PALO VERDE NUCLEAR GENERATING STATION

AUXILIARY FEEDWATER SYSTEM

RELIABILITY ANALYSIS

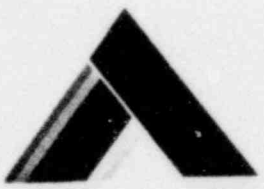


TABLE OF CONTENTS

PALO VERDE NUCLEAR GENERATING STATION

AFS RELIABILITY ANALYSIS

1.0 INTRODUCTION

1.1 Background

The Palo Verde AFS was analyzed considering various design alternatives as a result of the concerns expressed by the NRC. This study considered four different design alternatives. The first one is the current design which consists of one turbine-driven emergency feedwater train, one motor-driven emergency feedwater train, and a manual start non IE AC power motor-driven auxiliary feedwater train. In case 2 the startup auxiliary feedwater pump was given the capability of being powered from the Train A diesel generator by manual start. Case 2A is the same as Case 2 except automatic start is provided. In Case 3, a fourth feedwater pump train was added. This fourth train would be completely safety grade while keeping the manual start, non IE AC power, startup auxiliary feedwater pump. The design features of the four cases are shown on table 1-1.

1.2 Objectives

The objectives of this study are:

- To perform a reliability analysis for comparison of four design alternatives (current design plus three alternates).
- To meet the requirements of the NRC letter of March 10, 1980 (reference 12). The NRC letter requires a reliability analysis of AFS similar to analysis described in NUREG 0635.

1.3 Scope of Study

The Palo Verde AFS present design was analyzed along with three other configurations as described in table 1-1. Simplified functional diagrams of the trains are shown in figures 1-1 and 1-2.

This study goes beyond the analysis in NUREG 0635. Specifically, it includes error bounds on the results, incorporates common cause failures, provides a more conservative treatment of operator error in addition to using more realistic failure rate data in some important cases. However, to permit a comparison on a common basis with NUREG 0635 the analysis then "backs out" the differences and presents the results using the NUREG methodology.

The scope of this study was also limited to one top event also taken from the NUREG which states:

> The time interval of interest for all transient events considered is the unavailability of the auxiliary feedwater system during the period of time to boil the steam generator dry.

The 20-minute boil dry time stated in NUREG 0635 was also used in this study.

The following transient (initiating) events were required by NUREG 0635:

Event A - loss of main feedwater (LMFW) and a reactor trip occur together. LMFW/RT

Event B - The LMFW is coincident with a loss of all offsite (AC) power. LMFW/LOOP

Event C - the LMFW is coincident with a loss of all AC power, LMFW/LOAC, except for any which is derived from batteries.

Table 1-1

DESIGN CASES FOR NUREG-0635 RELIABILITY STUDY

AUXILIARY FEEDWATER SYSTEM

DESIGN CASE	TURBINE DRIVEN EMERGENCY FEEDWATER PUMP TRAINS	MOTOR DRIVEN EMERGENCY FEEDWATER PUMP TRAINS	MANUAL START NORMAL AC PWR MOTOR DRIVEN AUX FEEDWATER PUMP TRAINS	MANUAL START DIESEL CONNECTED MOTOR DRIVEN AUX FEEDWATER PUMP TRAINS	AUTOMATIC START DIESEL CONNECTED MOTOR DRIVEN AUX FEEDWATER PUMP TRAINS
CASE 1 (CURRENT PVNGS DESIGN)	1	1	1	–	–
CASE 2	1	1	–	1	–
CASE 2A	1	1	–	–	1
CASE 3	1	2	1	–	–

1.4 Method of Analysis

The primary basis of this analysis consists of the construction and evaluation of fault trees. For each of the four design cases, minimal cut sets were determined from a fault tree which contained all active components and single-failure passive component(s). Constants for common cause and human factors were also determined. Failure rates and the fault tree methodology were based on references 1 and 2.

For each fault tree, common causes and human factors were studied. The minimal cut sets were generated using the FTAP code of reference 6. Manual comparisons, checks and tests of reasonableness were also applied.

1.5 Criteria and Assumptions

The following analytical criteria, definitions and assumptions have been made:

A. Availability criterion - Given that one of the postulated demand events should occur, unit AFS availability is defined as a successful system startup (at least one train) within boil dry time of 20 minutes. The 20 minute boil dry time was obtained from NUREG 0635.

B. Availability of AFS power sources - The following assumptions are made with respect to the postulated demand events and the resulting mission for AFS success.

   1) LMFW - All AC and DC power available.

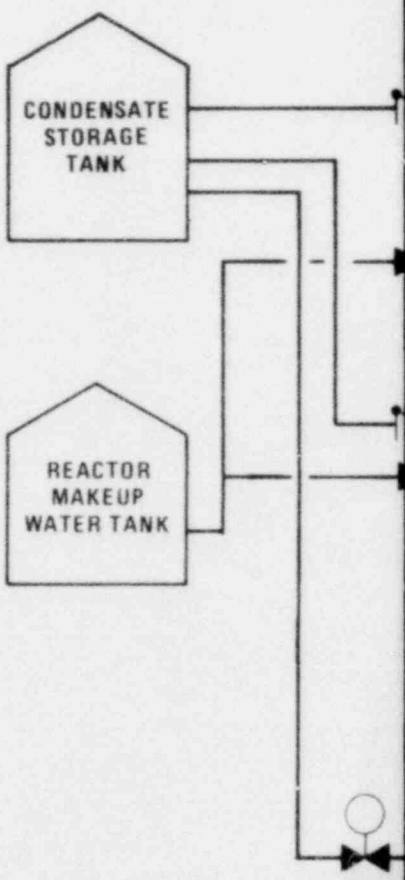
   2) LMFW/LOOP - Two diesel generators available.

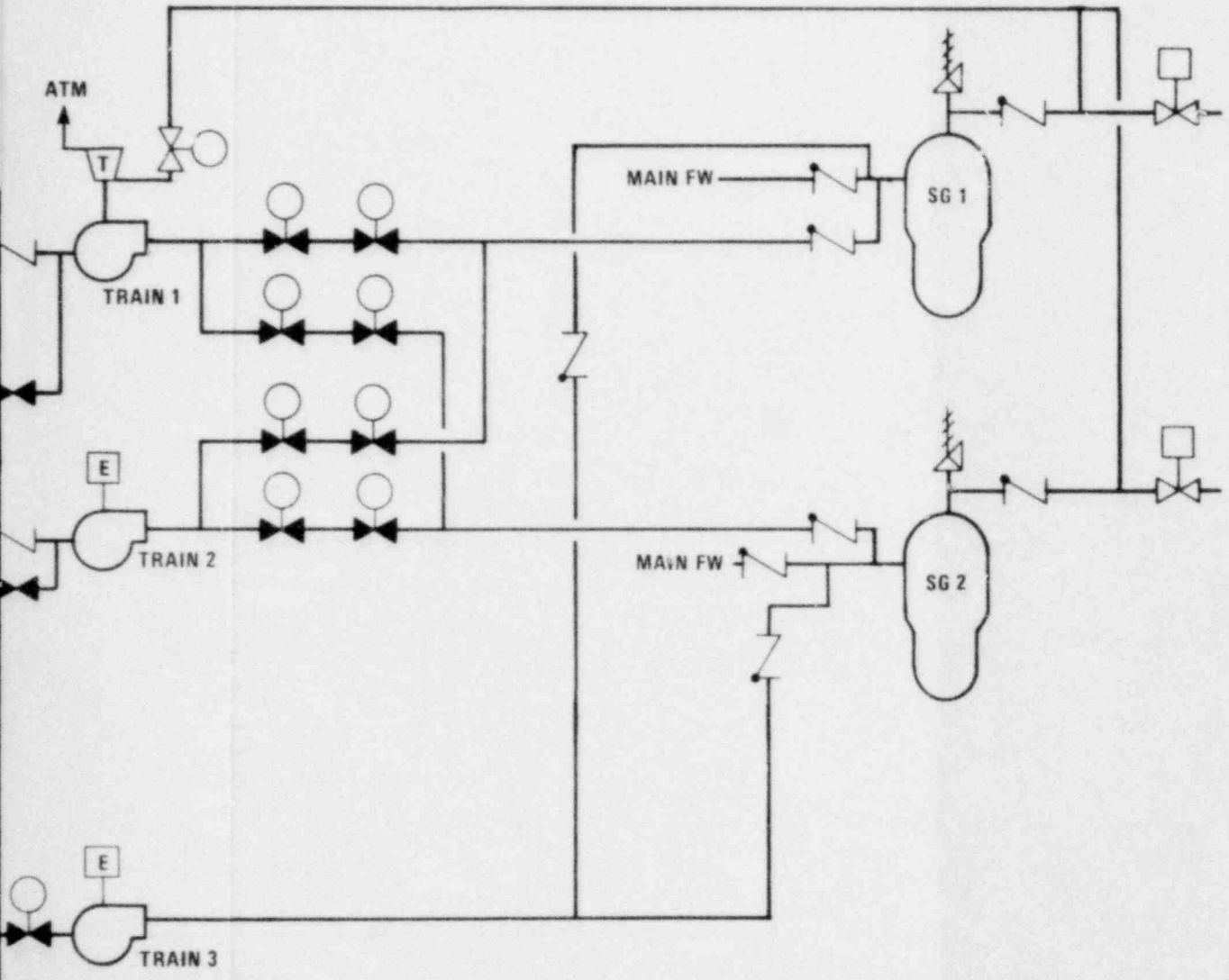
   3) LMFW/LOAC - DC and battery-backed AC available.

C. The failure rate data base used for quantification was taken primarily from NUREG 0635. The need for additional data were met by references 2 and 8. The rationale for data source and application are found in section 4.1.4.

D. Degraded failures - A partially successful performance of any active or passive component was not considered. Each component and each operator action was assumed to be either successful or failed.

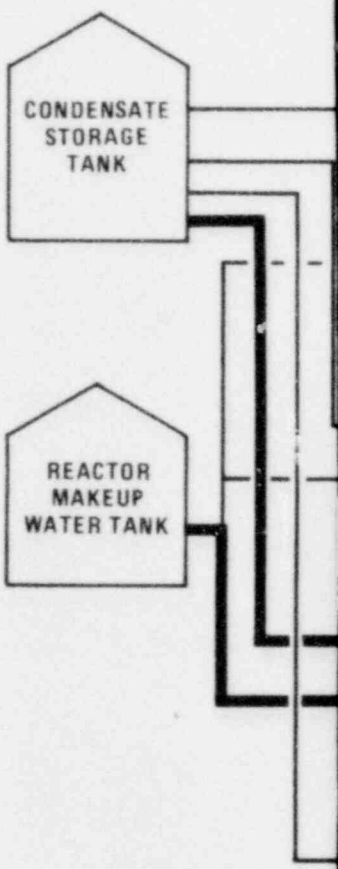
E. AFS actuation and control - For automatic operation during emergency shutdown conditions the Auxiliary Feedwater Actuation Signal (AFAS) will be initiated for either steam generator by a low steam generator level coincident with a steam generator not ruptured signal for that steam generator. The AFAS can be actuated manually.

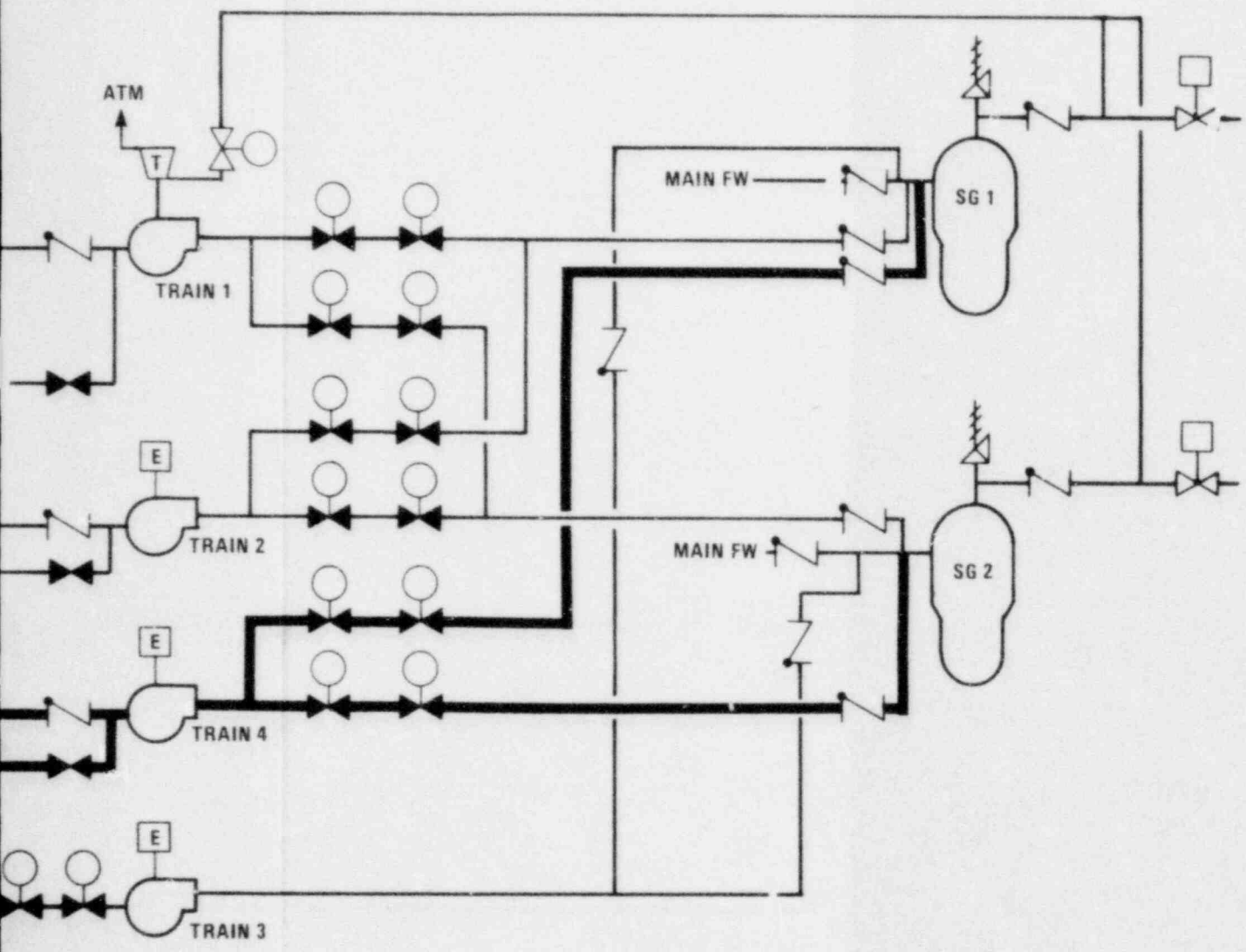

CONDENSATE
STORAGE
TANK
REACTOR
MAKEUP
WATER TANK



PALO VERDE 3 TRAIN AUXILIARY FEEDWATER SYSTEM

Figure 1-1


CONDENSATE
STORAGE
TANK
REACTOR
MAKEUP
WATER TANK



PALO VERDE 4 TRAIN AUXILIARY FEEDWATER SYSTEM

Figure 1-2

2.0 SUMMARY

2.1 Discussion

The two objectives of this study are to compare the reliability of the four design alternatives and to meet the requirements of the NRC letter of March 10, 1980 (reference 12) which cites NUREG 0635.

To make a more meaningful design alternative comparison, the first objective required the treatment of uncertainty and the use of data on steam turbine drives and diesel generators. The details of this approach are found in section 4.1. The results of the analysis are summarized on table 2-1.

The second objective requires an analysis of the AFS according to the requirements of NUREG 0635. The principle aim of the NUREG was to evaluate the variability of auxiliary feedwater system designs rather than evaluating the variability in data to be applied to a specific design.

The first objective went beyond the analyses in NUREG 0635. Specifically, it included error bounds on the results, common cause failures, and a more conservative treatment of operator error in addition to using more realistic failure rate data in some important cases. However, to permit a comparison on a common basis with NUREG 0635 the analysis then "backs out" the differences and presents the results using the NUREG methodology as shown in figures 2-1 and 2-2 and described in section 4.2.1.

2.2 Conclusions

The conclusion of the study is that the reliability of the AFS can be improved (refer to table 2-1) by modifying the

Table 2-1

AFS RELIABILITY ESTIMATE

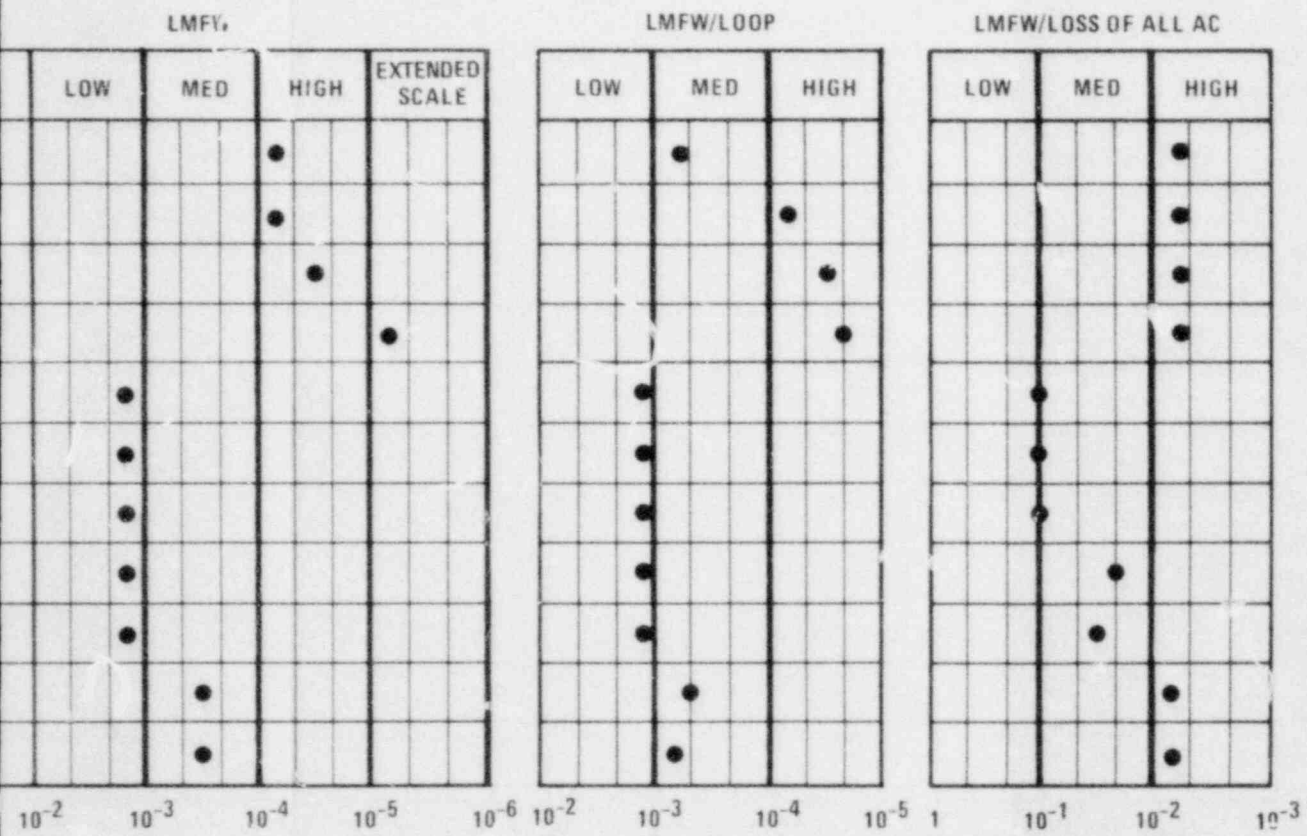
			INDEPEND. – STATISTICAL INDEPENDENT ESTIMATE C.C. – COMMON CAUSE ESTIMATE	UNAVAILABILITY TOTAL	$\overline{A}$ PER YEAR
3/YEAR	TOTAL LOSS OF MAIN FEEDWATER – LMFW	CASE 1	INDEPEND. C.C.	2.0E-4 1.1E-3	6.0E-4 3.3E-3
		CASE 2	INDEPEND. C.C.	2.0E-4 1.1E-3	6.0E-4 3.3E-3
		CASE 2A	INDEPEND. C.C.	1.5E-5 8.7E-4	4.5E-5 2.6E-3
		CASE 3	INDEPEND. C.C.	3.4E-6 8.6E-4	1.0E-5 2.6E-3
.2–.3/YEAR	TOTAL LOSS OF OFFSITE POWER – LOOP	CASE 1	INDEPEND. C.C.	3.5E-3 4.3E-3	8.8E-4 1.1E-3
		CASE 2	INDEPEND. C.C.	6.6E-4 1.6E-3	1.7E-4 4.0E-4
		CASE 2A	INDEPEND. C.C.	2.1E-4 1.1E-3	5.3E-5 2.8E-4
		CASE 3	INDEPEND. C.C.	2.0E-4 1.1E-3	5.0E-5 2.8E-4
$<10^{-3}$/YEAR	AC BLACK OUT	CASE 1	INDEPEND. C.C.	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 2	INDEPEND. C.C.	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 2A	INDEPEND. C.C.	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 3	INDEPEND. C.C.	6.1E-2 6.2E-2	6.1E-5 6.2E-5

design from the present Case 1 to design alternative Case 2. Specific recommendations are as follows:

- Provide the capability to manually supply Train 3 auxiliary feedwater pump from the Train A diesel generator (Case 2).
- Provide position indication in the control room on the pump test bypass valves.
- Provide power to the suction valves for Train 3 auxiliary feedwater pump from the Train A diesel generator.
- Perform a total system test once every 18 months.
- Perform testing on different shifts.

