal . Distributions for Stage A

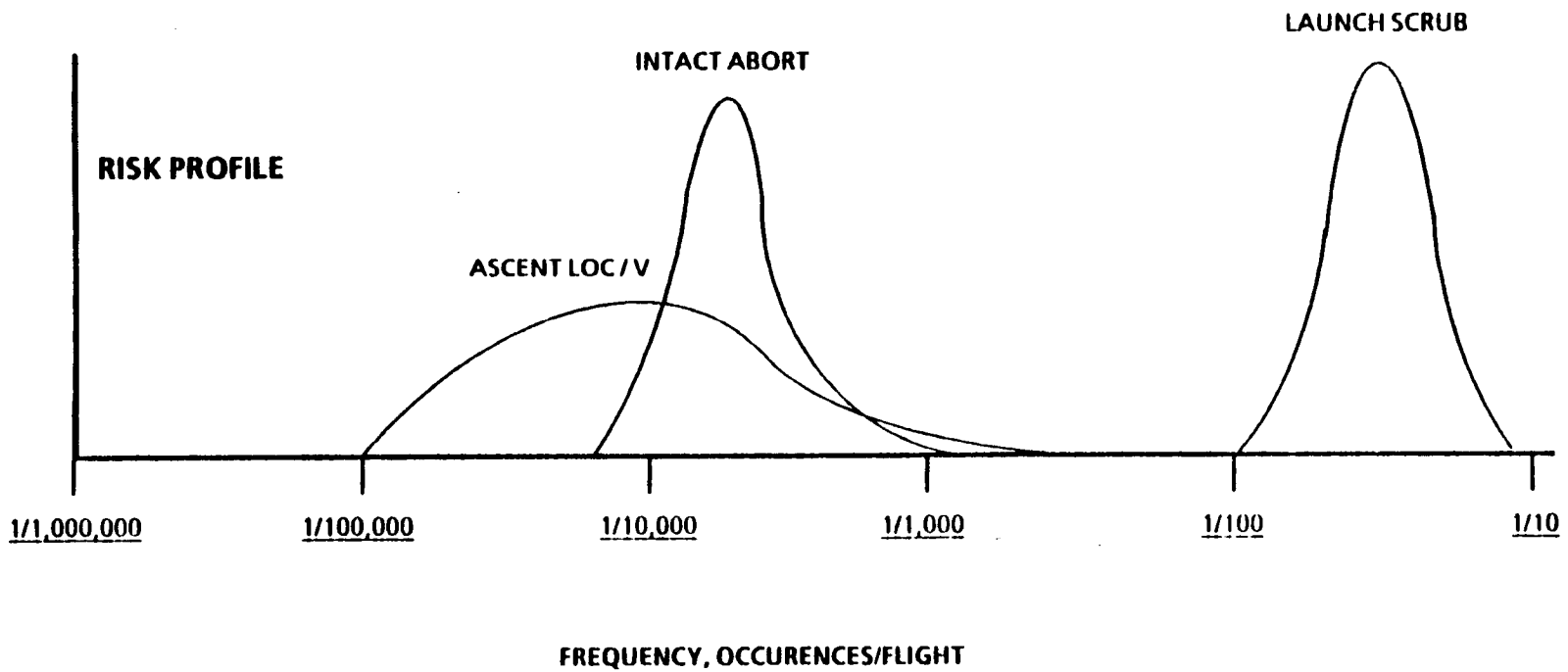


Figure 8-2. Probability Distributions for Stage A (Ascent)

From this study, one may conclude that very little risk is associated with an APU causing LOC/V during ascent during the life of the Shuttle program. Similarly, the results show that the range of possible frequencies of APU-caused launch scrubs lies between 1 in about 13 flights and 1 in about 90 flights. We are 90% confident that the fraction of flights in which APUs would cause a launch scrub lies between 1 in about 68 flights (5th percentile) and 1 in about 20 flights (95th percentile).

The average frequency with which APUs would cause a launch scrub was estimated to be 1 in about 32 flights. This result is quite consistent with the observed data of one APU-related launch scrub in the first 25 flights. The average frequency with which a PLS would be declared because of APU malfunctions was estimated to be 1 in about 120 flights. No probability distribution is provided for the PLS case; however, the PLS risk contributors are presented in Tables 8-1 and 8-6.

The study results show that the range of possible frequencies of APU-caused intact aborts is between 1 in about 2000 ascents and 1 in about 10,000 ascents. That is, one should not expect an APU-caused intact abort before 2000 flights, but an intact abort is almost certain within 10,000 flights. We are 90% confident that the frequency with which APUs would cause an intact abort during ascent lies between 1 in about 6,600 flights (5th percentile) and 1 in about 1,700 flights (95th percentile). The median frequency of occurrence is once in about 3,600 flights (50th percentile), and the mean occurrence is once in about 3,000 flights. From this study, one may conclude that there is little risk associated with an APU causing an intact abort during the life of the Shuttle program.

8.1.1.1 The Effects of APU Redundancy

The occurrence of a declared PLS associated with APUs is relatively more likely than the other in-flight damage states. This is because any permanent failure, any detected leak, or any other malfunctions associated with declaring an APU lost after lift-off would lead to a PLS in accordance with the Flight Rules. Since one of these malfunctions on any one of the three APUs can cause a PLS, the presence of three APUs, in effect, increases the potential for a PLS.

The risk model leads to an intact abort if any one of the three APUs fail during the thrust bucket. This damage state also derives no benefit from the fact that there are three APUs.

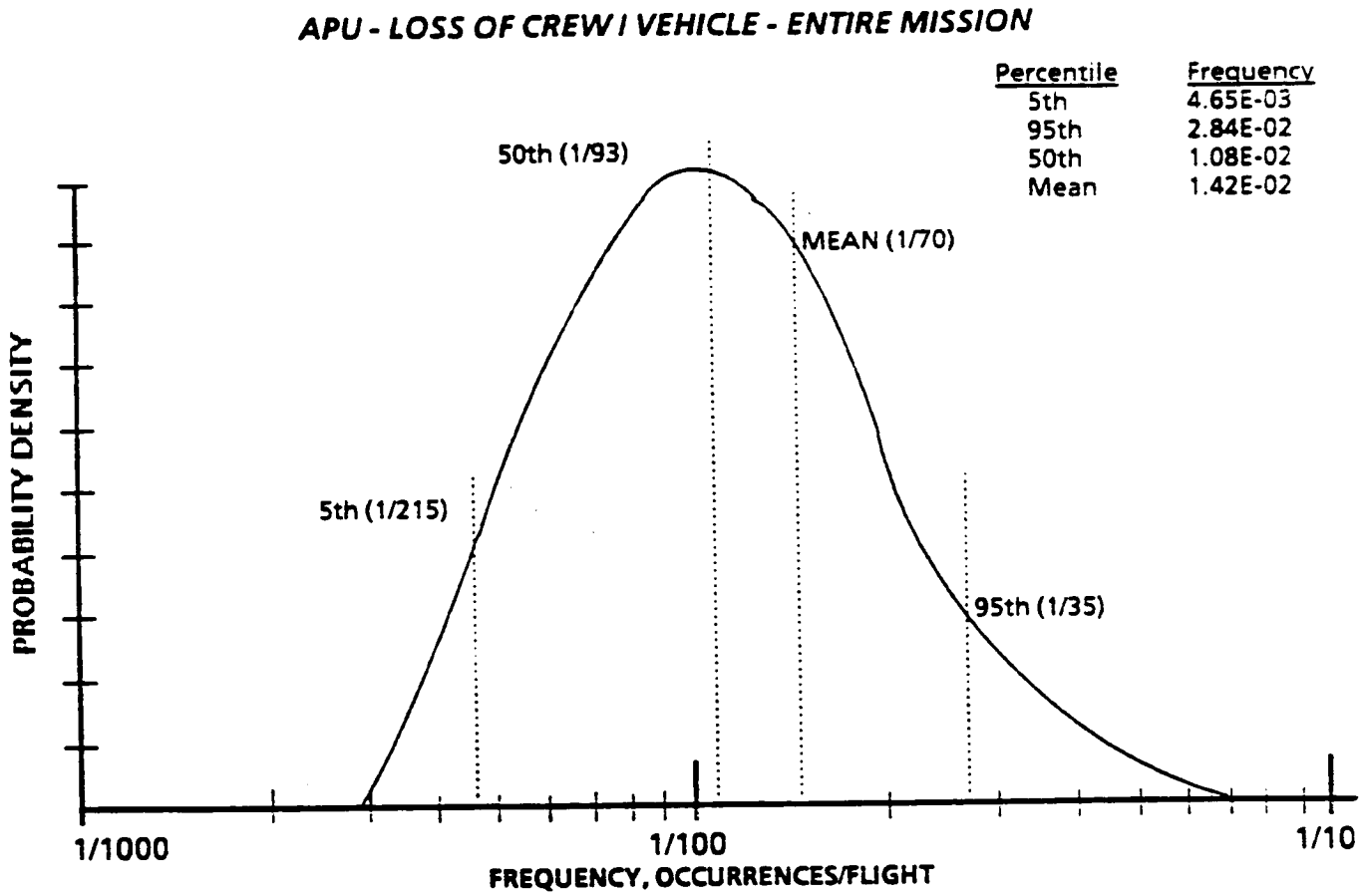
The occurrence of a launch scrub is also relatively likely because any failure to start an APU, any failure of an APU to continue running during the 5 minutes before lift-off, or virtually any other detected malfunction in an APU during this time period would lead to a launch scrub. Again, redundancy is not a benefit for this damage state.

The frequency of the intact abort and PLS damage states is aggravated by the predominately series nature of each APU. Only the isolation valves and control valves exhibit some redundancy to prevent an APU from failing during operation. In series systems every component must succeed for the system to succeed. The failure frequencies of components in series are summed to obtain the system failure frequency. For the above damage states, all of the components (or redundant component pairs) of all three APUs are summed.

Redundancy does, however, benefit the frequency of loss of crew or vehicle. All scenarios leading to this damage state involve failure of at least two APUs or one APU and flight critical equipment during ascent. Unfortunately, the effects of cascading damage from failure modes such as turbine fragmentation and the occurrences of common cause failures limit the benefits of this redundancy. Cascading damage effects are aggravated by the close proximity of APUs 1 and 2 and the close proximity of these APUs to flight critical equipment such as the liquid propellant lines of the main engines. Without the common cause and spatial interaction effects the fraction of flights leading to loss of crew or vehicle would be about one-half the current assessed value.

8.1.2 Mission Risk Profile

The probability distribution shown in Figure 8-3 represents the study conclusions about the frequency with which APU failures would result in loss of crew or vehicle from lift-off to APU shutdown after wheelstop (whole flight). These data were derived from the Stage A (ascent) and Stage B (orbit and entry) risk models combined.



PROOF-OF-CONCEPT STUDY RESULTS -
NOT APPROVED FOR DESIGN EVALUATION
OR FLIGHT CERTIFICATION

Figure 8-3. Probability Distribution for LOC/V – Entire Mission

The results show that the range of possible APU-caused LOC/V frequencies lies between 1 in about 15 flights, and 1 in about 300 flights. That is, one should not expect an LOC/V before 15 flights, and an LOC/V is almost certain within 300 flights. We are 90% confident that the frequency with which APUs would cause loss of crew or vehicle lies between 1 in about 215 flights (5th percentile) and one in about 35 flights (95th percentile). Interpretation of the risk profile (Figure 8-3) suggests that, based on this study, there is a substantial risk of an APU-caused LOC/V during the life of the Shuttle program.

The average frequency with which APU-initiated failures would cause a loss of crew or vehicle is 1 in about 70 flights. Comparison of this number with the one in about 3,800 for ascent clearly shows that the risk of the APUs to the vehicle occurs predominately after ascent. In fact, ascent accounts for only 1.3% of the total risk to the vehicle during a flight. The breakdown of the Stage B risk into scenarios, as will be discussed in succeeding sections, tells us, further, that the APU risk is predominately associated with entry.

The 1 in 70 flights is far more frequent than would be expected from 2 APUs failing independently during the flight. If independent failures were the only contributors to loss of vehicle, then the frequency would be about 10 times lower. This indicates that cascading effects across subsystem boundaries and common cause failures play a very significant role in the risk profile.

The results show that small fuel leaks from the APUs into the aft compartment initiate cascading effects that include fires and hydrazine damage to wiring insulation. The consequential damage to APUs or other flight critical equipment in the aft compartment from these hydrazine effects is the most important cause of loss of crew or vehicle. Leakage of fuel is one of the more frequent malfunctions of the APUs. The database indicated that leakage into the aft compartment could occur once in about 3,700 hours of flight time for each APU. The APUs can develop a fuel leak any time during the flight. A typical flight exposes each APU to hydrazine for approximately 154 hours. Therefore, APU leakage into the aft compartment can be expected on the average approximately once in every eight or nine flights. The information presented in Sections 6.6 and 7.6 indicated that damage to two APUs or flight critical equipment, given that hydrazine leakage into the aft compartment has occurred, is very likely during entry. The likelihood of loss of crew or vehicle because of a leak occurring on orbit or during entry is, therefore, also high.

The reasons that ascent represents a small portion of the risk to the vehicle are related to the likelihood of leakage and consequential damage from leakage. First, ascent represents only about 0.1% of the total exposure time for leaks to develop. Second, the aft compartment is purged with nitrogen to prevent fires from occurring. Third, the concentration of oxygen in the atmosphere quickly becomes too low to support combustion as the vehicle ascends. And fourth, the acceleration vector during ascent tends to force hydrazine to migrate away from ignition sources and critical APU equipment. APU equipment malfunctions also provide less of a contribution to risk during ascent because of the shorter run time. Furthermore, failures of an APU to start during stage A contribute to launch scrub and not to loss of crew or vehicle. During entry, on the other hand, failures to start do contribute to loss of crew and vehicle.

8.2 DESCRIPTION OF RISK CONTRIBUTORS

8.2.1 Failure Scenario Importance Ranking

Risk can be identified by two different means, each with its own advantages. The first method is a ranking of failure scenarios that contribute to each risk category; i.e., LOC/V, Loss of Mission, Launch Scrub, etc. This method clarifies the sequences of related or unrelated events that can lead to each damage state of interest.

The second method is a ranking of individual component failures or groups of components that contribute risk in one or more of the failure scenarios. This second method focuses on the individual component failures that contribute most greatly to the failure scenarios. These are the component failures which, if eliminated or reduced in frequency, can significantly lower the overall risk to the vehicle associated with the APU.

8.2.1.1 Loss of Crew or Vehicle During Ascent

Three scenarios provide 98% of the risk of loss of crew and vehicle due to APU failures during ascent (bear in mind that ascent represents only 1.3% of the overall APU risk). These are ranked and summarized in Table 8-1A. The most risk-significant scenario (71% of the frequency of loss of crew and vehicle) involves failure of an APU turbine such that the turbine breaks

into high energy fragments while it is operating at normal speed between lift-off and MECO. Breakup can occur either from a flaw which could contribute to accelerated crack propagation, from fatigue, or from other causes. Inspection of HPU turbines after flight has consistently shown cracks in turbine blades, and several incidents of turbine blade loss have occurred during APU and HPU testing. To date, however, no turbine wheel hub has come apart at normal speed.

Turbine breakup, of course, guarantees the failure of at least one APU. The turbine may fail in a way that causes it to wobble on its axis of rotation such that when it comes apart, the pieces are thrown out of the normal plane of rotation and miss the containment ring. Tests have demonstrated that the portion of the turbine housing that is not reinforced by the containment ring cannot retain the fragments. These fragments could become high energy projectiles capable of damaging other equipment in the aft compartment, including other APUs.

Potential targets within the projected path of the shrapnel were determined, and the strength of the materials that could be struck was analyzed. Among the likely targets of the shrapnel (as discussed in Section 6.6) are the liquid oxygen and liquid hydrogen propellant lines that pass from the external tank through the aft compartment to the main engines. It appears that shrapnel could be energetic enough to pierce both the outer and inner shells of these lines. Over-pressurization of the aft compartment, as well as fire and explosion, are likely outcomes of this event. Shrapnel could also hit and damage hydraulic lines, electrical wiring, and other APUs. The APU fuel tanks are within the spray pattern of shrapnel from APU 1 or APU 2. There is also some chance that a substantial hydrazine leak from a fuel tank could strip the Kapton insulation from electrical wiring in the aft compartment, thus failing other APUs or flight critical hardware despite the fact that the nitrogen purge of the aft compartment prevents the hydrazine from igniting.

The next most significant scenario to loss of crew or vehicle during ascent accounts for 23% of the risk. It involves independent APU failures such that two APUs cease to operate after lift-off. Even if the APUs should fail after MECO, it is assumed that entry and landing cannot be successful on only one APU. While the split fraction models described in Section 6.5 present numerous potential equipment failure combinations that cumulatively provide the total frequency of failures of two APUs, one of these combinations has been assessed as contributing about 70% of the frequency of this scenario. This combination entails

common cause restriction of lube oil circulation in two APUs during ascent. Inadequate lube oil circulation causes a rapid overheat and failure of the bearings on the rotating equipment in the gearbox. The restriction may be caused by hydrazine leakage from the fuel pump seal through the drain cavity and into the gearbox via the gearbox shaft seal which shares the same seal drain cavity, or it may be caused by foreign substances introduced into the gearboxes during ground servicing. The APU flight history database (see Section 7) exhibits several occurrences of high lube oil pressure and partial blockage of the lube oil filter. Two such occurrences were on the same flight, and resulted in a launch scrub. The database also reveals several incidents of contamination of the lube oil by H_2O, including contamination of all three APUs on the same flight.

Hydrazine reacts with the lube oil to form a waxy substance that collects on the lube oil filters and eventually blocks them. Among the identified commonality of causes that covered two APUs were choice of incompatible materials (lube oil and hydrazine), design and fabrication of the seals and seal drain system that allowed the two materials to intermingle, and failure to adequately inspect and clean the filters between missions. Although a flushing and inspection procedure has been added to lube oil system refurbishment, the other two causes remain for the baseline APU. This problem should be eliminated by the Improved APU seal cavity design.

The third risk-significant scenario accounts for 4% of the frequency of loss of crew and vehicle. This scenario involves failure of both the primary and secondary fuel control valves in the open position coupled with failure of the overspeed shutdown function to close the secondary valve. If both the primary and secondary valves fail open for more than about 200 milliseconds beyond the normal pulse period, the turbine speed could increase to a speed (about 108,000 rpm) at which the turbine hub would come apart. The containment ring could not withstand the energy of the fragments and the APU housing would be pierced, sending high energy shrapnel through the aft compartment. Even if the fuel isolation valves are closed by the overspeed shutdown circuit, sufficient hydrazine remains in the lines downstream of the isolation valves to power the turbine to overspeed. The remainder of the scenario is as described above for turbine rupture at normal speed.

8.2.1.2 Launch Scrub

Table 8-1B shows that about 97% of the frequency of launch scrub is provided by two scenarios. The most important scenario contributes 87% of the launch scrub frequency. This scenario represents those APU failures that occur upon attempting to start the APUs at 5 minutes before lift-off. A ranking of the most important start failures and their percent contribution is presented in Table 8-1B.

The other scenario accounts for 10% of the launch scrub frequency. This scenario involves failures of equipment in a single APU during the 5 minutes of run time before lift-off. These are failures that would cause the APU to cease operating. As noted earlier, violations of launch commit criteria that allow the APUs to continue operating were not included in the scope of this study. It was assumed that the launch control center could detect an APU failure and scrub the launch essentially right up to the launch command. A ranking of the most important individual APU run failures and their percent contribution is presented in Table 8-1B.

8.2.1.3 Intact Aborts and PLS

Failure of individual APUs to continue operating after launch are the most important scenarios for these damage states. Tables 8-1C and 8-1D summarize the most important APU run failures and their percent contributions to the frequencies of these damage states.

8.2.1.4 Loss of Crew or Vehicle Over the Entire Flight

The scenarios most important to risk to the vehicle from lift-off through APU shutdown after wheelstop are summarized in Table 8-2. Six scenarios provide 61% of the risk. They involve leakage of hydrazine from any one of the APUs or any two of the APUs in combination. Twenty five percent of the risk of these scenarios comes from combinations of two APUs leaking fuel during the same mission. This reflects the in-flight experience in which two APUs leaked fuel during the same mission (STS-9). The study assumed that an APU could develop a leakage during orbit. Since the APUs are shut down during orbit, the leak may not reveal itself until after the APUs have started for entry. Even then a small but dangerous leak could go undetected; this study assumed that such leaks are not detected (as opposed to large leaks, which would be

detected). Similarly, a small leak could develop any time during entry. The study assumed that leakages or leakage-induced failures that occur after wheelstop would not cause a loss of crew or vehicle.

The damage caused by leakage of hydrazine stems from three of its physical properties. First, hydrazine is corrosive to certain materials. One such material is the Kapton wiring insulation used extensively in the aft compartment. Second, hydrazine is flammable in as little as about 4% oxygen. Hot spots on the APUs themselves can provide an ignition source for a hydrazine-oxygen mixture. Third, hydrazine will auto-decompose to nitrogen, hydrogen and ammonia in an exothermic reaction when it comes in contact with certain materials such as metal oxides, which may be present in the aft compartment. Because of these properties, the experience with STS-9, and the density of critical equipment in the aft compartment, a high conditional probability (given that a fuel leak has occurred) was assigned (by expert opinion) to the event that a fuel leak in an APU would lead to loss of crew and vehicle during entry. These conditional probabilities are discussed in Section 7.6; they range between about 0.2 and 0.6. The study recognized that fires cannot occur until the vehicle is sufficiently low in the atmosphere. As a result, the study assumed that neither an APU nor flight critical equipment would fail above about 65,000 feet.

Another 16% of the risk of loss of crew of vehicle comes from 17 scenarios that involve hydrazine leakage either preceded by or followed by an independent failure of an APU. Such failures could occur upon starting the APUs for entry, while the APUs are running during entry, or from a hydrazine leak into a solenoid cavity within the gas generator valve module. Fuel leakage into a solenoid cavity was assumed to trigger an auto-decomposition reaction that causes a rupture of the valve cover and a loss of that APU.

Start failures, run failures, and heater failures of two APUs during orbit and entry comprise about 9% of the risk. Table 8-2 summarizes and ranks the individual APU failures that are important contributors to these scenarios.

About 4% of the risk was assessed to be initiated by hydrazine leakage into the solenoid cavity of one of the fuel tank isolation valves. If an auto-decompostion reaction and rupture of the valve cover followed this leakage, then the contents of the hydrazine tank were assumed to be dumped into the aft compartment. This event, therefore, was assumed to lead to loss of crew and vehicle.

The risk associated with turbine shrapnel from both normal speed and overspeed conditions comprises about 4% of the total risk. Occurrence of this incident during entry accounts for about four-fifths of this 4%. Only about one-twentieth of the risk from shrapnel is attributable to turbine overspeed, as opposed to turbine breakup at normal speed.

Only about 1% of the estimated risk to the vehicle due to APU-initiated scenarios is associated with a first-day PLS entry condition. These scenarios involve an APU failure during ascent and another APU failure during the abbreviated remainder of the mission (about 5.7 hours).

The remaining 5% of the risk is distributed among all other scenarios modeled in the event trees.

8.2.2 Component Failure Importance Ranking

Another way to dissect the results is to perform sensitivity studies on the importance of individual risk contributors to the overall frequency of each damage state. This was done by numerous requantifications of the APU risk model. For each requantification, a specific failure was assigned a failure frequency of zero. In other words, the component was assumed to be perfect with respect to that failure mode. In general, the requantification yields an estimate of the damage state frequency that is lower than the base case. The following importance parameter was, therefore, used to rank the individual failure modes:

$$I_j = \frac{\text{BASELINE QUANTIFICATION} - J^{th}\ \text{REQUANTIFICATION}}{\text{BASELINE QUANTIFICATION}}$$

The results shown in Tables 8-3 through 8-8 are normalized by a factor representing the summation of all Ij. The failures shown in the tables represent 90% or more of their respective damage state frequencies.

Table 8-7 represents the results of the first iteration of the loss of crew/vehicle for an entire flight. The large (74.6%) contribution from the general category of hydrazine leaks downstream of the isolation valves, and the desire to rank the risk contributors to a finer detail, led to a second iteration. The

second iteration results are shown in Table 8-8, and identifies, more specifically, the risk points of leakage downstream of the isolation valves. For example, 71.6% of this risk can be attributed to the first three leak sources. Fuel leakage into the fuel isolation valve remains high on the risk table. This second iteration is a result of modifying the model to quantify individual fuel leak sources and to eliminate the "MPU fail high" failures, which were determined to be non-credible. This recalculation of the results was facilitated by the capability of the PRA process to readily support iterations of the results for a more detailed examination of particular risk contributors or to incorporate new information.

The iteration was performed by setting the likelihoods of the "MPU fail high" failures to zero in the existing model, and by expanding the fuel leak model to encompass specific leak sources. This expanded fuel leak model took the form of a fault tree. The fuel leak events were quantified by a Bayesian update based on a combination of similarity data and Shuttle flight history data.

A second iteration was not performed to eliminate the "MPU Fail High" failure modes, shown in Tables 8-3 through 8-4, due to time constraints. However, it can be safely assumed that these failures would drop from the top 99% category, and that other failure modes would move up accordingly.

8.3 ASSESSMENT OF STUDY RESULTS

The contributions of this PRA pilot study are significant because of the following achievements.

a. The study was able to develop a multistage model that identified and ranked scenarios leading from APU failures to loss of crew or vehicle over the entire flight from lift-off to APU shutdown after wheelstop.

b. The study identified and ranked scenarios leading from APU failures to loss of crew and vehicle during ascent. Ascent was found to represent only about 1% of the total risk of loss of crew and vehicle.

c. The study identified and ranked scenarios leading from APU failures to loss of crew or vehicle during orbit, entry, and landing. The risk from entry and landing so dominated the risk of the flight that the overall flight risk is essentially equal to the risk from entry and landing.

d. The study identified and ranked scenarios leading from APU failures to other damage states, namely, launch scrub, intact abort and first-day PLS entry.

e. The study identified and ranked the individual component failures or groups of failures that contributed to each damage state. The results show that the bulk of the risk for each damage state is contributed by a relatively small number of failures. The PRA results suggest that these failures modes should receive additional attention in order to achieve significant risk reduction.

f. The study discovered that spatial interactions, failure effects propagating within the subsystem, failure effects cascading into other subsystems, and common cause failures led to a risk that was far greater than from independent APU failures alone.

g. The study found that the proximity of the APUs to each other and to flight critical equipment in the aft compartment, coupled with the APUs' potential for releasing hydrazine and shrapnel, and the requirement for two of three APUs for safe flight, constitute the bulk of the risk of these subsystems to the vehicle.

The risk of loss of crew or vehicle from the APUs is clearly dominated by leakage of hydrazine leading to propagating and cascading effects of fire, hydrazine corrosion, hydrazine decomposition reactions, and possibly detonation. These effects were assessed to lead to failure of two APUs or flight critical equipment during entry and landing with a frequency between 0.2 and 0.6, given that a leakage has occurred. The high conditional frequency of loss of crew and vehicle given a hydrazine leak in an APU resulted from the recognition that the aft compartment is crowded with equipment that is susceptible to the effects of hydrazine and within very close proximity to the source of hydrazine. There are no effective barriers between the hydrazine source and much of the equipment in the aft compartment. Unfortunately, the APUs themselves provide sufficient heat in the presence of oxygen to ignite leaking hydrazine. The effects of hydrazine ignition were dramatically demonstrated at the end of the flight of STS-9.

It should be noted that certain changes in APU design and operations have been implemented, or are in the process of being implemented, which should reduce the risk associated with the APUs. These changes include:

a. Improved fuel leak detection procedures during APU turnaround operations

b. Turbine wheel crack mapping program

c. Fuel isolation valve redesign to eliminate source of fuel leaks into solenoid cavity

d. Chromized gas generator injector tubes to reduce likelihood of fuel leaks

e. Redesign of fuel pump/gearbox seal cavity to eliminate fuel/lube oil mixing

The PRA proof-of-concept study model was built and quantified based on the pre-STS-51L configuration except where otherwise noted, and does not reflect any of the changes noted above.

A design change that would further reduce the risk posed by the APUs would be to erect barriers to isolate each APU from the rest of the aft compartment. Properly designed, these barriers would prevent or reduce the amount of hydrazine entering the compartment due to leakage, and would also serve to reduce the detrimental effects of shrapnel produced by turbine breakup during flight.

Another approach to reducing overall risk is to certify that the vehicle is capable of operating throughout the flight envelope (ascent as well as entry) on a single APU. A significant reduction to the risk of LOC/V, as determined from this study, would result since the study was heavily influenced by the assumption that two APUs were required for safe flight.

TABLE 8-1A

IMPORTANCE RANKING OF APU FAILURE SCENARIOS

LOC/V - ASCENT

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Turbine failure leading to shrapnel induced failure of second APU or flight critical equipment between launch and MECO	70.5
	Contributors and % Contribution to Scenario 1:	
	a. Turbine fragmentation at normal speed (100%)	
2	Equipment failure of 2 APUs between launch and APU shutdown after MECO	23.4
	Contributors and % Contribution to Scenario 2:	
	a. Lube oil circulation restricted in two APUs, causing bearing overheat and failure of rotating equipment in gearbox from both common cause and independent failures (73%)	
	b. Lube oil circulation restricted in one APU and independent failure of primary fuel control valve (stays closed while pulsing) (6%)	
	c. Two primary fuel valves in two APUs fail closed while pulsing (5%)	
	d. Either MPU 2 or MPU 3 fails high* in one APU and a primary fuel valve fails closed in another APU (3%)	
	e. Restricted lube oil circulation in one APU and either MPU 2 or MPU 3 fails high* in another APU (2%)	
	f. Turbine wheel failure in one APU and primary fuel valve fails closed in another APU (1%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-1A (Concluded)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
	g. Isolation valve switch fails to open upon APU shutdown in one APU and primary fuel valve fails closed during pulsing in another APU (1%)	
	h. Turbine wheel fails in one APU and lube oil circulation is restricted in another APU (0.7%)	
	i. Isolation valve drivers fail on upon APU shutdown in one APU and primary fuel valve fails closed while pulsing in another APU (0.6%)	
	j. Combinations of MPU, primary valve, lube oil circulation, spurious controller actuation, turbine wheel failure, gas generator failures, and isolation valve drivers and switches (6%)	
3	Turbine overspeed leading to fragmentation of the hub and shrapnel-induced failure of a second APU or flight critical equipment	3.8
	Contributors and % Contribution to Scenario 3:	
	a. MPU 3 fails low and secondary fuel valve fails to close due to mechanical failure (44%)	
	b. Primary fuel valve fails open during pulsing and secondary fuel valve fails to close on demand due to mechanical failure (29%)	
	c. MPU 3 fails low and secondary fuel valve fails open due to mechanical failure during pulsing (13%)	
	d. Primary and secondary fuel valves fail open pulsing due to mechanical failures (9%)	
4	All Others	2.3
	Total	100.0

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-1B

IMPORTANCE RANKING OF APU FAILURE SCENARIOS

LAUNCH SCRUB - ASCENT

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Failure to start an APU at 5 minutes prior to lift-off	87.4
	Contributors and % Contribution to Scenario 1:	
	a. Secondary fuel control valve leaks before isolation valves are opened, leading to elevated gas generator temperature (29%)	
	b. Secondary fuel valve fails to open on demand at start (11%)	
	c. Primary fuel valve fails to close on demand at start (11%)	
	d. MPU 1 fails low on demand at start (8%)	
	e. Electric power to secondary fuel valve is lost (7%)	
	f. MPU 1, 2, or 3 fails high* on demand at start (5% each = 15%)	
	g. Fuel pump bypass valve fails to open on demand at start (5%)	
	h. Fuel pump bypass valve fails to close after normal pump pressure is reached (5%)	
	i. Loss of electric power to fuel tank isolation valve at start (4%)	
	j. Primary or secondary fuel valve controller output fails off on demand at start (4%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-1B (Concluded)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
2	Failure of an APU to continue operating after start and before lift-off	9.5
	Contributors and % Contribution to Scenario 2:	
	SEE FAILURE OF AN APU TO OPERATE UNDER INTACT ABORT (TABLE 8-1C)	
3	Spurious shutdown of any one APU after start and before lift-off	2.6
	Contributors and % Contribution to Scenario 3:	
	SEE SPURIOUS SHUTDOWN UNDER PLS (TABLE 8-1D)	
4	All Others	0.5
	Total	100.0

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-1C

IMPORTANCE RANKING OF APU FAILURE SCENARIOS

INTACT ABORT - ASCENT

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Failure of an APU to operate while in the thrust bucket	76.6
	Contributors and % Contribution to Scenario 1:	
	a. Primary fuel valve fails closed during pulsing (43%)	
	b. Lube oil circulation restricted (26%)	
	c. MPU 2 fails high*, causing secondary fuel valve to close (6%)	
	d. MPU 3 fails high*, causing primary fuel valve to close (6%)	
	e. Turbine wheel failure (6%)	
	f. Fuel pump filter blocked (2%)	
	g. Gas generator fails to operate (1%)	
	h. Lube oil pump fails to run (0.8%)	
	i. Fuel pump fails to run (0.8%)	
	j. Loss of electric power to secondary fuel valve (0.5%)	
	k. Secondary fuel valve controller output failure (0.3%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-1C (Concluded)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
2	Spurious shutdown of any one APU while in the thrust bucket	20.7
	Contributors and % Contribution to Scenario 2:	
	SEE SPURIOUS SHUTDOWN UNDER PLS (Table 8-1D)	
3	All Others	2.7
	Total	100.0

TABLE 8-1D

IMPORTANCE RANKING OF APU FAILURE SCENARIOS

APU STAGE A (ASCENT)

PRIMARY LANDING SITE

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Failure of an APU to continue operating after lift-off, except in the thrust bucket	77.1
	Contributors and % Contribution to Scenario 1:	
	a. Primary fuel valve fails closed during pulsing (40%)	
	b. Lube oil circulation restricted (24%)	
	c. MPU 2 fails high*, causing secondary fuel valve to close (6%)	
	d. MPU 3 fails high*, causing secondary fuel valve to close (6%)	
	e. Turbine wheel failure (6%)	
	f. Isolation valve switch fails to open upon APU shutdown (4%)	
	g. Isolation valve drivers fail on (3%)	
	h. Fuel pump filter blocked (2%)	
	i. Gas generator fails to operate (1%)	
	j. Lube oil pump fails to run (0.8%)	
	k. Fuel pump fails to run (0.8%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-1D (Concluded)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
2	Spurious shutdown of any one APU after lift-off except in the thrust bucket	20.8
	Contributors and % Contribution to Scenario 2:	
	a. MPU 1 fails low, causing underspeed trip (77%)	
	b. MPU 1 fails high*, causing overspeed trip (22%)	
3	All Others	2.1
	Total	100.0

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-2

IMPORTANCE RANKING OF APU FAILURE SCENARIOS

LOC/V - WHOLE MISSION

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Hydrazine leak downstream of fuel isolation valves and into aft compartment during orbit or entry that leads to failure of two APUs or flight critical equipment **Contributors:** a. Leakage from any one APU (100%)	39.1
2	Hydrazine leak as above, but from two or three APUs concurrently **Contributors:** a. Leakage from combinations of two APUs (91%) b. Leakage from three APUs (9%)	26.5
3	Hydrazine leak from a single APU as above, with an independent failure of another APU **Contributors:** a. Hydrazine leak in one APU, with equipment failure of another APU while running (see below for breakdown into APU failure modes) (88%) b. Hydrazine leak in one APU, with start failure of another APU (see below for breakdown into APU failure modes) (12%)	6.4
4	Equipment failure of two APUs during orbit, entry, or landing (failures not related to APU start) a. Lube oil circulation restricted on two APUs (16%) b. Primary fuel valve fails closed while pulsing on one APU and fuel tank GN2 quick disconnect leaks on another APU (7%)	5.0

TABLE 8-2 (Continued)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
	c. Lube oil circulation restricted in one APU, and primary fuel valve fails open while pulsing on another APU (6%)	
	d. Primary fuel valve fails closed while pulsing in two APUs (6%)	
	e. Primary fuel valve fails closed while pulsing on one APU, and fuel tank diaphragm leaks on another APU (4%)	
	f. Lube oil circulation restricted in one APU, and fuel tank GN2 quick disconnect leaks on another APU (4%)	
	g. Fuel tank diaphragm leak on one APU, and fuel tank GN2 quick disconnect leaks on another APU (3%)	
	h. Next 36 scenarios have combinations of lube oil circulation restricted, tank diaphragm leaks, primary fuel valve closure, nitrogen leak from fuel tank, MPU failures, turbine failures, and loss of power to fuel tank isolation valves (34%)	
5	Fail to start one APU at TIG-5 in orbit and equipment failure of second APU while running	4.0
	Contributors:	
	IMPORTANT APU START FAILURES:	
	a. Secondary fuel valve fails to open on demand to start (18%)	
	b. MPU 1 fails low on demand to start (14%)	
	c. Electric power to secondary fuel valve fails at start (11%)	
	d. MPU 1 fails high* (9%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-2 (Continued)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
	e. MPU 2 fails high* (9%)	
	f. MPU 3 fails high* (9%)	
	g. Fuel pump bypass valve fails closed (9%)	
	h. Fuel pump bypass valve fails open (9%)	
	i. Electric power to fuel tank isolation valve fails at start (7%)	
	IMPORTANT APU EQUIPMENT FAILURES:	
	j. Primary fuel valve fails closed during pulsing (19%)	
	k. Fuel tak GN2 fill quick disconnect fails open (13%)	
	l. Heaters fail off by common cause (14%)	
	m. Lube oil circulation restricted (12%)	
	n. Fuel tank diaphragm leaks (8%)	
	o. Fuel tank nitrogen leakage (3%)	
	p. MPU 2 fails high* (3%)	
	q. MPU 3 fails high* (3%)	
	r. Turbine wheel failure (3%)	
6	Hydrazine leaks into isolation valve solenoid, auto-decomposes, ruptures valve cover, and contents of fuel tank are dumped into aft compartment	3.8
	Contributors:	
	a. Leakage into solenoid cavity (100%)	

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-2 (Concluded)

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
7	Turbine comes apart at normal speed during entry; shrapnel and hydrazine effects fail a second APU or flight critical equipment	3.1
	Contributors:	
	a. Turbine wheel comes apart and escapes housing (100%)	
8	Hydrazine leak from two APUs as above, with an independent failure of another APU	1.9
	Contributors:	
	a. Leakage with equipment failure of APU while running (100%)	
9	Turbine comes apart at normal speed during ascent; shrapnel effects fail a second APU or flight critical equipment	0.9
	Contributors:	
	a. Turbine wheel comes apart and escapes housing (100%)	
10	Equipment failure of one APU during ascent and another during orbit or entry	0.9
	Contributors:	
	a. Breakdown of APU failures provided previously	
11	All Others	8.4
	TOTAL	100.0

TABLE 8-3

IMPORTANCE RANKING OF APU FAILURES

LOC/V - ASCENT

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Turbine Wheel Failure	45.09
2	Lube Oil Circulation Restricted	22.67
3	Primary Fuel Valve Fails Closed During Pulsing	20.48
4	MPU 2 Fails High*	2.50
5	MPU 3 Fails High*	2.50
6	Isolation Valve Switch Fails to Open On Demand	1.65
7	Secondary Fuel Valve Fails to Close on First Demand	1.28
8	Isolation Valve A Drivers Fail On	0.88
9	MPU 3 Fails Low	0.85
10	Fuel Pump Filter Blocked	0.39
11	Primary Fuel Valve Fails Open During Pulsing	0.36
12	Gas Generator Fails to Operate	0.10
13	All Other Failures	1.25
	Total	100.00

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-4

IMPORTANCE RANKING OF APU FAILURES

LAUNCH SCRUB

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Secondary Fuel Valve Leaks Before APU Start	29.3
2	Secondary Fuel Valve Fails to Open On Demand	10.6
3	Primary Fuel Valve Fails to Close on the First Demand	10.6
4	MPU 1 Fails Low	8.0
5	Loss of Electrical Power to Secondary Fuel Valve	6.6
6	MPU 1 Fails High*	4.9
7	MPU 2 Fails High*	4.9
8	MPU 3 Fails High*	4.9
9	Fuel Pump Bypass Valve Fails to Open at APU Start	4.8
10	Fuel Pump Bypass Valve Fails to Close After APU Start	4.8
11	Loss of Power to Fuel Tank Isolation Valves	4.0
12	Primary Fuel Valve Fails Closed During Pulsing	3.5
13	Lube Oil Circulation Restricted	1.9
14	Secondary Fuel Valve Controller Output Fails Off On Demand	1.1
15	All Other Failures	0.1
	Total	100.0

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-5

IMPORTANCE RANKING OF APU FAILURES

INTACT ABORT

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Primary Fuel Valve Fails Closed During Pulsing	34.1
2	Lube Oil Circulation Restricted	19.5
3	MPU 1 Fails Low	17.0
4	MPU 1 Fails High*	5.0
5	MPU 2 Fails High*	5.0
6	MPU 3 Fails High*	5.0
7	Turbine Wheel Failure	5.0
8	Fuel Pump Filter Blocked	2.0
9	Gas Generator Fails to Operate	1.1
10	Lube Oil Pump Fails to Run	1.0
11	Fuel Pump Fails to Run	1.0
12	Loss of Electrical Power to Secondary Fuel Valve	0.5
13	Secondary Fuel Valve Controller Output Fails Off	0.5
14	All Other Failures	8.3
	Total	100.0

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-6

IMPORTANCE RANKING OF APU FAILURES

PLS

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Primary Fuel Valve Fails Closed During Pulsing	40.5
2	Lube Oil Circulation Restricted	24.0
3	MPU 2 Fails High*	5.8
4	Fuel Tank Isolation Valve Switch Fails to Open On Demand	4.3
5	Turbine Wheel Failure	3.0
6	Fuel Tank Isolation Valve Drivers Fail On	2.8
7	Over/Under Speed Control Circuit Spuriously Closes Secondary Fuel Valve	2.4
8	MPU 1 Fails Low	2.1
9	Fuel Pump Filter Blocked	1.8
10	MPU 1 Fails High*	1.8
11	Gas Generator Fails to Operate	1.3
12	All Other Failures	10.2
	Total	100.0

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-7

IMPORTANCE RANKING OF APU FAILURES

LOC/V - WHOLE FLIGHT - 1st ITERATION

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Fuel System Leak Into Aft Compartment From Location Downstream of Isolation Valve	74.6
2	Leak Into Fuel Isolation Valve Solenoid Cavity	3.8
3	Turbine Wheel Failure	3.8
4	Leak Into Primary Valve Solenoid Cavity (GGVM Detonation)	2.9
5	Primary Valve Fails Closed at APU Start	2.4
6	Lube Oil Circulation Restricted	2.3
7	Fuel Tank GN2 Fill Q.D. Leakage (Low Fuel Tank Pressure)	1.8
8	Any MPU Fails High at APU Start*	1.3
9	Fuel Tank Diaphragm Leakage	1.2
10	Secondary Fuel Valve Fails to Open at APU Start	0.9
11	Heater Pair 116/117 Fails Off on Orbit	0.8
12	Any MPU Fails High While APU is Running*	0.7
13	MPU 1 Fails Low at APU Start	0.7
14	Loss of Power to Secondary Fuel Valve at APU Start	0.6

* Later information indicates that MPU fail high may not be a credible failure mode

TABLE 8-7 (Concluded)

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
15	Loss of Power to Fuel Tank Isolation Valves at APU Start	0.6
16	Fuel Tank GN2 Leakage	0.5
17	Fuel Pump Bypass Valve Fails to Close After APU Start	0.4
18	Heater Pair 111/112 Fails Off On Orbit	0.3
19	Secondary Fuel Valve Controller Output Fails Off at APU Start	0.1
20	Fuel Isolation Valve Fails to Close at APU Shutdown (GGVM Large Leak)	0.08
21	Fuel Isolation Valve Leaks at Closure After Ascent	0.08
22	Loss of Power to Secondary Fuel Valve While APU is Running	0.02
23	Primary Fuel Valve Controller Output Fails On While APU Running	0.01
24	Secondary Fuel Valve Controller Output Fails Off While APU Running	0.01
25	All Other Failures	0.10
	Total	**100.00**

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

TABLE 8-8

IMPORTANCE RANKING OF APU FAILURES

LOC/V - WHOLE FLIGHT - 2nd ITERATION

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
1	Leakage From Gas Generator Injector Tube	35.5
2	Leakage From Fuel Lines and Fittings	23.3
3	Leakage From Fuel Pump	12.8
4	Leak Into Fuel Isolation Valve Solenoid Cavity	4.0
5	Leak Into Primary Valve Solenoid Cavity (GGVM Detonation)	3.3
6	Primary Valve Fails Closed While Pulsing	3.1
7	External Leakage From GGVM	3.0
8	Lube Oil Circulation Restricted	2.8
9	Fuel Pump Shaft Seal Detonation	1.8
10	Fuel Tank GN2 Fill Q.D. Leakage (Low Fuel Tank Pressure)	1.7
11	Heater Pair 111/112 Fails Off On Orbit	1.6
12	Heater Pair 116/117 Fails Off On Orbit	1.4
13	Fuel Tank Diaphragm Leakage	1.1
14	Secondary Fuel Valve Fails To Open At APU Start	0.9
15	MPU 1 Fails Low At APU Start Valves At APU Start	0.7
16	Loss Of Power To Secondary Fuel Valve At APU Start	0.5
17	Loss of Power To Fuel Tank Isolation Valves At APU Start	0.5

TABLE 8-8 (Concluded)

RANK	COMPONENT/ASSEMBLY FAILURE RISK CONTRIBUTORS	% CONTRIBUTION
18	Turbine Wheel Failure	0.4
19	Fuel Tank GN2 Leakage	0.4
20	Fuel Pump Bypass Valve Fails To Close After APU Start	0.3
	Subtotal	**99.1**
21	Leakage From Fuel Line Flex Hose	0.30
22	Secondary Fuel Valve Controller Output Fails Off At APU Start	0.09
23	Leakage From Fuel High Point Bleed Q.D.	0.05
24	Leakage From Fuel Test Port Q.D.	0.04
25	Fuel Isolation Valve Fails To Close At APU Shutdown	0.04
26	Fuel Isolation Valve Leaks At Closure After Ascent	0.04
27	Loss of Power To Secondary Fuel Valve While APU Is Running	0.04
28	Primary Fuel Valve Controller Output Fails On While APU Is Running	0.01
29	Secondary Fuel Valve Controller Output Fails Off While APU Is Running	0.01
30	All Other Failures	0.28
	Total	**100.00**

NOTE: Proof-of-concept study results. Not approved for design evaluation or flight certification.

9.0 HPU SCENARIO PRESENTATION

The first step in performing a Probabilistic Risk Assessment (PRA) is the task of damage state and failure-sequence definition, and system modeling. This task begins with a definition of the objectives of the study and the acquisition of a substantial amount of information on system design and operation. It progresses through the generation of system models, both inductive and deductive, to the identification of the failure-initiating events, component failures, procedural faults, and dependent-failure mechanisms that could cause these failure sequences to occur.

In the subsections below, the methodology described in Section 5.0 is traced step-by-step through an analysis of the HPU Subsystem. The results of this analysis provide the framework or model, which can then be evaluated using the failure frequency data described in Section 10.0.

Section 9.1 details the damage states selected for the analysis. Section 9.2 details the Master Logic Diagrams (MLDs) developed to show HPU-related failure combinations which can lead to these damage states.

The event sequence diagrams are presented in Section 9.3. These diagrams illustrate, in greater detail, how different damage states can result as a consequence of various types of HPU failures. The breakdown of HPU failure types and different damage states developed in the event sequence diagrams provide the framework for development of the event trees, presented in Section 9.4.

The event trees establish the decision points for which specific probabilities must be determined in order to arrive at overall probabilities for the ultimate damage states. The event trees are similar to flow charts; each decision point must be answered by a yes/no question. Each path through the event tree results in either a damage state or a state of no damage, based on system insight gained through the preceding steps of the analysis.

Each decision point in the event tree must be assigned a probability, called a split fraction. Determination of each split fraction depends on a logical combination of events, which is expressed in the form of a fault tree. The top event of the fault tree is the event for which the split fraction is to be determined. Development of these fault trees, or split fraction models, is presented in Section 9.5

9.1 HPU DAMAGE STATES

The damage states represent the ultimate undesirable events for this PRA. The damage states selected for this study were not peculiar to the HPU under study, but were of a broad category which would encompass any of the Space Shuttle's subsystems. In addition, the damage states were selected to be consistent with the National Aeronautics and Space Administration (NASA) Failure Mode and Effects Analysis (FMEA) as defined in National Space Transportation System Instructions for Preparation of Failure Modes and Effects Analysis and Critical Items List (CIL) (NSTS-22206). The ultimate damage states selected are Loss of Crew and/or Vehicle (LOC/V) and Loss of Mission.

Loss of mission implies that the ability to perform all or a substantial portion of the payload activities was lost. For the HPU assessment, loss of mission is limited to "launch scrub" during the pre-launch phase, which causes a launch delay representing a missed window of opportunity for at least one payload. The loss of mission damage state does not apply to the Ascent phase since no HPU failures lead to an intact abort. Loss of crew and/or vehicle is self-explanatory and applies to both the Prelaunch and Ascent phases.

Not all HPU subsystem failure modes lead to either of these two ultimate damage states. The analysis involves establishing which failure sequences do lead to these damage states, and attaching probabilities to them.

Once the ultimate damage states for the phases were defined, the next step in the study was to develop a set of Master Logic Diagrams (MLDs) using the damage states as the Top Events from which to build failure scenarios.

9.2 MASTER LOGIC DIAGRAM (MLD) DEVELOPMENT

After the damage states have been established for each mission phase, the next step in the analysis is to determine how Hydraulic Power Unit (HPU) system failures can initiate scenarios that lead to these damage states.

9.2.1 General Development Process

The damage states represent the top events for the mission stages being analyzed (see Appendix C9.2-1). A damage state is the

outcome of a scenario. A damage state usually is an undesired event selected because of a need to understand its frequency of occurrence. The second level of each diagram was developed in the form of broad categories depicting functional ways that might lead to the top event or damage state. Not all of these Level II events were developed further.

Level III of the MLD introduces failure modes that were judged to be results of HPU system failures, and succeeding levels break them down into more specific functional paths until specific HPU system failure modes appear at levels as low as Level VI. This "top down" approach aids in identifying unanticipated failure effects involving the HPU.

Many paths were developed that dealt with physical processes about which there is some uncertainty. These physical processes were flagged as technical issues to be resolved through in-house analysis, technical references, and reliance on expert opinion. These issues deal with failure effects from a hydrazine fuel fire, detonation of hydrazine, shrapnel due to turbine wheel rupture and the effects of hot gas due to an exhaust duct leak. The detailed resolution of these issues is discussed in Sections 9.6 and 10.5.

9.2.2 MLD Descriptions

An MLD was developed for each damage state. The MLDs presented in Appendix C9.2-1 and C9.2-2 are discussed individually below.

MLD #1 - Loss of Mission, Launch Scrub

This MLD documents HPU failures that can result in a launch scrub by violating the Space Shuttle Launch Commit Criteria. Any of the four HPUs can shut down, resulting in hydraulic system performance degradation and Thrust Vector Control (TVC) system malfunction which would result in an automatic launch scrub. An HPU can exhibit a performance degradation due to high or low turbine speed, fuel system, low pressure or malfunction or loss of system instrumentation prior to launch. Violation of these HPU performance redlines would cause an automatic launch hold and launch scrub.

MLD #2 - Loss of Crew and Vehicle

MLD #2 documents HPU failures that lead to loss of crew and vehicle during the prelaunch and ascent phases. The effects

of HPU failures were determined to be associated with two of the Level 2 major cause categories: (1) loss of control, and (2) loss of vehicle structural integrity. Loss of vehicle structural integrity applies to both the prelaunch and ascent phases.

Loss of crew/vehicle scenarios for the prelaunch and ascent phases involve loss of structural integrity due to high energy detonations in the SRB aft skirt area. High energy release caused by HPU failures must consider such scenarios as: detonation of hydrazine caused by shrapnel from an HPU turbine coming apart, fire from a random- or shrapnel-induced hydrazine leak, an exhaust leak. These scenarios are spatial in nature and their effects on loss of crew/vehicle are discussed in detail in Sections 9.6 and 9.2.

Loss of vehicle control leads to loss of crew/vehicle during the ascent phase. The HPU failures which lead to loss of control are: loss of 2 HPUs in either Solid Rocket Booster (SRB) and subsequent loss of hydraulic power or loss of flight critical equipment such as ATVC wiring or control electronics due to HPU turbine shrapnel, hydrazine fire or HPU exhaust leak.

9.3 EVENT SEQUENCE DIAGRAM FOR HPU INITIATED SCENARIOS

Event Sequence Diagrams (ESD) illustrate sequences of events leading from initial failure categories, defined by the master logic diagrams, to damage states. They tell how an initial failure (i.e., failure mode) causes a damage state (i.e., effect). When quantified by the use of event trees and fault trees, the scenarios and the events within the scenarios can be ranked with respect to their importance to a damage state such a Loss of Crew/Vehicle (LOC/V).