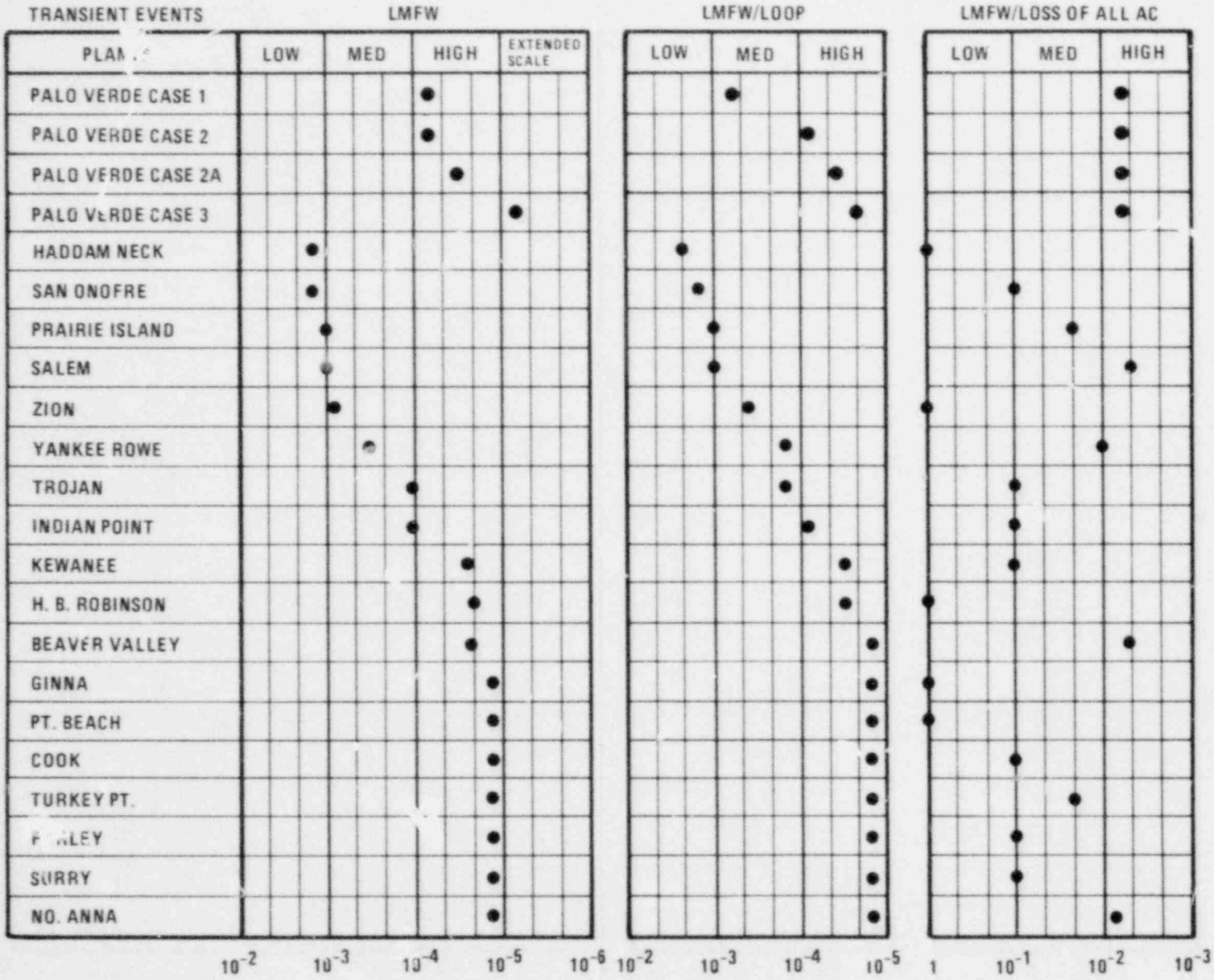
TRANSIENT EVENTS

PLANTS
PALO VERDE CASE 1
PALO VERDE CASE 2
PALO VERDE CASE 2A
PALO VERDE CASE 3
CALVERT CLIFFS
PALISADES
MAINE YANKEE
MILLSTONE
ST. LUCIE
ARK. NUC. NO. 2
FT. CALHOUN



RELIABILITY CHARACTERIZATIONS FOR AFS DESIGNS IN PLANTS USING THE COMBUSTION ENGINEERING NSSS AND PALO VERDE

Figure 2-1



RELIABILITY CHARACTERIZATIONS FOR AFS DESIGNS
IN PLANTS USING THE WESTINGHOUSE NSSS
AND PALO VERDE
Figure 2-2

3.0 SYSTEM DESCRIPTION

3.1 General Description

The AFS consists of one safety-related Seismic Category I motor-driven AFS pump, one safety-related Seismic Category I steam turbine-driven AFS pump, and one non-safety related non-Seismic Category I motor-driven AFS pump, associated piping, controls, and instrumentation. Appendix A contains the piping and instrumentation diagram of the system. The non-safety-related motor-driven pump will accrue the most duty because it is used for startup, hot standby, and normal shutdown operations.

The primary source of auxiliary feedwater is the condensate storage tank. A minimum capacity of 300,000 gallons is required by the AFS; during emergency shutdown conditions 330,000 gallons are provided. This provides an orderly RCS cooldown to the shutdown initiation conditions. The total tank capacity is 550,000 gallons. The secondary or backup source of auxiliary feedwater is the reactor makeup water tank. Its maximum capacity is 480,000 gallons.

The safety-related motor-driven auxiliary feedwater pump and its motor-operated valves can receive Class 1E power from both onsite and offsite power sources. In the event of a loss of offsite power, power is supplied to this motor-driven pump by its standby diesel generator. The loading of the emergency bus is sequential and automatic. The standby diesel generator powers this auxiliary feedwater pump and the necessary valves and controls to ensure system operability.

The turbine-driven AFS pump is supplied with steam from the main steam lines of either steam generator upstream

of the main steam isolation valves. The power and controls for the valves associated with this pump receive power from the Class 1E dc buses A and C.

The two safety-related auxiliary feedwater pumps are separated by a physical barrier. Piping and components are located, separated, or protected to preclude damage from missile and environmental effects.

3.2 System Operation

For emergency operation, normal flow is from the condensate storage tank to both the safety-related motor-driven AFS pump and to the steam turbine-driven AFS pump. An alternative supply of water is provided by local manual cross connections to the reactor makeup water tank.

A minimum flow recirculation system is provided on each pump discharge with recirculation to the condensate storage tank. Each of these pumps can supply either steam generator with feedwater. Condensate recirculation lines are provided downstream of the AFW pump to allow for full flow pump testing.

Either auxiliary feedwater pump can supply the necessary feedwater for reactor decay heat removal and reactor cooldown to 350F.

For normal AFS operation the non-safety-related pump, located in the turbine building, is employed.

One manually operated auxiliary feedwater path to the steam generators is provided for the non-safety-related motor-driven auxiliary feedwater pump through the feedwater header.

At a reactor coolant temperature of 350F, the shutdown cooling system is placed in operation. The AFS duty cycle is then completed and it is returned to standby status.

A minimum flow path is provided for each pump. Approximately 13% of the pump capacity is recirculated back to the condensate storage tank whenever a pump is operating. The minimum flow line is provided to prevent pump overheating in the event the pump discharge line is shut off. If a break is postulated to occur in the recirculation line downstream of the flow restriction orifice, system operation is not affected. The pump still delivers required flow to the steam generators. The water inventory of the condensate storage tank has been calculated to include the possibility of a 13% flow water loss through the recirculation line while maintaining a sufficient quantity of water to provide the required cooling.

One pump motor driver is powered from a separate engineered safety features (ESF) bus which is powered by the Train B diesel generator. The steam turbine-driven pump's associated valving is powered from the battery-backed essential dc bus A and C. The turbine for this pump is supplied with steam from either of the steam generators. The turbine controls are also powered from the dc bus A.

Auxiliary feedwater control is normally from the control room, but instrumentation is provided for operation from the remote shutdown station in the unlikely event that the control room must be evacuated.

Signals from the auxiliary feedwater actuation signal (AFAS) (automatic/manual) start the safety-related motor-driven auxiliary feedwater pump and the steam turbine-driven auxiliary feedwater pump, shut all isolation valves, and open the associated isolation valves to the downcomer nozzles of the intact steam generator(s). The non-safety-related motor-driven pump is started manually and its associated valves are opened manually from the control room.

3.3 Inspection and Testing Requirements

The AFS pumps are capable of being tested while the plant is in normal operation. A recirculation and full flow test line to the condensate storage tank enables the pumps to be operationally tested. Control room discharge pressure and local flow indicators are provided to monitor pump performance.

Containment isolation valves can be tested during normal plant operation. However, by technical specification, these valves will be tested during refueling shutdown.

3.4 Instrumentation and Control

Control room instrumentation includes steam generator level controls and hand switches plus position indicators for all power operated valves.

Control logic for the AFS is a manually overridable automatic two-of-four input signal system, part of the Engineered Safety Features Actuation System (ESFAS). Steam generator pressure and water level are the monitored variables for automatic protective action.

The following main control room monitors are provided for purposes of AFS control:

- System trip status light.
- Discharge pressure of each AFS pump.
- Auxiliary feedwater flow to each steam generator.
- Two status lights for each regulator valve.
- RPM of the turbine (pump-driving).
- Status lights for all motor operated-remote manual valves.

The AFAS performs the following functions as intended by design:

A. Start the safety-related, motor-driven auxiliary feedwater pump whenever an AFAS occurs for either steam generator.

B. Open the steam supply valving to start the steam turbine driver whenever an AFAS occurs for either steam generator.

C. Determine whether a steam generator is intact in the event of a secondary system break.

D. Open the auxiliary feedwater regulating valves to the intact steam generator using the trip channel logic. The same logic is used to provide a closing signal to the auxiliary feedwater valves to a non-intact steam generator to prevent flow to that generator.

E. Close the steam generator blowdown line isolation valves whenever an AFAS occurs for either steam generator.

F. Prevent a high water level condition in the intact steam generator(s) by closing the auxiliary feedwater regulating valves when the level is reestablished above the low level trip setpoint. The valve logic is not latched in the actuated state in order that this control can be accomplished. When the level and pressure conditions for valve opening are again met, the valves are automatically reopened.

G. Start the diesel generators whenever an AFAS occurs for either steam generator.

H. An AFAS aligns tne AFS regulating and isolation valves to feed the intact steam generator(s). Once the steam generator level is restored, the pumps continue to operate, but the regulating and isolation valves close. The valves continue to cycle with steam generator level fluctuation. The steam generator level should be stabilized to avoid undue cycling of the regulating valves.

The system is designed such that loss of electric power to two of the four like channels in the measurement channels, or initiating logic, or to the selective two-out-of-four actuating logic would actuate the auxiliary feedwater system.

Manual control of the auxiliary feedwater system is provided by means of hand controllers on the main control panel. The operator may override the automatic system under all operating and accident conditions by controlling the AFS regulating valves from the main control room.

Manual control of the safety-related portion of the auxiliary feedwater is also provided, from a remote shutdown station external to the control room should the control room become inaccessible. The safety-related, motor-driven auxiliary feedwater pump can be controlled from its appropriate switchgear. The steam turbine-driven pump can be controlled locally.

3.5 Supporting Systems and Sources

The active components of the AFS are dependent upon diverse sources of electrical power. Lube oil and cooling subsystems are supplied from the same source as the primary component. All valves and controls in the same train are similarly matched to the same power source as its pump, and key devices can be manually or locally

actuated as well. Four independent transmission lines supply the offsite power, and two dedicated diesel generators back up the onsite Class 1E power busses.

There is a backup water supply source at the reactor makeup water tank. Up to 480,000 gallons of demineralized water can be made available to the AFS suction cross-tie by means of hand valve V019 of the chemical and volume control system, then through 8-inch pipings to the safety-related motor-driven pump and to the turbine driven pump.

3.6 Technical Specification Limitations

Technical Specifications require the availability of 300,000 gallons of water in the condensate storage tank for AFS use. Tank volumes below 530,000 gallons, 330,000 gallons and 20,000 gallons are alarmed and annunciated in the main control room.

A maximum of 72 hours out of service is allowed for maintenance or repair of a safety-related pump while the reactor is critical. If that time is exceeded the reactor must be put in hot shutdown within the next 12 hours.

Surveillance Requirements (CESSAR Chapter 16):

1) Each emergency feedwater pump shall be demonstrated operable:

   A. At least once per 30 days by:

      (1) Verifying turbine driven pump develops discharge pressure of $\geq$1260 psig at flow of $\geq$987 GPM when the secondary steam supply pressure is greater than 1035 psig.

      (2) Verifying each valve (manual, power operated or automatic) in the flow path that is not locked, sealed, or otherwise secured in position, is in correct position.

B. At least once per 18 months during shutdown by:

(1) Verifying each automatic valve in the flow path actuates to its correct position on MSIS and EFAS test signals.

(2) Verifying motor driven pump starts automatically upon receipt of an EFAS test signal.

2) The condensate storage tank shall be demonstrated operable at least once per 12 hours by verifying the contained water volume is within its limits when the tank is the supply source for the emergency feedwater pumps.

3) The applicable alternative service water system (reactor makeup water tank is the alternate for PVNGS) shall be demonstrated operable at least once per 12 hours by verifying that at least one service water loop is operating and that the service water system - emergency feedwater system isolation valves are either open or operable whenever the service water system is the supply source for the emergency feedwater pumps.

4.0 RELIABILITY EVALUATION

4.1 Analytical Approach

The primary basis of this analysis consists of the construction and evaluation of fault trees. For each of the four design cases, minimal cut sets were determined from a fault tree which contained all active components and single-failure passive component(s). Constants for common cause and human factors were also determined. Failure rates and the fault tree methodology were based on references 1 and 2.

For each fault tree, the common causes and human factor causes were studied. The minimal cut sets were generated using the FTAP code of Reference 6. Manual comparisons, checks and tests of reasonableness were also applied.

The basic tasks (see figure 4-1) required for the analysis are:

Task 1 - Analysis Inputs

Task 2 - Fault Tree Development

Task 3 - Generation of Minimal Cut Sets

Task 4 - Statistically Independent Hardware, Test and Maintenance and Human Error Quantification

Task 5 - Common Cause Hardware, Test and Maintenance and Human Error Analysis

Task 6 - Propagation of Uncertainty

Task 1 consists primarily of gathering information required to establish the boundary conditions (initiating events, top events, system boundary, and surveillance requirements, for example) needed to carry out the analysis. This includes the time necessary to study and become familiar with the system.

Task 2 differs from Task 1 in that the information obtained is then translated graphically into the master fault tree of appendix C.

Task 3 is the first step in analyzing the fault tree. In this task, all of the combination of component failures are generated. These various combinations of component failures which cause system failure are known as minimal cut sets. In this study the minimal cut sets were generated by a computer code (reference 6).

Task 4 employs the minimal cut sets of Task 3 and the data of appendix H to determine the statistical independent unavailabilities of each design alternative.

In Task 5 common cause analysis was performed both qualitatively and quantitatively, qualitatively to identify potential sources of common cause failures and quantitatively to indicate the limited effect that increased redundancy can have on the reliability of a system.

Task 6 propagated the uncertainty of the input data to the overall results. The uncertainty range between design alternatives can effect the decision making process and thus was considered.

These calculations are then combined into one overall unavailability number (table 4-1) accompanied by figures 4-5, 4-6 and 4-7 which graphically show the effect of uncertainty.

4.1.1 Task 1 - Analysis Inputs

Task one consisted primarily of gathering the necessary information required to establish boundary conditions for the analysis and to become familiar with the system. The information required was obtained from CESSAR Chapter 16, the PVNGS FSAR and NUREG 0635.

Chapter 16 of CESSAR was used to establish Technical Specification (surveillance requirements, see Section 3.6) from which the unavailability of the AFS due to testing was calculated (Reference 1). All pumps were conservatively assumed to be tested once per month although it was only required for the turbine pump. The PVNGS FSAR was primarily used for system description and operating requirements.

NUREG 0635 was used to establish the top event of the master fault tree, the initiating events/event trees and as the basic guide for the analysis. The top event is taken from NUREG 0635 which states:

> The time interval of interest for all transient events considered is the unavailability of the auxiliary feedwater system during the period of time to boil the steam generator dry.

The 20 minute boil dry time stated in NUREG 0635 was also assumed for this study.

System familiarization was accomplished by:

- Reviewing Piping and Instrumentation Drawings (P&ID's - see appendix A), system descriptions and technical specifications.
- Developing Reliability Block Diagrams (figure 4-2 and appendix B). A simplified system functional diagram was also developed (see figures 1-1 and 1-2).
- Seeking clarification with cognizant engineers.

4.1.2 Task 2 - Fault Tree Development

A master fault tree was constructed from the P&ID's. (See appendix C.) This tree is for the most complex design alternative, namely, Case 3. For the less complex alternatives, the non-applicable portions were assumed not to

exist. This tree includes all the "active" components and the "passive" single failure components. The master fault tree was used for the hardware/operator error unavailability of the AFS.

Fault trees for the test and maintenance and human error unavailability were also constructed and are included in appendix D and E. Various portions of the master tree are incorporated in these fault trees.

All the above fault tree models were developed assuming statistical independence for hardware/operator failures, human error and test and maintenance failures as the simplified fault tree of figure 4-3 illustrates. A description of how common cause failures are treated is found in section 4.1.5.

4.1.3 Task 3 - Generation of Minimal Cut Sets

Minimal cuts sets were generated for this study by the Fault Tree Analysis Program (FTAP) developed at the Lawrence Livermore Laboratory (reference 6). A sample minimal cut set is found in appendix G. The quantification and integration of the minimal cuts sets into the master fault tree is developed in the next section.

4.1.4 Task 4 - Statistically Independent Hardware, Test and Maintenance and Human Error Quantification

The failure rate data base used for the quantification of the fault trees is given in appendix H. The preferred source of data was NUREG 0635. In some cases, failure rates for such components as diesel generators were not given in NUREG 0635. In these cases, Appendices III and IV of WASH 1400 (reference 2) were used. There was no failure rate information available for Steam Turbine

driven pumps (STDP) from either of the above sources so the LER information on STDP's of reference 8 was used. All failure rates were treated on a demand basis for the unavailability calculations. This is due to the boil dry time constraint.