9.3.1 Interpretation of the ESD

One ESD was developed to represent both prelaunch and ascent stages of the Hydraulic Power Unit (HPU) mission, and is presented in Figure 9.3-1. The model includes the time from HPU start at Time of Ignition L/O -30 seconds to Solid Rocket Booster Separation (SRB SEP) (about 2.1 minutes after launch).

The ESD was developed solely from the perspective of HPU performance during the mission. Interfacing systems were out of scope, as were scenarios that couple performance margins of other

systems with the HPU. For example, coupling the scenarios of Auxiliary Power Unit (APU) failures with HPU failures was not attempted in this study.

The boxes in an ESD ask questions about the occurrence (or non-occurrence) of a category of events. For example, the question in Figure 9.3-1, "Hydraulic System OK?", may be viewed as asking a large number of questions. Each question would refer to a component in the hydraulic system, for example, "Is the pump OK?". An ESD is not meant to illustrate the detailed logic that is involved in determining combinations of failure modes that lead to HPU failure. This is achieved in the split fraction models described in Section 9.5. An ESD illustrates the overall flow of events that lead from an initial HPU failure to Shuttle damage states such as LOC/V and LOM.

9.3.1.1 Interpretation of Initial Failure Categories

The questions relating to the initial failure categories are found in the boxes across the top of the ESD. The categories are phrased as questions such that a successful event (i.e. no initial failure) receives a "yes" answer to the question and a horizontal line is then followed to the next event. For example, the initial failure categories of equipment failure, turbine overspeed, fuel leakage, and exhaust gas leak are represented in Figure 9.3-1, as follows:

1. No permanent HPU failures? (equipment failures)
2. Turbine speed control OK?(turbine overspeed)
3. Fuel boundary remains intact? (fuel leak)
4. Exhaust gas boundary remains intact? (exhaust gas leak)

The question "No hydraulic system failures?" is also asked, even though the hydraulic system is out of the scope of this PRA, to demonstrate how an ESD can diagram the interdependencies between subsystems and include sequences of events that cross subsystems.

A line pointing downward from an initial failure category indicates that an initial failure has occurred (i.e. a "no" answer to the question). A sequence of boxes and lines that follow the arrows from an initial failure to a damage state is called a scenario. A success of the HPU occurs when, according to the principles of scenario structuring described in Section 5, all the answers to the questions across the top of the ESD are yes.

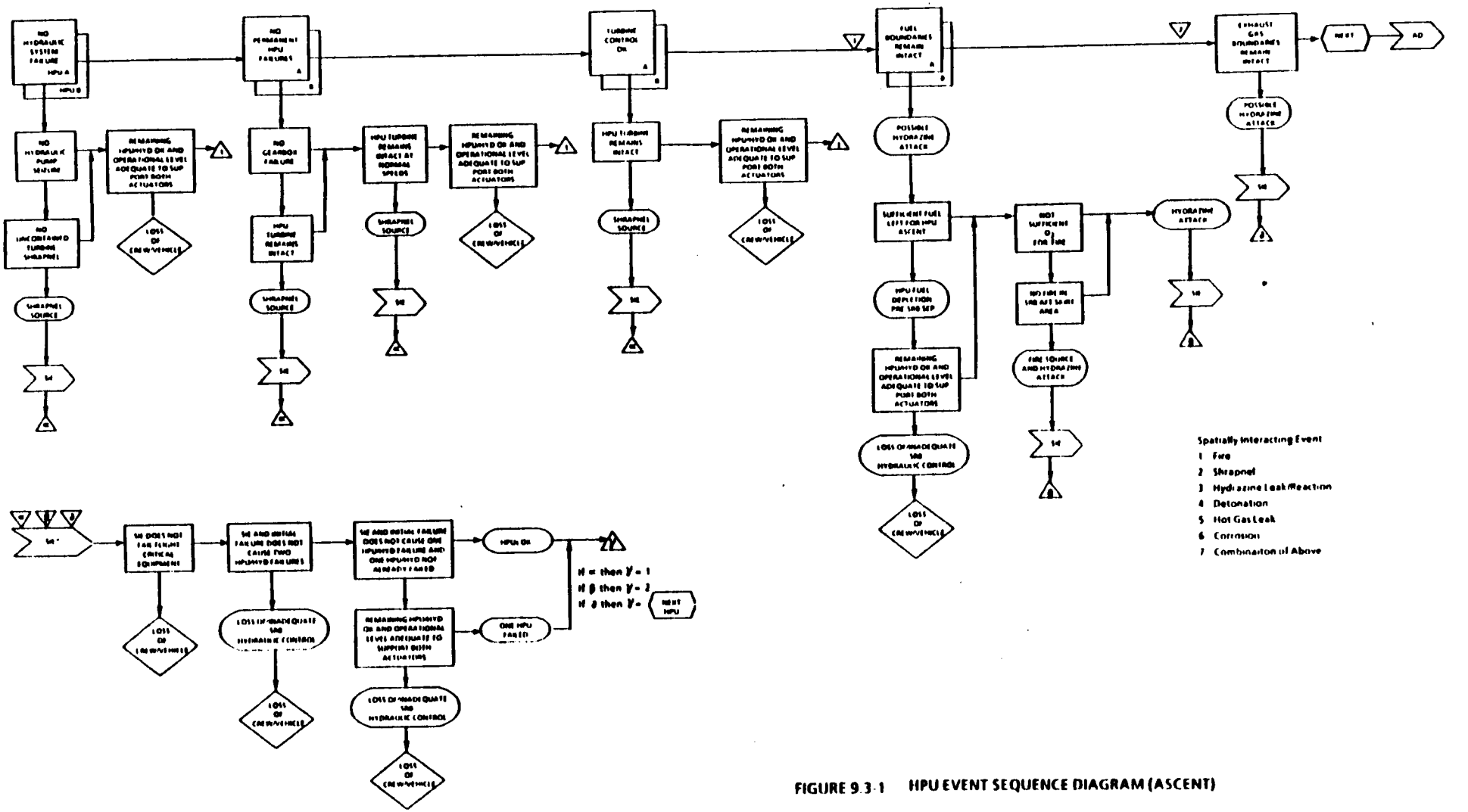


FIGURE 9.3-1 HPU EVENT SEQUENCE DIAGRAM (ASCENT)

HPU EVENT SEQUENCE DIAGRAM

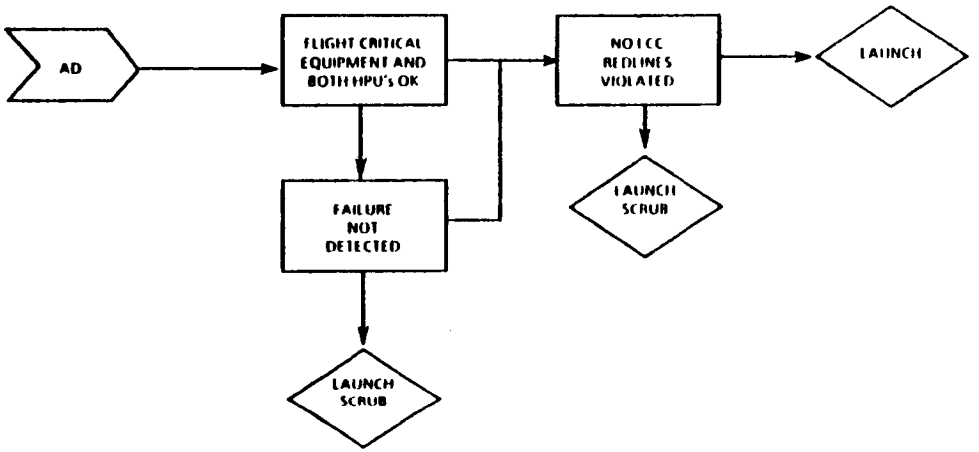


FIGURE 9.3-1

Since the boxes across the top represent a complete set of initiating failure categories, then in the absence of initiating failures the HPU must have operated successfully. Any scenario that has a vertical (down) line must, therefore, be less than completely successful. The actual damage of the scenario depends on the number and type of subsequent failures and the timing of these failures. The ESD explicitly shows cascading damage associated with spatial interactions as well as functional dependencies and independent failures.

9.3.1.2 Diagramming Dependencies in an ESD

An example of a functional dependency is shown in the sequence initiated by a failure of the hydraulic system. The failure mode is one that causes a hydraulic pump seizure. This situation could potentially be caused by a sudden large rupture of a hydraulic fluid line. Should a seizure of the hydraulic pump occur, the kinetic energy of the system could possibly cause a rupture of the HPU turbine rotor. This is represented by the question "HPU turbine remains intact?" in Figure 9.3.1. Thus the HPU turbine functionally depends on the avoidance of catastrophic hydraulic pump seizure. Of course, a more obvious functional dependency is that the hydraulic system pump operation depends on HPU operation.

An example of a scenario that includes cascading damage is shown if the HPU turbine is not intact. A negative answer to the question "HPU turbine remains intact?" means that the turbine rotor has come apart and the pieces have not been contained. In that situation, the HPU has failed and it allows hydrazine to escape into the aft skirt. Questions about cascading damage concern such items as whether there is sufficient oxygen in the aft skirt to support combustion, whether other conditions necessary for a fire are present, whether autodecomposition of hydrazine will cause further damage, and whether shrapnel from the rotor itself will cause further damage to the other HPU or "flight critical equipment" in the aft skirt. The term flight critical equipment is defined for this study to be any component or groups of components that are not part of the HPU and whose failure directly causes a LOC/V in conjunction with previous failures in the scenario. More detailed discussions of phenomena related to cascading damage are provided in Section 9.6.

9.3.1.3 Modeling Spatial Interaction Events in an ESD

Spatial interaction events (SIE) denote potential failures of equipment by virtue of their spatial proximity to the phenomena such as shrapnel and hydrazine reactions that tend to lead to cascading damage. The spatial interaction phenomena considered in this study are as follows:

1. Hydrazine reaction with materials in the aft skirt causing deterioration of either wire insulation or other material in the aft skirt following hydrazine leakage

2. Exothermic hydrazine decomposition reaction in an oxygen poor environment following hydrazine leakage

3. Fire in the aft skirt caused by hydrazine combustion following hydrazine leakage is assumed to be of negligibly small likelihood because the environment in the aft skirt is made inert with nitrogen. Consideration of ground crew failures, in particular, failure to purge the aft skirt is beyond the scope of this study.

4. Shrapnel caused by turbine rotor failure at either normal speed or turbine runaway conditions

5. Detonations caused by compression of hydrazine bubbles, leakage into solenoids of the fuel isolation or control valves, or hydrazine decomposition reaction caused heating of hydrazine in the fuel tank or fuel lines

6. Leakage of hot gas into the aft skirt caused by exhaust duct failure

The ESD also recognizes that certain failures may cascade and cause others. For example, shrapnel generated by turbine rupture or hydrazine failures detonation could cause hydrazine leakage into the aft skirt which, in turn, could result in a decomposition reaction which, in turn, could cause another detonation, etc. A more detailed discussion of the damage potential of these events is found in Section 9.6.

Below the SIE in Figure 9.3-1 is a triangle with a Greek character printed within. This denotes a transfer to another place in the ESD that has another triangle with the same character within. The SIE diagram asks questions concerning

the number of HPUs that have failed and if flight critical equipment has failed as a result of the phenomena contributing to spatial interactions.

The ESD asks if spatial interactions have failed flight critical equipment. Then the ESD asks if two HPUs have failed as a result of the initial failure and the spatial interaction. The model assumes a LOC/V if either occurs.

Finally the ESD asks if two, one or no HPUs have failed as a result of the initial failure, spatial interaction, and potential independent failure of another HPU.

We have so far given examples of how an ESD diagrams functional dependencies, cascading damage, and spatial interactions. Independent failures are diagrammed in a similar manner. Although the the combination of two or more failures occurring independently is probably of lower frequency than dependent failures, the ESD recognizes their potential. (The PRA assesses the frequency of the scenarios by the use of event trees, split fraction models, and data later in the study.)

Suppose, for example, that an HPU fails because of a problem in the gearbox, but the remaining HPU is ok and able to support both hydraulic actuators. That same HPU could also be leaking hydrazine. The transfer triangle with a "1" within leads to the next question, which is about whether the hydrazine fuel boundary remains intact. A leakage in this scenario (that is, following a gearbox failure but with no other failures) would be a second failure of the same HPU, occurring independently; that is, not caused by or related to the gearbox failure.

All scenarios in the HPU ESD ask if either hydrazine leakage or exhaust gas leakage or both can occur. This recognizes that virtually any HPU malfunction or failure can also be accompanied by the initial failure categories of hydrazine and exhaust gas leakage.

The ESD accounts for two HPUs in an SRB and diagrams scenarios in which failures can occur in more than one HPU in the same mission. The shadow boxes of the initial failure categories across the top of Figure 9.3-1 illustrates the diagrammatic device used to represent this. The diagram is read left to right for each HPU. Scenarios for the HPUs of the two SRBs are considered to be completely identical to each other but to occur independently.

In summary, an ESD is capable of exhibiting scenarios that include failures, malfunctions, multiple subsystems, dependent events, cascading damage, spatial interactions, human actions, and damage states for each stage of the mission. The remainder of Section 9.3 describes the events found in the HPU ESD. Since, as discussed above, hydraulic system failures are included for illustrative purposes only, the following discussion will not include hydraulic system-initiated scenarios.

9.3.2 HPU Scenarios from L/O-30 Seconds to SRB SEP

The ESD in Figure 9.3-1 covers the mission between L/O-30 seconds when the HPU starts and HPU shutdown at the time of SRB SEP, about 2.1 minutes after launch.

9.3.2.1 Scenarios Initiated by Permanent HPU Failure Category

This initiating failure category includes a number of failures of HPU equipment. It includes, for example, failure to start the HPU, failures of the pump, valves, turbine, and gearbox to continue running, plugging of the lube oil system and plugging of the fuel line. A complete description of all initiating failures included in the model of this category is found in Section 9.5.2. This category does not include hydrazine leakages to the aft skirt or into valve solenoids. It does not include turbine runaway events.

The gearbox and the turbine, have been singled out for additional attention in the diagram because certain failure modes of these components could potentially lead to spatial interaction events. The following describes the scenarios in Figure 10.3-1 that are beneath the box with the question "No permanent failures?".

The next event beneath this category asks if the gearbox is OK. This event includes all failure modes of the gearbox. A negative answer to this question could mean that the gearbox has failed in a way, that could cause rapid seizure of the turbine shaft. The question "HPU turbine remains intact?" is, therefore, asked. A negative answer means that the gearbox failure may (or may not) have caused an energetic failure of the turbine rotor with subsequent failure to contain the pieces within the HPU. If the gearbox is OK, then the ESD asks about independent turbine failure at normal turbine speed. If the HPU turbine remains intact, then the diagram asks if the remaining HPU is OK and can

adequately support both hydraulic actuators. A key contributor to this question is whether the remaining HPU switches to high speed mode.

If the turbine does not remain intact, the same questions related to cascading failure phenomena and spatial interaction events as those described in Sections 9.3.1.2 and 9.3.1.3 become relevant in order to describe the various sequences of events that could arise from turbine failure. Tracing through the ESD from page 1 of Figure 9.3-1 to page 2 of that figure, the diagram recognizes that, indeed, further damage might not occur to other HPUs and flight critical equipment, leaving only the initial failure of an HPU. It is also recognized that subsequent failures occurring as a consequence of shrapnel and hydrazine leakage could lead to a LOC/V.

9.3.2.2 Scenarios Initiated by Turbine Speed Control Failure Category

This initial failure category includes all failures that cause an overspeed of the HPU turbine. The combinations of control valve, controller, electric power and other failures contributing to turbine overspeed are in the split fraction models described in Section 9.5.2.1.

Unlike the APU, there is no HPU overspeed trip to prevent a turbine runaway. Therefore, the next question to be asked is if the HPU turbine remains intact (i.e., does not come apart or contains the rotor pieces). If both the primary and secondary valves fail open, then turbine speed would be expected to reach over 136,000 rpm in about 200 milliseconds. At this speed the HPU turbine is unlikely to remain intact. The expected event is that the turbine rotor would come apart in three pieces and the pieces would not be contained by the containment ring mounted inside the turbine housing. Shrapnel would enter the aft skirt, accompanied by hydrazine, which would escape the HPU through the holes created by the pieces of turbine rotor. The shrapnel would tend to spray a pattern subtending a 30 degree arc centered on the turbine rotor plane of rotor plane of rotation. Some of the shrapnel could be quite energetic, enough to damage flight critical electrical/ electronic equipment in the aft skirt, compartment bulkheads, and HPU fuel tanks.

Hydrazine leakage would not be expected to cause a fire in the aft skirt because the compartment is purged with nitrogen and low atmospheric oxygen conditions are quickly attained as the

shuttle gains altitude. Hydrazine is capable of an exothermic decomposition reaction that tends to strip insulation from wires and could cause heatup and detonation of hydrazine in other HPUs. The potential for LOC/V dramatically increases if a hydrazine fuel tank is punctured, thereby flooding the area around the HPUs with hydrazine. More detailed discussion about individual phenomena is presented in Section 9.6.

9.3.2.3 Scenarios Initiated by Hydrazine Leakage Category

This initial failure category includes hydrazine leakage from any part of the HPU into the aft skirt, into the fuel pump seal drain line, and into the isolation valve or control valve solenoids. The situation in which hydrazine contaminates and causes blockage of lube oil flow is included within the permanent failure category. Scenarios resulting from hydrazine leakage follow a negative answer to the question "Fuel boundary remains intact?". They are described below.

The notation "possible hydrazine attack" refers to the highly corrosive property of hydrazine and its autodecomposition property. Certain materials in the aft skirt such as wire insulation serve as catalysts such that with sufficiently high temperatures, hydrazine will decompose into its constituent parts of nitrogen, hydrogen and ammonia. Unfortunately, operating HPUs provide surfaces of sufficient temperature to initiate this reaction. Furthermore, materials inside the aft skirt such as Kapton wire insulation are subject to rapid deterioration under contact with hydrazine.

A negative answer to "fuel boundary remains intact?", leads to the question of whether the leakage is severe enough to deplete the fuel before SRB SEP. In such a severe case, the ESD asks if the remaining HPU can support the remainder of the mission. If not, loss of SRB hydraulic control is assumed to cause a LOC/V.

For less severe leaks, and for the situation in which the remaining HPU is adequate, questions about the potential adequate conditions for fire are asked.

Whether or not a fire occurs (one would not be expected), the ESD transfers to the SIE questions to decide on the potential further damage caused by escaping hydrazine. This part of the ESD was covered in Section 9.3.1.3. More discussion on the damage potential of hydrazine is presented in Section 9.6.

9.3.2.4 Scenarios Initiated by Exhaust Gas Leakage Category

This category includes failures in the exhaust gas duct that allow hot gas to flow into the aft skirt. It also includes failure of a small high pressure transducer line downstream of the turbine. Damage to HPUs and flight critical equipment may be caused by a large leak such that hot gas impingement on electronic equipment may cause failures of components. Such situations are phenomena that are considered extremely unlikely.

Since exhaust duct leakage itself does not fail an HPU, the ESD models all potential scenarios from this initial failure category as spatial interaction events. These have been described in Section 9.3.1.3.

9.3.2.5 Defining the Damage States for HPU Scenarios

The logic used to define damage states associated with HPU initiated scenarios is summarized in the part of the ESD with the designator "AD".

If any failures occur, any leakage detected or any redlines violated before launch, then the scenario would lead to a launch scrub. If an HPU fails after launch (a yes answer to "After launch?"), then LOC/V is assumed to occur if either a second HPU fails or the second HPU fails to switch to high speed mode. These scenarios and damage states apply to the two HPUs in either SRB.

9.3.3 Summary

Section 9.3 discussed the event sequence diagram used to develop and illustrate scenarios that begin with initial failures of the HPU and eventually lead to one of three damage states: OK, launch scrub, and LOC/V.

Although ESDs are useful for the development and communication of scenarios, they are not adequate for quantifying the risk of the HPU. Event trees and split fraction models are used for this and are discussed in the next two sections.

9.4 EVENT TREE FOR HPU INITIATED SCENARIOS

The ESD presented in the previous section was developed to clearly describe the sequential flow of events for HPU-initiated

scenarios that could lead to LOC/V, launch scrub or a successful mission. An event tree was developed from the ESD to facilitate quantification because computer techniques are available for obtaining the frequency of scenarios expressed in the form of event trees. Because quantification is the goal of an event tree, the top events need not have a one-to-one correspondence with the boxes in the event sequence diagram, and the top events need not be shown from left to right in their expected order of occurrence. Instead, the top events represent either a group of boxes in the ESD or a breakdown of an individual box. Their order is established to best capture the inter-event dependencies and facilitate the development of scenario dependent split fractions. The construction of an event tree depends on the analysts' skill and experience, knowledge of the data, and knowledge of the split fraction models. The objective is to best utilize the available data to obtain an accurate estimate of the frequency of each scenario.

The HPU event tree is shown in Figure 9.4-1. It consists of the initial event, which is the attempted start of the HPUs in one SRB, followed by 13 top events, and ending with the damage state of each sequence. The damage state is represented by an "X" beneath one of four possibilities: loss of crew or vehicle (LV), launch scrub (LS), one HPU failed but the mission successful (HP), and no HPUs failed (OK). Taken together, a line of X's at the end of a sequence is called a damage vector. Each sequence is associated with a damage vector and two or more sequences can have the same damage vector. A transfer in the tree (e.g. XFR1) means that the dotted line is to be replaced by a previously defined group of sequences with their associated damage vectors. For example, the dotted lines that end with XFR1 are to be replaced by the group of sequences and their associated damage vector to the right of the "X1" mark beneath top event "FH".

9.4.1 Relationship of ESD to Event Tree

Table 9.4.1 presents a summary description of each top event. Table 9.4.2 relates each top event to one or more ESD questions.

9.4.2 Overview of the Event Tree

The sequences in Figure 9.4-1 may be thought of as falling into five categories:

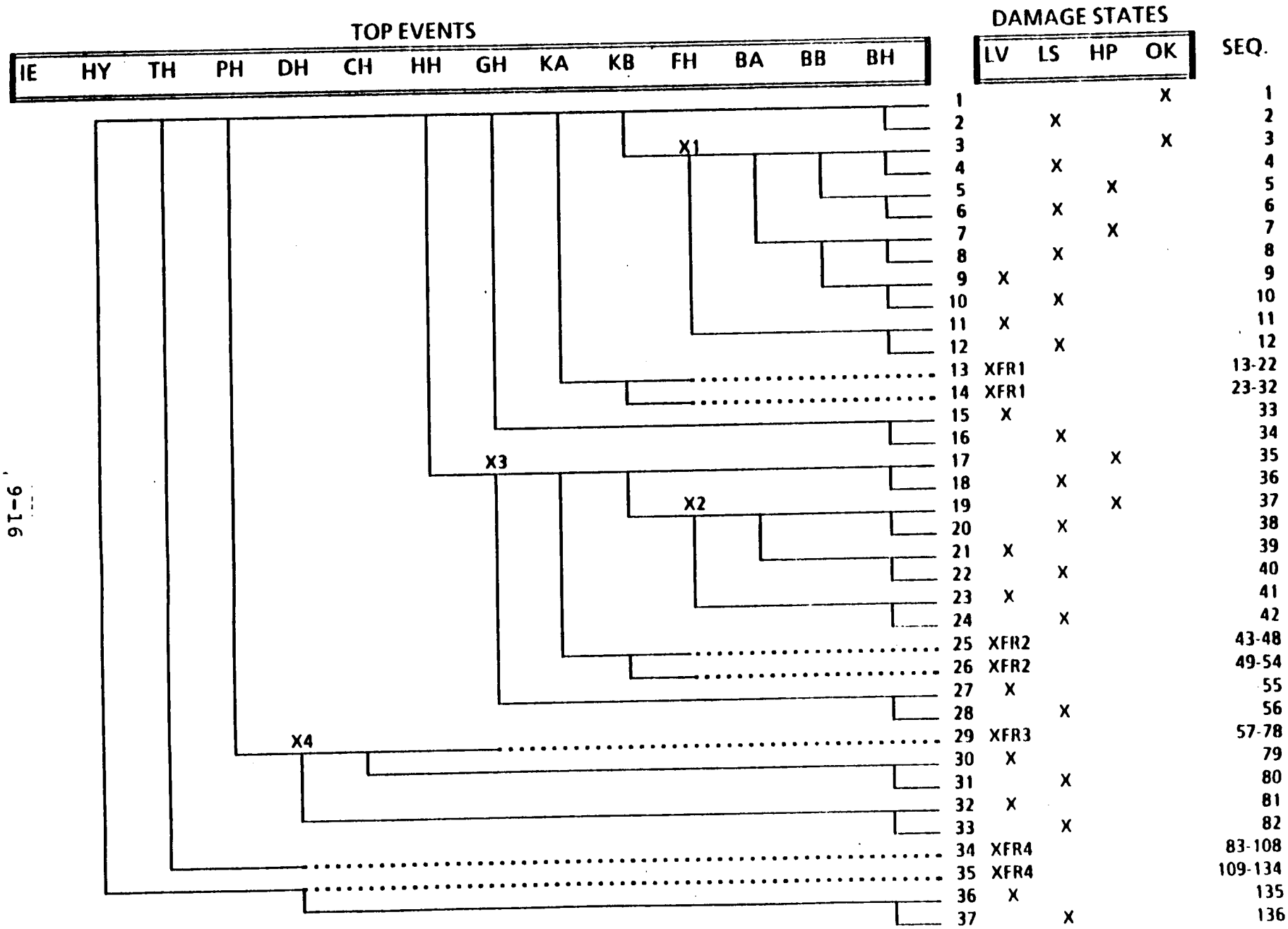


Figure 9.4-1 Event Tree

1. Sequences numbered 1 through 32 are characterized by spatial interaction failures associated with hydrazine leakages.

2. Sequences numbered 33 through 56 are characterized by spatial interaction failures associated with combinations of hydrazine leakage and exhaust has leakage.

3. Sequences numbered 57 through 78 are characterized by equipment failures in one HPU combined with spatial interaction failures associated with hydrazine leakage and exhaust gas leakage.

4. Sequences numbered 79 through 82 are characterized by equipment failures in both HPUs or by turbine rupture in one HPU causing a shrapnel or hydrazine induced failure of the second HPU or other flight critical equipment.

5. Sequences numbered 83 to 108 are characterized by turbine overspeed induced shrapnel.

The assumptions, groundrules and approximations used to construct the tree are:

1. HPU failure is defined as the inability to power its associated hydraulic pump to the extent that the second HPU must operate at higher speed in order to provide sufficient pressure to the hydraulic actuators.

2. Two HPU failures in a single SRB lead to loss of crew or vehicle (LV). A second HPU is considered failed if it does not shift into high speed following failure of the first HPU.

3. The total frequency of each damage state for both SRBs is assumed to be twice the frequency of that damage state minus the damage state frequency squared, where the damage state frequency is calculated from Figure 9.4-1.

4. The event tree is to be quantified from TIG-30 seconds to SRB SEP.

5. Large hydrazine leakages are defined as leaks for which the HPU will deplete all fuel and thereby, fail before SRB SEP.

TABLE 9.4-1

TOP EVENT DEFINITIONS-HPU EVENT TREE

SYMBOL	DEFINITION
IE	Demand for HPU Start
HY	Hydraulic System Failure*
TH	Turbine Overspeed
PH	Equipment Failure of One HPU After it Starts
DH	Failure of the Second HPU After it Starts
CH	Failure of the Second HPU or Failure of Flight Critical Equipment Due to Spatial Interactions Initiated by Failure of the First HPU
HH	Failure of One HPU Due to Exhaust Gas Leak
GH	Failure of Flight Critical Equipment of the Second HPU Due to Exhaust Gas Leak
KA	Leakage of Hydrazine from HPU A
KB	Leakage of Hydrazine from HPU B
FH	Failure of Flight Critical Equipment or Two HPUs Due to Spatial Interactions Initiated by Hydrazine Leakage
BA	Hydrazine Leakage Causes Failure of HPU A, Given That Two HPUs Have Not Failed
BB	Hydrazine Leakage Causes Failure of HPU B, Given That Two HPUs Have Not Failed
BH	Failure of One or Two HPUs Upon Start or While Running Before Launch

*This Top Event is Included to Show How an Event Tree Can Include Scenarios that Cross Subsystem Boundaries. Quantitative Evaluation of the Hydraulic System is Out-of-Scope.

TABLE 9.4-2

RELATIONSHIP OF TOP EVENTS TO HPU ESD

TOP EVENT	QUESTIONS FROM FIGURE 9.3-1
HY	"Hydraulic System OK?" and All Boxes Beneath That Question
TH,DH	"Turbine Control OK" and All Boxes Beneath That Question
PH,DH	"No Permanent HPU Failure" and All Boxes Beneath That Question
CH	All Questions Following "SIE". They Include: "SIE Does Not Fail Flight Critical Equipment" "SIE and Initial Failure Does Not Cause Two HPUs to Fail" "SIE and Initial Failure Does Not Cause the Second HPU to Fail With One Already Failed" The Questions Relate to Spatial Interactions That Could Follow Failures Involving Shrapnel
HH,GH	"Exhaust Gas Boundary Remains Intact?" and All Spatial Interaction Questions Beneath It. The Spatial Interaction Questions Now Refer Only to the Damage Potentially the Damage Potentially Caused by Exhaust Gas Release
KA,KB	"Fuel Boundaries Remain Intact"
FH	All Questions Following "SIE". The Spatial Interaction Questions Now Refer to the Damage Potentially Caused by Hydrazine in the Aft Compartment to Flight Critical Equipment or HPUs
BA,BB	"Sufficient Fuel Left for HPU Ascent" and All Questions Following "SITE". These Spatial Interaction Questions Now Refer to the Damage Potentially Caused by Hydrazine in the Aft Compartment to an Individual HPU
BH	The Question "After Launch" and All Questions Following It. This Top Event Determines the Fraction of Each Scenario That Occurs Before or After Launch. It is Used to Decide on Whether the Scenario Ends in Launch Scrub or LOC/V

6. All failures that occur before launch are assumed to lead to launch scrub. The potential for HPU failures to cause loss of crew or vehicle while sitting on the pad is considered negligibly small.

7. The HPUs are assumed to be identical and spatially symmetrical to each other so that frequencies and consequences are independent of which HPU has failed. Therefore, HPU B has been assigned as the failed HPU with no loss of generality or quantitative accuracy when TH, PH, or HH fail.

8. The possibility of two HPUs failing independently in the same flight from turbine overspeed is not modeled because the frequency of this sequence is much smaller than the frequency of sequences leading to loss of crew or vehicle that involve one turbine overspeed with other failures.

9. The frequency of failure of a running HPU before launch is approximated by the ratio of the time it runs before launch to the total time from L/O-5 to SRB SEP. All start failures are modeled as occurring before launch.

9.4.3 Description of Top Events

A summary description of each top event and its relationship to the rest of the event tree is provided in this section. The detailed model that provides the basis for assessing the frequency of occurrence of each top event split fraction is provided in Section 9.5. The data required by these models is described in Section 10.

Top Event HY: Hydraulic System Failure

This event is included as an illustration of how an event tree can include scenarios that cross subsystem boundaries. A failure of HY implies that its associated HPU is useless. The event tree, therefore, treats HY failure as if an HPU had failed.

Top Event TH: Turbine Overspeed

This event occurs if both the primary and secondary control valves fail in the open position while the HPU is operating. Mechanical, electrical and controller causes are included. Turbine overspeed implies that the HPU has failed. It is then appropriate to ask if

the resulting shrapnel and hydrazine escape have caused a second HPU or other flight critical equipment in the aft compartment (i.e., Top Event CH) to fail. The tree also asks if the other HPU could have failed independently from the turbine overspeed either by equipment failure (e.g., Top Event DH) or by leakages. Occurrence, of this event after launch and in the absence of other failures leads to the HP damage state.

Top Event PH: HPU Equipment Failure After HPU Start

This event occurs if any piece of equipment or combinations of equipment combine to prevent an HPU from providing sufficient power to its hydraulic pump as defined above. For example, this event includes failure of the turbine rotor at normal speed. This event excludes, however, turbine overspeed, leakages, and start failures. This top event does not include failures caused by erroneous commands from sources external to the HPU (e.g., the GPCs). Such failures are outside the scope of this study. The combinatorial failures included in this top event are described in detail in Section 9.5. Occurrence of this event after launch and in the absence of other failures leads to the HP damage state.

Top Event DH: Failure of Second HPU After HPU Start

This event is asked if either PH occurs or TH occurs. It occurs if the second HPU fails given that one HPU is known to have failed. The same combinations of equipment failures that contribute to PH are also relevant here. Occurrence of this event after launch leads to loss of crew or vehicle.

Top Event CH: Spatial Interaction Failure of Second HPU or Flight Critical Equipment

This event includes failure of the second HPU or flight critical equipment due to shrapnel or hydrazine induced cascading damage. It considers the possibility that shrapnel and hydrazine could be produced by turbine rotor failure either in an overspeed or normal speed condition. Occurrence of this event after launch leads to loss of crew and vehicle.

Top Event HH: Exhaust Gas Leakage Fails One HPU

This event includes the possibility, no matter how remote, that exhaust gas leakage can fail an HPU. Occurrence of this event after launch and in the absence of other failures leads to the HP damage state.

Top Event GH: Exhaust Gas Leakage Fails Second HPU

This event includes the possibility that exhaust gas leakage fails a second HPU, given that one HPU is known to have failed from exhaust gas leakage or from other causes. Occurrence of this event after launch leads to loss of crew and vehicle.

Top Event KA: Hydrazine Leakage in HPU A

This event includes leakages of hydrazine from anywhere in HPU A to the aft skirt.

Top Event KB: Hydrazine Leakage in HPU B

This event includes leakages of hydrazine from anywhere in HPU B to the aft skirt. The event tree structure involving KA and KB includes all combinations of HPUs leaking individually or together in the same mission.

Top Event FH: Leakage Induced Failure of Both HPUs or Flight Critical Equipment

This event includes those spatial interactions due to the presence of hydrazine in the aft skirt around the HPUs which causes failure of both HPUs or other flight critical equipment. Occurrence of this event after launch leads to loss of crew and vehicle.

Top Event BA: Leakage Induced Failure of HPU A

This event includes spatial interaction-induced failure of HPU A from the presence of hydrazine in the aft skirt, given that two HPUs have not failed. Occurrence of this event after launch and in the absence of other failures leads to the HP damage state.

Top Event BB: Leakage Induced Failure of HPU B

This event includes spatial interaction-induced failure of HPU B from the presence of hydrazine in the aft skirt, given that two HPUs have not failed. Occurrence of this event after launch and in the absence of other failures leads to the HP damage state.

Top Event BH: Failure Occurs Before Launch

This event includes all combinations of start failures of either or both HPUs. It also includes that portion of running failures of either or both HPUs that occurs before launch. Occurrence of this event leads to the launch scrub damage state.

9.5 SPLIT FRACTION MODEL DEVELOPMENT

9.5.1 Introduction

A guiding principle for the modeling and computational effort was to place more emphasis and detail in those aspects of the model that promised to be important to risk. This meant, for example, that many scenarios involving large numbers of failure occurrences would not be important because of their low associated probabilities. Such scenarios can be quickly estimated by a preliminary analysis using a general knowledge of the model and the basic event data. It was not difficult, for example, to estimate the order of magnitude of the total LOC/V frequency from a knowledge of the event tree, HPU design, and the failure history database, without going through the formal computer analysis. In some cases, however, knowledge to make such initial assessments was not available to the team until late in the study. It was necessary to include such events in the analysis. One of the most prominent examples is the case of consequential permanent failures resulting from exhaust gas leaks. Exhaust gas leaks were identified in the master logic diagrams as an initiating failure and were, therefore, included in the event trees. Their frequency of occurrence and the conditional probability of consequential failure of an HPU was not assessed until models were under development. Their contribution to risk was determined to be negligibly small (less than 0.1 per cent of the total LOC/V frequency). The exhaust models are, therefore, more complex than necessary.

In developing the interrelated event tree and fault tree models, it was also necessary to strike a balance in modeling complexity between these two types of logic trees. This was an iterative process that began by developing a simple first-cut event tree and its associated fault trees. The fault trees were found to be too complex to be analyzed easily. This led to a more complex event tree, and the associated fault trees were found to be much more tractable. This iterative process was continued until a reasonable balance was achieved.

The fault tree construction was influenced by data availability. As discussed in Section 5.0, it is pointless to model components at a level below that for which data exists. Furthermore, the availability of data in a particular form influences the way basic events are expressed in the fault tree. The process of split fraction modeling is iterative and highly interactive with the event tree development and data analysis process.

As indicated in Section 9.4, the event tree for HPU is a logic diagram that shows the various admissible combinations of top event occurrences and nonoccurrences that constitute the various scenarios to be analyzed. In order to be able to compute the scenario occurrence frequencies, it is necessary to compute the appropriate split fractions for the top events appearing in each scenario. In some cases, these split fractions are single numbers determined from all available evidence, as described in Section 5.0. In other cases, however, the top events represented a substantial part of the HPU, and the corresponding split fractions were computed from fault tree analyses. The paragraphs that follow describe the fault trees that were developed for calculating the split fractions for the event tree top events. The outcome of the split fraction models when evaluated by the data for the basic events is a set of split fraction cause tables as described in Section 5.

Before describing the fault trees, it is appropriate to describe some general ground rules, assumptions, and analysis considerations that are fundamental to all of the fault trees. One of the assumptions concerns the basic symmetry in HPU physical locations. Because there is no fundamental probabilistic importance associated with HPU location, there is no particular significance to the name of an HPU that fails. That is, if an unidentified, unnamed HPU fails in conjunction with one of the top events in the event tree (call that event E1), then that failed HPU can be "named" HPU B without any loss of generality. The actual name of that failed HPU is of no importance in determining probabilities. Consider now some other top event (call it E2) that appears to the right of event E1 in the event tree. Fault tree models can now be constructed for event E2 in which the failed HPU B does not appear. This represents a great simplification in the modeling process. After some preliminary modeling and quantification of exhaust duct leakage, it was concluded that exhaust duct leakage would be extremely negligible contributor to loss of crew and vehicle. The reason for this is:

1. The frequency of occurrence of exhaust duct leakage either from shrapnel or from random failure is very low (approximately 1E-5 per hour of HPU operation.)

2. Exhaust duct leakage does not constitute loss of an HPU.

3. The probability of failing an HPU or flight critical equipment in the aft skirt of the SRB as a consequence of exhaust gas impingement is quite low (approximately 1E-3 per leak).

4. We would, therefore, expect that a LOC/V owing to exhaust gas leak would occur approximately once in 100 million missions.

Rather than produce a detailed quantification for such a remote occurrence, we chose to simplify the effort and assess the frequency of all scenarios associated with exhaust duct leaks as negligible, even though a detailed model had already been developed.

Prior analysis experience has shown that common cause failures tend to be important risk contributors because multiple failures can occur as a result of a single failure condition common to two or more units. Usually this is at a substantially higher probability than that associated with multiple independent failures. Hence, it was important to include such potential contributors wherever they were indicated by the recorded APU and HPU failure history database.

In most cases the fault trees are intended to provide probabilistic results that serve directly as the split fractions for their associated top events. In some cases, however, the fault trees provide intermediate numerical results that must be combined with the numerical results of other models to obtain the required top event split fractions. For example, two consecutive top events in the event tree in Figure 9.4-1 are labeled PH and DH. PH represents the event in which one or more HPUs have a permanent failure, while DH represents the event in which both HPUs fail given that at least one has failed. The numeric quantification of the fault tree for PH yields the associated split fraction directly. However, the numeric quantification of the fault tree for DH yields the probability that both HPUs fail. To obtain the split fraction for the DH event, divide the DH result by the PH result, thereby giving the probability of both HPUs failing given that one or more failures are known to have occurred. This type of analysis also applies to the top events HH and GH in that same event tree.

Event trees are simply logic diagrams that indicate what specific combinations of events occur and do not occur; such trees do not ordinarily convey any information as to the order in which events occur. Thus, the fault tree models have to be carefully constructed to account for order when order is of concern. For example, in the HPU event tree shown in Figure 9.4.1, there are top events labeled TH and DH. TH accounts for the potential for a turbine runaway, and DH accounts for the possibility of a second independent

permanent failure of an HPU. Since the TH event appears first in the event tree, the fault tree for it models the potential for a runaway of one out of two HPUs. The DH event must then consider the implications of the order in which the two events occur. If the TH event occurs first (which is taken to occur with a probability of 0.5), then the TH analysis based on one HPU failing out of two is correct, and the DH fault tree must consider the potential for the one remaining HPU to fail (because the other one, which is named HPU B, has already failed by runaway). However, if DH occurs first (with a probability of 0.5), then the DH fault tree must be based on one out of two failing, and the TH fault tree should be based on failing the one remaining HPU. Since the TH analysis is already based on one out of two, a correction factor must be included in the DH fault tree to correct from the one-out-of-two TH analysis to the proper one-out-of-one basis needed for TH in this case. In summary, some complexity is added to the fault trees to accurately account for the order in which top events in the event tree could occur. Such correction factors will be found below in a number of the fault trees, and the "secondary" fault trees needed to cover the one-out-of-one case for TH (and other such top events) are also presented below. The specific TH/DH case mentioned here is discussed (with the appropriate fault trees) in Section 9.5.2.3. A special naming convention has been used in all of the fault trees. The first two characters are the same as the two characters in the event tree top event for which the fault tree was developed. For the basic events, the third and fourth characters identify the type of component being modeled, and the fifth character identifies its particular failure mode. For the gates, the third, fourth, and fifth characters identify the level of the gate in the fault tree and distinguish between gates at each level. The last (sixth) character is A or B to identify the specific HPU in which the component or gate resides. If the last character is a 0, then it identifies a generic component or gate -- that is, something (such as a common cause failure) not associated with any specific HPU. The details about the first five characters in these designators are given in Section 11.0.

To simplify the general appearance of the fault trees, they are shown in full only for HPU A. That detailed development is shown as a transfer with a label of the form XYA. The other HPU is then represented as transfers in with a label of the form XYB. All gates and basic events shown in subtree XYA that end with an A are converted to a B in subtree XYB.

While there are quite a number of similarities between the Orbiter APUs and the HPUs, there are a number of differences. These

differences do not affect the overall methods, assumptions, groundrules, or approaches to the analyses, but they do affect the details of the analyses. The primary difference between the APUs and the HPUs is that there are three APUs involved in the Shuttle Orbiter, while only two HPUs are used for each of two SRBs. Since only one SRB at a time is modeled, only two HPUs at a time are modeled.

The primary gas generator valve provides the control for both normal and high-speed operation of the HPU turbine (whereas the secondary valve provides high-speed control for the APU). Overall, the GGVM control circuitry for the HPU is much simpler than for the APU. In particular, no dedicated circuitry is provided to trip the HPU turbine in the event of an overspeed or underspeed of the HPU turbine (although circuitry is provided to give the secondary gas generator valve a backup controlling function in the event that the primary valve fails to control at either normal or high speed). Hence, there is no over/underspeed inhibit circuit for the HPU. Also, the fuel tank has no diaphragm, and there is only one fuel tank isolation valve (instead of the two valves found in the APUs). No cooling water systems are provided for the gas generator injector, the GGVM, the fuel tank or lines, or the lube oil. Furthermore, there are no heater circuits for the tanks or lines, but heater circuitry is provided for the gas generator to permit control of GG temperature to within the limits required for safe startup of the HPU during prelaunch operations. All of these these simplifications in the HPU hardware result in corresponding simplifications in the fault tree models developed to quantify the HPU split fractions. The paragraphs that follow provide a brief description of the fault tree models developed to compute the split fractions for the top events in the HPU event tree shown in Figure 9.4-1. In general, the HPU fault trees are very similar to the corresponding APU fault trees described in Sections 6.5.2 and 6.5.3. The primary differences arise from the fact that the HPUs are simpler in design and operation than the APUs.

9.5.2 HPU Fault Tree Models

Top Event TH

The first top event in the HPU event tree shown in Figure 9.4-1 is TH. This event represents a specific type of HPU permanent failure -- namely, one involving turbine runaway, in which failures cause the turbine speed to increase above normal operating levels. This particular failure mode has been separated from all

of the other permanent failures because of the potential for consequential failure of the other HPU or flight-critical equipment due to the high-energy shrapnel generated by the overspeed.

The fault trees developed for TH are shown in Appendices C9.5-1 and C9.5-2. The first fault tree (labeled TH) covers the model for the case of one runaway out of two HPUs, while the second one (labeled TH-D) models the case of one runaway out of one HPU. The second fault tree is provided to support top events to the right in the event tree where the order in which events occur is a consideration. Both fault trees model runaway in terms of having both the primary and secondary control valves open. The numerical result computed from fault tree TH in Appendix C10.5-1 directly yields the requisite split fraction for the top event TH in the event tree.

Top Event PH

The second top event in the HPU event tree shown in Figure 9.4-1 is PH. This event represents all but two contributors to the permanent failure of at least one of the two HPUs, where the two exceptions are: (1) the turbine runaway failures covered by TH, and (2) the start failures, which are more conveniently analyzed in the top event BH (the failures occurring before lift-off and contributing to launch scrub).

The fault trees developed for PH are shown in Appendices C9.5-3-1 through C9.5-3-4 and C9.5-4. The first fault tree (labeled PH) models the permanent failure of at least one out of two HPUs, while the second one (labeled PH-T) models the permanent failure of one out of one HPUs. This second fault tree is provided to support top events to the right of event PH in the event tree where the order in which events occurs is a consideration.

Both PH fault trees model permanent failures in terms of the following primary failure modes:

Fuel line blockage
Fuel pump failure
Low fuel tank pressure
Turbine fails to run
Turbine wheel shutdown failure
Gearbox fails to run
Gas generator run failure
Fuel tank isolation valve fails closed
Common cause failure of lube oil blockage due to hydrazine leakage through a gearbox shaft seal

The numerical result computed from fault tree PH in directly yields the requisite split fraction for the top event PH in the event tree.

Top Event DH

The third top event in the HPU event tree is DH. This event represents all but two contributors to the permanent failure of both of the HPUs, where the two exceptions are (1) the turbine runaway failures covered by TH, and (2) the start failures, which are more conveniently analyzed in the top event BH (the failures occurring before lift off and contributing to launch scrub). The only basic difference between this event and the event PH is that DH accounts for both of the HPUs failing, while PH accounts for at least one out of two HPUs failing.

The PH event represents the probability of an independent permanent failure occurring in at least one HPU, and the DH event represents the probability of an independent permanent failure occurring in both HPUs given that at least one is known to have occurred. The scenario in which PH occurs and DH does not occur represents the case in which exactly one HPU has an independent permanent failure. The scenario in which both PH and DH occur represents the case in which both HPUs have independent permanent failures. When the TH event occurs in the event tree, only the DH event is questioned with regard to the occurrence of a second permanent failure as a result of an independent cause; that is, this case is not addressed via event PH. This is simply an analysis convention that was adopted for convenience; this situation could have been addressed by using PH.

The fault trees developed for DH are shown in Appendices C9.5-5-1 through C9.5-5-3. Fault tree applies to the first (uppermost) node for DH in the event tree and models the permanent failure of both HPUs (for use in conjunction with event PH). Fault tree applies to the second (lower) node for DH in the event tree. This models the second permanent failure that occurs in conjunction with the turbine runaway failure modeled by the TH event and also models the case of the permanent failure of the one remaining HPU, which is provided to support top events to the right of event DH in the event tree where another failure occurs and the order in which failures occur is a consideration.

Fault tree DH2 in is an illustration of the logic required to account for the order in which events occur, as discussed in Section 9.5.1. If event TH occurs first, then the TH one-out-of-

two fault tree model is correct, and the DH logic must consider one-out-of-one failure logic. This situation is shown on the right side of the diagram in Appendix C9.5-5-6. If, on the other hand, DH occurs first, then the TH one-out-of-two logic must be corrected to one-out-of-one logic, and the correct logic for DH is one-out-of-two. The correction factor represented by the basic event DHTCF0 is the ratio of the result from the TH-D tree to that from the TH tree.

All of the fault trees needed for the DH event model permanent failures in terms of the following primary failure modes:

Fuel line blockage
Fuel pump failure
Low fuel tank pressure
Turbine fails to run
Turbine wheel shutdown failure
Gearbox fails to run
Gas generator run failure
Fuel tank isolation valve fails closed
Common cause failure of lube oil blockage due to hydrazine leakage through a gearbox shaft seal

The numerical result from fault tree DH1 must be divided by the numerical result from fault tree PH to obtain the split fraction needed for node 1 for the event DH; this split fraction is the conditional probability of both HPUs failing by permanent failure given that one or more permanent failures are known to have occurred. The numerical result computed from fault tree DH2 in directly yields the requisite split fraction for node 2 of top event DH in the event tree.

Top Event CH

The fourth top event in the HPU event tree is CH. This event represents the consequential permanent failure of flight critical equipment or of at least one HPU following the permanent failure of the other HPU.

The CH fault tree is shown in two parts in Appendices C9.5-6 and C9.5-7. Fault tree CH1 applies to the first (uppermost) node for CH in the event tree and models the consequential failure of flight critical equipment or of the one remaining HPU following the non-runaway permanent failure of one HPU (from event PH). Fault tree applies to the second (lower) node for CH in the event tree. This models the consequential permanent

failure of flight critical equipment or of the one remaining HPU following a turbine runaway failure (from event TH). Separate fault trees are required because the potential for consequential failure following a turbine runaway is higher than for other forms of permanent failure. The numerical results computed from both fault trees CH1 and CH2 directly yield the requisite split fractions for nodes 1 and 2 of top event CH in the event tree.

Top Event HH

The fifth top event in the HPU event tree is HH. This event represents the failure of at least one HPU as a consequence of an exhaust gas leak in at least one HPU. The model is based on the realization that the potential for a non-leaking HPU to fail is extremely remote. Thus, the model only accounts for failures of HPUs that are themselves experiencing hot gas leaks. This is also a very low frequency, as described earlier.

The fault tree developed for HH is shown in Appendix C9.5-8. That fault tree (labeled HH) models the permanent failure of at least one out of two HPUs as a consequence of exhaust gas leaks. The numerical result computed from fault tree HH directly yields the requisite split fraction for the top event HH in the event tree. A subset of the HH top event deals with a path in which one failure has already occurred. The split fraction for this path is modeled as the HHT tree in Appendix C9.5-9.

Top Event GH

The sixth top event in the HPU event tree is GH. This event represents the failure of at least two HPUs as a consequence of exhaust gas leaks in both HPUs, given that at least one HPU is known to have failed as a consequence of a gas leak. The model is based on the realization that the potential for a non-leaking HPU to fail is extremely remote. Thus, the model only accounts for failures of HPUs that are themselves experiencing hot gas leaks.
The fault trees developed for GH are shown in Appendices C9.5-10 and C9.5-11. The numerical results computed from those four fault trees are used in the same basic manner as described above for event DH to provide the requisite split fractions for the four nodes of top event GH in the event tree.

Top Events KA, KB

The seventh and eighth top events in the HPU event tree are KA and KB. These events represent the independent occurrence of a fuel leak in HPU A and B. Rather than consider the logic for these two

top events in terms of a fault tree or a set of two fault trees, it was much simpler to express the logic in terms of a simple event tree as a means of representing the probability values needed for the various combinations of leakage occurrences. This event tree is shown in Appendix C9.5-12. The split fraction to be used for each node of each top event in the event tree is shown at the appropriate node in this figure. Lambda represents the failure rate with which independent leakage occurs, and "t" is the time interval of interest over which the leak can occur. Beta represents a common cause factor, which is a measure of the conditional probability that a second HPU has a fuel leak given that one is already known to be leaking. Lambda and beta can both be estimated from the Shuttle experience data, as discussed in Section 11.0.

An important characteristic of the split fraction formulas given for the various nodes in Appendix C9.5-12 is that the scenario probabilities shown for the two scenarios having exactly one HPU leaking are both identical. Also, the sum of the probabilities for all four scenarios is exactly one.

To use the leakage split fractions listed in Appendix C9.5-12, it is simply a matter of matching the nodes in that figure with the corresponding nodes in the event tree. That is, the split fraction P21 for node 1 of the event KB is matched to all nodes in the event tree for which KB occurs when KA does not occur. Likewise, the split fraction P22 for node 2 of the event KB is matched to all nodes in the event tree for which KA does occur.

Top Event FH

The ninth top event in the HPU event tree is FH. This event represents the permanent failure of flight critical equipment as a direct consequence of a fuel leak in one or more HPUs. No fault tree was constructed for this event since the requisite split fraction is simply one number that depends only on the specific leakage conditions for the scenario being analyzed. The development of those single split fractions is discussed in Section 10.0.

Top Events BA, BB

The tenth and eleventh top events in the HPU event tree are BA, and BB. These events represent the consequential failure of either HPU due to a fuel leak in one of the HPUs (the leak can be in either HPU, the specific condition depending entirely on the particular event tree scenario being analyzed).

No fault tree was constructed for this event since the requisite split fractions are simply single numbers that depend only on the specific leakage conditions for the scenario being analyzed. The development of those single split fractions is discussed in Section 10.0.