The failure rate information in the above references are given as median values which associated error factors. This information was converted to means and variances which are necessary to propagate uncertainty through the model. These means and variances are based on the log-normal distribution as described on page II-43, Appendix II of reference 2.

With the data above, the dominant minimal cut sets were manually identified and quantified (see appendix I). The highest failure rate sets were selected and quantified to estimate the failure probabilities or the unavailabilities.

A check on the manual calculations was performed by the "Importance" computer code which is an adjunct to FTAP (reference 7).

For the hardware/operator error unavailability estimate, the master fault tree was used as applicable for the various cases and initiating events. The minimal cut sets were generated by FTAP, the dominate minimal cut sets were manually calculated, and the sum of the dominant minimal cut set values is the unavailability of that branch of the tree.

For the test and maintenance and human error unavailability, the master fault tree was used as applicable. This result was incorporated into the test/maintenance and human error fault tree to calculate respective unavailabilities (see appendix I).

4.1.4.1 Single Failures

Since the AFS availability is defined as a success system start up within an assumed boil dry time of 20 minutes, no local manual operation was assumed possible. Due to this assumption, the condensate tank and the pipings and valves connected to this tank has a potential to be "passive" single failure points if any of these components were to have a severe leak or rupture.

If the loss of condensate storage tank were to occur during plant operation, level alarms, one normal low level and two low low level, are in the control room to alert the operator of the problem. An automatic condensate storage tank fill system (demineralizer water system - non Class 1E) will provide 125,000 gallons of water at a rate of 250 gal/min. The reactor makeup water tank (480,000 gallons) can be local manually transferred to the AFS and local manually valving off the condensate tank water source. The tank, pipes, and valves rupture failure rates was estimated to be 4.7E-7/h (reference 2). Individual instrumentation failure rate was assumed to be 2.7E-6/h. Operator error with no duress was assessed at 1.2E-4/h. Thus, the failure probability, assuming 1 hour duration, is less than 10^{-16} (the product of the above failure rates, since they all must fail).

If the loss of condensate storage tank water were to occur simultaneously with the-AFS start and assuming a single rupture failure, a 10-inch diameter offset rupture area, the normal storage tank capacity of 530,000 gallons will provide adequate water for more than 85 minutes, during this time, the reactor make up tank water can be local manually transferred to the AFS pumps. The greatest single rupture failure rate was assessed to be 3.3E-7/h. Utilizing the same rationale as before, the failure probability will again be in the order of 10^{-16}.

4.1.5 Task 5 - Common Cause Hardware, Test and Maintenance and Human Error Analysis

Common cause analysis was performed both qualitatively and quantitatively. Qualitatively to identify potential sources of common cause failures and quantitatively to indicate the limited effect that increased redundancy can have on the reliability of a system.

Qualitative Analysis - The identification of common or similar hardware, test, maintenance, human actions or physical links between redundant trains was the first step in this analysis. An example of this type of classification is shown on figure 4-4. Definitions and terms used in figure 4-4 are found in appendix F. The basic approach details are found in reference 4.

An in-house computer code was developed to indicate the number and type of commonalities that exist between components of the various redundant trains. The dominant minimal cut set components were compared with this listing since the remainder of the minimal cut sets had less commonality. The greater the commonality, the greater the potential for common cause may exist. There are 25 possible categories of commonality but the maximum number of common categories found were 6. All sets of components with 5 or 6 commonalities were selected (there were 52) and these sets were compared to the minimal cut sets. No serious potential for common cause were found using this approach.

As a final qualitative check, the potential for common cause failures as discussed in reference 5 were reviewed and are addressed below. Reference 5, Table 5-2, listed seven "common cause" failures that occurred in 1975 AFS

experience. These failures are discussed below as to the effect if they were to occur in the Palo Verde AFS:

A. Operator failed to open the valve from the condensate storage tank to the two AFWS pumps. The two AFWS pump loops failed to be available on demand as required by technical specifications. Docket 50-317-516.

   This failure indicates that a "single" valve provided condensate to the two AFWS pumps. This indicates to be a "single" failure point. The Palo Verde AFS has separate supply lines and valves to each of the AFS pumps. Thus, a single valve closure will not cause AFS failure. Only a true common cause failure, multiple redundant inadvertant valve closure, will cause an AFS failure in the Palo Verde design.

B. Filters (in parallel) on suction side of three pumps plugged up with foreign material which restricted flow. Docket 50-305-354.

   Palo Verde AFS pumps have startup suction filters. Train 1 and 2 pumps have full flow test capabilities that will detect any restricted flow.

C. Condensate storage tank water level was intentionally drawn down below technical specification limits to maintain maximum steam generator blowdown. Failure to maintain water supply to multiple AFWS pumps within specifications. Docket 50-315-340.

   Palo Verde condensate storage tank maintain a maximum of 550,000 gallons and, when the volume decreases to 530,000 gallons, an automatic refill system can provide 125,000 gallons at a rate of 250 gal/min. The AFS requirement is 330,000 gal. In addition, the reactor makeup water tank with a maximum capacity of 480,000 gal can be local manually transferred to the AFS.

D. Condensate storage tank water level was intentionally drawn down below technical specification limits because makeup water supply was dirty (high oxygen content). Failure to maintain water supply to multiple AFWS pumps within specifications. Docket 50-247-449.

The Palo Verde condensate storage tank nitrogen blanket is maintained at about 2 psig. This system is to prevent re-entrainment of oxygen which is removed by the makeup demineralizer degasifier, thus this problem should not exist or is greatly reduced in the Palo Verde design.

E. Two AFWS pumps failed to start because of defective control switches which failed to close contacts. Docket 50-305-350.

This could happen in the Palo Verde AFS, however, since train 1 pump is a turbine drive and the train 2 pump is an electric drive, the control switches will most likely be different, thus tends to be [illegible] independent failures as opposed to a common cause failure. The common switches/breakers will be in the Auxiliary Feedwater Actuation Signal (AFAS) system.

F. A breaker accidentally opened and interrupted power to the turbine overspeed protection (which tripped the reactor), and also interrupted power to an AFWS lube oil pump preventing start of the related AFWS pump. Docket 50-305-361.

The Palo Verde AFS lube oil pump is a direct mechanical drive off of the turbine driven feed pump. Thus this should have no effect on the Palo Verde AFS.

G. Two AFWS valves were upgraded during the licensing process and were not seismically qualified because of oversight. Docket 50-289-491.

All safety related valves on the Palo Verde AFS are seismically qualified.

Quantitative Analysis - The method of reference 13 was used to quantitatively estimate the effect of common cause failures. This approach is known as the β-factor method. Simply stated, the β-factor method assumes that a fraction of the operationally independent failure probabilities (Q) of one loop of a redundant system will result in the loss of all redundant loops in that system. The analysis below uses a β-factor of $\beta = 2.7 \times 10^{-2}$. This β-factor is a mean value based on an assumed range of 10^{-1} to 10^{-3}. Again, the log normal distribution is assumed. The mean and range allows the β-factor to be included in the uncertainty calculations.

The common cause failure probability, Q_{cc}, for a redundant system can be approximated by the failure probability of one loop of a redundant system, Q_{loop}, times β added to the independent failures.

In general, the β-factor approach to common cause failure estimates shows its greatest impact on system reliability for highly redundant and simultaneous operating systems, to the extent that more than a single-failure-proof redundancy is generally not warranted if β-factor common cause methodology is assumed.

For this analysis, the following assumptions were made:

1. The cross-over MOV's, check valves, DC/vital instrument buses, AFAS (auxiliary feedwater automatic start) signal, electric pump end buses, operator error, and the diesel generators were identical or similar and thus subject to the common cause β-factor.
2. The turbine drive and electric drive pumps were diverse and not subject to the common cause β-factor.

3. The inter-train common cause failures were considered.

The common cause failure probability contributions to the AFS were calculated and added to the independent failure probabilities. The results are shown in table 4-1.

Table 4-1

AFS RELIABILITY ESTIMATE

				FAILURE PROBABILITY (UNAVAILABILITY)				$\bar{A}$ PER YEAR
INDEPEND. – STATISTICAL INDEPENDENT ESTIMATE C.C. – COMMON CAUSE ESTIMATE				OP. ERROR HARDWARE	TEST & MAINT.	HUMAN ERROR	TOTAL	
3/YEAR	TOTAL LOSS OF MAIN FEEDWATER – LMFW	CASE 1	INDEPEND. C.C.	3.7E-5 1.5E-4	3.7E-5 4.0E-5	1.3E-4 8.7E-4	2.0E-4 1.1E-3	6.0E-4 3.3E-3
		CASE 2	INDEPEND. C.C.	3.7E-5 1.5E-4	3.7E-5 4.0E-5	1.3E-4 8.7E-4	2.0E-4 1.1E-3	6.0E-4 3.3E-3
		CASE 2A	INDEPEND. C.C.	1.1E-6 1.1E-4	3.0E-6 6.1E-6	1.1E-5 7.5E-4	1.5E-5 8.7E-4	4.5E-5 2.6E-3
		CASE 3	INDEPEND. C.C.	8.1E-7 1.1E-4	5.6E-7 4.5E-6	2.0E-6 7.5E-4	3.4E-6 8.6E-4	1.0E-5 2.6E-3
.2–.3/YEAR	TOTAL LOSS OF OFFSITE POWER – LOOP	CASE 1	INDEPEND. C.C.	1.1E-3 1.2E-3	5.3E-4 5.3E-4	1.9E-3 2.0E-3	3.5E-3 4.3E-3	8.8E-4 1.1E-3
		CASE 2	INDEPEND. C.C.	2.6E-4 4.0E-4	8.8E-5 1.0E-4	3.1E-4 1.1E-3	6.6E-4 1.6E-3	1.7E-4 4.0E-4
		CASE 2A	INDEPEND. C.C.	6.7E-5 2.1E-4	3.3E-5 4.4E-5	1.1E-4 8.9E-4	2.1E-4 1.1E-3	5.3E-5 2.8E-4
		CASE 3	INDEPEND. C.C.	5.1E-5 1.9E-4	3.3E-5 4.6E-5	1.2E-4 8.9E-4	2.0E-4 1.1E-3	5.0E-5 2.8E-4
$<10^{-3}$/YEAR	AC BLACK OUT	CASE 1	INDEPEND. C.C.	2.4E-2 2.4E-2	8.1E-3 8.1E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 2	INDEPEND. C.C.	2.4E-2 2.4E-2	8.1E-3 8.1E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 2A	INDEPEND. C.C.	2.4E-2 2.4E-2	8.1E-3 8.1E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 3	INDEPEND. C.C.	2.4E-2 2.4E-2	8.3E-3 8.3E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5

Hardware Estim es for common cause β-factor calculation

$10^{-3} < \beta < 10^{-1}$ β (mean) = 2.7E-2

Single t. n: crossover and check valves

(2x1.2E-3 + 1.2E-4)(2.7E-2) = 6.8E-5

More than one train:

Crossover and Check Valves
(2x1.2E-3 + 3x1.2E-4)(2.7E-2) = 7.45E-5

D/C Vital buses
(1.2E-3)(2.7E-2) = 3.24E-5

} 1.128E-4 Turb/Elec Train Redundancy

AFAS
(2.2E-4)(2.7E-2) = 5.9E-6

Elec. Pump and buses
(1.2E-3 + 1.2E-3)(2.7E-2) = 6.48E-5

} 1.776E-4 Elec Train Redundancy

D/G
(4E-2)(2.7E-2) = 1.08E-3

} 1.257E-3 Elec Train/DG Redundancy

DG/Elec Pump and Turb. Pump
D/G Elec Pump β factor Turb. Pump
(4E-2 + 2.4E-3) (2.7E-2) (2E-2) = 2.3E-5

DG/Elec Pump and Turb. Pump
and balance = 2.3E-5 + 1.13E-4 = 1.36E-4

Elec Pump and Turb. Pump
(6.5E-5)(2E-2) = 1.3E-6

	Hardware/Operator Error Failure Probability Estimates			
	Case	CC	Indep.	Σ
LOMF	1	1.1E-4	3.7E-5	1.5E-4
	2	1.1E-4	3.7E-5	1.5E-4
	2A	1.1E-4	1.1E-6	1.1E-4
	3	1.1E-4	8.1E-7	1.1E-4
LOOP	1	1.1E-4	1.1E-3	1.2E-3
	2	1.4E-4	2.6E-4	4.0E-4
	2A	1.4E-4	6.7E-5	2.1E-4
	3	1.4E-4	5.1E-5	1.9E-4
AC Black-out	1	6.8E-5	2.4E-2	2.4E-2
	2	6.8E-5	2.4E-2	2.4E-2
	2A	6.8E-5	2.4E-2	2.4E-2
	3	6.8E-5	2.4E-2	2.4E-2

The above results show the common cause and independent contributions to the hardware/operator error failure probability estimates utilizing the common cause factors.

Similarly, the hardware/operator error common cause and independent contributions to the test and maintenance and human error fault tree models were estimated and incorporated into the various branches. Only in the human error fault tree model, a common cause between the all branch seemed feasible, thus another common cause β-factor was included (see appendix I).

4.1.6 Task 6 - Propagation of Uncertainty

There are two objectives for this study; a reliability comparison of four design alternatives and to provide an analysis to meet the requirements of the NRC letter dated March 10, 1980 (reference 12). Reference 12 cites NUREG 0635.

The principle aim of NUREG 0635 was to evaluate the variability of auxiliary feedwater system designs rather than evaluating variability in data to be applied to a specific design. Thus propagation of uncertainty is not a requirement of NUREG 0635.

Since propagation of uncertainty can affect the decision making process among design alternatives, it was considered in this study.

Propagation of uncertainty requires that all median data points based on the log normal distribution be converted to mean values according to the equations of page II-43, Appendix II of reference 2. The converted values (means) are shown on table H-1 of Appendix H.

The equations used to calculate the means and variances of item failure data are:

$$f(\lambda;\mu,\sigma) = \frac{1}{\sqrt{2\pi}\,\sigma\lambda} \exp - \left[\frac{(\ln \lambda - \mu)^2}{2\sigma^2}\right]$$

$$\lambda_{.50} = e^{\mu}$$

$$\lambda_{.95} = e^{\mu} + 1.645\,\sigma$$

$$\lambda_{.05} = e^{\mu} - 1.645\,\sigma$$

$$\text{Mean } (\alpha) = e^{\mu + \frac{\sigma^2}{2}}$$

$$\text{Var. } (\beta^2) = \alpha^2 \left[e^{\sigma^2} - 1\right]$$

$$\sigma^2 = \ln\left[\frac{\beta^2}{\alpha^2} + 1\right]$$

$$\mu = \ln \alpha - \frac{\sigma^2}{2}$$

where:

λ = item failure rate

μ,σ = parameters of the log normal distribution

Calculations of Means and Variances of Dominant Minimal Cut Sets are accomplished by using the following equations (from reference 11).

2nd order Minimal Cut Set

$$\text{Mean } (\alpha)_2 = \alpha_1\alpha_2$$

$$\text{Var } (\beta^2)_2 = \alpha_1^2\,\beta_2^2 + \alpha_2^2\,\beta_1^2 + \beta_1^2\,\beta_2^2$$

3rd order Minimal Cut Set

$$\text{Mean } (\alpha)_3 = \alpha_1 \alpha_2 \alpha_3$$

$$\text{Var } (\beta^2)_3 = \alpha_1^2\, \alpha_2^2\, \beta_3^2 + \left(\alpha_3^2 + \beta_3^2\right)\left(\alpha_1^2\, \beta_2^2 + \alpha_2^2\, \beta_1^2 + \beta_1^2\, \beta_2^2\right)$$

Care was taken to ensure that all 2nd order and higher dominant minimal cut set distributions were statistically independent from one another. This was accomplished by identifying all minimal cut sets of a given branch of the tree which had one or more items in common. The common items were then re-factored and stated in an independent form before calculating the uncertainty.

If, for example, two minimal cut sets were:

#1 (A, B)

#2 (A, C)

Then the distribution for A is shared by cut sets #1 and #2 thus are not independent.

This problem can be circumvented by rearranging as follows:

$U = A \cdot B + A \cdot C$

$= A\ (B + C)$

and then applying the rules for combination of means and variances.

4.2 Results and Conclusions

4.2.1 Presentation of Results

The results of the analysis are presented in three forms. The first contains all calculated results in tabular form (table 4-2) without the effects of uncertainty. The far right hand column shows unavailability as a function of each initiating event. The "Total" column are the results given that the initiating event has occurred. The common cause numbers shown on the table include the effects of independent failures. All the failure probabilities are mean log normal values.

Figures 4-5, 4-6, and 4-7 are graphical comparisons of the "Total" column of table 4.1. In these figures the effect of uncertainty is shown as well as the mean and median values.

Figures 4-8 and 4-9 are the results of the analysis shown on the NUREG 0635 format. The following steps are required to convert the preceding results to the NUREG 0635 format:

1. All pumps must have the same failure rate.
2. Mean values must be converted to median values.
3. Both diesel generators are considered available in the event of LMFW/Loop.
4. A less conservative approach to operator error.
5. Include the effect of dominant common causes.

In step 1 instead of using a mean turbine pump failure to start frequencies of 2×10^{-2} and a mean motor driven pump failure to start frequencies of 1.2×10^{-3}, a median value of 10^{-3} was used for all pumps.

Table 4-2

AFS RELIABILITY ESTIMATE

				FAILURE PROBABILITY (UNAVAILABILITY)				$\bar{A}$ PER YEAR
INDEPEND. – STATISTICAL INDEPENDENT ESTIMATE C.G. – COMMON CAUSE ESTIMATE				OP. ERROR HARDWARE	TEST & MAINT.	HUMAN ERROR	TOTAL	
3/YEAR	TOTAL LOSS OF MAIN FEEDWATER – LMFW	CASE 1	INDEPEND.	3.7E-5	3.7E-5	1.3E-4	2.0E-4	6.0E-4
			C.C.	1.5E-4	4.0E-5	8.7E-4	1.1E-3	3.3E-3
		CASE 2	INDEPEND.	3.7E-5	3.7E-5	1.3E-4	2.0E-4	6.0E-4
			C.C.	1.5E-4	4.0E-5	8.7E-4	1.1E-3	3.3E-3
		CASE 2A	INDEPEND.	1.1E-6	3.0E-6	1.1E-5	1.5E-5	4.5E-5
			C.C.	1.1E-4	6.1E-6	7.5E-4	8.7E-4	2.6E-3
		CASE 3	INDEPEND.	8.1E-7	5.6E-7	2.0E-6	3.4E-6	1.0E-5
			C.C.	1.1E-4	4.5E-6	7.5E-4	8.6E-4	2.6E-3
.2–.3/YEAR	TOTAL LOSS OF OFFSITE POWER – LOOP	CASE 1	INDEPEND.	1.1E-3	5.3E-4	1.9E-3	3.5E-3	8.8E-4
			C.C.	1.2E-3	5.3E-4	2.6E-3	4.3E-3	1.1E-3
		CASE 2	INDEPEND.	2.6E-4	8.8E-5	3.1E-4	6.6E-4	1.7E-4
			C.C.	4.0E-4	1.0E-4	1.1E-3	1.6E-3	4.0E-4
		CASE 2A	INDEPEND.	6.7E-5	3.3E-5	1.1E-4	2.1E-4	5.3E-5
			C.C.	2.1E-4	4.4E-5	8.9E-4	1.1E-3	2.8E-4
		CASE 3	INDEPEND.	5.1E-5	3.3E-5	1.2E-4	2.0E-4	5.0E-5
			C.C.	1.9E-4	4.6E-5	8.9E-4	1.1E-3	2.8E-4
$<10^{-3}$/YEAR	A C BLACK OUT	CASE 1	INDEPEND.	2.4E-2	8.1E-3	2.9E-2	6.1E-2	6.1E-5
			C.C.	2.4E-2	8.1E-3	3.0E-2	6.2E-2	6.2E-5
		CASE 2	INDEPEND.	2.4E-2	8.1E-3	2.9E-2	6.1E-2	6.1E-5
			C.C.	2.4E-2	8.1E-3	3.0E-2	6.2E-2	6.2E-5
		CASE 2A	INDEPEND.	2.4E-2	8.1E-3	2.9E-2	6.1E-2	6.1E-5
			C.C.	2.4E-2	8.1E-3	3.0E-2	6.2E-2	6.2E-5
		CASE 3	INDEPEND.	2.4E-2	8.3E-3	2.9E-2	6.1E-2	6.1E-5
			C.C.	2.4E-2	8.3E-3	3.0E-2	6.2E-2	6.2E-5

Step 2 relates to step 1 in that all mean failure rate values listed in table 4-1 must be converted to median values to be consistent with NUREG 0635.

In both of the above steps, component specific failure rates and mean values (needed to propagate uncertainty) were used to make a more meaningful comparison of the four design alternatives. Although this is beyond the requirements of NUREG 0635, it was deemed necessary to prevent the possibility of introducing errors. This is not inconsistent since the principle aim of the NUREG was to evaluate the variability of auxiliary feedwater system designs now operating rather than evaluating the variability in data to be applied to a specific design or design alternatives.

Step 3 required the assumption that the dedicated diesel generators were available on loss of offsite power, although NUREG 0635 assumed one diesel generator was always available. The assumption that the dedicated diesel generators were available was necessary in order to show the effect of three train configurations on reliability.

Step 4 required that one operator error in the Master Fault Tree of Appendix C replace three operator errors, A04, A05 and A06. Although there were nine operator errors in the fault tree, only the above three appear in the dominant minimal cut sets. The effect on the results due to the use of one operator error will be small due to the redundancy in the system.

Steps 4 and 5 are not purely quantitative, thus, engineering judgement enters into the consideration of the effect on unavailability. For instance the potential of Case 2A for safety and operational control systems interaction reduces the difference between Cases 2 and 2A as would a less

conservative approach to the consideration of the human factor involved in activating train 3 in Case 2. Under these conditions it is not unreasonable to expect Cases 2 and 2A to be closer in terms of unavailability.

4.2.2 Discussion of Results

4.2.2.1 Dominant Failure Modes

The analysis indicated that the greatest unavailability was due to human error. The human error was inadvertently leaving the pump recirculation valve open after a test and inadvertently leaving the pump discharge locked open manual valve closed after maintenance on the pump. These valves are not provided with position indicators in the control room. The locked-open pump discharge maintenance valve will not be tested or checked with pump operations after pump maintenance. The estimated human error failure probability for this was assessed at 2.7E-2 per demand. By tech specs, the pump recirc valve will be opened for pump testing - once a month per train. All pumps were assumed to be tested monthly. The data source indicates that the failure rate of valves with position indicators in the control room is assessed at about 1/2 order less than the valves without position indicators.

The AFS pump discharge valves, both the check and locked open manual valves, V015 & V016 and V024 & V025, do not indicate to be flow tested in any of the surveillance requirement. A pressure indicator is provided downstream of these valves, but this does not fully assure that these valves are or will fully open.

The two check valves, V079 and V080, which go to the feedwater headers to the steam generators, again do not indicate to be checked or tested in any of the surveillance requirements. The technical specification states that pump tests

shall be performed monthly and the crossover valves be tested at least once in 18 months, but no explicit total system testing is stated. These check and locked-open manual valves can only be tested during a total system test. Thus, it is recommended that total system test be required at least once every 18 months.

4.2.3 Conclusions

The conclusions of the study are as follows:

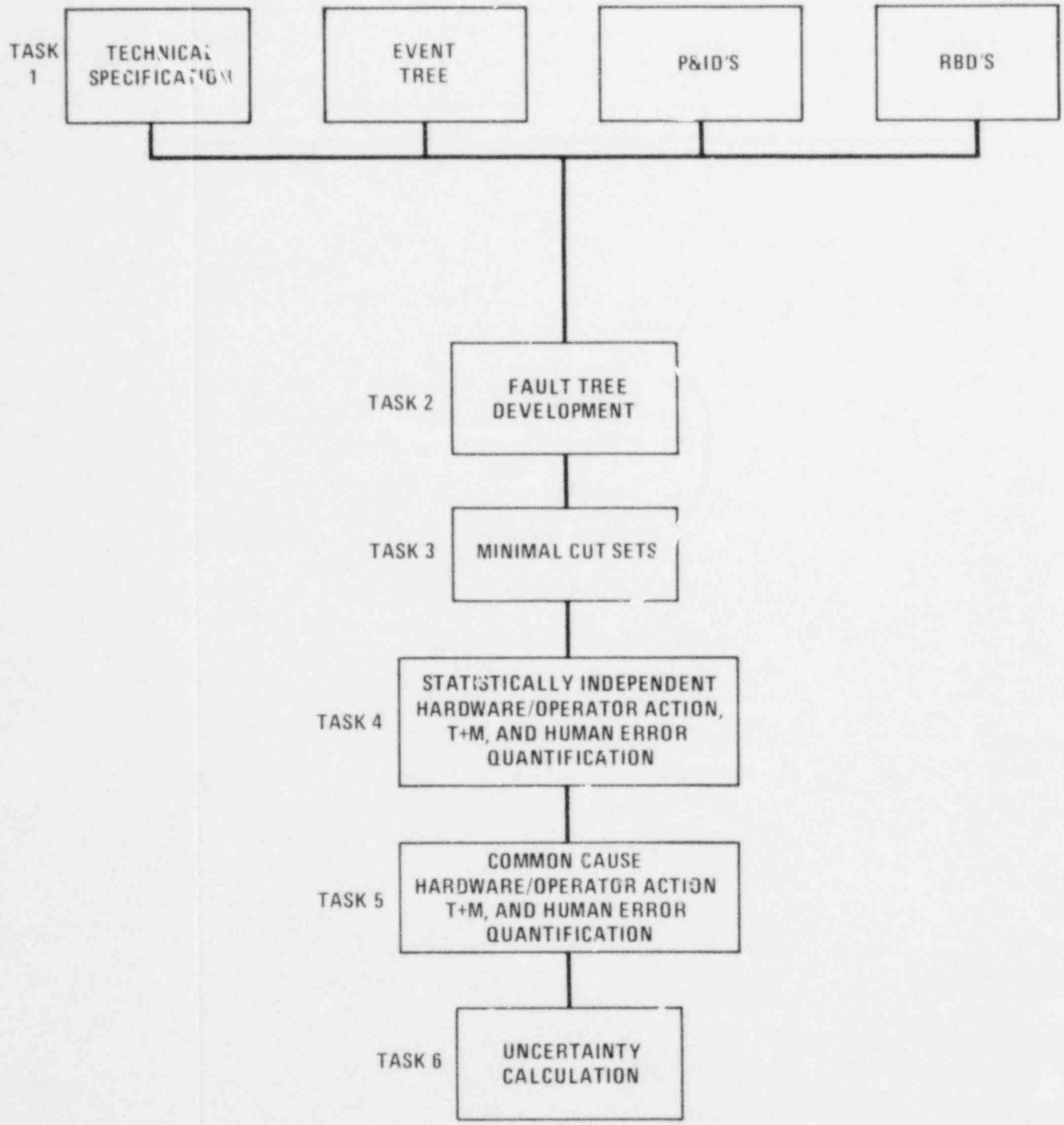
A. Provide the capability to supply train 3 auxiliary feedwater pump from the train A diesel generator (Case 2).

B. Provide position indication in the control room on the pump test by-pass valves.

C. Provide power to the suction valves for train 3 auxiliary feedwater pump from the train A diesel generator.

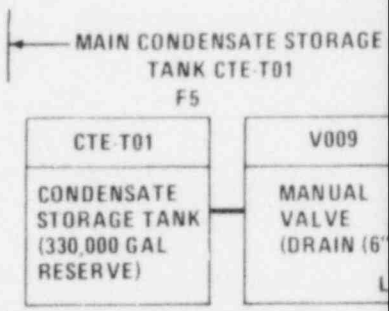
D. Perform a total system test once every 18 months.

E. Perform testing on different shifts.

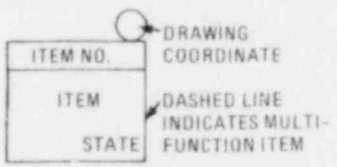


AFS RELIABILITY TASKS

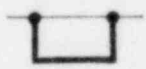
Figure 4-1

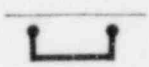


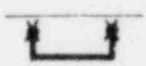
LEGEND:

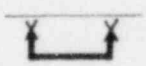


REDUNDANCY TYPE


ACTIVE


AUTOMATIC STANDBY


REMOTE MANUAL STANDBY

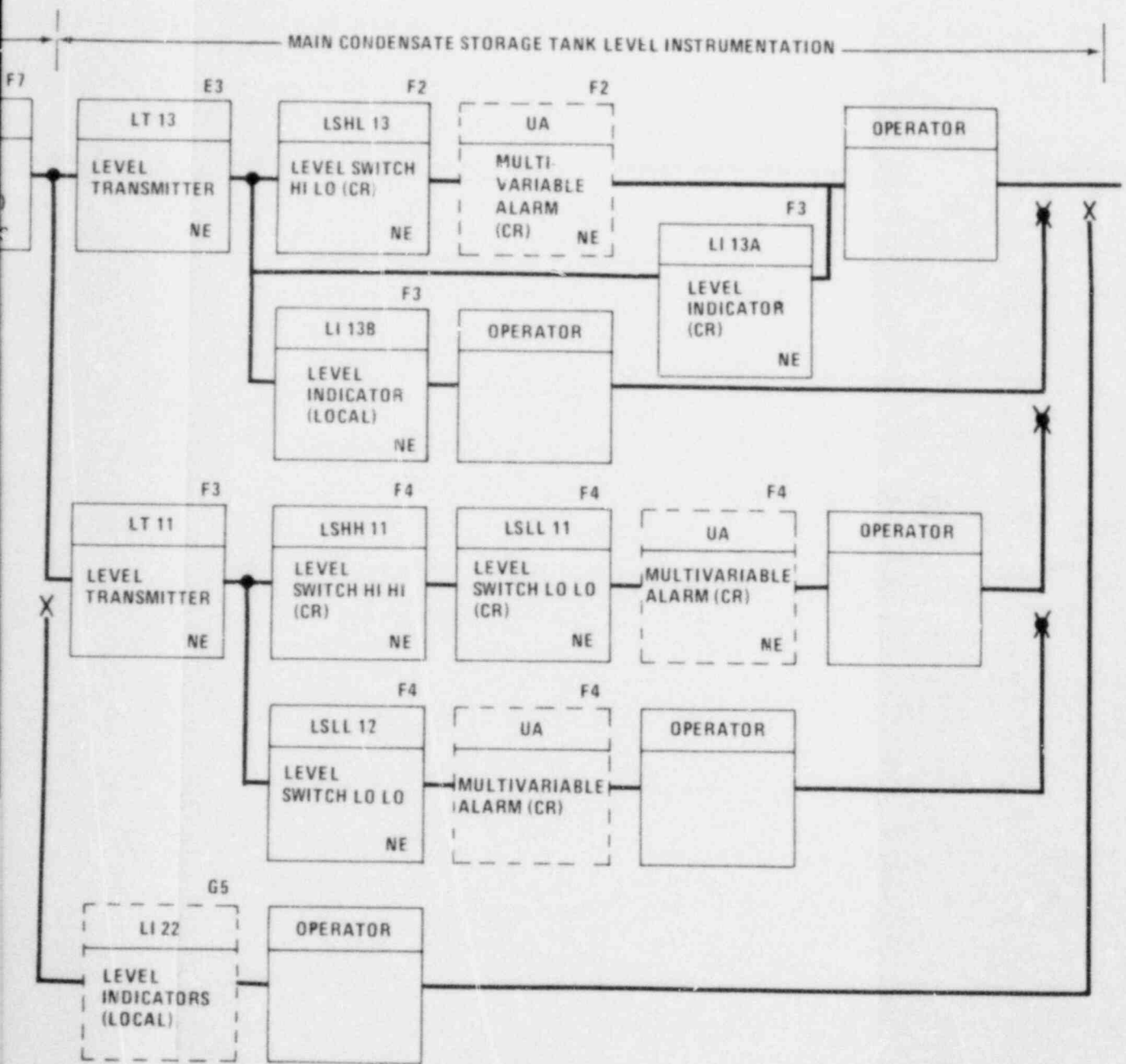

LOCAL MANUAL STANDBY

STATE (PLANT AT POWER):

NO – NORMALLY OPEN
NC – NORMALLY CLOSED
LO – LOCKED OPEN
LC – LOCKED CLOSED
ND – NORMALLY DE-ENERGIZED
NE – NORMALLY ENERGIZED

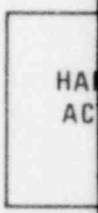
ITEM:

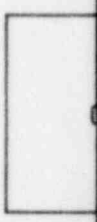
EOV – ELECTRIC OPERATED VALVE
AOV – AIR OPERATED VALVE
CR – CONTROL ROOM
RS – REMOTE SHUTDOWN

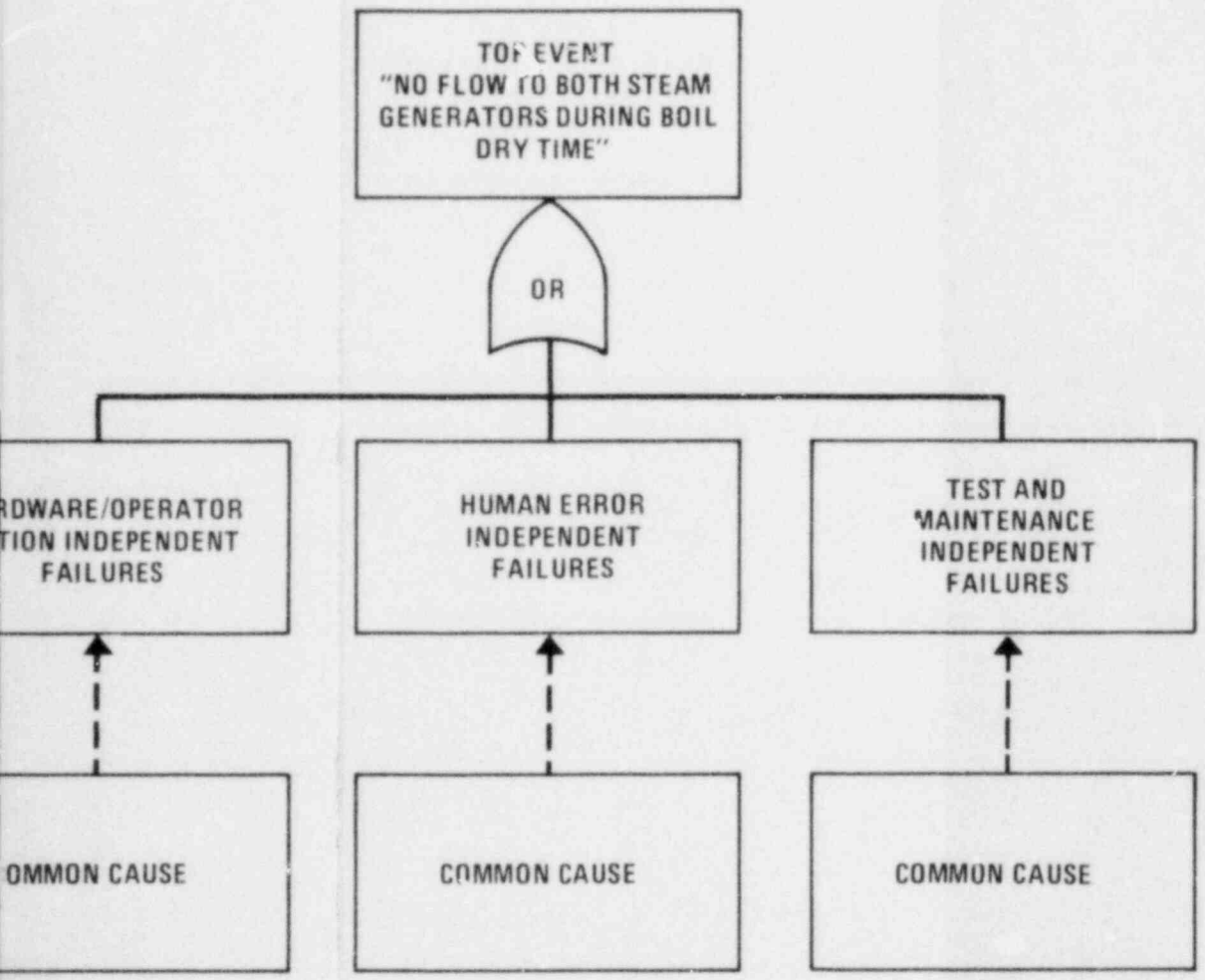


DNG 13-M-CTP-001 REV 2 (PVNGS)

Figure 4-2


HA
AC





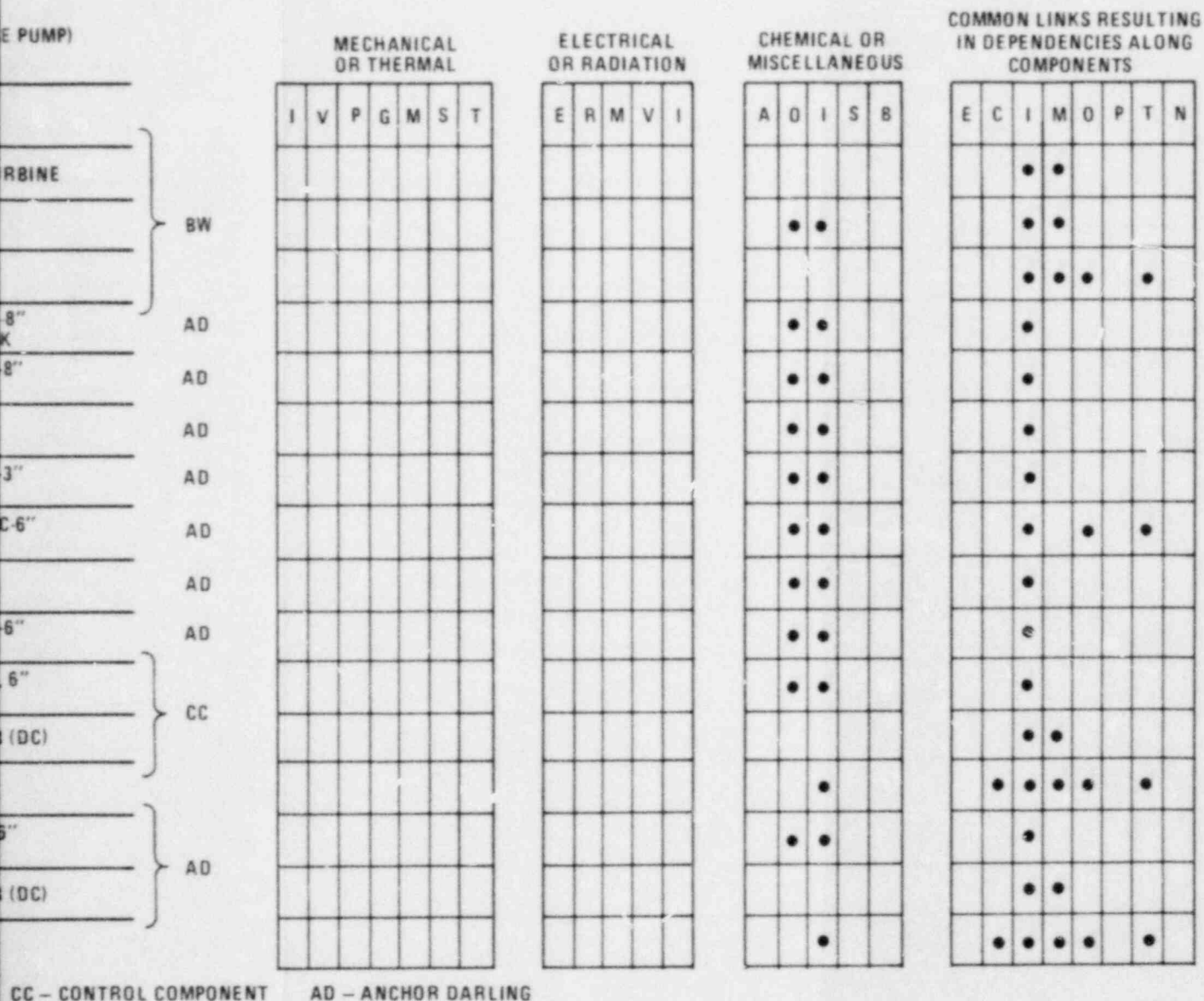
TASK 2

Figure 4-3

TRAIN 1 (TURBINE DRIV

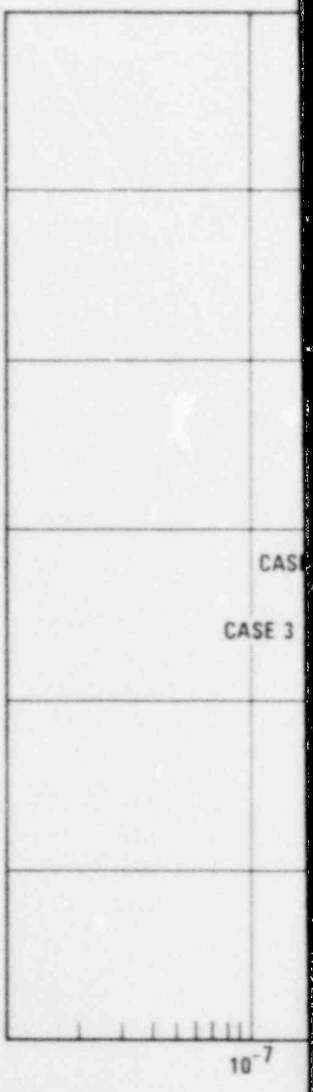
	COMPONENT
AFPAD	DRIVER-STEAM TU
AFPAP	PUMP
AFPAC	PUMP CONTROL
V015	MANUAL GATE-LO CONDENSATE TAN
V006	MANUAL GATE-LO PUMP INLET
V007	CHECK-NC-8" PUMP INLET
V017	MANUAL GATE-LO PUMP RECIRC
V018	MANUAL GLOBE-N TEST
V015	CHECK-NC-6" PUMP DISCHARGE
V016	MANUAL GATE-LO PUMP DISCHARGE
HV32	VALVE GLOBE, NC AFW TO SGI
HV32D	VALVE ACTUATOR
HV32C	VALVE CONTROL
UV36	VALVE GATE, NC, AFW TO SGI
UV36D	VALVE ACTUATOR
UV36C	VALVE CONTROL