Top Event BH

The twelfth top event in the HPU event tree is BH. This event represents a correction factor to distinguish between failures occurring before and after lift-off. The prior events in the event tree account for all run failures, regardless of the time at which they occur while the HPUs are running. Failures occurring before lift-off ordinarily result in launch scrub, while failures occurring afterward can result in either LOC/V or success, depending on their severity.

The fault trees developed for BH are shows in Appendices C9.5-13 and C9.5-14. Two trees are shown: one labeled BH0 applies only to the first node for the BH event in the event tree; the other, labeled BH, applies to all other nodes. The BH0 fault tree accounts for all start failures which are not otherwise taken into account in the fault trees developed for all other top events in the event tree. Start failures, of course, all occur before lift-off and are, therefore, all prelaunch failures that ordinarily lead to launch scrub. Such failures should not be considered elsewhere in the event tree logic. The BHn fault tree accounts for the start failures and the proportion of run time that constitutes the pre-lift-off period. This is a simple time ratio prelaunch run time to the total HPU run time. The prelaunch run time is 30 seconds, while the post-launch HPU run time is 2.1 minutes, yielding a ratio of R = 0.5/2.6 for scenarios in which one HPU has failed. The ratio becomes $2R - R^2$ for scenarios in which two HPUs have failed. The numerical result computed from fault tree BH directly yields the requisite split fraction for top event BH in the event tree.

9.6 SPATIAL INTERACTIVE EVENTS (SIEs)

An SIE is a cascading failure within one system that results from an initiating failure or condition in another system. To be an SIE, a consequential failure must also be initiated by means of a physical interactive mechanism such as hot gas or shrapnel that results from failure of or degraded operation of the system. Thus, a detonation of fuel in an HPU Gas Generator Valve Module

(GGVM) because of an exhaust leak in another HPU is a spatial interaction event, whereas loss of an HPU because of a secondary fuel valve failing in the closed position in the GGVM is not.

The split fraction representing an SIE is modeled as a conditional probability distribution as described in Section 5.5. The SIE split fractions discussed in this analysis are a subset of the set of all split fractions defined by the node points on the HPU event trees.

Three types of SIEs have been identified as significant for this PRA. They are (1) events related to HPU turbine breakup, (2) events related to HPU fuel (hydrazine) leakage, and (3) events related to hot exhaust gas leakage. The three categories of SIEs are discussed in the paragraphs below.

9.6.1 Events Related to HPU Turbine Breakup

The SIEs that result from HPU turbine breakup are identical in nature to those for the APU discussed in Section 6.6.1. There are, however, significant differences between the HPU and APU design and their operating environment that affect the SIE conditional probabilities. The frequency of SIEs initiated by HPU turbine fragments are described by conditional probability distributions defined in Section 10.5.1. The differences which affect these probabilities are discussed below.

Conditional probabilities related to HPU turbine breakup are affected by two design differences. First, the fuel control valves in the HPU Gas Generator Valve Module (GGVM) are different from those in the APU. The valves in the HPU are considered less likely to fail open and thus cause an HPU overspeed. Secondly, the HPU containment ring is 26% larger than the APU ring. This means that there is a much lower probability of uncontained fragments. It also means that any fragments that are uncontained may be at a lower energy level and hence less likely to damage other equipment.

The probability that an HPU turbine will break up at normal speed is significantly lower than that for an APU because, the HPU only runs 160 seconds during a mission, is not required to restart in flight after liftoff, and is disassembled, inspected, and refurbished after each mission.

The probability that an item of flight critical equipment will be struck by a turbine fragment is lower for the HPU than for the

APU for two reasons. There are fewer pieces of flight critical equipment in the Solid Rocket Booster (SRB) aft section than in the Orbiter compartment, and the location and orientation of the HPUs are such that turbine fragments from an HPU cannot directly impact a second HPU, its fuel line, or its fuel tank.

The location and orientation of the HPUs also preclude a turbine fragment from directly striking the external tank.

9.6.2 Events Related to HPU Fuel Leakage

The SIEs that result from HPU fuel leakage are those in which leakage of HPU fuel leads to damage of flight critical equipment or an HPU. This section presents information that is relevant to the establishment of split fractions for the associated conditional probabilities to be input to the Probabilistic Risk Analysis (PRA) model. The frequency of SIEs associated with HPU fuel leakage is reflected in conditional probabilities defined in Section 10.5.

Leaking HPU fuel (hydrazine) can damage equipment by means of corrosion, fire, or detonation.

9.6.2.1 Corrosion Damage Resulting from HPU Fuel Leakage

Hydrazine can dissolve Kapton used for wire insulation in the SRB aft compartment. However the 160 seconds maximum possible exposure of the Kapton to leaking hydrazine is believed to be too short a period for serious damage to occur.

9.6.2.2 Fire Damage Resulting from HPU Fuel Leakage

Prior to HPU activation the SRB aft skirt area is purged with nitrogen until the oxygen level is reduced to less than 4 percent by volume (Reference 52). A hydrogen fire is not possible with so little oxygen. A hydrazine fire is also unlikely under these conditions (see References 88 and 89 for additional information). A flexible barrier separates the SRB aft skirt area from the external atmosphere. This skirt prevents the oxygen level from increasing to an unsafe level during ascent.

9.6.2.3 Detonation Damage Resulting from HPU Fuel Leakage

Since hydrazine combustion cannot occur in the atmosphere of the SRB aft skirt area, no fire-induced hydrazine detonation can result from HPU fuel leakage. But detonation damage resulting from HPU fuel leakage into solenoid cavities of the fuel isolation and control valves is still a potential problem which the HPU shares with the APU. This was discussed in Section 6.6.2.2.

9.6.3 Events Related to Hot HPU Exhaust Gas Leakage

The SIEs that result from hot HPU exhaust gas leakage are those in which hot gas leakage damages Flight Critical Equipment (FCE) or an HPU. This section presents information that is relevant to the establishment of split fractions for the associated conditional probabilities to be input to the PRA model. Values assigned to the split fractions are discussed in Section 11.2.

9.6.3.1 High Pressure Hot HPU Exhaust Gas Leakage

SIEs associated with high pressure hot HPU exhaust gas leakage are identical in nature to those discussed in Section 6.6.3.1. The possibility of damage from this event is considered remote and as a simplifying assumption in the PRA, the probability was considered negligible.

9.6.3.2 Low Pressure Hot HPU Exhaust Gas Leakage

Low pressure hot HPU exhaust gas leakage is a potential problem common with the APU.

9.6.3.2.1 Solid Rocket Booster (SRB) aft area damage. - The HPU exhaust consists of a mixture of N_2, H_2, and NH_3 gases at a temperature which varies with time from HPU startup, with positions along the exhaust duct, with altitude, and with the rate of fuel flow. No insulation is employed to protect the HPUs, the hydrazine fuel lines, or the hydraulic lines from exposure to hot gas leaking from the uninsulated HPU exhaust ducts.

Pressure and temperature of the exhaust are highest at the HPU end of the exhaust duct mainly because of drag. Assuming the

pressure in the aft skirt area is the same as that of the environment into which the exhaust duct terminates, then the pressure difference between the exhaust and the aft skirt area is less than 5.4 Pounds per Square Inch (psi). The maximum temperature of 1035°F occurs only at the end of the 160 second HPU run time when the SRB is at high altitude.

An exhaust leak at the point where the exhaust duct joins the HPU could conceivably damage the HPU by damaging the associated electrical wiring insulation. The wiring insulation is Teflon with Kapton tape wrapping, which is destroyed by sustained exposure to temperatures of 500°F or above.

The HPUs are protected by obstructions from direct exhaust leak plume impingement unless the leak occurs immediately at the HPU. The SRB nozzle actuators, the hydraulic lines, and the HPU fuel lines are protected from thermal damage by the flow of a heat absorbing fluid.

Exhaust leakage from an HPU may impinge upon the associated Fuel Supply Module (FSM) but not upon the FSM of the other HPU. Thus an explosion of the FSM due to hydrazine detonation cannot occur since since the associated HPU will first be disabled by the internal detonation of hydrazine which has been heated to the detonation temperature when passing through the HPU itself.

9.6.3.2.2 HPU shutdown due to hydrazine detonation. - An analysis has been performed to gain insight regarding conditions leading to hydrazine detonation given HPU exhaust leak impingement upon a FSM (Reference 83).

Gas flowing through the HPU exhaust duct is treated as being an ideal gas flowing with constant friction in an adiabatic manner. Hot gas leakage is assumed to occur at a location nearest the FSM which would place the leak 24 inches from the exhaust outlet of the 2 inch Inside Diameter (ID) duct. Data from Reference 33 suggests a friction factor of 0.58 would be appropriate for the exhaust duct. This value reflects a degree of roughness of the exhaust duct which allows the use of a constant friction factor over a range of Reynolds numbers resulting from a large variation in mass flow rate and temperature. Temperature of gas flowing past the leak point will vary roughly linearly as a function of time between 78°F and 1006°F during the 160 second run of the HPU.

Reference 33 indicates that the maximum design inlet temperature of hydrazine to the APU is 150°F and the maximum operating temperature of the GGVM is 200°F. Above 200°F hydrazine is known to form bubbles which in principle could lead to detonation, if adiabatic compression causes a local temperature in excess of the autodecomposition temperature of about 445°F. Experiment will be required to determine the actual maximum allowed temperature and whether this maximum temperature can result from adiabatic compression of bubbles or from the heating of hydrazine when passing through the gas generator injection tube. In any case, one may conclude that the temperature of the hydrazine increases by 50°F between the inlet into the APU and the exit from the GGVM. Thus the maximum allowed FSM temperature must lie within the wide temperature range of 150°F to 395°F.

The minimum distance between the FSM and the HPU exhaust duct is about 3.75 inches. At high altitude the leaking exhaust gas will lose energy by expanding and propagating a shock wave into the compartment atmosphere. The 15 inch diameter FSM occupies 25 percent of the solid angle in the hemisphere defined by the nearest leak location and a line connecting the center of the FSM. This is suggestive of a low efficiency of thermal transfer between the leaking exhaust jet and the FSM.

Clearly, small HPU exhaust duct leaks (which are expected to be far more common than larger leaks) will not lead to a loss of an HPU. The most extreme leak -- diverting all of the HPU exhaust flow would still need to transfer a significant fraction of its thermal energy to the FSM in order to result in loss of the HPU.

Since the FSM has been covered with a foam insulation to a depth of 1.25 inches. The insulation is, in turn, surfaced with aluminized tape, even the largest exhaust leak is not expected to lead to loss of the associated HPU by means of hydrazine detonation.

The possibility of damage resulting from hot HPU exhaust gas leakage is considered to be remote. The probability of such damage was considered negligibly small.

10.0 HPU DATA DEVELOPMENT

This section describes the process used to develop probability distributions for HPU component failure rates. Probability distributions are used in this context to reflect the fact that component failure rates are uncertain. The use of probability distributions provides a complete description of our state of knowledge about the failure rates of the equipment in question, including any sources of variability among similar components. By contrast, use of a point estimate would imply a degree of exactness that is not justified by the data.

It is important to bear in mind that the existence of uncertainty about component failure rates does not imply that the results are inaccurate or that they reflect a state of ignorance on the part of the analysts. Rather, uncertainty arises from a number of sources:

a. The relatively small amount of data that is available on many components

b. The possibility of missing data (e.g., failures that are not captured by the data collection process)

c. Decisions about whether incipient failures should be included in the data analysis

d. Estimation of the applicable exposure data (e.g., the total number of hours that a component operated)

e. The application of data from one situation (e.g., checkout) to other situations such as actual flights

f. The assumption that failure rates are constant over time

g. Differences in component reliability from one mission to another (e.g., due to differences in the quality of refurbishment)

h. Differences in component reliability from one HPU to another, or between similar components in the same HPU

i. The extrapolation of failure rate estimates developed for other applications (e.g., aircraft) to the space shuttle

j. The environmental factors that should be used in adjusting failure rate estimates from one application to another

The approach used in this study to describe and quantify such uncertainties is the Bayesian theory of probability. In this approach, each basic event frequency is described by a probability distribution specifying the various possible values for that frequency and how likely each value is. The Bayesian approach is capable of taking into account both engineering judgment about the event frequency, and also empirical data such as the actual number of failures and operating hours accrued to date for the HPU.

In particular, a prior probability distribution is specified to reflect all the available information on similar components in other applications, as tempered by the engineering judgment of the analysis team. This distribution is generally then updated with the observed HPU data to yield a revised (i.e., posterior) distribution. In other cases, the posterior distribution is simply set equal to the prior distribution, and no update is performed. This is done in cases where little or no HPU data is available for use in the update; e.g., in modeling hourly failure rates for failures that have not occurred to date.

The use of judgment is in keeping with the Bayesian theory of probability. In particular, the judgment of an analysis team that is knowledgeable about equipment reliability is a valid form of evidence for use in formulating distributions; experience has shown that the judgment of experienced analysts is often remarkably close to actual data when the two have been compared. For example, several studies of component reliability have found expert estimates of component failure rates to be typically within a factor of 2 to 4 from the observed failure rates.

Section 10.1 describes the raw data sources from which HPU failure data was obtained. These sources include such documents as MSFC Problem Assessment System reports, anomaly reports, and so on. For most spatial interaction events (SIE), virtually no empirical data was available. Therefore, judgmental distributions were developed for the frequencies of these events (e.g., the likelihood of damaging an HPU as the result of a turbine overspeed).

The process used for developing SIE distributions and the resulting judgmental distributions are described in Section 10.5. These

distributions were based on extensive knowledge of such events, and also on a number of analytical studies performed specifically in support of this PRA.

Section 10.3 describes the categories of component failures for which data was collected, and the guidelines and criteria that were used for determining which events (e.g., incipient failures) would be considered failures in this study.

In general, the criteria specified in Section 10.3 are fairly conservative. For example, checkout data was included in the database on exactly the same basis as flight data. Despite this, however, no HPU failures were identified in the flight and checkout data reviewed in this study. Finally, Section 10.4 presents the actual prior and posterior distributions that were developed for the categories of components specified in Section 10.3. The sources of data used to generate and update the distributions for the various failure rates are also indicated.

The Bayesian analysis that was used to develop the posterior distributions automatically determines the appropriate weights to assign to the observed data and the prior distribution, based on the relative strength of the two types of evidence in each particular situation. For example, if the prior distribution is extremely broad (reflecting a high degree of uncertainty on the part of the analysis team) and there is a moderate amount of empirical data available, then the data will tend to dominate the posterior distribution. By contrast, if there is very little empirical data available, then the posterior distribution will tend to look similar to the prior distribution.

Due to the high reliability of the components and the extremely limited amounts of flight and hot firing time accrued to date, no flight or checkout failures were identified. The distributions for the various demand failure rates were updated based on the observed data of zero failures in the total number of demands to date, using exactly the same procedure as would be used if failures had occurred. The posterior distribution resulting from this process tends to be somewhat lower than the prior, especially when the prior distribution extends to very high failure rates, which are inconsistent with the observation of zero failures.

Because of the very limited amount of flight and checkout operating time accrued to date, it was clear that the posterior distributions for hourly failure rates would look virtually identical to the priors. Because of this, no updates were performed for the hourly failure rates, but a great deal of

effort was devoted to the development of the prior distributions for these failure rates. In particular, available information from many different sources of reliability data (e.g., the Non-electronic Parts Reliability Data handbook prepared by the Rome Air Development Center) was used to guide the engineering judgment of the analysis team.

10.1 HPU RAW DATA SOURCES

The accuracy of any technical study or report is dependent on the accuracy, quality, and availability of the input data. It was recognized prior to the start of this study that collection and validation of the HPU data would be important to the quality and accuracy of the final results. Particular attention was given to the use of engineering judgment in the data development process, especially in light of the limited amount of HPU operating experience accumulated to date.

Two basic types of data were required: (a) exposure data indicating how long the various HPU components had operated; and (b) data indicating how many failures each given component had experienced over the exposure period. For those components that did experience failures information would also be needed on the failure modes that were observed.

It was judged that utilizing Qualification Test (Qual) data would not produce reasonable failure rates. The failures associated with the Qual test program phase would likely represent flaws in the early design or manufacturing process. These failures would not necessarily be indicative of the final flight or production components or of later refinements in the manufacturing process.

The Acceptance Test (ATP) phase is the next level of component development for which data was known to be available. This data was considered to be of value in tracking failures from the time of contractor component, or system delivery, to end-of-life.

However, it was decided to exclude the ATP data from the analysis because of: (a) the lack of information on actual design changes resulting from ATP failures, (b) the inability to screen out facility failures and anomalies caused by facility or test setups, and (c) the lack of time and funding available in this study to ensure that the failures identified in the ATP data were representative of actual flight configurations.

Launch checkout and flight data were selected as the most meaningful data to support this analysis. This data represents the HPU system in the flight configuration and environment. Moreover, it was judged that any valid failure modes identified in Qual or Acceptance tests, and not corrected, would be reflected in flight failure rates, thus reducing the effect of not including data from these development categories.

Several sources of launch checkout and flight data were found to be available and accessible during the study time frame; these sources are described below. These sources were utilized to develop mission time histories dating from 1 January 1981 through Flight #24. Other sources such as NASA/contractor test reports and discussions with knowledgeable personnel were used as an information base to assist in the development of probability distributions for the Spatial Interactive Events.

The information from all sources was analyzed using a specific set of criteria to track and identify legitimate HPU failures. These criteria are discussed in Section 10.3.

The salient information needed to develop flight rates and mission sequences was compiled as a basis for developing model input data. The individual data sources and their use in this study are discussed below.

a. Marshall Space Flight Center (MSFC) Problem Assessment System, Problem Reports

b. Shuttle Flight Data and In-flight Anomaly List

c. JSC Mission Reports, Missions 1 through 23

d. Study and test reports from NASA and contractor sources and published technical documents

10.1.1 MSFC Problem Assessment System

Each problem record pertaining to the SRB Thrust Vector Control Subsystem was extracted from the MSFC Problem Assessment System database and screened for applicability to the HPU. Review of this data determined that no flight or Hot fire test anomalies or failures were experienced. The fact that the HPU experienced no flight or hot fire test failures represents, success, data and the application of this data for establishing HPU failure distributions is discussed in Section 10.3.

10.1.2 Shuttle Flight Data and In-Flight Anomaly List

The Shuttle Flight Data and In-flight Anomaly List is a historical report of flight-related information. It also includes in-flight anomalies and references to problems encountered during the STS missions.

a. Initial altitude and inclination

b. Mission sequence number, flight and orbiter number

c. Solid Rocket Booster (SRB) Separation (SEP) time

d. Other mission-related data

The mission related portion of the data was used to develop a mission timeline database, combining similar information from contractor furnished HPU run times.

10.1.3 JSC Mission Reports

The JSC Mission Reports were used to collect mission-related data. These reports were also used as a reference when mission information obtained from other data sources required further clarification.

10.1.4 Study Reports, Test Results, & Personal Communications

Some of the failure modes under consideration during this study have a very low likelihood of occurrence. Some are of such a nature that directly applicable test data does not exist; e.g., some catastrophic SIEs. In order to estimate these likelihoods, information from a large number of study and test reports from NASA and contractor sources and other technical publications was utilized.

Quite a lot of information used to supplement the written reports was obtained through telecons with various knowledgeable people in specialized fields JSC, MSFC, and other locations. Tests are presently being conducted at White Sands Proving Grounds on the properties of Hydrazine and its effect on certain materials. The results were not available for consideration and application for this study.

10.2 SPATIAL INTERACTIVE EVENT DATA

Table 10.2-1 presents the HPU SIE split fraction distributions in the format used for entry into the PRA model. These distributions and the information supporting their development are discussed individually in Section 10.5 and are presented here for clarity and convenience.

10.3 DATA CATEGORIZATION

A number of guidelines and criteria were established for the HPU data categorization task. These are each discussed below.

a. Failures occurring before January 1, 1981, were omitted from the database on the grounds that the HPU was still undergoing design development prior to that time.

b. Failures occurring during qualification tests (QUAL), acceptance tests (ATP), helium leak tests, or HPU assembly, and refurbishment were not included in the database for this project. These tests were thought to be largely inapplicable, on the basis that bench tests of individual components or sub-assemblies do not reflect the actual operation of a completed HPU. In addition, since these tests are often performed early in the process of readying an HPU for flight, they detect many types of failures that would not be expected during an actual flight.

c. Both checkout tests (CKO) and actual flights (FLT) were considered relevant for inclusion in the database. However, no applicable flight or checkout failures were identified.

d. Incipient failures (e.g., turbine blade cracking) were not explicitly included in the database as actual failures. However, the history of incipient failures to date was taken into account qualitatively in establishing appropriate prior distributions.

TABLE 10.2-1

SPATIAL INTERACTIVE EVENT HPU ASCENT DISTRIBUTIONS

BASIC EVENT	FAILURE	MEAN	5th PERCENTILE	MEDIAN	95th PERCENTILE
CH2F1	Turbine Failure Given Primary and Secondary Valves Fail Open	1.	1.	1.	1.
CH2F3	Uncontained Shrapnel Produced Given Turbine Overspeed Failure	5.2632E-01	2.9669E-01	5.1996E-01	6.8997E-01
CH1F3N	Uncontained Shrapnel Produced Given Turbine Failure at Normal Speed	9.0909E-01	7.8177E-01	9.1423E-01	9.6951E-01
CH1F5	Failure of 2nd HPU or FCE Given Shrapnel Due to Turbine Failure	1.5600E-01	4.6639E-02	1.2824E-01	3.4456E-01
K12F7	Hydrazine Leak Given Uncontained Shrapnel From Another HPU	2.6635E-05	1.0000E-06	1.0000E-05	1.0000E-04
FHF12	Hydrazine Failure Given a Small Leak in That HPU	1.6140E-02	1.9024E-03	9.7847E-03	4.8681E-02
FHF13	HPU Failure Given a Small Leak in Another HPU	5.7056E-03	9.5734E-04	3.9254E-03	1.5619E-02

e. Failures of components that are outside the scope of our HPU model were excluded from the data base for obvious reasons. For example, an HPU failure due to an erroneous signal from a bite circuit was excluded from consideration for this reason.

f. Data for components that are significantly different in design and/or operation was not grouped. For example, the number of demands experienced by the isolation valve was analyzed separately from the number of demands for the gas generator valves, since the gas generator valves experience pulsing operation and might therefore have a different failure rate. Analyzing such components together might have resulted in the use of inapplicable data for a particular component.

Based on the guidelines and criteria established above, distributions were developed for the frequencies of various types of components and component failure modes. The components used for the HPU model are specified in Table 10.3-1.

10.4 FAILURE RATES

Once the data has been categorized, as a basis for determining the components and failure modes for which failure rate distributions will be needed, the next step is to specify prior distributions for those failure rates. After that, one must specify the relevant data for each component failure mode; i.e., the number of observed HPU component failures, and the number of operating hours and/or demands to which each component was subject. Finally, the data must be combined with the prior distributions to yield posterior distributions. The results of these three steps are presented in the sections below.

10.4.1 Development of Prior Distributions

A number of sources were used as background information in developing prior distributions. These include the Nonelectronic Parts Reliability Data (NPRD) handbook, prepared by the Rome Air Development Center; MIL-HDBK-217D (which was used particularly for electronic components); the Reliability Engineering Data Series report on Failure Mechanisms, prepared by the Avco Corporation; NASA operating life limits for the APU; and the engineering judgment of the analysis team (based on previous risk assessments and data analyses).

TABLE 10.3-1

COMPONENT CATEGORIES CONSIDERED IN THE HPU MODEL

COMPONENT CATEGORY	FAILURE	SPECIFIC COMPONENT(S)
Bypass valve	Fails to open on demand	Fuel pump bypass valve
	Fails to close on demand	Fuel pump bypass valve
Solenoid valve	Fails to open on demand	Isolation valve Secondary valve
	Fails to close on demand	Isolation valve Primary valve Secondary valve
	Fails closed while pulsing	Primary valve Secondary valve
	Fails open while pulsing	Primary valve Secondary valve
	Leaks at start-up	Secondary valve
	Leaks into solenoid cavity	Primary valve Secondary valve Isolation valves
	Transfers closed (i.e., plugs)	Isolation valves
Valve driver	Fails on or off	Secondary valve driver Isolation valve driver
	Fails at start-up	Isolation valve driver

TABLE 10.3-1 (Continued)

COMPONENT CATEGORY	FAILURE	SPECIFIC COMPONENT(S)
Fixed displ. pump	Fails while operating	Fuel pump Lube oil pump
	Fails at start-up	Fuel pump Lube oil pump
Turbine	Fails while operating	N/A
	Fails at start-up	N/A
	Generates shrapnel/overspeed	N/A
	Generates shrapnel/normal spd.	N/A
Gearbox	Leaks	N/A
	Fails while operating	N/A
	Fails at start-up	N/A
Gas generator	Fails while operating	N/A
	Fails at start-up	N/A
Tank	Leaks	Fuel tank (GN2 side)
Fuel system	Leaks	Single HPU Multiple HPUs
Hot gas exh. housing & duct	Leaks	N/A

TABLE 10.3-1 (Concluded)

COMPONENT CATEGORY	FAILURE	SPECIFIC COMPONENT(S)
Filter	Blocked	Fuel inline filter Fuel pump filter
Lube oil system	Circulation restricted	Single HPU Multiple HPUs
Electric power	Fails while operating	Power to isolation valve Power to primary valve Power to secondary valve
	Fails at start-up	Power to isolation valve Power to primary valve Power to secondary valve
Controller	Fails on at start-up Fails off at start-up	Primary valve controller Primary valve controlled Secondary valve controlled
	No signal while operating	Primary valve controller Secondary valve controller
	Spur. signal while operating	Secondary valve controller Primary valve controller
MPU	Fails high while operating Fails low while operating Fails high at start-up Fails low at start-up	MPUs MPUs MPUs MPUs

In many cases, adjustments to the information obtained from these sources were needed. For example, many of the failure rate estimates obtained from NPRD were for components in aircraft or ground-based environments rather than missile environments.

Environmental adjustment factors were judged to be a reasonable way to account for many of these differences; factors for this purpose were obtained from the Avco Failure Mechanisms report. In addition, all the failure rate estimates in NPRD are presented on a per-hour basis (H), while many of the failure rates for the HPU risk study were needed on a per-demand basis (D). In such cases, the number of demands per hour in a typical application was estimated as a basis for converting the failure rate to the desired units.

In a few cases, estimates were not available from sources such as NPRD or MIL-HDBK-217D. In such cases, observed APU failure experience was to be used in the development of the HPU priors, since no HPU failures were available to aid in quantification.

Finally, after the initial assessment of prior distributions, the distributions for similar components or related failure modes were compared with each other as a reasonableness check. For example, the failure rates for different types of rotating equipment (e.g., the turbine, pumps, and gearbox) were compared to assure that they were roughly comparable, and that the assigned failure rates were consistent with engineering knowledge, such as differing speeds at which the various types of equipment operate.