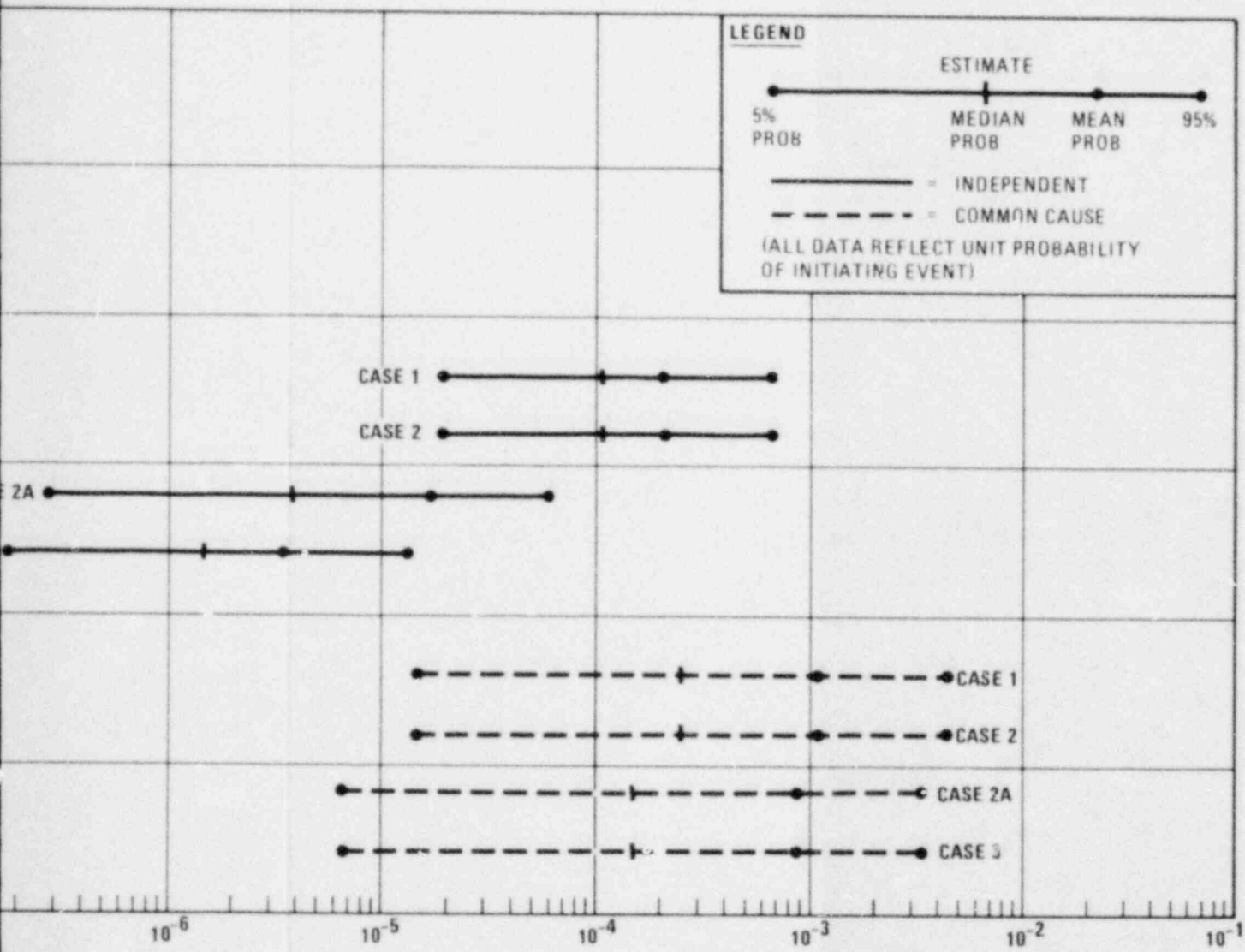
BW – BINGHAM WILLAMET



COMMON CAUSE GENERIC CAUSES – MOST SIGNIFICANT AUXILIARY FEEDWATER SYSTEM

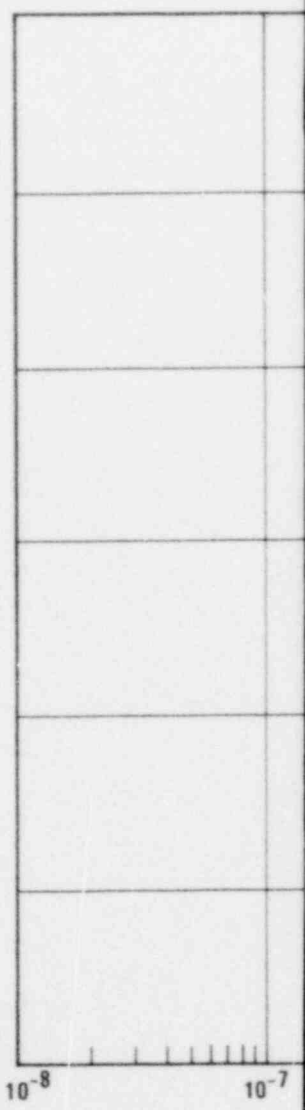
Figure 4-4

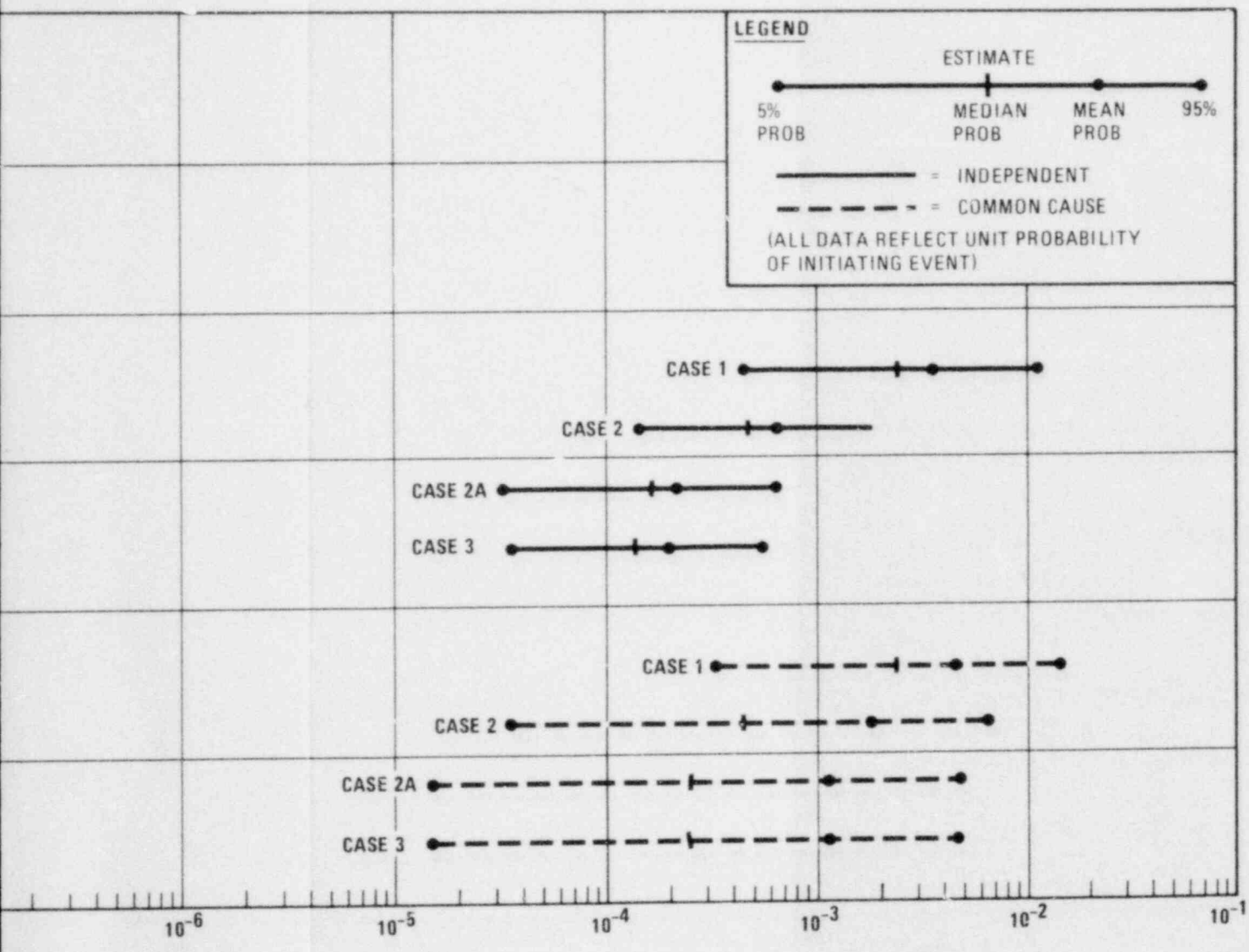

CAS
CASE 3
10^{-7}



FAILURE PROBABILITY LMFW

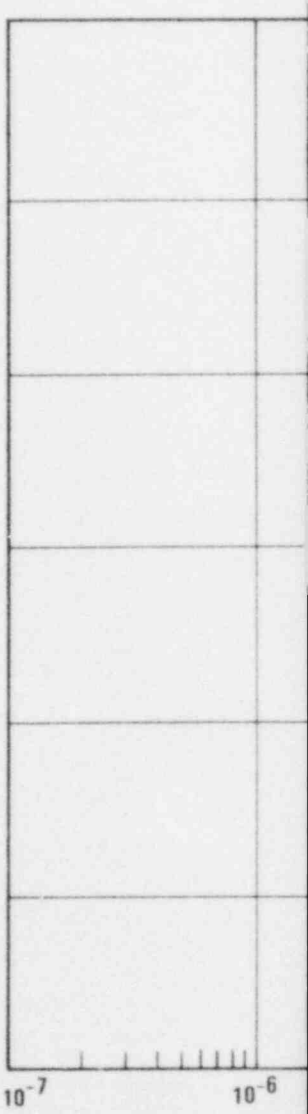
Figure 4-5

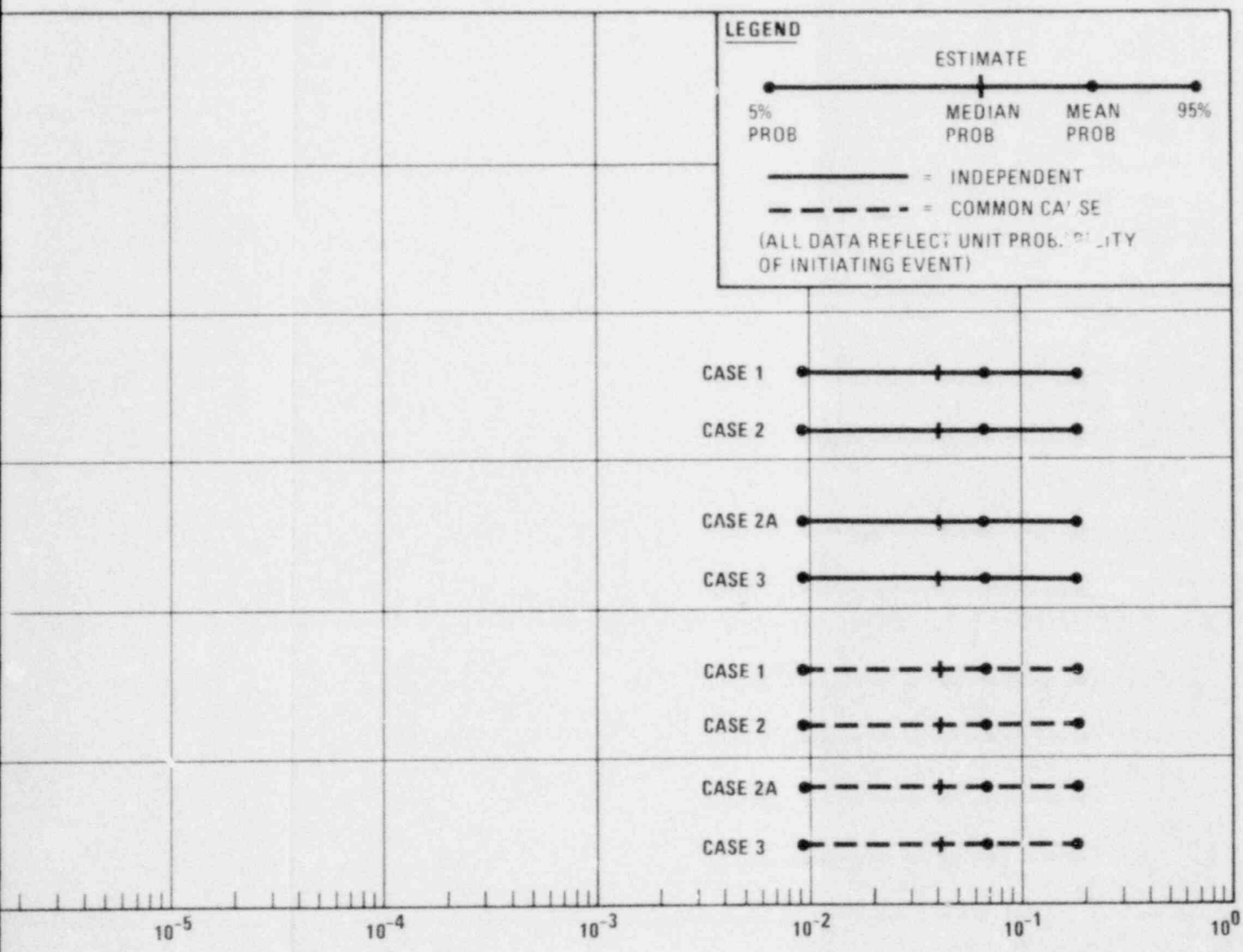

10^{-8}
10^{-7}



FAILURE PROBABILITY LMFW/LOOP

Figure 4-6


10^{-7}
10^{-6}

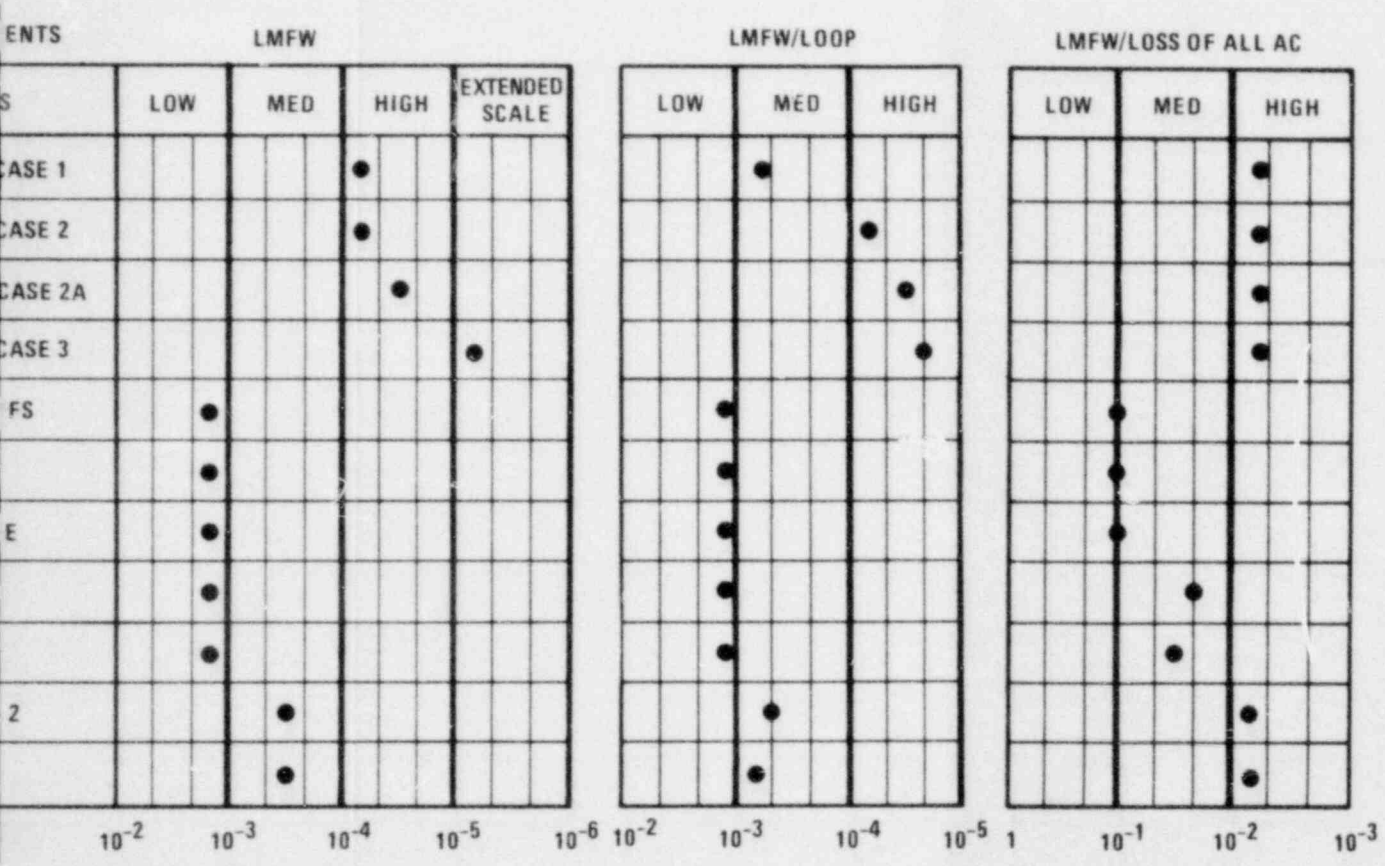


FAILURE PROBABILITY LMFW/LOAC

Figure 4-7

TRANSIENT EV

PLANT
PALO VERDE
PALO VERDE
PALO VERDE
PALO VERDE
CALVERT CLI
PALISADES
MAINE YANKE
MILLSTONE
ST. LUCIE
ARK. NUC. NO
FT. CALHOUN

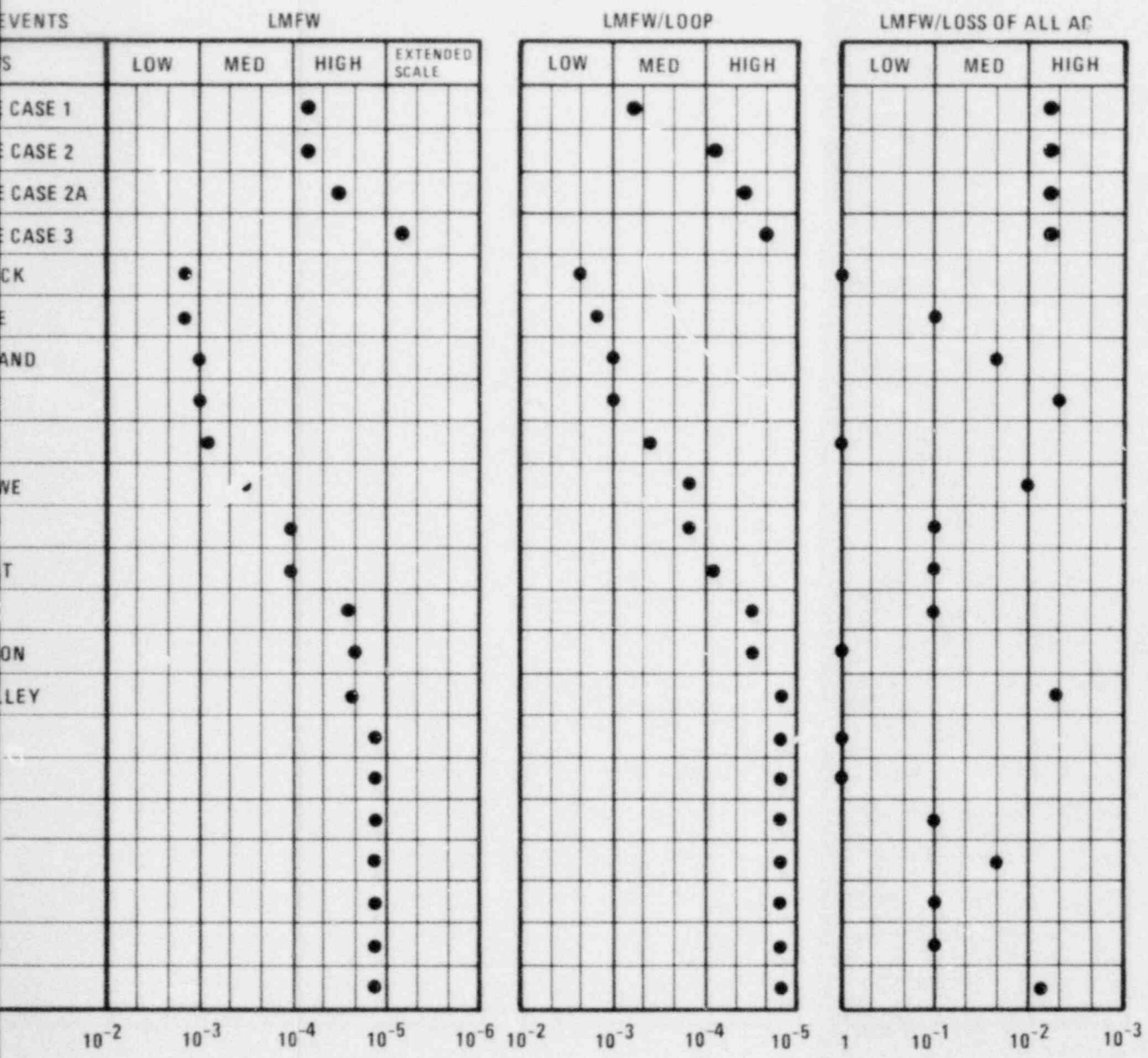


RELIABILITY CHARACTERIZATIONS FOR AFS DESIGNS IN PLANTS USING THE COMBUSTION ENGINEERING NSSS AND PALO VERDE

Figure 4-8

TRANSIENT

PLANT
PALO VERD
PALO VERD
PALO VERD
PALO VERD
HADDAM NE
SAN ONOFR
PRAIRIE ISL
SALEM
ZION
YANKEE RO
TROJAN
INDIAN POIN
KEWANEE
H. B. ROBINS
BEAVER VA
GINNA
PT. BEACH
COOK
TURKEY PT.
FARLEY
SURRY
NO. ANNA



RELIABILITY CHARACTERIZATIONS FOR AFS DESIGNS IN PLANTS AND USING THE WESTINGHOUSE NSSS AND PALO VERDE

Figure 4-9

5.0 REFERENCES

1. NUREG-0635 "Generic Evaluation of Feedwater Transients and Small Break Loss of Coolant Accidents in Combustion Engineering Designed Operating Plants".
2. WASH-1400 (NUREG-75/014) Reactor Safety Study an Assessment of Accident Risks in U.S. Commercial Nuclear Plants.
3. NUREG-0572 Review of Licensee Event Reports (1976-1978).
4. COMCAN II - "A Computer Program for Common Cause Failure Analysis" (Tree-1298) by D. M. Rasmuson, et al., of EG&G Idaho, Inc. September 1978.
5. Common Cause Failure Experience in Nuclear Plant Auxiliary Feedwater Systems for Reliability Analysis (WARD-SR-3045-4) Topical Report by G. E. Edison of Westinghouse Advanced Reactors Division for D.O.E.
6. Computer Aided Fault Tree Analysis (FTAP) by R. R. Willie of Operations Research Center University of California Berkeley OC 78-14 August 1978. Available through Dr. H. Lambert University of California, Berkeley.
7. Importance Computer Code by H. E. Lambert and F. M. Gilman. Available through H. Lambert University of California, Berkeley.
8. A Study of Steam Turbine Driven Pump LER's - September 1978. Prepared by Bechtel Power Corporation.
9. NUREG-75/087 Standard Review Plan for Auxiliary Feedwater Systems.

10. ANPP System Description titled "Auxiliary Feedwater", Rev. 1 November 1979, prepared by Bechtel Power Corporation.

11. Probability Intervals for the Top Event Unavailability of Fault Tree by Y. T. Lee and G. E. Apostolakis UCLA Report Number UCLA-ENG-7663, June 1976.

12. NRC Letter of March 10, 1980.

TO ALL PENDING OPERATING LICENSE APPLICANTS OF NUCLEAR STEAM SUPPLY SYSTEMS DESIGNED BY WESTINGHOUSE AND COMBUSTION ENGINEERING

SUBJECT: ACTIONS REQUIRED FROM OPERATING LICENSE APPLICANTS OF NUCLEAR STEAM SUPPLY SYSTEMS DESIGNED BY WESTINGHOUSE AND COMBUSTION ENGINEERING RESULTING FROM THE NRC BULLETINS AND ORDERS TASK FORCE REVIEW REGARDING THE THREE MILE ISLAND UNIT 2 ACCIDENT

13. "A Reliability Model for Common Mode Failure in Redundant Safety Systems", K. N. Fleming General Atomics Report No. GA-A13284 April 18, 1975.

APPENDIX A

PVNGS AUXILIARY FEEDWATER SYSTEM PIPING AND INSTRUMENTATION DRAWINGS

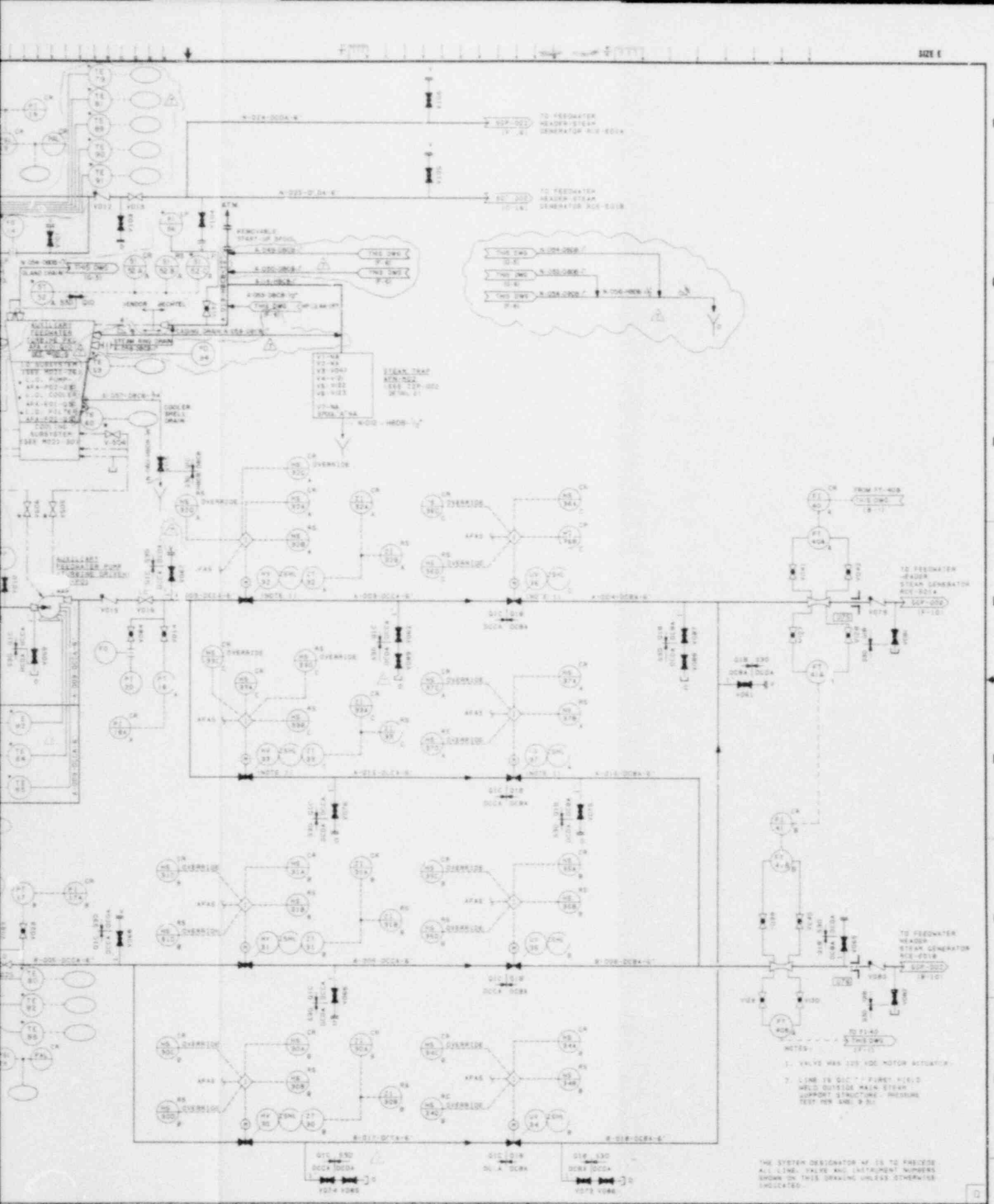
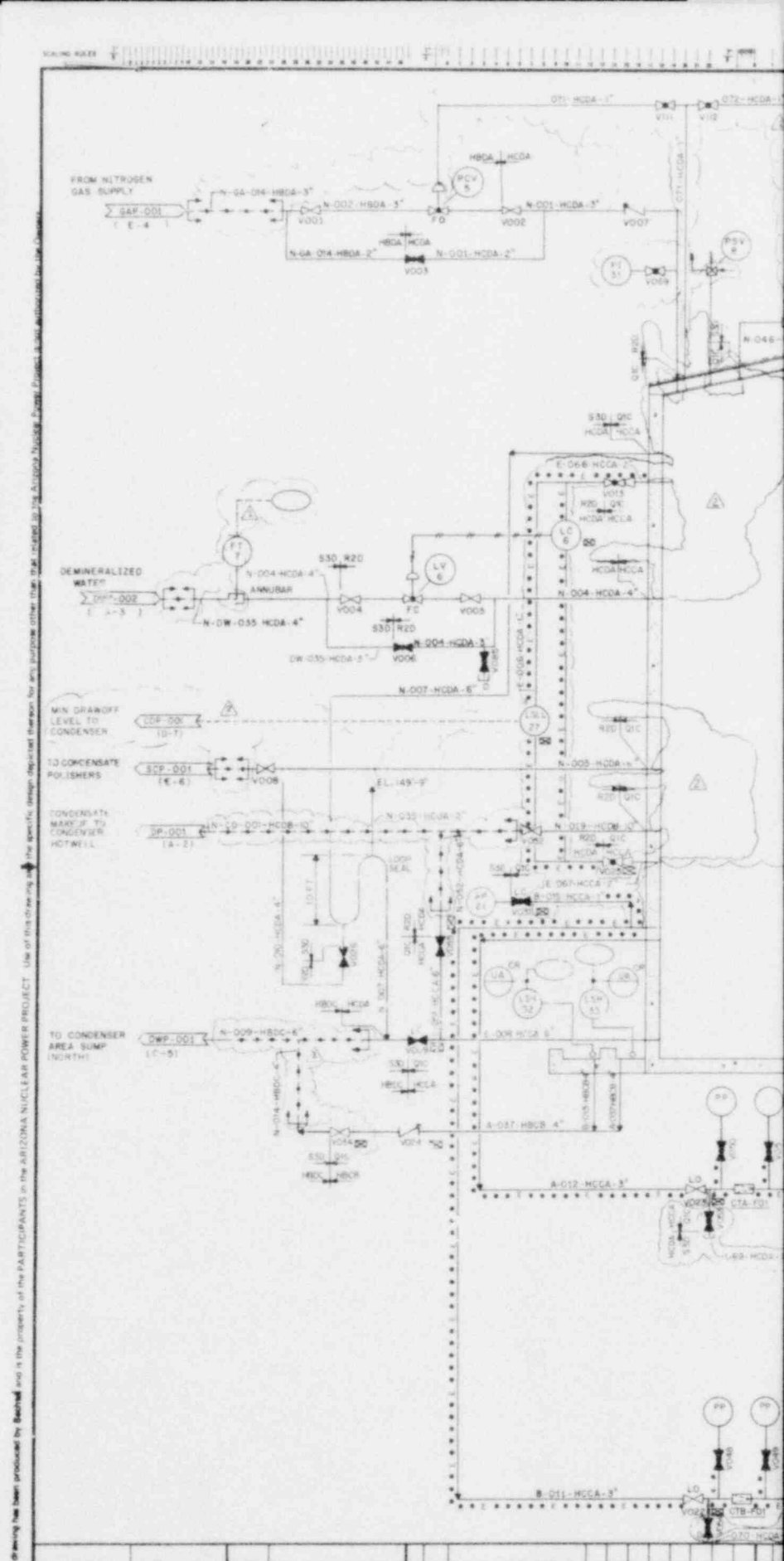

BECHTEL
LOS ANGELES
ARIZONA NUCLEAR POWER PROJECT
PALO VERDE NUCLEAR
GENERATING STATION
P & I DIAGRAM
AUXILIARY-FEEDWATER
SYSTEM
10407
13-M-AFP-001
7
THE SYSTEM DESIGNATOR AF IS TO PRECEDE ALL LINE, VALVE AND INSTRUMENT NUMBERS SHOWN ON THIS DRAWING UNLESS OTHERWISE INDICATED.

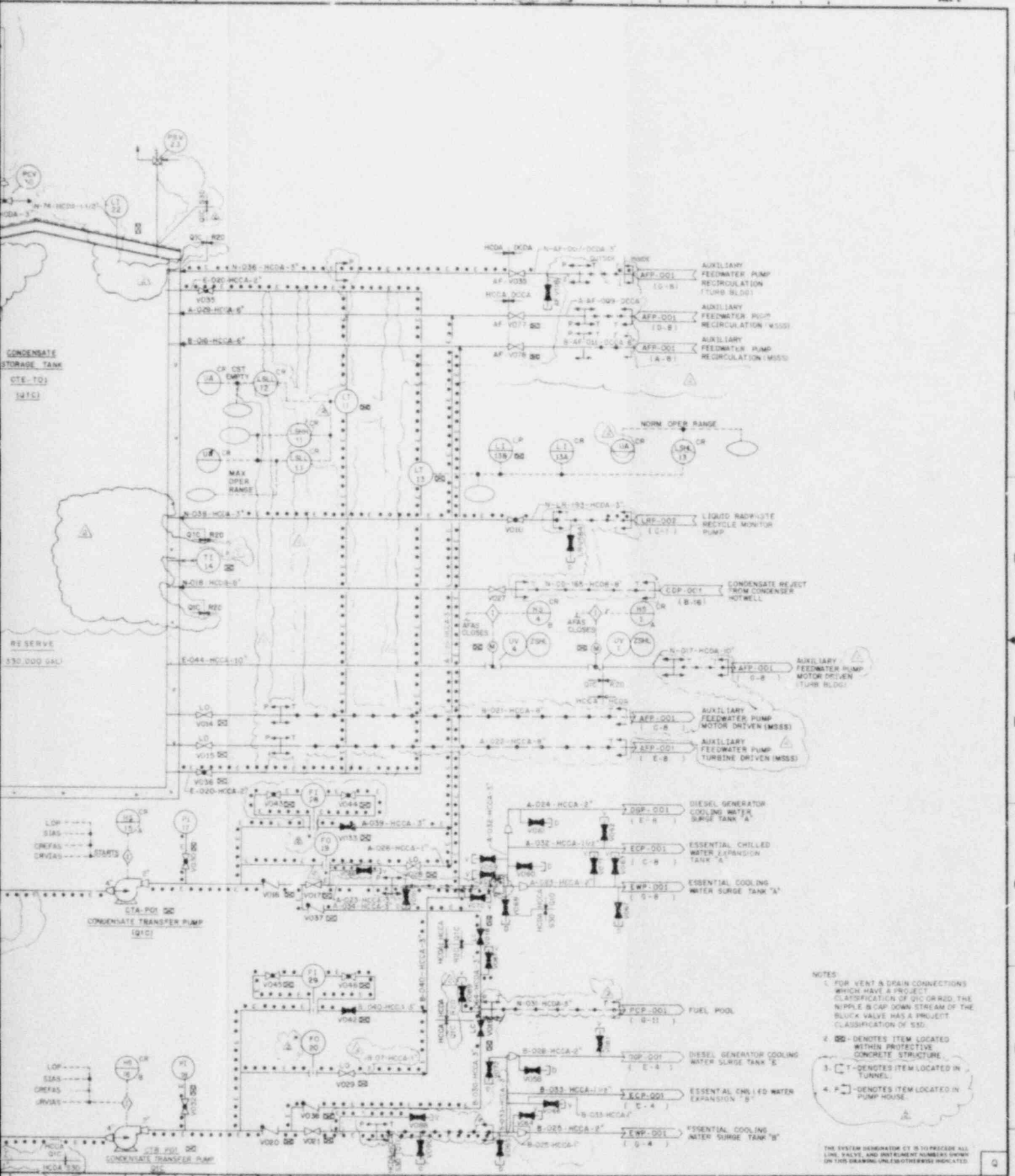
Figure A-1



This drawing has been produced by Bechtel and is the property of the PARTICIPANTS in the ARIZONA NUCLEAR POWER PROJECT. Use of this drawing is the specific design depicted thereon for any purpose other than that related to the Arizona Nuclear Power Project is unauthorized by the Owners.