This type of comparison was performed to assure that the various failure rates reflected the correct relative ranking. The comparison process, which was especially important since many of the prior distributions were based on different data sources and/or different applications, did result in the adjustment of several distributions to correspond more closely with what the analysis team considered realistic for application to the space shuttle.

The process described above is the same process as was used to develop prior distributions for the APU. Consideration was given to adjusting these distributions to reflect the more extensive testing and refurbishment performed on the HPU. This testing includes the following steps:

a. Sundstrand bench tests (i.e., acceptance tests)

b. Inspection & checkout on receipt at Kennedy Space Center

c. Helium leak testing

d. GN_2 spin test of the HPU turbine

e. Bite tests before hot firing

f. Hot firing of the HPU

g. Post-flight disassembly, refurbishment, and testing

The extent of post-flight disassembly and refurbishment in particular are significant additions to the testing and refurbishment that are performed on the APU, and might thus be expected to result in lower HPU flight failure rates than for the APU. However, these lower failure rates are counteracted by the harsher environments experienced by the HPU -- in particular, the immersion of the HPU in salt water after each mission. It was judged that the competing effects of increased testing and a harsher environment roughly canceled each other out, and that the HPU prior distributions were within the range of uncertainty of the APU priors.

Table 10.4-1 presents the prior distributions that resulted from this process. For each distribution, the table specifies the category of components to which the distribution applies, the relevant failure mode or modes, the 5th and 95th percentiles of the prior distribution; and the sources used in developing that prior. (Engineering judgment is nearly always used in the development of distributions, because there is rarely enough data to unambiguously specify a distribution.) Virtually all the prior distributions were assumed to be lognormal in form, as is common practice in PRAs. For these distributions, the medians can be found as the geometric mean of their 5th and 95th percentiles. The only exception to the assumption of lognormality is the conditional frequency of leaks in the fuel systems of additional HPUs, given that one HPU is leaking. Because the 95th percentile of this frequency was quite high, a lognormal distribution would not have been reasonable; in particular, it would have allowed conditional probabilities of leak significantly greater than 1.0. Therefore, a beta distribution was used for this parameter instead of a lognormal distribution.

TABLE 10.4-1

PRIOR DISTRIBUTIONS

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED*
			5TH PERCENTILE	95TH PERCENTILE	
VBPD	Bypass valves	Fail to open or close on demand	$2x10^{-5}$/D	$3x10^{-3}$/D	NPRD, ENVF, DMD/HR
VSNC	Solenoid valves (non-H_2O systems)	Fail to close on demand	$8x10^{-5}$/D	$7x10^{-3}$/D	SACS
VSNO	Solenoid valves (non-H_2O systems)	Fail to open on demand	$8x10^{-5}$/D	$7x10^{-3}$/D	SACS
VSND	Solenoid valves (non-H_2O systems)	Fail to reset properly when closed	$8x10^{-5}$/D	$7x10^{-3}$/D	SACS
VSNR	Solenoid valves (non-H_2O systems)	Fail open or closed while pulsing	$1x10^{-4}$/H	$1x10^{-2}$/H	NASOL

---

* Key to Sources

AVCO - AVCO Corporation
CWOD - Comparison With Other Distributions
D - Demand
DMD/HR - Demands Per Hour
ENVF - Environmental Factor
H - Hour
MIL - MIL-HDBK-217D
NASOL - NASA Operating Life Limit
NPRD - Nonelectronics Parts Reliability Data
SACS - Shuttle APU Containment Study (Reference 25)

TABLE 10.4-1 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED*
			5TH PERCENTILE	95TH PERCENTILE	
VSNT	Solenoid valves (non-H_2O systems)	Plugged while open or transfer closed	$5x10^{-8}$/H	$4x10^{-6}$/H	SACS
CKTR	Controller board	Fail to operate or spurious signal	$1x10^{-6}$/H	$1x10^{-3}$/H	MIL, NPRD, ENVF
TSPR	MPU (magnetic speed sensor)	Read high or low	$5x10^{-5}$/H	$5x10^{-3}$/H	NPRD, ENVF
PVLK	Tank or pressure vessel	Leak	$3x10^{-7}$/H	$3x10^{-5}$/H	NPRD, CWOD
ACLK	Gearbox	Loss of pressure	$5x10^{-6}$/H	$1x10^{-3}$/H	NPRD, CWOD
PFXR	Fixed displ. pump	Fail to run	$3x10^{-6}$/H	$3x10^{-4}$/H	NPRD, ENVF, CWOD
FLLP	Lube oil filter	Blocked	$1x10^{-4}$/H	$1x10^{-2}$/H	APUD
FTLK	Fuel system	Leak	1x10-5/H	1x10-3/H	APUD
FTL2	Fuel System	Leak in 2nd HPU given, HPU leaking	$2x10^{-2}$/H	$5x10^{-1}$/H	APUD
GGNR	Gas generator	Fail to operate	$1x10^{-6}$/H	$7x10^{-4}$/H	NPRD, ENVF
THLK	Hot gas exh. duct	Leak	$1x10^{-6}$/H	$1x10^{-4}$/H	NRPD, ENVF

TABLE 10.4-1 (Continued)

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED*
			5TH PERCENTILE	95TH PERCENTILE	
TBNR	Gas turbine	Fail to operate	3x10-5/H	3x10-3/H	NPRD, ENVF
DRON	Driver	Fail on or off while operating	$1x10^{-6}$/H	$1x10^{-3}$/H	MIL, APUD
DRST	Driver	Fail on demand	$3x10^{-7}$/D	$3x10^{-5}$/D	MIL, APUD, DMD/HR
FFPL	Fuel in line filter	Blocked	$3x10^{-7}$/H	$3x10^{-5}$/H	NPRD, ENVF
FPPL	Fuel pump filter	Blocked	$3x10^{-6}$/H	$1x10^{-3}$/H	NPRD, ENVF
RPIM	Gearbox	Persistent leak given a leak	$1x10^{-3}$/D	$1x10^{-1}$/D	APUD
EPSF	Isolation valves power supply	Single train fails off	$1x10^{-6}$/H	$2x10^{-4}$/H	MIL
GBXR	Gearbox	Fail to run	$1x10^{-6}$/H	$1x10^{-4}$/H	CWOD
CCLO	Lube oil	Flow restricted in 2nd HPU given 1 HPU flow restricted	$1x10^{-2}$/D	$2x10^{-1}$/D	APUD
PFXS	Pump	Fail to start	$1x10^{-7}$/D	$5x10^{-5}$/D	APUD

TABLE 10.4-1 (Concluded)

PRIOR DISTRIBUTION DESIGNATOR	COMPONENT CATEGORY	FAILURE	PARAMETERS OF PRIOR DISTRIBUTION		SOURCES USED*
			5TH PERCENTILE	95TH PERCENTILE	
TBNS	Turbine	Fail to start	$1x10^{-7}$/D	$5x10^{-5}$/D	APUD
GBXS	Gearbox	Fail to start	$1x10^{-7}$/D	$5x10^{-5}$/D	APUD
EP1S	Isolation valve electric power	Fail to start on demand	$1x10^{-4}$/D	$3x10^{-3}$/D	CWOD
CKTS	Controller	Fail to start on demand	$1x10^{-6}$/D	$1x10^{-3}$/D	SACS
TSPS	MPU	Fail to start on demand	$5x10^{-5}$/D	$5x10^{-3}$/D	CWOD

10.4.2 Specification of Failure Data

Once prior distributions has been developed for each category of components and each failure mode, the next step is to specify the relevant data for each category; i.e., the number of observed component failures of each type, and the number of operating hours (H) and/or demands (D) to which each component was subject, which can be referred to as exposure data.

No actual component failures were identified for the HPU during flight. The estimation of exposure data requires determination of whether the relevant failure mode is likely to occur over time or on a per-demand basis, and whether a failure would likely be detected if one occurred.

The total amount of run time accumulated on all HPUs to date during flights and hot firings is only about 23 hours - too small to make a difference in the failure rate estimates used in this study, which are mostly less than 10^{-3}. Therefore, updates were not performed for hourly failure rates.

For demand-based failures, the number of demands experienced by a typical component during flights and hot firings was calculated to be 603, due to the large number of hot firing tests performed on the HPU. This total, assumes that the component in question experiences exactly one demand during each firing of an HPU.

Care must be taken in attributing exposure data to particular components, however. For example, failures of the normal speed logic gate may not be detected unless a change to high speed is required during a mission, and thus the relevant exposure time for this particular failure is likely to be zero.

Table 10.4-2 presents the prior distribution and the failure and exposure data for each basic event included in the analysis. As can be seen from that table, the prior distributions for hourly failure rates were not updated and were used directly as posterior distributions, because of the small amount of exposure time and lack of failures for those events.

TABLE 10.4-2

PRIOR DISTRIBUTIONS AND OBSERVED DATA FOR APU BASIC EVENTS

PRIOR DISTR DESIG	PARAMETERS OF PRIOR DISTRIBUTION		BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXP. DATA
	5TH PERCENTILE	95TH PERCENTILE					
VBPD	$2x10^{-5}$/D	$3x10^{-3}$/D	BHBVO	Fuel Bypass Vlv.	Fail To Open On Dmd.	0	603 D
			BHBVC	Fuel Bypass Vlv.	Fail To Open On Dmd.	0	603 D
VSNC	$8x10^{-5}$/D	$7x10^{-3}$/D	PHSVC	Sec. Valve	Fail To Close On Dmd.	1	603 D
			BHPVC	Primary Vlv.	Fail To Close On Dmd.	0	603 D
VSNO	$8x10^{-5}$/D	$7x10^{-3}$/D	BHIVO	Isolation Vlv.	Fail To Open On Dmd.	0	603 D
			BHSVO	Secondary Vlv.	Fail To Open On Dmd.	0	603 D
VSND	8x10-5/D	7x10-3/D	BHSVL	Secondary Vlv.	Leak At Startup (Because of Previous Closure)	0	603 D
VSNR	$1x10^{-4}$/H	$1x10^{-2}$/H	THPVE	Primary Valve	Fail Open When Pulsing	0	23 H*

* Prior Distribution not updated;, data would have negligible effect.

Key to abbreviations:

Dmd - Demand Htr - Heater Press - Pressure Trans - Transfe

TABLE 10.4-2 (Continued)

PRIOR DISTR DESIG	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXP. DATA
			PHPVD	Primary Valve	Fail Closed When Pulsing	0	23 H*
			THSVE	Secondary Valve	Fail Open When Pulsing	0	0 H
			PHSVD	Secondary Valve	Fail Closed When Pulsing	0	0 H
VSNT	$5x10^{-8}$/H	$4x10^{-6}$/H	PHIVK	Isolation Valve	Plugged While Open	0	23 H*
CKTR	$1x10^{-6}$/H	$1x10^{-4}$/H	THSCU	Sec.Controller	Fail On	0	0 H
			THPVQ	Prim.Controller	Loss of Signal	0	23 H*
			PHPVU	Prim.Controller	Fail On	0	23 H*
			PHSVQ	Sec. Controller	Loss Of Signal	0	23 H*
			CHSLF	Normal Speed Logic Gate	Fail To Transfer	0	0 H*
TSPR	$5x10^{-5}$/H	$5x10^{-3}$/H	THM1L	MPU	Fail Low	0	23 H*
			PHM1H	MPU	Fail High	0	23 H*
PVLK	$3x10^{-7}$/H	$3x10^{-5}$/H	PHFNL	Fuel Tank	Nitrogen Leak	0	23 H

TABLE 10.4-2 (Continued)

PRIOR DISTR DESIG	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXP. DATA
ACLK	$5x10^{-6}$/H	$1x10^{-3}$/H	PHGBL	Gearbox	Leak	0	23 H*
PFXR	$3x10^{-6}$/H	$3x10^{-4}$/H	PHFPR	Fuel Pump	Fail To Run	0	23 H*
			PHLPR	Lube Oil Pump	Fail To Run	0	23 H*
FLLP	$1x10^{-4}$/H	$1x10^{-2}$/H	PHLOF	Lube Oil System	Loss Of Flow	0	23 H*
FTLK	$1x10^{-5}$/H	$1x10^{-3}$/H	LHLK1	Fuel System	Leak	0	23 H*
FTL2	$2x10^{-2}$/H	5x10-1/H	LHLK2	Fuel System	Leak in 2nd HPU Given 1 Is Leaking	2	0 D
GGNR	$1x10^{-6}$/H	$7x10^{-4}$/H	PHGGR	Gas Generator	Fail To Run	0	23 H*
THLK	$1x10^{-6}$/H	$1x10^{-4}$/H	HHHGL	Hot Gas Exh.Duct	Leak	0	23 H
TBNR	$3x10^{-5}$/H	$3x10^{-3}$/H	PHTBR	Turbine	Fail To Run	0	23 H*
GBXR	$1x10^{-6}$/H	$1x10^{-4}$/H	PHGBD	Gearbox	Fail To Run	0	23 H*
CCLO	$1x10^{-2}$/D	$2x10^{-1}$/D	DHLCC	Lube Oil System	Block In 2nd HPU Given 1 Blocked	0	0 D
PFXS	$1x10^{-7}$/D	$5x10^{-5}$/D	BHFPS	Fuel Pump	Fail To Start	0	603 D
			BHLPS	Lube Oil P'	Fail To Start	0	6C

TABLE 10.4-2 (Continued)

PRIOR DISTR DESIG	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXP. DATA
TBNS	$1x10^{-7}$/D	$5x10^{-5}$/D	BHTBS	Turbine	Fail To Start	0	603 D
GBXS	$1x10^{-7}$/D	$5x10^{-5}$/D	BHGBD	Gearbox	Fail To Start	0	603 D
EP1S	$1x10^{-4}$/D	$3x10^{-3}$/D	BHIVP	Iso.Vlv.Elec.Pwr.	Fail To Start	0	603 D
			BHSVP	Sec.Vlv.Elec.Pwr.	Fail To Start	0	603 D
			BHPVP	Prim.Vlv.Elec. Power	Fail to Start	0	603 D
CKTS	$1x10^{-6}$/D	$1x10^{-3}$/D	BHPVQ	Prim. Valve Controller	Fail On At Start	0	603 D
			BHSVQ	Sec. Valve Controller	Fail To Start	0	603 D
TSPS	$5x10^{-5}$/D	$5x10^{-3}$/D	BHM1H	MPU	Fail High At Start	0	603 D
			THM1L	MPU	Fail Low At Start	0	0 D
DRON	$1x10^{-6}$/H	$1x10^{-3}$/H	THSDO	Sec.Vlv.Driver	Fail On	0	0 H
			PHVDQ	Iso.Vlv.Driver	Fail Off	0	23 H*
FFPL	$3x10^{-7}$/H	$3x10^{-5}$/H	PHLFB	Fuel In Line Filter	Blocked	0	23 H*

TABLE 10.4-2 (Concluded)

PRIOR DISTR DESIG	PARAMETERS OF PRIOR DISTRIBUTION 5TH PERCENTILE	95TH PERCENTILE	BASIC EVENT	COMPONENT	FAILURE	FAILURES	EXP. DATA
TBNS	$1x10^{-7}$/D	$5x10^{-5}$/D	BHTBS	Turbine	Fail To Start	0	603 D
FPPL	$3x10^{-6}$/H	$1x10^{-3}$/H	PHPFB	Fuel Pump Filter	Blocked	0	23 H*
GQDL	$2x10^{-6}$/H	$2x10^{-4}$/H	PHNLQ	Fuel Tank GN2 Line Quick Disconnect	Leak	0	23 H*
RPIM	$1x10^{-3}$/D	$1x10^{-1}$/D	PHLLL	Gearbox	Severe Leak Given a Leak	0	0 D
EPSF	$1x10^{-6}$/H	$1x10^{-4}$/H	PAVAP	Isolation Valve Electric Power	Fail Off	0	23 H*
			PHSVP	Secondary Valve Electric Power	Fail Off	0	23 H*
			PAPVP	Primary Valve Electric Power	Fail Off	0	23 H*
DRST	$3x10^{-7}$/D	$3x10^{-5}$/D	BHVDQ	Iso.Vlv.Driver	Fail To Start	0	603 D

10.4.3 Development of Posterior Distributions

The Bayesian updating process for demand failure rates was performed using the RISKMAN 4 computer software on an IBM personal computer. The resulting distributions for demand failure rates, as well as the distributions for hourly failure rates, are shown in Table 10.4-3. This table shows the mean frequency for each basic event, and also the 5th, 50th and 95th percentiles.

The Bayesian analysis used to develop the demand-based distributions shown in Table 10.4-3 automatically assigns the appropriate weights to the observed data and the prior distribution, respectively, based on the relative strength of the two types of evidence in each particular situation. For example, when a great deal of empirical data is available, then the data will tend to dominate the posterior. Similarly, when relatively little empirical data is available, then the posterior distribution will tend to resemble the prior; in this case, the data is simply not strong enough to override the information contained in the prior.

For of the basic events shown in Table 10.4-3, no failures were observed, so the posteriors are slightly lower than the priors. This is a result of the Bayesian inference process, and is also intuitively reasonable. This effect is greatest when the prior distribution extends to include fairly high failure rates, which are inconsistent with the lack of observed failures. The frequencies of a few basic events were described by point estimates instead of distributions, usually on the basis that their frequencies were negligible. For the purpose of this study these events were assigned frequencies of zero. The events in this category included the following:

a. A number of start-up failures, which were considered extremely unlikely: GN2 leakage into the fuel tank at start; failure of the gas generator at start; plugging of the inline fuel filter and the fuel pump filter at start; and inadvertent opening of the fuel pump relief valve.

b. Common cause failure of two or more HPUs due to a cause other than lube oil blockage. The frequency of other common cause failure modes was considered to be dominated by the frequency of lube oil plugging.

TABLE 10.4-3

RESULTS OF HPU DATA ANALYSIS

EVENT	FAILURE	MEAN	PERCENTILE	MEDIAN	PERCENTILE
BHBVC	Bypass Valves Fails On Demand	3.3E-04	1.2E-05	1.4E-04	9.7E-04
PHSVC	Sec.Vlv. Fails To Close On Demand	6.3E-04	4.3E-05	3.3E-04	1.7E-03
BHPVC	Pri.Vlv. Fails To Close On Demand	6.3E-04	4.3E-05	3.3E-04	1.7E-03
BHIVO	Iso.Vlv. Fails To Open On Demand	6.3E-04	4.3E-05	3.3E-04	1.7E-03
BHSVO	Sec.Vlv. Fails To Open On Demand	6.3E-04	4.3E-05	3.3E-04	1.7E-03
BHSVL	Secondary Valve Leaks At Start	6.3E-04	4.3E-05	3.3E-04	1.7E-03
THSVE	Sec.Vlv. Fails Open When Pulsing	2.7E-03	9.3E-05	9.7E-04	9.7E-03
THPVE	Pri.Vlv. Fails Open When Pulsing	2.7E-03	9.3E-05	9.7E-04	9.7E-03
PHPVD	Pri.Vlv. Fails Clsd. When Pulsing	2.7E-03	9.3E-05	9.7E-04	9.7E-03
PHSVD	Sec.Vlv. Fails Clsd. When Pulsing	2.7E-03	9.3E-05	9.7E-04	9.7
PHIVK	Isolation Valve Plugs Due To Contamination When Open	1.1E-03	4.7E-08	4.3E-07	3.9
THSCU	Secondary Controller Fails On	2.7E-05	9.3E-07	9.7E-06	9.7E-05
THPVQ	Primary Controller Loss Of Signal	2.7E-05	9.3E-07	9.7E-06	9.7E-05

TABLE 10.4-3 (Continued)

EVENT	FAILURE	MEAN	PERCENTILE	MEDIAN	PERCENTILE
PHPVU	Primary Controller Fails On	2.7E-05	9.3E-07	9.7E-06	9.7E-05
PHSVQ	Sec. Controller Loss Of Signal	2.7E-05	9.3E-07	9.7E-06	9.7E-05
THM1L	Magnetic Pickup Unit Fails Low/Up Unit (MPU) No. 1 Fails Midrange	1.3E-03	4.7E-05	4.8E-04	4.8E-03
SAM1H	Mag. Pickup Unit (MPU) Fails High	1.3E-04	4.7E-05	4.8E-04	4.8E-03
PHFNL	Fuel Tank Leak - GN2 Side	8.0E-06	2.8E-07	2.9E-06	2.9E-05
PHGBL	Gearbox Leak	2.6E-04	4.6E-06	6.8E-05	9.7E-04
PHFPR	Fuel Pump Fails To Run	8.0E-05	2.8E-06	2.9E-05	2.9E-04
PHLPR	Lube Oil Pump Fails To Run	8.0E-05	2.8E-06	2.9E-05	2.9E-04
PHLOF	Lube Oil Circulation Restricted	2.7E-03	9.3E-05	9.7E-04	9.7E-03
LALK1	Fuel System Leak	2.7E-04	9.3E-06	9.7E-05	9.7E-04
LHLK2	Fuel System Leak In 2nd APU Given 1 Is Leaking	2.4E-01	2.1E-02	2.1E-01	4.9E-01
PHGGR	Gas Generator Fails To Run	1.9E-04	9.1E-07	2.5E-05	6.8E-04
HHHGL	Hot Gas Exhaust Duct Leak	2.7E-05	9.3E-07	9.7E-06	9.7E-05
PHTBR	Turbine Fails To Run	8.0E-04	2.8E-05	2.9E-04	2.9E-03
PHGBD	Gearbox Fails To Run	2.7E-05	9.3E-07	9.7E-06	9.7E-05

TABLE 10.4-3 (Continued)

EVENT	FAILURE	MEAN	PERCENTILE	MEDIAN	PERCENTILE
DHLCC	Flow Restricted Lube Oil System in 2nd HPU Given 1 HPU Flow is Restricted	6.8E-02	9.5E-03	4.4E-02	1.9E-01
BHFPS	Fuel Pump Fails To Start	1.2E-05	9.1E-08	2.1E-06	4.5E-05
BHLPS	Lube Oil Pump Fails To Start	1.2E-05	9.1E-08	2.1E-06	4.5E-05
BHTBS	Turbine Fails To Start	1.2E-05	9.1E-08	2.1E-06	4.5E-05
BHGBD	Gearbox Fails To Start	1.2E-05	9.1E-08	2.1E-06	4.5E-05
BHIVP	Electric Power To The Isolation Valve Fails To Start	5.6E-04	6.6E-05	3.4E-04	1.4E-03
BHPVP	Electric Power to Primary Valve Fails To Start	5.6E-04	6.6E-05	3.4E-04	1.4E-03
BHSVP	Failure Of Electric Power (Or 1 of 2 Switches) To Secondary Valve	5.6E-04	6.6E-05	3.4E-04	1.4E-03
BAPVQ	Pri. Valve Controller On At Start	1.1E-04	8.6E-07	2.1E-05	3.0E-04
BHSVQ	Sec.Vlv.Cntlr. Fails Off at Start	1.1E-04	8.6E-07	2.1E-05	3.0E-04
BHM1H	MPU Fails High At Start	5.0E-04	2.8E-05	2.5E-04	1.3E-03
BHM1L	MPU Fails Low At Start	1.3E-04	4.7E-05	4.8E-04	4.8E-03
THSDO	Secondary Valve Driver Fails On	2.9E-04	9.1E-07	3.0E-05	9.7E-04
PHLFB	Fuel Inline Filter Plugs	8.0E-06	2.9E-07	2.9E-06	2.9E-05

TABLE 10.4-3 (Concluded)

EVENT	FAILURE	MEAN	PERCENTILE	MEDIAN	PERCENTILE
DHLCC	Flow Restricted Lube Oil System	6.8E-02	9.5E-03	4.4E-02	1.9E-01
PHPFB	Fuel Pump Filter	2.6E-04	2.8E-06	5.3E-05	9.7E-04
PHNLQ	Fuel Tank GN2 Line QD Leaks	5.3E-05	1.9E-06	1.9E-05	1.9E-05
PHLLL	Severe GB Leak (Conditional On a Leak)	2.7E-02	9.3E-04	9.7E-03	9.7E-02
PHIVP	Failure Of Electric Power To An Isolation Valve	2.7E-05	9.3E-07	9.7E-06	9.7E-05
PHSVP	Failure Of Electric Power (Or Switch) To Secondary Valves	2.7E-05	9.3E-07	9.7E-06	9.7E-04
THPVP	Failure Of Electric Power (Or Switch) To Primary Valve	2.7E-05	9.3E-07	9.7E-05	9.7E-05
PHVDQ	Isolation Valve Driver Fails Off	2.9E-04	9.1E-07	3.0E-05	9.7E-04
BHVDQ	Iso.Vlv. Driver Fails To Start	7.8E-06	2.8E-07	2.9E-06	2.8E-05
CHSLF	Normal Speed	2.7E-05	9.3E-07	9.7E-06	9.7E-05

c. Common cause failure of both GGVM valves in the open position. This is considered much less likely than independent failure of both valves due to mechanical and/or control problems, because one of the valves fails in the open position upon loss of power and the other one fails closed. The detached valve seat single point failure is likewise considered to be of very low probability.

10.5 HPU SIE DATA DEVELOPMENT

Based on the discussion of Section 9.6, two types of SIEs are significant for the HPUs as for the APUs, namely:

a. Events related to HPU turbine failure and fragmentation

b. Events related to HPU fuel (hydrazine) leakage

The approach to developing the Auxiliary Power Unit (APU) SIE data for input into the Probability Risk Analysis (PRA) is discussed in Section 7.6 is valid for HPU SIE data also. There are differences, however, between the APU and HPU operation, design, and environment that lead to differences in conditional probabilities. The HPU starts once and runs for 160 seconds during ascent, then is disassembled and refurbished after recovery; whereas, the APU starts at least twice per mission is inspected after 20 hours run time (approximately 14 missions). The HPU, since it only runs during ascent in the nitrogen purge environment, is not subject to fuel (hydrazine) fires; whereas, the APU, as seen on STS-9, is subject to hydrazine fires during descent because of air drawn into the aft compartment. The HPU housing has a 26% larger containment ring than the APU. Moreover, there is significantly less flight critical equipment in the Solid Rocket Booster (SRB) aft skirt area than in the Orbiter aft compartment.

Table 10.5-1 presents the split fractions required for input into the HPU PRA. For each SIE conditional probability, the paragraphs below discuss the probability of frequency distribution developed for input into the PRA.

10.5.1 SIE Data Related to HPU Turbine Failure and Fragmentation

The following paragraphs present the probability of frequency distributions developed to represent the conditional probabilities related to HPU turbine breakup and discuss the data that support these distributions.