DWG. NO.	REFERENCE	NO.	DATE	REVISIONS	DR	CH'K	DGS	ENG	EGS	CHP ENG	PRJ ENG	NO.	DA

8 7 6



NO.	DATE	REVISIONS	DR	CHK	DSG	ENG	EQR	CHF ENG	PRJ ENG	QA
2	12/	ADD VENTS, DRAINS, HEAT TRACING & REVISE INSTRUMENTATION								
1	7/	INCORPORATES DCN 1,2 & 3								
0		ISSUED FOR CONSTRUCTION								

BECHTEL
LOS ANGELES

ARIZONA NUCLEAR POWER PROJECT
PALO VERDE NUCLEAR GENERATING STATION

P AND I DIAGRAM
CONDENSATE STORAGE AND TRANSFER SYSTEM

SCALE	JOB NO.	DRAWING NO.	REV.
	10407	13-M-LTP-001	2

Figure A-2

DOCUMENT/ PAGE PULLED

ANO. 8102250260

NO. OF PAGES 3 maps

REASON

☐ PAGE ILLEGIBLE

☐ HARD COPY FILED AT: PDR CF

OTHER _____

☐ BETTER COPY REQUESTED ON ____/____/____

☑ PAGE TOO LARGE TO FILM

☑ HARD COPY FILED AT: (PDR) CF

OTHER _____

☑ FILMED ON APERTURE CARD NO 8102250260

260-02

APPENDIX B

RELIABILITY BLOCK DIAGRAMS

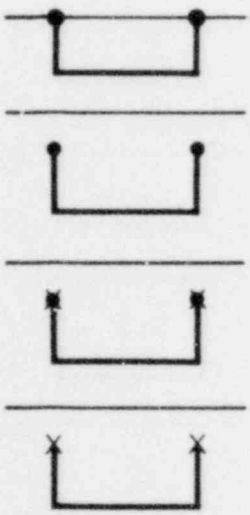
MULTI-FUNCTION ITEM –

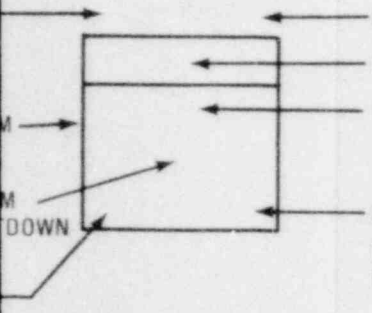
DASHED LINE:
MULTI-FUNCTION ITE

LOCATION:
CR – CONTROL ROO
RS – RESERVE SHUT
STATION

VITAL INSTRUMENT BUS

REDUNDANCY TYPE:





DRAWING COORDINATE

ITEM NUMBER

ITEM DESCRIPTION: E/P – ELECTRO PNEUMATIC
E/H – ELECTRO HYDRAULIC

STATE (PLANT AT POWER)

NO – NORMALLY OPEN
NC – NORMALLY CLOSED

LO – LOCKED OPEN
LC – LOCKED CLOSED
FL – FAILED LOCKED

ND – NORMALLY DEENERGIZED
NE – NORMALLY ENERGIZED
NA – NORMALLY ACTIVE

CTIVE

UTOMATIC
TANDBY

EMOTE MANUAL
TANDBY

OCAL MANUAL
TANDBY

BLOCK DIAGRAM SEQUENCE:

SHEET 2	SHEET 3	SHEET 4	SHEET 5	SHEET 6	SHEET 7	SHEET 8	SHEET 10
						SHEET 9	SHEET 11

PVNGS AFS RELIABILITY BLOCK DIAGRAM

Figure B-1 (Sheet 1 of 11)

APPENDIX C

MASTER FAULT TREE

DOCUMENT/ PAGE PULLED

ANO. 8102250260

NO. OF PAGES 10 maps

REASON

☐ PAGE ILLEGIBLE

☐ HARD COPY FILED AT: PDR CF

OTHER _____

☐ BETTER COPY REQUESTED ON ____/____/____

☑ PAGE TOO LARGE TO FILM

☑ HARD COPY FILED AT: (PDR) CF

OTHER _____

☑ FILMED ON APERTURE CARD NO 8102250260

260-09

DOCUMENT/ PAGE PULLED

ANO. 8102250260

NO. OF PAGES 1 maps

REASON

☐ PAGE ILLEGIBLE

☐ HARD COPY FILED AT: PDR CF

OTHER _____

☐ BETTER COPY REQUESTED ON ____/____/____

☒ PAGE TOO LARGE TO FILM

☒ HARD COPY FILED AT: (PDR) CF

OTHER _____

☒ FILMED ON APERTURE CARD NO 8102250260

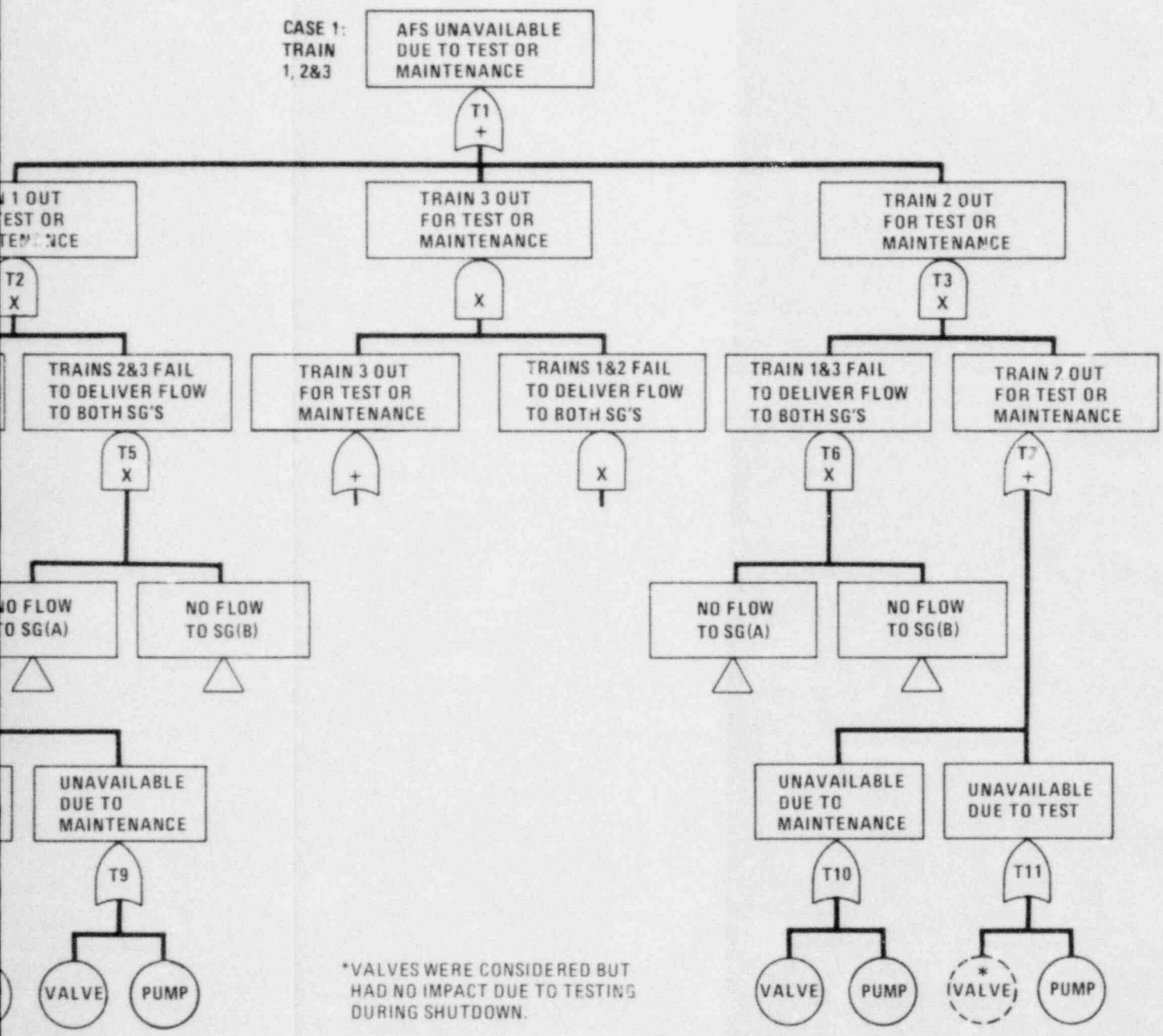
APPENDIX D

TEST AND MAINTENANCE FAULT TREE

APPENDIX E

HUMAN ERROR FAULT TREE

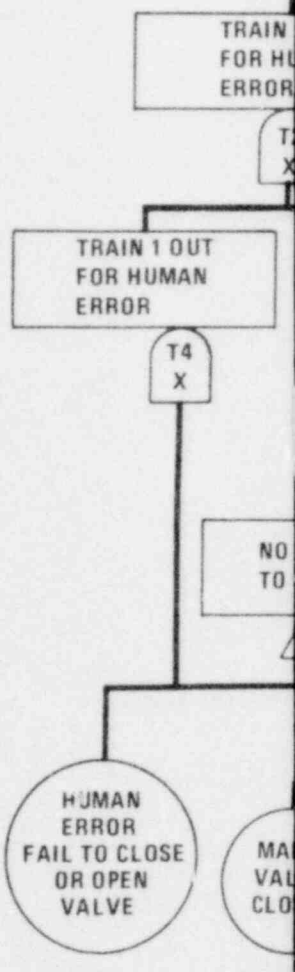

TRAIN 1 OUT
FOR TEST OR
MAINTENANCE
T4
UNAVAILABLE
DUE TO TEST
T8
VALVE
PUMP

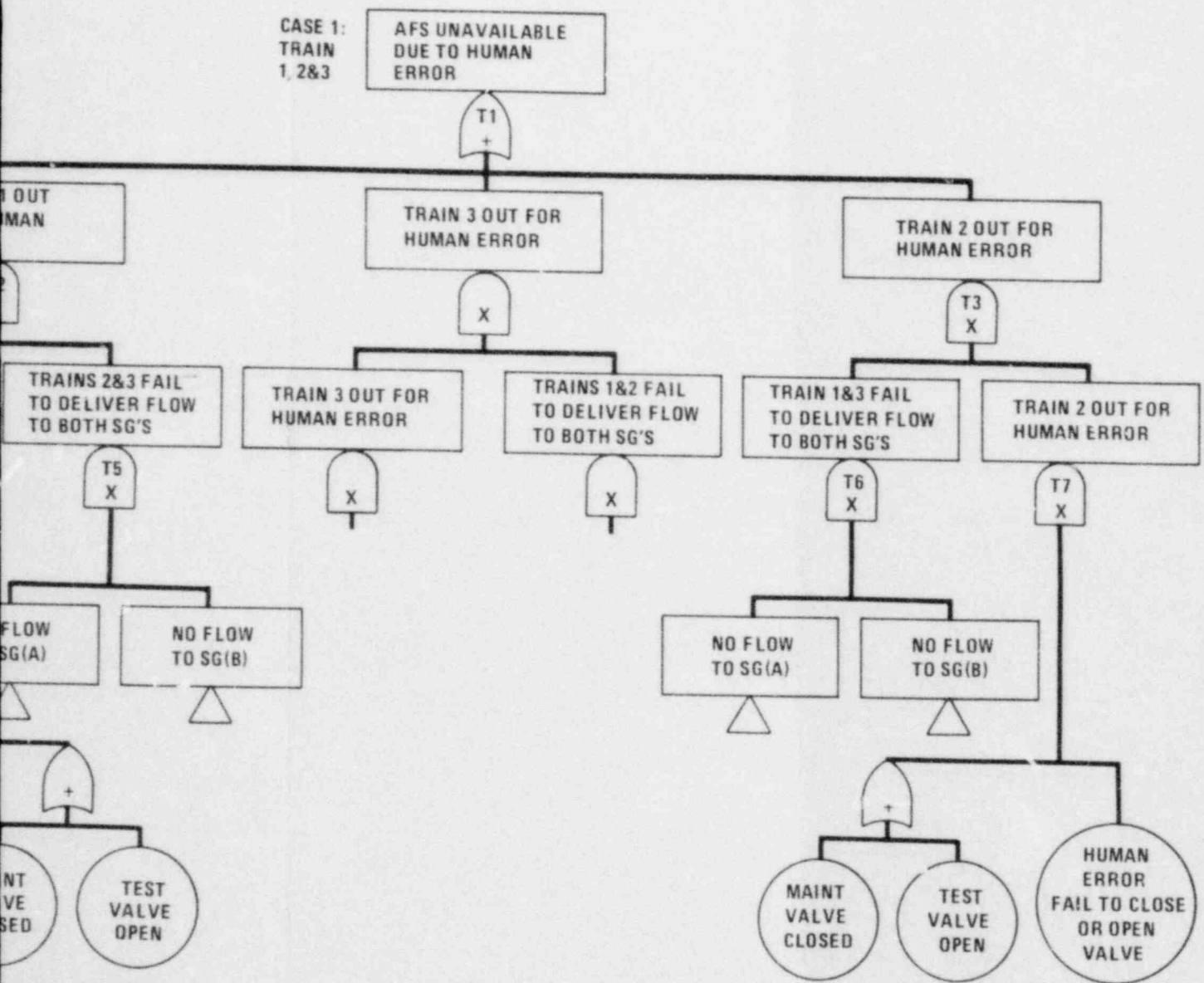


*VALVES WERE CONSIDERED BUT HAD NO IMPACT DUE TO TESTING DURING SHUTDOWN.

T & M FAULT TREE

Figure D-1


TRAIN
FOR HU
ERROR
T
X
TRAIN 1 OUT
FOR HUMAN
ERROR
T4
X
NO
TO
HUMAN
ERROR
FAIL TO CLOSE
OR OPEN
VALVE
MA
VAL
CLO



HUMAN ERROR FAULT TREE

Figure E-1

APPENDIX F

COMMON CAUSE CLASSIFICATIONS AND DEFINITIONS

APPENDIX F

COMMON CAUSE CLASSIFICATIONS AND DEFINITIONS

Common Links	N	Energy flow path	Same hydraulic, electric, air loop
	T	Test Procedure	Faulty Test Procedure
	P	Proximity	Location
	O	Operator or Operation	Operator disable or overstressed
	M	Maintenance	Incorrect procedure, poorly trained
	I	Installation Contractor	Same subcontractor or crew
	C	Calibration	Misprinted calibration instruction, test equipment faulty
	E	Energy Source	Common drive shaft, same power supply
Chemical or Misc.	B	Biological hazards	Poisonous gases, explosives, missiles
	S	Similar	Same generic component, i.e., valve, centrifugal pump, electric motor, etc.
	I	Identical	Same manufacture, size, design
	O	Corrosion (Oxidation)	In a water medium, or around high temperature metals (i.e., filaments)
	A	Corrison (Acid)	Boric acid from neutron control system, acid used for removing rust and cleaning

Electrical or Radiation	I	Current - out of tolerance	Short circuit, power surge
	V	Voltage - out of tolerance	Power surge
	M	Conducting medium	Moisture, combustion gases
	R	Radiation damage	Neutron sources, charged particle radiation
	E	Electromagnetic Interference (EMI)	Welding equipment, rotating elec. machinery, lightning, power supply
Mechanical or Thermal	T	Temperature	Fire, lightning, welding equipment, cooling system faults, elec. short circuits
	S	Stress	Thermal stress at welds of dissimilar metals, bending moments
	M	Moisture	Condensation, pipe rupture, rain, flood
	G	Grit	Dust, metal fragments generated by moving parts with inadequate tolerances
	P	Pressure	Explosion, out-of-tolerance system changes (pump overspeed, flow blockage)
	V	Vibration	Machinery in motion, earthquake
	I	Impact	Pipe whip, water hammer, missiles, earthquakes, structural failure

APPENDIX G

SAMPLE MINIMAL CUT SET

Table G-1

TYPICAL MINIMAL CUT SET LMFW (CASE 3)

FAIL PATH NUMBER	CONCURRENT HARDWARE FAILURE(S) REQUIRED TO CAUSE AFS FAILURE		
1	CTET01		
2	CTEPV3		
3	EAAC	AFASB	
4	EFAC	EAAC	EEAC
5	EBAC	AFASB	V007
6	EBAC	AFASB	AFASA
7	EBAC	EFAC	V007
8	EBAC	EFAC	AFASA
9	EBAC	EFAC	EAAC
10	EDAC	EAAC	EEAC
11	EDAC	EBAC	V007
12	EDAC	EBAC	AFASA
13	EDAC	EBAC	EAAC
14	ECDC	EBAC	AFASB
15	ECDC	EBAC	EFAC
16	ECDC	EDAC	EBAC
17	EADC	EBAC	AFASB
18	EADC	EBAC	EFAC
19	EADC	EDAC	EBAC
20	V015	EBAC	AFASB
•			
•			
•			
280			

APPENDIX H

FAILURE RATES

Table H-1. Failure Rates (Sheet 1 of 4)

Item	Mean	Variance	Failure Mode
V079	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
UV34	1.2E-03	9.3E-07	MOV FAIL TO OPEN
AFASA	2.2E-04	5.0E-07	MOV INITIATING SIGNAL FAILURE AUTO-MANUAL
EBAC	1.2E-03	9.3E-07	ESSEN ELEC SUPPLY B FAILURE AC
HV30	1.2E-03	9.3E-07	MOV FAIL TO OPEN
V024	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
AFBP01	1.2E-03	9.3E-07	ELEC PUMP FAIL TO START
EEAC	1.2E-03	9.3E-07	ESSEN ELEC SUPPLY FAILURE AC
V022	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
ECDC	1.2E-03	9.3E-07	ESSEN ELEC SUPPLY C FAILURE DC
AFASB	2.2E-04	5.0E-07	MOV INITIATING SIGNAL FAILURE AUTO-MANUAL
UV36	1.2E-03	9.3E-07	MOV FAIL TO OPEN
EADC	1.2E-03	9.3E-07	ESSEN ELEC SUPPLY A FAILURE DC
HV32	1.2E-03	9.3E-07	MOV FAIL TO OPEN
V015	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
AFAP01	2.0E-02	2.6E-04	TURB PUMP FAIL TO START
V007	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
V080	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
UV35	1.2E-03	9.3E-07	MOV FAIL TO OPEN
HV31	1.2E-03	9.3E-07	MOV FAIL TO OPEN
UV37	1.2E-03	9.3E-07	MOV FAIL TO OPEN
HV33	1.2E-03	9.3E-07	MOV FAIL TO OPEN

Table H-1. Failure Rates (Sheet 2 of 4)

Item	Mean	Variance	Failure Mode	
CTET01	1.0E-16	N.A.	CONDENSATE STORAGE TANK RUPTURE	See
CTEPV	1.0E-16	N.A.	TANK PIPE AND VALVE RUPTURE	Sec. 4.1.4
V652	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	
V642	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	
AO1	2.7E-02	4.4E-03	OPERATOR ERROR-15 MIN	
UV130	4.0E-04	1.0E-07	AOV FAIL TO OPEN	
AO2	2.7E-02	4.4E-03	OPERATOR ERROR-15 MIN	
UV172	4.0E-04	1.0E-07	AOV FAIL TO OPFN	
AO3	2.7E-02	4.4E-07	OPERATOR ERROR-15 MIN	
FV1113	4.0E-04	1.0E-07	FCV FAIL TO OPEN	
V002	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	
V012	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	
AO4	2.7E-02	4.4E-03	OPERATOR ERROR-15 MIN	
AFNP01	1.2E-03	9.3E-07	ELEC PUMP-NON ESSEN FAIL TO START	
AO5	2.7E-02	4.4E-09	OPERATOR ERROR-15 MIN	
EAAC	1.2E-03	9.3E-07	ESSEN ELEC SUPPLY A FAILURE AC	
UV1	1.2E-03	9.3E-07	MOV FAIL TO OPEN	
UV4	1.2E-03	9.3E-07	MOV FAIL TO OPEN	
AO6	2.7E-02	4.4E-03	OPERATOR ERROR-15 MIN	
V653	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	
V693	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	

Table H-1. Failure Rates (Sheet 3 of 4)

Item	Mean	Variance	Failure Mode
AO7	2.7E-02	4.4E-03	OPERATOR ERROR-15 MIN
UV135	4.0E-04	1.0E-07	AOV FAIL TO OPEN
AO8	2.7E-02	4.4E-03	OPERATOR ERROR-15 MIN
UV175	4.0E-04	1.0E-07	AOV FAIL TO OPEN
AO9	2.7E-02	4.4E-03	OPERATOR ERROR-15 MIN
FV1123	4.0E-04	1.0E-07	FCV FAIL TO OPEN
V008	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
UV234	1.2E-03	9.3E-07	MOV FAIL TO OPEN
EDAC	1.2E-03	9.3E-07	ESSEN ELEC SUPPLY D FAILURE AC
HV230	1.2E-03	9.3E-07	MOV FAIL TO OPEN
V224	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
AFCP01	1.2E-03	9.3E-07	ELEC PUMP FAIL TO START
EFAC	1.2E-03	9.3E-07	ESSEN ELEC SUPPLY FAILURE AC
V222	1.2E-04	9.3E-09	CHECK FAIL TO OPEN
UV235	1.2E-03	9.3E-07	MOV FAIL TO OPEN
HV231	1.2E-03	9.3E-07	MOV FAIL TO OPEN
AS	1.2E-03	9.3E-07	AIR SUPPLY
EPEB	4.0E-02	1.0E-03	B DIESEL GEN FAIL TO START
EPEA	4.0E-02	1.0E-03	A DIESEL GEN FAIL TO START
AFAP02	1.9E-03	4.2E-06	TURB PUMP TEST UNAVAIL
AFAP03	5.8E-03	2.8E-04	TURB PUMP MAINT UNAVAIL
AFBP02	1.9E-03	4.2E-06	ELEC PUMP TEST UNAVAIL
AFBP03	5.8E-03	2.8E-04	ELEC PUMP MAINT UNAVAIL

Table H-1. Failure Rates (Sheet 4 of 4)

Item	Mean	Variance	Failure Mode	
AFCP02	1.9E-03	4.2E-06	ELEC PUMP-NON ESSEN-TEST UNAVAIL	
AFCP03	5.8E-03	2.8E-04	ELEC PUMP-NON ESSEN-MAINT UNAVAIL	
CTEPV1	1.0E-16	N.A.	TANK PIPE AND VALVE RUPTURE	See Section 4.1.4
CTEPV2	1.0E-16	N.A.	TANK PIPE AND VALVE RUPTURE	
CTEPV3	1.0E-16	N.A.	TANK PIPE AND VALVE RUPTURE	
V279	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	
V280	1.2E-04	9.3E-09	CHECK FAIL TO OPEN	

APPENDIX I

SAMPLE CALCULATIONS

Appendix I, will present sample calculations for the AFS Reliability estimate. Case 1 of the LMFW will be used as a sample - see Table I-1, 1st row.