10.5.1.1 Probability of Turbine Failure at Normal Speed

The discussion of the probability of APU turbine failure at normal speed in Section 7.1 is valid also for the HPU. The analysis included the the fact that the HPU is disassembled and inspected after each mission.

10.5.1.2 Probability of Turbine Failure Due to Overspeed

This probability is equal to unity. Since there is no overspeed shutoff circuitry on the HPU to limit the overspeed peak rate as on the APU, any condition that causes overspeed will cause turbine breakup.

Table 10.5-1 HPU Split Fractions

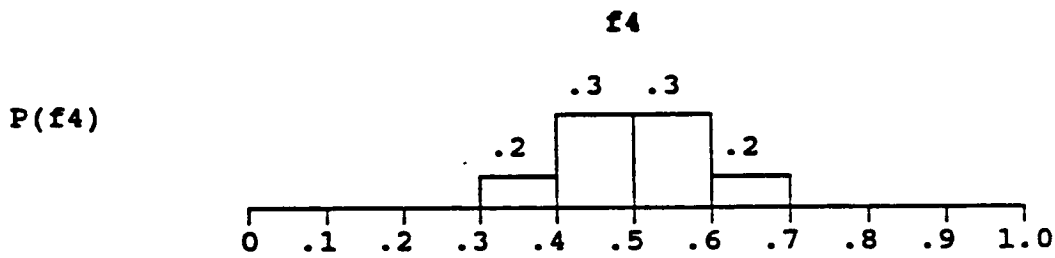
Name	Split Fractions
F1	Pr (HPU Turbine Fail | Primary and Secondary Valves Fail Open)
F3	Pr (Uncontained Shrapnel | Turbine Breakup Due to Overspeed)
F3N	Pr (Uncontained Shrapnel | Turbine Breakup at Normal Speed)
F5	Pr (Failure of Second HPU or FCE | Uncontained Shrapnel)
F7	Pr (Fuel Leak | Uncontained Shrapnel From Second HPU)
F12	Pr (HPU Fail | Small Leak in That HPU)
F13	Pr (HPU fail | Small Leak in Another HPU

10.5.1.3 Probability of Uncontained HPU shrapnel as a Consequence of Turbine Breakup at Overspeed

As discussed in Section 7.6.1.3, the probability of having uncontained fragments as a result of a turbine failure is determined by the expected breakup speed and the ability of the APU structure to contain fragments at the expected energy levels. The expected turbine failure speed of 108,000 RPM (150%) presented for the APU is valid for the HPU as well.

Reference 25 presents calculations to estimate APU/HPU turbine overspeed required to burst the containment ring and produce shrapnel. However, the calculations in this reference are based on the OV101 APU/HPU containment ring design. Since the date of this reference, the HPU containment rings were redesigned to increase the HPU containment ring yield speed to 108,090 RPM (150%). This increased the volume by 26%. Thus, the likelihood of HPU fragments being uncontained is the likelihood that the fragmentation speed will exceed 108,000 RPM. Since the expected fragmentation speed presented is 108,000 RPM, the likelihood of exceeding the HPU containment ring yield speed is 50%.

Allowing for uncertainty, this is expressed as:



Frequency of Occurrence

P(f4)	.2	.3	.3	.2
f4	.35	.45	.55	.65

This distribution was used in the evaluation of event tree top event CH following occurrence of TH.

10.5.1.4 Probability of Uncontained HPU Shrapnel as a Consequence of Turbine Failure at Normal Speed

The information presented in 10.5.1.3 is also valid for assessing the effects of turbine failure at normal speed. However, even though unit S/N 105 broke up at a speed below that required to burst the containment ring, fragments bypassed the containment ring and exited through the APU housing. This was attributed to the effects of notches in the turbine hub (Reference 96). The group, in considering this failure, judged that any turbine that broke up at normal speed would have to be seriously flawed and, hence, would bypass the larger containment ring. The same discrete distribution presented in 7.1.4 was assigned for the HPU. This distribution was used in the evaluation of event tree top event CH following occurrence of PH.

10.5.1.5 Probability of a Second HPU or Flight Critical Equipment Failure as a Consequence of Uncontained Shrapnel from a Turbine Failure at Overspeed

Given uncontained shrapnel from a turbine failure at overspeed, the likelihood that this shrapnel would cause a second HPU or flight critical equipment to fail is determined by three factors: the energy level of uncontained shrapnel, the likelihood of an uncontained fragment striking the equipment, and the vulnerability of the equipment.

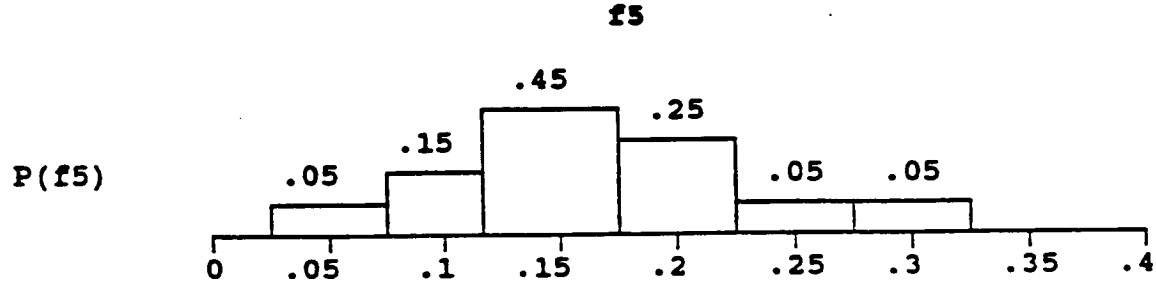
Using the approach of Section 7.1.5, the energy of the uncontained fragments can be estimated as the energy of the turbine hub fragments minus the minimum energy required to burst the containment ring. Reflecting the fact that the HPU containment ring is 26% larger than the APU containment ring, the minimum energy required to burst the containment ring is calculated to be 24,048 lb-ft. The energy of HPU turbine fragments and the energy of resulting uncontained fragments at various speeds, are presented in Table 10.5-2.

The likelihood of an uncontained fragment striking a piece of equipment must consider both the fragment spray pattern and the location of the equipment in the SRB aft skirt area. As in the APU, the fragment spray pattern that would result from an uncontained HPU hub fragmentation is difficult to define because of the lack of data and the complex HPU containment ring geometry. The HPU fragment spray pattern was assumed to be the same as that for the APU discussed in Section 7.1.5.

Table 10.5-2
HPU Uncontained Fragment Energies

% Oper. Speed	W (RPM)	Fragment Energy (lb-ft)	APU Uncont. Frag Energy (lb-ft)
100	72,000	10,688	0
110	79,200	12,932	0
120	86,400	15,390	0
130	93,600	18,063	0
140	100,800	20,948	0
150	108,000	24,048	0
160	115,200	27,361	3,277
170	122,400	30,888	6,804
180	129,600	34,629	10,545
190	136,800	38,584	14,500
200	144,000	42,752	18,668

Much less information was available to support the assessment of the likelihood of an uncontained HPU fragment striking flight critical equipment and the vulnerability of the equipment. A number of items of equipment are potentially subject to being struck. However, most items are components of the HPU/Hydraulic system containing the failed HPU and, hence, would contribute little additional risk. The exceptions to this are the hydraulic lines. An HPU turbine breakup has a finite likelihood of cutting a hydraulic line from the second HPU. This possibility is judged to be the predominant source of risk from an HPU turbine failure. The following probability distribution was assigned.



P(f5)	.05	.15	.45	.25	.05	.05

f5	.05	.1	.15	.2	.25	.3

This distribution was used in the evaluation of event tree top event CH after the occurrence of TH.

10.5.1.6 Probability of a Hydrazine Leak as a Consequence of Uncontained Shrapnel from Another HPU

The occurrence of a hydrazine leak as a consequence of uncontained shrapnel from another HPU is considered an unlikely event. Because of the locations and orientations of the HPU, it is judged that this could only occur as a result of a fragment ricochet or secondary shrapnel. This is expressed by assigning

P(f7)	1.0
f7	10^{-5}

This value was used in the evaluation of event tree top event FH after the occurrence of TH or PH without the occurrence of CH.

10.5.2 SIE Data Related to HPU Fuel Leakage

The following paragraphs present the probability of frequency distributions developed to represent the conditional probabilities related to HPU fuel leakage, and discuss the data that supports these distributions. Only those split fractions which proved significant to the model are discussed.

As indicated in Section 9.6.2 above, leaking HPU fuel (hydrazine) can damage equipment by means of corrosion, fire, or detonation. Due to the lack of oxygen in the SRB aft skirt area during prelaunch and ascent, combustion cannot occur. Like the APU, electrical wiring for the HPU has insulation consisting of an inner layer of Teflon and an outer layer of Kapton. Although given sufficient time liquid hydrazine can dissolve Kapton, it will not dissolve Teflon. In addition, the time available for hydrazine to affect wiring in the aft skirt area is very limited before SRB SEP. Thus, corrosion is not considered a credible mechanism by which hydrazine may damage the HPUs.

10.5.2.1 Probability of HPU Failure Given a Small Fuel Leak in That HPU

HPU failure given a small fuel leak in that HPU is a potential

problem shared by the APU. Development of the appropriate split fraction for the APU is discussed in Section 7.6.3.1. The ruling out of possible hydrazine corrosion damage to the HPU is the most significant difference between the two cases.

After consideration of the expert opinion, which was surveyed at the 1 October 1987 meeting, the probability of frequency distribution adopted for the split fraction associated with HPU failure given a small fuel leak in that HPU has the following characteristics:

Mean Frequency	1.6140×10^{-2}
5th Percentile Frequency	1.9024×10^{-3}
Median Frequency	9.7847×10^{-3}
95th Percentile Frequency	4.8681×10^{-2}

This distribution was used in the evaluation of event tree top events BA or BB after occurrence of KA or RB respectively.

10.5.2.2 HPU Failure Given a Small Fuel Leak in Another HPU

The probability of HPU failure given a small fuel leak in another HPU is less than the probability of HPU failure given a small fuel leak in the same HPU. Internal fuel leakage in another HPU poses a lesser risk since the resulting detonation will produce, at most, low energy shrapnel. Risk resulting from thermal damage to the HPU by catalytically-induced hydrazine decomposition is less because of the distance between HPUs.

After consideration of the expert opinion, the probability of frequency distribution adopted for the split fraction associated with HPU failure given a small fuel leak in another HPU has the following characteristics:

Mean Frequency	5.7036×10^{-3}
5th Percentile Frequency	9.5734×10^{-4}
Median Frequency	3.9254×10^{-3}
95th Percentile Frequency	1.5619×10^{-2}

This distribution was used in the evaluation of event tree top events BA or BB after occurrence of KB or KA respectively.

11.0 QUANTITATIVE RESULTS OF THE HPU PRA

The Probabilistic Risk Analysis (PRA) model was constructed from the top down. It began with illustrating the major functions of the Shuttle, interruption of which would cause loss of crew or vehicle, in the Master Logic Diagram (MLD). That diagram was developed to the level of initial failure categories of the Hydraulic Power Unit (HPU) that could lead to the damage states Loss of Crew/Vehicle (LOC/V) after launch or launch scrub before launch. Event sequence diagrams were used to define and described all significant scenarios that could lead from an initial failure to one of the damage states. The event trees and split fraction models provided further detail of the scenarios in a form that is also quantifiable. The level of detail was commensurate with the data that was collected from various sources throughout the National Aeronautics and Space Administration (NASA) and was generally at a component or sub-component level.

Quantification is performed from the bottom up. Probability distributions that reflect actuarial information about the HPU, analysis, maintenance procedures and engineering judgment were developed for each component, sub-component, and event in the model. The minimal cut sets of the split fraction models were obtained and the appropriate probability distribution assigned to each basic event in the cut sets. The RISKMAN software facilitates the development of algebraic equations that represent each split fraction and using the assigned probability distributions, obtained the numerical value of each split fraction in the HPU event tree. Another module of RISKMAN combined the split fractions to obtain the frequency of each scenario. Since each scenario was associated with a damage state (or the OK state), scenarios frequencies are summed, as shown in Section 5.10, to obtain the total damage state frequency.

The results of this study are presented in terms of the following:

a. Risk profiles of each damage state and the interpretation of the profiles

b. Description of scenarios in order of their importance to the risk profiles

c. Description of HPU component failure modes in order of their importance to the risk profile

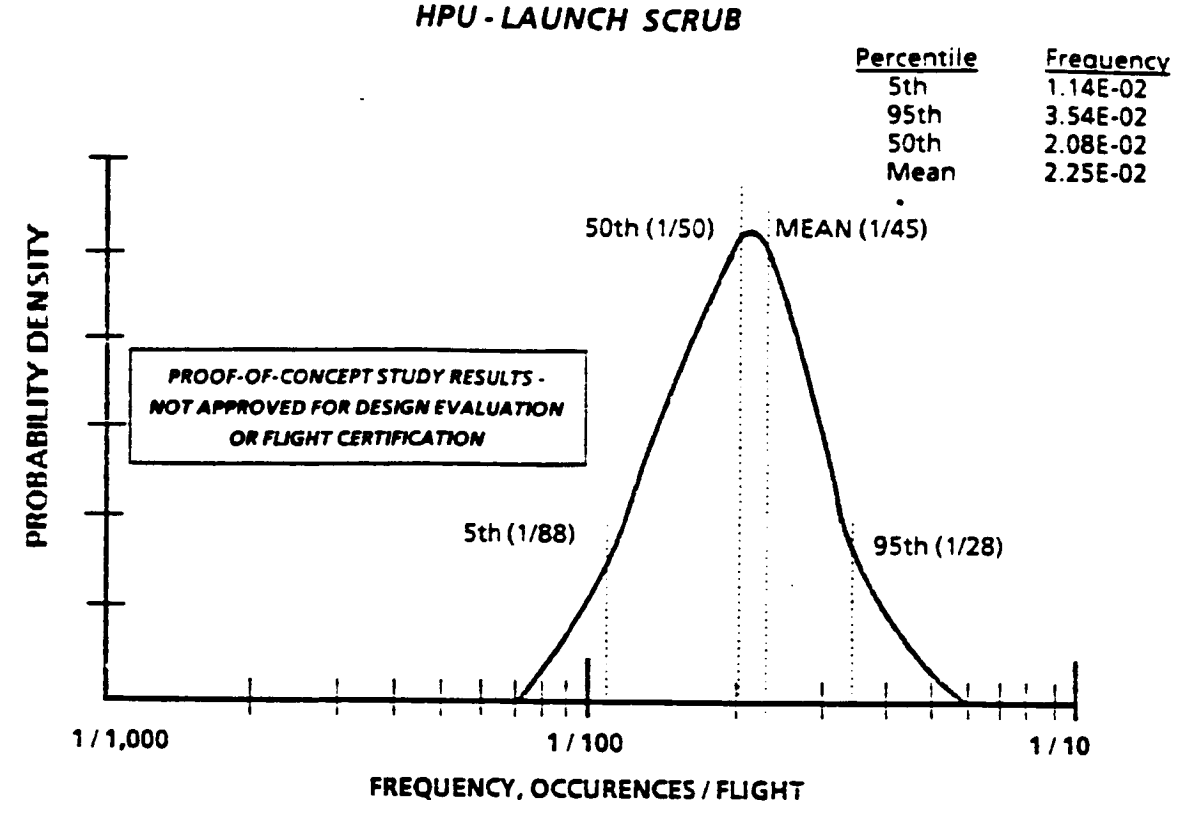
11.1 RISK PROFILES

The probability distributions shown in Figure 11.1-1 represent the state of knowledge about the fraction of missions in which HPU failures on either Solid Rocket Booster (SRB) would result in loss of crew or vehicle, and the fraction of missions in which HPU failures on either SRB would result in launch scrub. The former fraction includes the time from launch to SRB SEP. The latter fraction includes the time from L/O -30 seconds to launch.

A great deal of information is contained in these distributions even without looking further into what scenarios contribute most to them. The results show that it is extremely unlikely that HPUs would cause a loss of crew or vehicle more often than once in about 3300 missions. On the other hand, it is extremely unlikely that HPUs would cause a loss of crew or vehicle less often than once in about 4 million missions. The 90% confidence bounds are that the fraction of missions in which HPUs would cause loss of crew or vehicle lies between one in about 1.1 million missions and one in about 17,600 missions.

Similarly, the results show that it is extremely unlikely that HPUs would cause a launch scrub more often than once in about 17 missions. On the other hand, it is extremely unlikely that HPUs would cause a launch scrub less often than once in about 143 missions. The 90% confidence bounds are that the fraction of missions in which HPUs would cause a launch scrub lies between 1 in about 88 missions and 1 in about 28 missions.

It is sometimes convenient to talk about probability distributions in terms of a measure of central tendency. The mean of the distribution is used as this measure. The mean fraction of missions in which HPUs would cause loss of crew or vehicle was estimated to be one in about 52,000 missions. The mean fraction of missions in which HPUs would cause a launch scrub was estimated to be one in about 44 missions. It was also estimated that 97.6% of mission will be accomplished with all HPUs operating throughout.



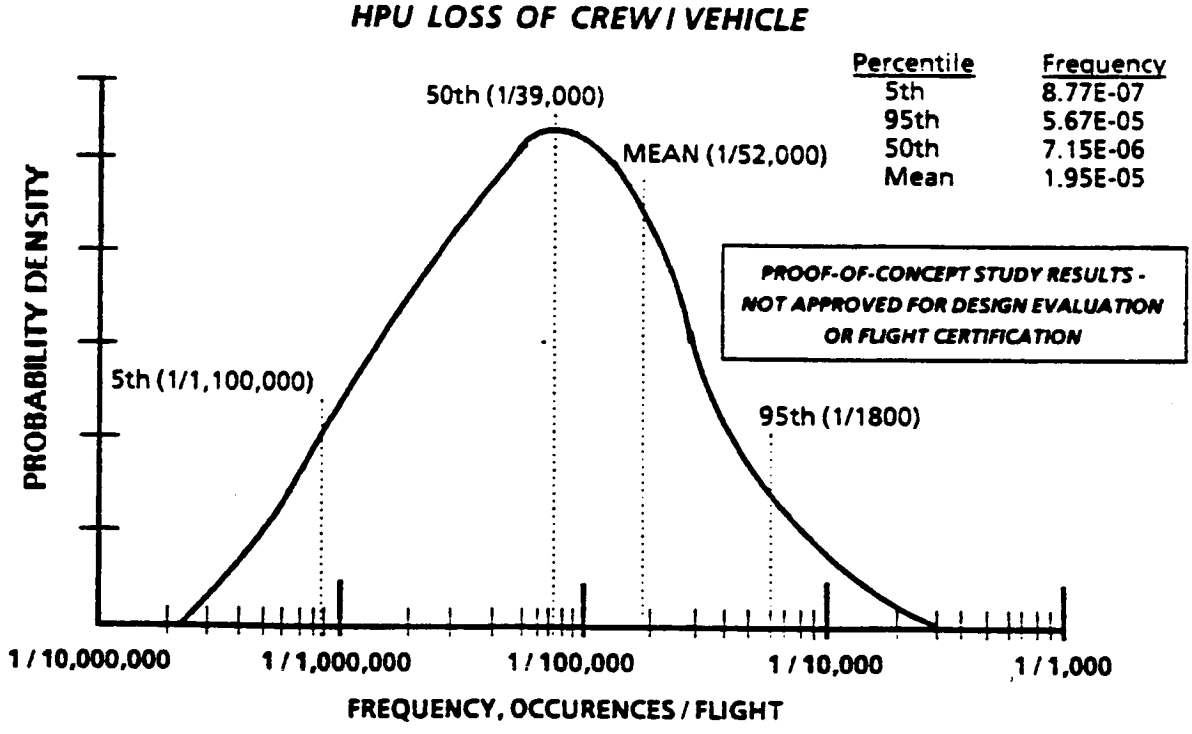


Figure 11.1 - HPU Failure Probability Distribution

The occurrence of loss of crew or vehicle associated with HPUs is quite unlikely. This is consistent with data collected during this study that indicated HPU components did not fail during flight nor during hot fire tests. The low frequency is also indicative of the prelaunch countdown procedure in which HPU malfunctions that are detected before launch would automatically scrub the launch. Indeed, an HPU associated malfunction was the cause of a launch delay although the cause was a circuitry error leading to a command shutdown rather than a malfunction in the HPU itself. (Modeling this kind of circuitry malfunction was outside the scope of this study.)

Three general factors lead to the low frequency of HPU caused loss of crew or vehicle. The first is the very short duration of the mission. The HPUs are required to operate for a much shorter time before being disassembled, inspected and refurbished than the Auxiliary Power Units (APUs). Equipment with the same failure rate is, therefore, far less likely to fail during the short HPU mission than during a longer APU mission.

The second is design specification. The HPUs are to be designed with specifications similar to the APUs. The HPUs have a far less taxing mission not only in terms of duration, but in terms of the environmental extremes that must be endured during a mission and still operate. It is appears that the HPUs have a substantial design margin from a reliability standpoint. The third factor is the extensive disassembly, inspection, refurbishment and testing that takes place for each HPU component between flight. We believe that this process (described in Section 10.4.1) is largely responsible for the low incidents of failures during hot fire tests before launches despite the immersion of the HPUs in sea water at the end of each mission.

11.2 DESCRIPTION OF RISK SIGNIFICANT SCENARIOS

11.2.1 Loss of Crew or Vehicle

Over 99% of the risk of loss of crew and vehicle due to HPUs is attributed to two scenarios. These are summarized in Table 11.2-1A. The most risk significant scenario (56.8% of the frequency of loss of crew or vehicle) involves loss of two HPUs

on the same SRB from equipment malfunctions after launch and before Solid Rocket Booster Separation (SRB SEP) on the same SRB. While the split fraction models described in Section 9.5 present numerous potential equipment failure combinations, one of these combinations has been assessed as contributing over 99% of the frequency of this scenario. This scenario is common cause blockage of the lube oil flow path. Lube oil flow path blockage causes a rapid overheat and failure of the bearings on the rotating equipment in the gearbox. The blockages may be caused by hydrazine leakage from the fuel pump seal through the drain cavity and into the gearbox via the gearbox shaft seal. The gearbox shaft seal shares the same seal drain cavity.

Hydrazine reacts with the lube oil to form a waxy substance that collects on the lube oil filters and eventually blocks them. The identified commonality of causes that covered two HPUs were choice of incompatible materials (lube oil and hydrazine), and design and fabrication of the seals and seal drain system that allowed the two materials to intermingle. The recorded data from APUs for this event (Table 7.5-3) indicated that three APUs had suffered flow blockages during flights, two of which were on the same APU during the same flight. This was one of the more significant contributors the loss of crew and vehicle frequency in the APU analysis for ascent.

Unlike the APUs, the recorded HPU failure history database of the HPUs did not exhibit symptoms (such as high lube oil pressure) to indicate flow blockages in HPUs. Nevertheless, because of the similarity of the HPU design to that of the APU in this area, the possibility of this event occurring on the HPU could not be ruled out. However, the probability distribution for the frequency of common cause failure of two HPUs due to lube oil flow blockage was appropriately reduced to reflect the lack of incidents and the shorter mission time. Although the percentage contribution is high, the frequency of the event has been assessed as being very small for the HPU (once in about 99,000 missions).

The other risk significant scenario accounts for 43% of the frequency of loss of crew or vehicle. It involves failure of an HPU turbine such that the turbine breaks into high energy fragments while it is operating at normal speed. Breakup can occur either from a flaw which could contribute to accelerated crack propagation, from fatigue, or from other causes. Inspection of HPU turbines after each flight have consistently shown cracks in turbine blades.

TABLE 11.2-1A

IMPORTANCE RANKING OF HPU FAILURE SCENARIOS

LOC/V

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Equipment failure of 2 HPUs on the same SRB between launch and SRB SEP	56.8
	Contributors and % Contribution to Scenario 1:	
	a. Common cause restriction lube oil flow causing bearing overheat and failure of rotating equipment in the gearbox (99%)	
2	Turbine failure leading to shrapnel induced failure of a second HPU or other flight critical equipment between launch and SRB SEP	43.0
	Contributors and % Contribution to Scenario 2:	
	a. Turbine fragmentation at normal speed (100%)	
3	All Others	0.2
	TOTAL	**100.0**

Turbine breakup, of course, guarantees the failure of at least one HPU. The turbine may fail in a way that causes it to wobble on its axis of rotation such that when it comes part, the pieces are not thrown precisely radially outward on the normal plane of rotation and therefore, miss the containment ring. Tests have demonstrated that the portion of the turbine casing that is not reinforced with the containment ring does not retain the fragments. These fragments become high energy projectiles capable of damaging other equipment.

The potential path and range of energy of the shrapnel was analyzed along with the strength of the materials that could be in its path. There is a chance that the shrapnel will pierce the hydrazine tank of the same HPU that suffered the turbine failure. The subsequent release of large amounts of hydrazine could damage the insulation of wiring associated with the other HPU, thereby, failing the second system. Wiring Insulation material of the HPU is made of teflon which is resistant to the corrosive property of hydrazine. A very low distribution was assigned for the frequency of failing the second HPU or some other flight critical equipment in the aft skirt. The distribution estimates that about 1 in 100 turbine failures would result in shrapnel-induced damage leading to loss of crew or vehicle. The overall frequency of this scenario is about one in 128,000 missions.

11.2.2 Launch Scrub

Table 11.2-1B shows that over 99% of the frequency of launch scrub is attributed to two failure scenarios. The most important scenario involves 98.4% of the launch scrub frequency. This scenario represents those HPU failures that occur upon attempting to start the HPUs at L/O -30 seconds.

The other scenario comprises 1.5% of the launch scrub frequency. It involves run failures of equipment in a single HPU during the 30 seconds before launch. These are failures that would cause the HPU to cease operating. Violations of launch commit criteria that allow the HPUs to continue operating were not included in the scope of this study.

TABLE 11.2-1B

IMPORTANCE RANKING OF HPU FAILURE SCENARIOS

LAUNCH SCRUB

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
1	Failure to start an HPU at Lift-off -30 seconds	98.4
	Contributors and % Contribution to Scenario 1:	
	a. Secondary control valve leaks before isolation valve is opened (11%)	
	b. Fuel tank isolation valve fails to open at start (mechanical failure) (11%)	
	c. Primary control valve fails to close at start (mechanical failure) (11%)	
	d. Secondary control valve fails to open at start (mechanical failure) (11%)	
	e. Failure of electric power to isolation valve (10%)	
	f. Failure of electric power to secondary valve (10%)	
	g. MPU 1 fails high at start (9%)	
	h. MPU 2 fails high at start (9%)	
	i. Fuel pump bypass valve fails to open (6%)	
	j. Fuel pump bypass valve fails to close (6%)	
	k. Primary valve controller fails off (2%)	
	l. Secondary valve controller fails off (2%)	

TABLE 11.2-1B (Concluded)

IMPORTANCE RANKING OF HPU FAILURE SCENARIOS

LAUNCH SCRUB

RANK	FAILURE SCENARIO RISK CONTRIBUTORS	% CONTRIBUTION
2	Failure of the HPU to continue operating after start and before launch	1.5
	Contributors and % Contribution to Scenario 2:	
	a. Primary control valve transfers closed and stays closed while pulsing (27%)	
	b. Lube oil flow path blocked (27%)	
	c. MPU 1 output fails high (13%)	
	d. MPU 2 output fails high (13%)	
	e. Turbine wheel fragments while running at normal speed (8%)	
	f. Fuel pump filter blocked (3%)	
	g. Gas generator fails (2%)	
3	All Others	0.1
	TOTAL	**100.0**

11.3 FAILURE MODE IMPORTANCE RANKING

Another way to dissect the results is to perform sensitivity studies on the importance of individual failure modes to the overall frequency of each damage state. This was done by numerous requantifications of the HPU risk model. For each requantification a different failure mode was assigned a failure frequency of zero. In other words, the component was assumed to be perfect with respect to that failure mode. In general, the requantification yields an estimate of the damage state frequency that is lower than the base case. The following importance parameter was, therefore, used to rank the individual failure modes:

$$I_j = \frac{\text{BASELINE QUANTIFICATION} - J^{th}\ \text{REQUANTIFICATION}}{\text{BASELINE QUANTIFICATION}}$$

The results shown in Table 11.2-2 are normalized by a factor representing the summation of all I_j. The failure modes shown in the Table represent over 99% of their respective damage state frequencies.

11.4 INTERPRETATION OF RESULTS

Loss of crew or vehicle associated with HPU-initiated scenarios has been assessed as highly unlikely relative to the risk to the vehicle from APU-initiated scenarios. This is primarily because of the much shorter HPU mission duration. It appears that the extensive refurbishment and pre-flight checkout procedure of the HPUs effectively compensates for their immersion in sea water at the end of each flight.

Only two HPU failure modes contribute about 98% of the frequency of loss of crew or vehicle. These are restricted lube oil circulation and turbine wheel failure.

The results indicate that the APU should receive much higher management attention for resource allocation to reduce the risk to the vehicle than should the HPU.

For those resources that are, nevertheless, allocated to the HPU, the above two items should receive a far higher priority than all other failures. Although other failures can also lead to loss of crew and vehicle, they have been estimated to be of such low frequency that fixing them would provide negligible reduction of risk.

TABLE 11.2-2

IMPORTANCE RANKING OF HPU FAILURE MODES

LOSS OF CREW OR VEHICLE

RANKING	COMPONENT/ASSEMBLY RISK CONTRIBUTORS	% CONTRIBUTION
1	Lube oil circulation restricted	55.0
2	Turbine wheel failure	43.0
3	Primary control valve transfers closed while pulsing	1.0
4	All other failures	1.0
	TOTAL	100.0

TABLE 11.2-2 (Concluded)

IMPORTANCE RANKING OF HPU FAILURE MODES

LAUNCH SCRUB

RANKING	COMPONENT/ASSEMBLY RISK CONTRIBUTORS	% CONTRIBUTION
1	Secondary control valve leaks before isolation valves open	12.0
2	Fuel tank isolation valve fails to open on demand	12.0
3	Primary control valve fails to close when HPU started (mechanical failure)	12.0
4	Secondary control valve fails to open when HPU started (mechanical failure)	12.0
5	Loss of electric power to isolation valves	10.5
6	Loss of electric power to secondary control valve	10.5
7	MPU 1 fails high on start	9.0
8	MPU 2 fails high on start	9.0
9	Fuel pump bypass valve fails to open on start	6.0
10	Fuel pump bypass valve fails to close on demand when pump is operating	6.0
11	All Other Failures	1.0
	TOTAL	100.0

To reduce the likelihood of risk associated with the HPUs, we would recommend the following actions:

a. Change the design of the seal leakage cavity such that the flow path from the fuel pump seal to the gearbox shaft seal is eliminated.

b. Continue thorough flushing and cleanup of the lube oil lines and filter.

c. Investigate and determine the cause of turbine wheel blade cracking. Change design or operation to eliminate the cause.

The study results indicate that resources spent on other failure modes to be of far less benefit.

12.0 PROOF-OF-CONCEPT STUDY REFERENCES

The following are the references used in the development of this study. The JSC documents are listed first, followed by the MSFC documents, followed by MDAC study information. Miscellaneous reports and analyses are listed last. Information gathered from study reports, personal conversations and teleconferences is not listed.

JSC REFERENCES

1. STS-1 Orbiter Final Mission Report. JSC-17378, August 1981.

2. STS-2 Orbiter Mission Report. JSC-17959, February 1982.

3. STS-3 Orbiter Mission Report. JSC-18348, June 1982.

4. STS-4 Orbiter Mission Report. JSC-18553, September 1982.

5. STS-4 Orbiter Mission Report (Supplement). JSC-18553, November 1982.

6. STS-5 Space Shuttle Program Mission Report. JSC-18735, December 1982.

7. STS-6 Space Shuttle Program Mission Report. JSC-19020, May 1983.

8. STS-7 Space Shuttle Program Mission Report. JSC-19095, July 1983.

9. STS-8 National Space Transportation Systems Program Mission Report. JSC-19278, October 1983.

10. STS-9 National Space Transportation Systems Program Mission Report. JSC-19448, January 1984.

11. STS 41-B National Space Transportation Systems Program Mission Report. JSC-19541, March 1984.

12. STS 41-C National Space Transportation Systems Program Mission Report. JSC-19642, May 1984.

13. STS 41-D National Space Transportation Systems Program Mission Report. JSC-20086, September 1984.

14. STS 41-G National Space Transportation Systems Program Mission Report. JSC-20168, November 1984.

15. STS 51-A National Space Transportation Systems Program Mission Report. JSC-20216, December 1984.

16. STS 51-B National Space Transportation Systems Program Mission Report. JSC-20578, June 1985.

17. STS 51-C National Space Transportation Systems Program Mission Report. JSC-20393, March 1985.

18. STS 51-D National Space Transportation Systems Program Mission Report. JSC-20570, May 1985.

19. STS 51-F National Space Transportation Systems Program Mission Report. JSC-20770, September 1985.

20. STS 51-G National Space Transportation Systems Program Mission Report. JSC-20672, July 1985.

21. STS 51-I National Space Transportation Systems Program Mission Report. JSC-20785, October 1985.

22. STS 51-J National Space Transportation Systems Program Mission Report. JSC-20955, December 1985.

23. STS 61-A National Space Transportation Systems Program Mission Report. JSC-20956, March 1986.

24. STS 61-B National Space Transportation Systems Program Mission Report. JSC-22070, May 1986.

25. APU (Auxiliary Power Unit)Containment. NASA TM-NB/ 77-M419.

26. Scott, W.: APU Exhaust Gas Temperature (EGT) Measurement. NASA Memo EP2-84-M173, Sept. 7, 1984.

27. Flight Data File Entry Checklist, All Vehicle: Basic, Rev. B, PCN-1, JSC 18540, May 1986.

28. JSC Full Problem Report (FPR). Auxiliary Power Unit, Report M4001002, July 17, 1986.

29. Mechanical Systems Console Handbook: Systems Briefs, Vol. II, Basic, Rev. A, PCN-3. JSC-18341, February 1986.

30. Orbiter Vehicle Operation Configuration, Failure Mode Effects Analysis, Auxiliary Power Unit Subsystem. Change No. 2. STS82-0027, January 1983.

31. Shuttle Flight Data and Inflight Anomaly List, Rev. H, JSC-19413, January 1986.

32. Shuttle Flight Data and Inflight Anomaly List. Rev. J, JSC 19413, June 1987.

33. Shuttle Operational Data Book: Shuttle System Performance Constraints Data, Vol. I, Rev. D, Amendment 208. JSC-08934, November 1985.

34. Shuttle Flight Operations Manual: Auxiliary Power Unit/Hydraulics, Vol. 9, Basic. JSC-12770, March 1981.

35. Shuttle Flight Operations Manual: Solid Rocket Booster Systems, Vol. 8B, Preliminary. JSC-12770, October 1979.

36. Space Shuttle Operations and Maintenance Requirements and Specification Document, V46 File III: Auxiliary Power Units Subsystem. JSC-08171, April 1986.

37. Space Shuttle Systems Handbook. Rev. C, PCN-5. JSC-11174, September 1985.

38. Lance, R.J.; and Camp, D.W.: STS-9 APU Anomaly Final Report. NASA-JSC.

39. STS Operational Flight Rules, Final, PCN-1. JSC-12820, April 1987.

40. APU/Hydraulics Systems Training Manual. APU/HYD TM 2102, NASA-JSC, November 1985.

41. Tuthill, W.: Auxiliary Power Unit Subsystem (APUS) FMEA/CIL Review, Vol. II: Electrical Power, Displays and Control (EPD&C). Presentation to NSTS Level I/II Review Board (NASA-JSC), October 1987.

42. Scott, W: Auxiliary Power Unit Subsystem (APUS) FMEA/CIL Review, Vol. I: Hardware. Presentation to NSTS Level I/II Review Board (NASA-JSC), October 1987.

43. Scott, W.: Exhaust Gas Temperature Measurements. NASA-JSC Memo EP2-84-M173, November 7, 1984.

44. Solid Rocket Booster Workbook. SRB 2101, CG6-013, NASA-JSC, November 1978.

MSFC REFERENCES

45. MSFC Problem Assessment System, Thrust Vector Control Subsystem, July 16, 1987.

46. Solid Rocket Booster Operations and Maintenance Requirements and Specifications, Prelaunch. April 17, 1987.

47. Specification for hydrazine fuel isolation valve, SRB TVC Subsystem, 10SPC-0056 SCN 006, May 29, 1985.

48. Specification for hydrazine fuel supply module, SRB TVC Subsystem, 10SPC-0049 SCN 003, May 29, 1985.

49. SRB Critical Items List. Electrical and Instrumentation Subsystem, PCIN 40202, CR S40202C, July 1987.

50. SRB Critical Items List. Thrust Vector Control Subsystem, PCIN 40202, CR S40202E, July 1987.

51. SRB Electrical and Instrumentation Subsystem. Failure Mode Effects Analysis, Rev. Basic, September 12, 1986.

52. SRB FMEA/CIL Thrust Vector Control Subsystem. Space Shuttle CIL Review Board, Summary, May 8, 1987.

53. Thrust Vector Control Subsystem Failure Mode Effects Analysis (FMEA). Rev. Basic, December 12, 1986.

STUDY ACTION ITEM MEMOS & TRANSMITTALS

54. Response to Action Item 8, Rev 1, NRA 020R1, September 14, 1987. (A study to determine the altitude that the RCS thrusters are 1) considered no longer effective for orbiter control and 2) disabled to prevent usage.)

55. Response to Action Item 10, NRA-024, July 22, 1987. (A study to determine the surface temperature that leads to Hydrazine combustion.)

56. Response to Action Item 14, NRA-026, July 29, 1987. (The possibility of structural damage to the Orbiter due to an APU fuel tank rupture.)

57. Response to Action Item 11, NRA-032, August 11, 1987. (The minimum 02 concentration necessary to support a hydrazine fire and the corresponding altitude during ascent and descent.)

58. Response to Action Item 13, NRA-033, August 11, 1987. (The possibility of fire in the aft compartment prior to liftoff and during ascent.)

59. Response to Action Item 29, NRA-034, August 11, 1987. (The prelaunch aft skirt nitrogen purge reduction of oxygen content to levels below the hydrazine combustion level.)

60. Response to Action Item 26 and response to Action Item 27, NRA-035, August 11, 1987. (The conditions under which a leaking APU can cause hydrazine detonation if restarted.)

61. Response to Action Item 22, NRA-039, September 12 , 1987. (Survey of test data and/or analysis of turbine structural failure.)

62. Response to Action Item 23, NRA-040, August 28, 1987. (The conditions under which hydrazine detonation causes energetic shrapnel.)

63. Response to Action Item 24 and 25, NRA-041, August 29, 1987. (The possibility of fire in the aft compartment (or SRB aft skirt) due to hydrazine leakage and subsequent degradation towards electronic equipment, power or control cables, main engine performance, main engine fuel lines, avionics, or flight and landing control.)

64. Response to Action Item 1, NRA-042, September 9, 1987. (Abort Resulting from Main Engines stuck in the thrust bucket.)

65. Response to Action Item 17, NRA-043, September 9, 1987. (Structural integrity of the APU/HPU following seizure of the hydraulic pump.)

66. Response to Action Item 18, NRA-044, September 9, 1987. (Conditions leading to hydraulic pump seizure.)

67. Response to Action Item 19, NRA-045, September 9, 1987. (The conditions under which an uncontrolled turbine overspeed is caused by a secondary GG valve stuck in mid-position.)

68. Response to Action Item 37, NRA-046, September 9, 1987. (Loss of control due to loss of two APUs during ascent.)

69. Response to Action Item 15, NRA-048, September 8, 1987. (Overheating and rupture of the fuel tank isolation valves or GG control valves.)

70. Response to Action Item 16, NRA-049, September 8, 1987. (Overheating of the APU cooling system valves while energized.)

71. APU electrical failure fault trees and failure rates. NRA-050, September 8, 1987.

72. Response to Action Item 36, NRA-051, September 12, 1987. (The Lube Oil ignition temperature in the gearbox and leaking lube oil ignition in the aft compartment.)

73. Response to Action Item 5, NRA-052, September 9, 1987. (The possibility of main engine (propellant) detonation due to an APU fuel fire.)

74. Estimated failure rates for Hybrid Drivers & Remote Power Controllers. NRA-053, September 11, 1987.

75. Response to Action Item 7, NRA-054, September 9, 1987. (Estimation of damage to the Orbiter structure due to APU exhaust leak.)

76. Response to Action Item 35, NRA-056, September 10, 1987. (Energetic shrapnel caused by gearbox and/or its associated gears and shafts failing.)

77. Response to Action Item 12, NRA-057, September 12, 1987. (Gradual GG bed contamination as an impending failure mode).

78. Response to Action Item 2, NRA-059, September 16, 1987. (The possibility of damage to the aft Avionics Bays due to an APU fuel fire.)

79. Response to Action Item 4, NRA-060, September 16, 1987. (OMS tank detonation due to an APU Fuel Fire.)

80. Response to Action Item 6, NRA-061, September 16, 1987. (The possibility of main engine (propellant) detonation due to APU shrapnel.)

81. Response to Action Item 9, NRA-062, September 23, 1987. (Temperature of a GG leak which the APU exhaust duct can handle.)

82. Response to Action Item 3, NRA-064, September 1987. (Electronics damage in the aft Avionics Bays due to an APU exhaust leak.)

83. Response to Action Item 6, NRA-067, October 9, 1987, (Damage to HPU components due to HPU exhaust duct failure.)

MISCELLANEOUS REFERENCES

84. Vinh, F.Q.: APU Exhaust Gas Sensitivity To Gas Generator Leakage. Rockwell-Downey, March 18, 1985.

85. Carpentier, R.H.: APU Exhaust Plume Ignition OV101 ALT Program. Rockwell-Downey.

86. APU Turbine Wheel Containment. NASA-JSC Reliability Division, August 1977.

87. Farkas, T.: APUS Overview Briefing. Rockwell-Downey, December 1985.

88. Benz, F.J.; and Pippen, D.L.: Autoignition, Flammability, and Explosion Properties of Hydrazine and Monomethydrazine. 1980 JANNAF Safety and Environmental Protection, April 1980.

89. Perkins, J.H.; and Riehl, W.A.: Autoignition of Hydrazine by Engineering Materials. Paper presented at the 16th AIAA Aerospace Sciences Meeting, (Huntsville, Alabama), January 1978.

90. Ledoux, P.W.: Auxiliary Power Unit (APU) Single Barrier Failures. MDAC TM No. 11-TM-ES86025-82, June 22, 1986.

91. Scott, F.E.; Burns, J.J.; and Lewis, B.: Explosive Properties of Hydrazine. U.S.Bureau of Mines, R.I. 4660, May 1949, p. 16.

92. Schmidt, E.W.: Hydrazine and It's Derivatives. John Wiley & Sons, 1984.

93. Integrated System Schematic - Orbiter OV099 APU, Rev. A9. VS70-946099, May 1985.

94. Integrated System Schematic - SRB, Change 14. VS72-948102.

95. Deventhal, Rex: JSC N2H4 Adiabatic Compression Test Status in Orbiter Improved APU Program Review. Paper presented at Sundstrand Advanced Technology Group (Rockville, Ill.), July 1987.

96. Johnson, B.: JSC Request For Information Concerning APU Turbine Overspeed Bursts. Sundstrand Advanced Technology Group. 486-BGJ-M14, April 1986.

97. Military Handbook, Reliability Prediction of Electronics Equipment. MIL-HDBK-217D, January 15, 1982.

98. MIL-HDBK-5B. Change Notice 3, pp. 6-37 through 6-43, August 15, 1974.

99. Rossi, M. J.: Nonelectronic Parts Reliability Data. Reliability Analysis Center, Rome Air Development Center. NPRO-3, October 1985.

100. Kaplan, S.: On a 'Two Stage' Bayesian Procedure for Determining Failure Rates from Experiential Data, PLG-0191, IEEE Transactions on Power Apparatus and Systems, Vol. PAS-102, No. 1, January 1983.

101. Farkas, T.: Overspeed Issues. Rockwell-Downey, October 1986.

102. Rockwell International Procurement Specification: Auxiliary Power Unit. MC201-0001, Rev. G, Amended March 1986.

103. Rockwell International Procurement Specification. MC271-0880, Rev. D, Amended April 28, 1978.

104. Schematic Diagram - Auxiliary Power Unit Subsystem, Rev. G. VS70-460109, Jan. 27, 1987.

105. Coombe, T.W.; and Vovles, D.F.: Structural Effects of Engine Burst Non-Containment. AGARD Conference Proceedings No. 196, January 1976.

106. Kaplan, S.: The Bayesian Approach to Data Reduction in Probabilistic Risk Analysis, PLG-0207, September 1981.

13.0 PROOF OF CONCEPT STUDY ACRONYMS LIST

AFB	- Air Force Base
Al	- Aluminum
AOA	- Abort-Once-Around
APU	- Auxiliary Power Unit
ARCS	- Aft Reaction Control System (Subsystem)
ASSY	- Assembly
ATCS	- Active Thermal Control Subsystem
ATO	- Abort-To-Orbit
ATP	- Acceptance Test Procedure
ATT	- Attitude
ATVC	- Ascent Thrust Vector Control
AV	- Avionics
BITE	- Built-In Test Equipment
C&W	- Caution and Warning
CAL	- Calibration
CAR	- Corrective Action Reports
CB	- Circuit Breaker
CIL	- Critical Items List
CKO	- Checkout
CKT	- Circuit
CL	- Close (Closed)
cls	- Closes
CMD	- Command, Commander
CNTL	- Control
CNTLR	- Controller
CO	- Carbon Monoxide
CO2	- Carbon Dioxide
C/O	- Checkout
CR	- Confidence Run
CRES	- Corrosion Resistant Steel
CRIT	- Criticality
CRT	- Cathode-Ray Tube
D&C	- Displays and Controls
D	- Demand
D/O	- Deorbit
delta P	- Differential Pressure
DFI	- Development Flight Instrumentation
displ	- Display
DIST	- Distribution
DMD/HR	- Demand per hour
DOD	- Department of Defense
DSC	- Dedicated Signal Conditioner
EGT	- Exhaust Gas Temperature
EI	- Entry Interface (400,000 ft. During Entry)
Elec	- Electrical
ENA	- Enable

ACRONYMS (Continued)

EPDC - Electrical Power Distribution and Control
EPS - Electrical Power System
ESD - Event Sequence Diagram
ET - External Tank, Event Tree
Exh - Exhaust
Exhst - Exhaust
F - Fahrenheit
FA - Flight Aft
FCE - Flight Critical Equipment
FCS - Flight Control System
FDLINE - Feed Line
FDA - Fault Detection and Annunciation
FDF - Flight Data File
FF - Flight Forward
FIV - Fuel Isolation Valve
FLT - Flight
FM - Failure Mode
FMEA - Failure Modes and Effects Analysis
FPL - Full Power Level (Main Engine @ 109% Rated Thrust)
frag. - Fragment
FRCS - Forward Reaction Control System (Subsystem)
FRF - Flight Readiness Firings
FPR - Full Problem Record
FSM - Fuel Supply Module
FSSR - Flight Systems Software Requirements
FSW - Flight Software
ft - Feet
FU - Fuel
FWD - Forward
G - Gravity
GB - Gearbox
Gen - Generator
GFE - Government Furnished Equipment
GG - Gas Generator
GGVM - Gas Generator Valve Module
GN2 - Gaseous Nitrogen
GNC - Guidance, Navigation, and Control
GND - Ground
GO2 - Gaseous Oxygen
GPC - General Purpose Computer
GPM - Gallons per Minute
GSE - Ground Support Equipment
H - Hours
H2 - Hydrogen
H2O - Water
HA - Hazard Analysis

ACRONYMS (Continued)

HDC	- Hybrid Driver Controller
He	- Helium
HEX	- Heat Exchanger
Hg	- Mercury
HPU	- Hydraulic Power Unit
HW	- Hardware
HYD	- Hydraulics
IA	- Intact Abort
IEA	- Integrated Electrcnics Assembly
ID	- Identifier
ID	- Inside Diameter
IFM	- In-Flight Maintenance
INS	- Insertion
IOA	- Independent Orbiter Assessment
ISO	- Isolation
ISOL	- Isolation
JSC	- Johnson Space Center
Kft	- 1000 Feet
KSC	- Kennedy Space Center
L	- Left
LA	- Launch Abort
lb	- pound
L/O	- Lift Off
L/OFF	- Lift Off
LF	- Launch Forward
LH	- Left Hand
LH2	- Liquid Hydrogen
LL	- Launch Left
LO2	- Liquid Oxygen
LOCV	- Loss Of Crew/Vehicle
LOM	- Loss of Mission
LOX	- Liquid Oxygen
LPS	- Launch Processing System
LR	- Launch Right
LRU	- Line Replaceable Unit
LS	- Launch Scrub
LT	- Light
LUBE	- Lubrication, Lubricating
LV	- Loss Of Crew or Vehicle
MAN	- Manual
MANF	- Manifold
MCC	- Mission Control Center (JSC)
MDAC	- McDonnell Douglas Astronautics Company
MDAC-ES	- McDonnell Douglas Astronautics Company-Engineering Services
MDF	- Minimum Duration Flight

ACRONYMS (Continued)

MDM - Multiplexer/Demultiplexer
ME - Main Engine
MECO - Main Engine Cutoff
MET - Mission Elapsed Time
MLD - Master Logic Diagram
MLG - Main Landing Gear
MM - Major Mode
MMH - Monomethyl Hydrazine
MEC - Master Events Controller
MN - Main
MON - Monitor
MPL - Minimum Power Level (Main Engine @ 65% Rated Thrust)
MPS - Main Propulsion System (Subsystem)
MPU - Magnetic Pickup Unit
ms - Millisecond
MSFC - Marshall Space Flight Center
MTR - Motor
MUX - Multiplexer
N2 - Nitrogen
N2H4 - Hydrazine
N2O4 - Nitrogen Tetroxide
N/A - Not Applicable
NA - Not Applicable
NASA - National Aeronautics and Space Administration
NC - Normally Closed
NGTD - Nose Gear Touch Down
NH3 - Ammonia
NLG - Nose Landing Gear
NO - Normally Open, Number
NPRD - Nonelectronic Parts Reliability Data
NRA - Numerical Risk Assessment
NSTS - National Space Transportation System
NW - Nose Wheel
NWS - Nose-Wheel Steering
O2 - Oxygen
OFT - Orbital Flight Test
OI - Operational Instrumentation
OMI - Operational Maintenance Instructions
OMS - Orbital Maneuvering System
OP - Open
Oper - Operation
OPS - Operations Sequence
OXID - Oxidizer
P/L - Payload
PC - Personal Computer, Printed Circuit
Pc - Chamber Pressure

ACRONYMS (Continued)

PF - Payload Forward, Permanent Failure
PI - Principal Investigator
PL - Primary Landing Site Entry
PLB - Payload Bay
PLG - Pickard, Lowe and Garrick, Inc.
PLS - Primary Landing Site
PLT - Pilot
PM - Project Manager
PNL - Panel
POS - Position
PRA - Probabilistic Risk Assessment
PRCS - Primary Reaction Control System (jet)
PREP - Preparation
PRESS - Pressure
Prim - Primary
psi - Pounds per Square Inch
psia - Pounds per Square Inch Absolute
psid - Pounds per Square Inch Differential
psig - Pounds per Square Inch Gage
PWR - Power
QC - Quality Control
QD - Quick Disconnect
QRA - Quantitative Risk Assessment
QUAL - Qualfication Test
R - Right, Roll
RCS - Reaction Control System
Ref. - Reference
REV - Revision
RF - Recoverable Failure
RH - Right Hand
RPC - Remote Power Controller
RPL - Rated Power Level (Main Engine @ 100% Rated Thrust)
RPM - Revolutions Per Minute, Rotations Per Minute
Rt - Right
RTLS - Return to Launch Site
S/N - Serial Number
scfm - Standard Cubic Feet per Minute
SD - Shutdown
S/D - Shutdown
SEC - Secondary
SEP - Separation
SFOM - Shuttle Flight Operations Manual
SFP - Single Failure Point
SIE - Spatial Interaction Event
SPEC - Specification
SR - Stop Roll

ACRONYMS (Concluded)

SR&QA - Safety, Reliability and Quality Assurance
SRB - Solid Rocket Booster
SRM - Solid Rocket Motor
SSM - Subsystem Manager
SSME - Space Shuttle Main Engine
SSSH - Space Shuttle Systems Handbook
STS - Space Transportation System
SW - Switch
SYS - System
T-0 - Time Zero (Also Commonly Used for L/Off)
TAEM - Termianl Area Energy Management
TAL - Transatlantic Abort Landing
TD - Touch Down (Vehicle)
Ti - Titanium
TIG - Time Of Ignition
TK - Tank
TPS - Thermal Protection System
trans. - Transducer
TVC - Thrust Vector Control
uncont. - uncontained
U.S. - United States
USBI - United Space Boosters Inc.
VAX - A computer manufactured by Digital Equipment Corporation
VDC - Volts, dc
VERN - Vernier
VLV - Valve
VRCS - Vernier Reaction Control System (jet)
WONG - Weight on Nose Gear
WOW - Weight on Wheels (Main Landing Gear)
WS - Wheel Stop
WSB - Water Spray Boiler
WUC - Work Unit Code
XDCR - Transducer
Xo - X-Axis of Orbiter
XFR - Transfer
Y - Yaw