A. Operator Error/Hardware:

1. Independent estimate = 3.7E-5:

   Table I-2, Cases 1 & 2 LMFW, Hardware/Operator Error, is the dominate portion of its minimal cut set (MCS) as developed from the master fault tree in Appendix C. The second order MCS's failure probability (Q), or un-availability, was 3.47E-5. The 3rd order MCS was estimated to be about 2E-6. Thus, the total Q is 3.5E-5 + 2E-6 = 3.7E-5.

2. Common Cause estimate = 1.5E-4

   From the common cause quantitative factors in section 4.1.6, 1.1E-4, Turb/Elec Train redundancy factor, was chosen because all components between these trains were considered the same except the turbine pump and the electric pumps. Thus, the common cause contribution (1.1E-4) added to the independent estimate (3.7E-5) will total to 1.5E-4.

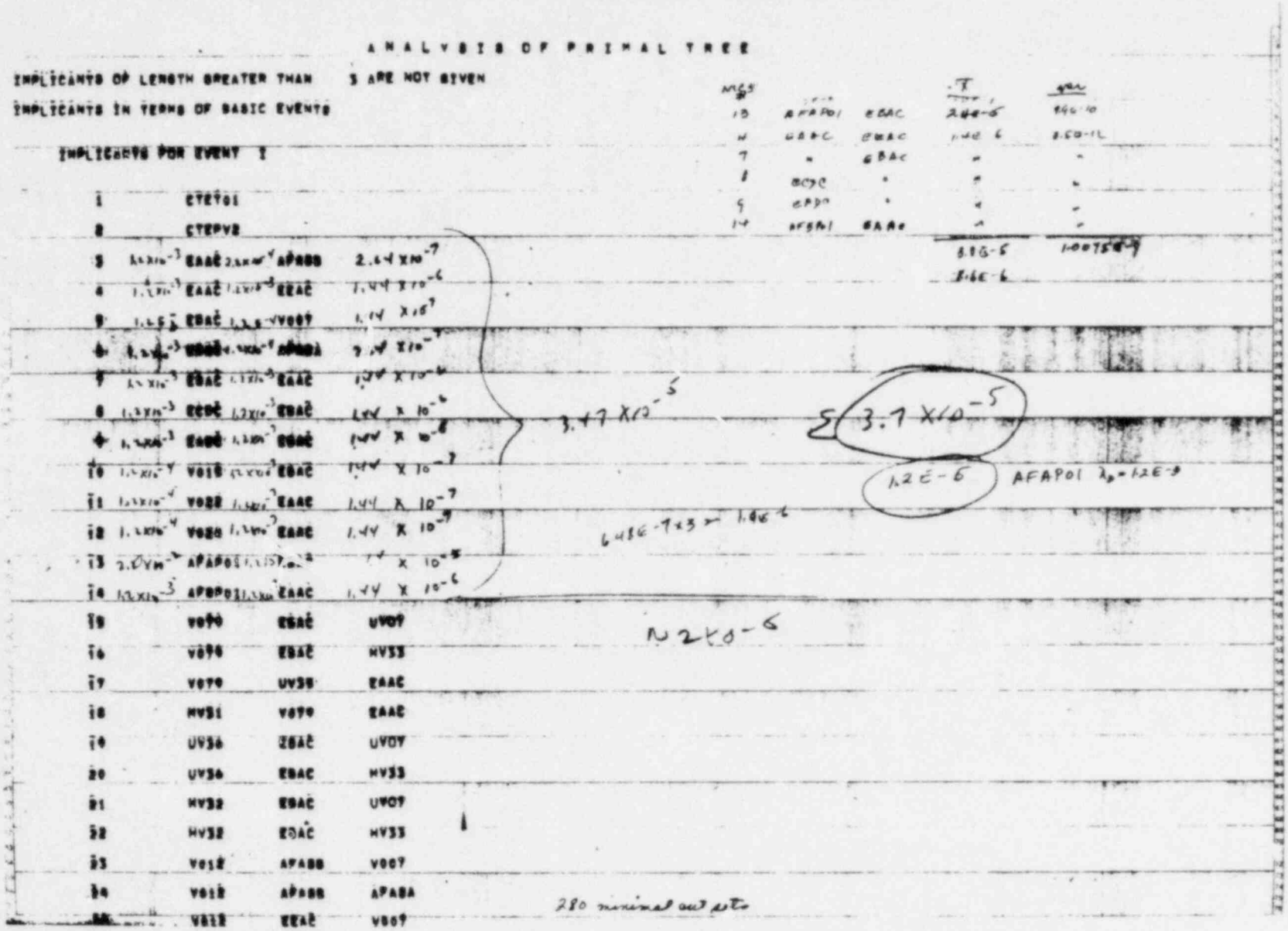
Table I-1

AFS RELIABILITY ESTIMATE

				FAILURE PROBABILITY (UNAVAILABILITY)				$\bar{A}$ PER YEAR
INDEPEND. – STATISTICAL INDEPENDENT ESTIMATE C.G. – COMMON CAUSE ESTIMATE				OP. ERROR HARDWARE	TEST & MAINT.	HUMAN ERROR	TOTAL	
3/YEAR	TOTAL LOSS OF MAIN FEEDWATER – LMFW	CASE 1	INDEPEND. C.C.	3.7E-5 1.5E-4	3.7E-5 4.0E-5	1.3E-4 8.7E-4	2.0E-4 1.1E-3	6.0E-4 3.3E-3
		CASE 2	INDEPEND. C.C.	3.7E-5 1.5E-4	3.7E-5 4.0E-5	1.3E-4 8.7E-4	2.0E-4 1.1E-3	6.0E-4 3.3E-3
		CASE 2A	INDEPEND. C.C.	1.1E-6 1.1E-4	3.0E-6 6.1E-6	1.1E-5 7.5E-4	1.5E-5 8.7E-4	4.5E-5 2.6E-3
		CASE 3	INDEPEND. C.C.	8.1E-7 1.1E-4	5.6E-7 4.5E-6	2.0E-6 7.5E-4	3.4E-6 8.6E-4	1.0E-5 2.6E-3
.2–.3/YEAR	TOTAL LOSS OF OFFSITE POWER – LOOP	CASE 1	INDEPEND. C.C.	1.1E-3 1.2E-3	5.3E-4 5.3E-4	1.9E-3 2.6E-3	3.5E-3 4.3E-3	8.8E-4 1.1E-3
		CASE 2	INDEPEND. C.C.	2.6E-4 4.0E-4	8.8E-5 1.0E-4	3.1E-4 1.1E-3	6.6E-4 1.6E-3	1.7E-4 4.0E-4
		CASE 2A	INDEPEND. C.C.	6.7E-5 2.1E-4	3.3E-5 4.4E-5	1.1E-4 8.9E-4	2.1E-4 1.1E-3	5.3E-5 2.8E-4
		CASE 3	INDEPEND. C.C.	5.1E-5 1.9E-4	3.3E-5 4.6E-5	1.2E-4 8.9E-4	2.0E-4 1.1E-3	5.0E-5 2.8E-4
$<10^{-3}$/YEAR	AC BLACK OUT	CASE 1	INDEPEND. C.C.	2.4E-2 2.4E-2	8.1E-3 8.1E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 2	INDEPEND. C.C.	2.4E-2 2.4E-2	8.1E-3 8.1E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 2A	INDEPEND. C.C.	2.4E-2 2.4E-2	8.1E-3 8.1E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5
		CASE 3	INDEPEND. C.C.	2.4E-2 2.4E-2	8.3E-3 8.3E-3	2.9E-2 3.0E-2	6.1E-2 6.2E-2	6.1E-5 6.2E-5

Table I-2

CASES 1 AND 2 LMFW HARDWARE/OPERATOR ERROR



ANALYSIS OF PRIMAL TREE

IMPLICANTS OF LENGTH GREATER THAN 3 ARE NOT GIVEN

IMPLICANTS IN TERMS OF BASIC EVENTS

IMPLICANTS FOR EVENT T

1	CTETO1		
2	CTEPV2		
3	EAAC	APABB	2.64×10^{-7}
4	EAAC	EEAC	1.44×10^{-6}
5	EBAC	VV007	1.14×10^{-7}
6	EBBC	APABA	7.14×10^{-7}
7	EBAC	EAAC	1.14×10^{-6}
8	EBBC	EBAC	1.44×10^{-6}
9	EABC	EBAC	1.44×10^{-6}
10	VO1B	EBAC	1.44×10^{-7}
11	VO2B	EAAC	1.44×10^{-7}
12	VO2B	EAAC	1.44×10^{-7}
13	APAFO1		7.4×10^{-5}
14	APBFO1	EAAC	1.44×10^{-6}
15	VO10	EBAC	UV07
16	VO10	EBAC	HV33
17	VO10	UV36	EAAC
18	HV31	VO10	EAAC
19	UV36	EBAC	UV07
20	UV36	EBAC	HV33
21	HV32	EBAC	UV07
22	HV32	EBAC	HV33
23	VO1B	APABB	VV007
24	VO1B	APABB	APABA
25	VO1B	EEAC	VV007

280 minimal cut sets

I-3

B. Test and Maintenance - Figure I-1

1. Independent Estimate = 3.7E-5

a.[1] Pump Test = 1.9E-3

$$Q_{Test} = \frac{(\text{hrs/test})(\text{tests/year})}{(\text{hrs/year})} = \frac{1.4 \times 12}{8760}$$

$$= 1.9E\text{-}3$$

b. Pump Maintenance = 5.8E-3

$$Q_{Maint} = \frac{.22\ (\text{hrs/maint})}{720} = \frac{.22 \times 19}{720} = 5.8E\text{-}3$$

c. Valve Maintenance = 1.2E-6

$$Q_{Maint} = \frac{(1.2E\text{-}4)(7)}{720} = 1.26E\text{-}6$$

Since the AFS is a standby system and since no repair can take place during the boildry time, the only way any portion of the system can be down for maintenance is as a result of a failure during test. The only full system test takes place during refueling thus has no effect on AFS unavailability.

The AFS is a non-pressurized standby system. MOV's are only tested during shutdown. The only active valve that would be cycled during pump testing will be the pump suction check valve. The demand failure rate of a check valve is assessed at 1.2E-4. Thus it was assumed that the likelyhood of valve maintenance per month be 1.2E-4.

d. Thus for any train out for T or M will be the sum of a + b + c, or 7.8E-3.

---

1. Note: All lower case letters refer to locations on the fault trees.

e. Trains 2 & 3 Fails = 1.4E-3

Table I-3, Cases 1 & 2 LMFW, Train 1 out, is the dominate portion of the MCS as developed from the master fault tree in Appendix C. The Q for this branch was estimated to be 1.4E-3.

f. Train 1 out and Trains 2 & 3 fails = 1.1E-5

This is the product of the Train 1 unavailability (7.8E-3) and Trains 2 & 3 fails (1.4E-3) equal to 1.1E-5.

g. Trains 1 & 3 Fails = 3.3E-3

Table I-4, Cases 1 & 2 LMFW, Train 2 out, is the dominate portion of the MCS as developed from the master fault tree in Appendix C. The Q for this branch was estimated to be 3.3E-3.

h. Train 2 out and Trains 1 & 3 Fails = 2.5E-5

This is the product of the Train 2 unavailability (7.8E-3) and Trains 1 & 3 fails (3.3E-3) equal to 2.5E-5.

i. Trains 1 & 2 Fails = 9.6E-5

Table I-5, Cases 1 & 2, LMFW, Train 3 out, is the dominate portion of the MCS as developed from the master fault tree in Appendix C. The Q for this branch was estimated to be 9.6E-5.

j. Train 3 out and Trains 1 & 2 fails = 7.5E-7 this is the product of the Train 3 unavailability (7.8E-3) and Trains 1 & 2 fails (9.6E-5) equal to 7.5E-7.

Table I-3

CASES 1 AND 2 LMFW TRAIN 1 OUT (Sheet 1 of 2)

ANALYSIS OF PRIMAL TREE

IMPLICANTS OF LENGTH GREATER THAN 3 ARE NOT GIVEN

IMPLICANTS IN TERMS OF BASIC EVENTS

IMPLICANTS FOR EVENT M1

1	EBAC		
2	CTET01		
3	CTEPV		
4	EAAC	APABB	
5	EAAC	EEAC	
6	V012	APABB	
7	V012	EEAC	
8	V022	EAAC	
9	V022	V012	
10	V024	EAAC	
11	V024	V012	
12	AFNP01	APABB	
13	AFNP01	EEAC	
14	AFNP01	V022	
15	AFNP01	V024	
16	AFBP01	EAAC	
17	AFBP01	V012	
18	AFBP01	AFNP01	
19	AOS	APABB	
20	AOS	EEAC	
21	AOS	V022	
22	AOS	V024	
23	AOS	AFBP01	
24	UV1	APABB	
25	UV1	EEAC	

Table I-3

CASES 1 AND 2 LMFW TRAIN 1 OUT (Sheet 2 of 2)

26	UV1		V022		
27	UV1		V024		
28	UV1	(5)	AFBP01		
29	AD6	✓	AFA3H		
30	AD6	✓	EEAC	3.2x6-5	
31	AD6	(3)	V022		
32	AD6	(4)	V024		
33	AD6	✓	AFBP01	3.2x6-5	
34	AD4	3	AFA3B		3 x 5.94E-6 = 1.78E-5
35	AD4	✓	EEAC	3.2x6-5	
36	AD4	(3)	V022		
37	AD4	(4)	V024		6x 3.24E-6 = 1.94E-5
38	AD4	✓	AFBP01	3.2x6-5	6x3.24E-5 = 1.94E-4
39	UV4	✓	AFA3B	4	
40	UV4	(5)	EEAC		
41	UV4		V022		
42	UV4		V024		
43	UV4	(8)	AFBP01		
44	A8	✓	AFA3B	5	5 x 3.64E-7 = 1.82E-6
45	A8	(2)	EEAC		
46	A8		V022		
47	A8		V024		
48	A8	(10)	AFBP01		10 x 1.44E-6 = 1.44E-5
49	AFA3B		UV172	UV175	
50	AFA3B		V653	UV172	
51	AFA3B		V693	UV172	
52	AFA3H		UV135	UV172	
53	AFA3H		UV130	UV175	
54	AFA3B		UV130	V653	534 Minimal Cut Sets
55	AFA3H		UV130	V693	

Table I-4

CASES 1 AND 2 LMFW TRAIN 2 OUT (Sheet 1 of 3)

ANALYSIS OF PRIMAL TREE

IMPLICANTS OF LENGTH GREATER THAN 3 ARE NOT GIVEN

IMPLICANTS IN TERMS OF BASIC EVENTS

IMPLICANTS FOR EVENT H3

1	EAAC		
2	CTET01		
3	CTFPV		
4	EBAC	V007	
5	EBAC	AFABA	
6	ECDC	EBAC	
7	EADC	EBAC	
8	V015	EBAC	
9	V012	V007	
10	V012	AFABA	
11	V012	ECDC	
12	V012	EADC	
13	V012	V015	
14	AFAP01	EBAC	2.9E-5
15	AFAP01	V012	2.9E-6
16	AFNP01	V007	
17	AFNP01	AFABA	
18	AFNP01	ECDC	
19	AFNP01	EADC	
20	AFNP01	V015	
21	AFNP01	AFAP01	1.4E-5
22	AOS	V007	
23	AOS	AFABA	
24	AOS	ECDC	
25	AOS	EADC	

1.4E-6 (1E-1)
1.4E-7
1.4E-6

MCS #	1		
1	EAAC		1.2E-3
27	2 AFAP01	3 AOS	5.4E-4
39	"	4 AO6	"
45	"	5 AO4	"
24	AOS	ECDC	2.2E-5
25	"	EADC	"
36	AO6	ECDC	"
37	"	EADC	"
42	AO4	ECDC	"
43	"	EADC	"
14	AFAP01	EBAC	2.4E-5
21	"	AFNP01	"
59	"	VV1	"
61	"	VV4	"
67	"	AS	"
15	"	V012	3.4E-6
16	"	V007	"
			3.204E-3

3 x 5.94E-6 = 1.78E-5
6 x 3.24E-6 = 1.94E-5
4 x 2.4E-5 = 9.6E-5
10 x 1.4E-6 = 1.4E-5

3rd order
8 x 2.6E-5 = 2.1E-4

Σ 3.204E-3

Σ Vol = V1 + V2 (V3 + V4 + V5)
= 9.3E-7 + 2.6E-4 (4.4E-3 + 4.4E-3 + 4.4E-3)
= 4.4 E-6

Table I-4

CASES 1 AND 2 LMFW TRAIN 2 OUT (Sheet 2 of 3)

	26	AOS	V015
2.2E-5	27	AOS	AFAP01 5.4E-4
	28	UV1	V007
	29	UV1	AFABA
	30	UV1	ECDC
	31	UV1	EADC
	32	UV1	V015
1.4E-6	33	UV1	AFAP01 1.7E-5
	34	AO6	V007
	35	AO6	AFABA
	36	AO6	ECDC
	37	AO6	EADC
	38	AO6	V015
3.2E-5	39	AO6	AFAP01
	40	AO4	V007
	41	AO4	AFABA
	42	AO4	ECDC
	43	AO4	EADC
	44	AO4	V015
2.2E-5	45	AO4	AFAP01
	46	UV4	V007
	47	UV4	AFABA
	48	UV4	ECDC
	49	UV4	EADC
	50	UV4	V015
1.4E-6	51	UV4	AFAP01
	52	AB	V007
	53	AB	AFABA
	54	AB	ECDC
	55	AB	EADC

Table I-4

CASES 1 AND 2 LMFW TRAIN 2 OUT (Sheet 3 of 3)

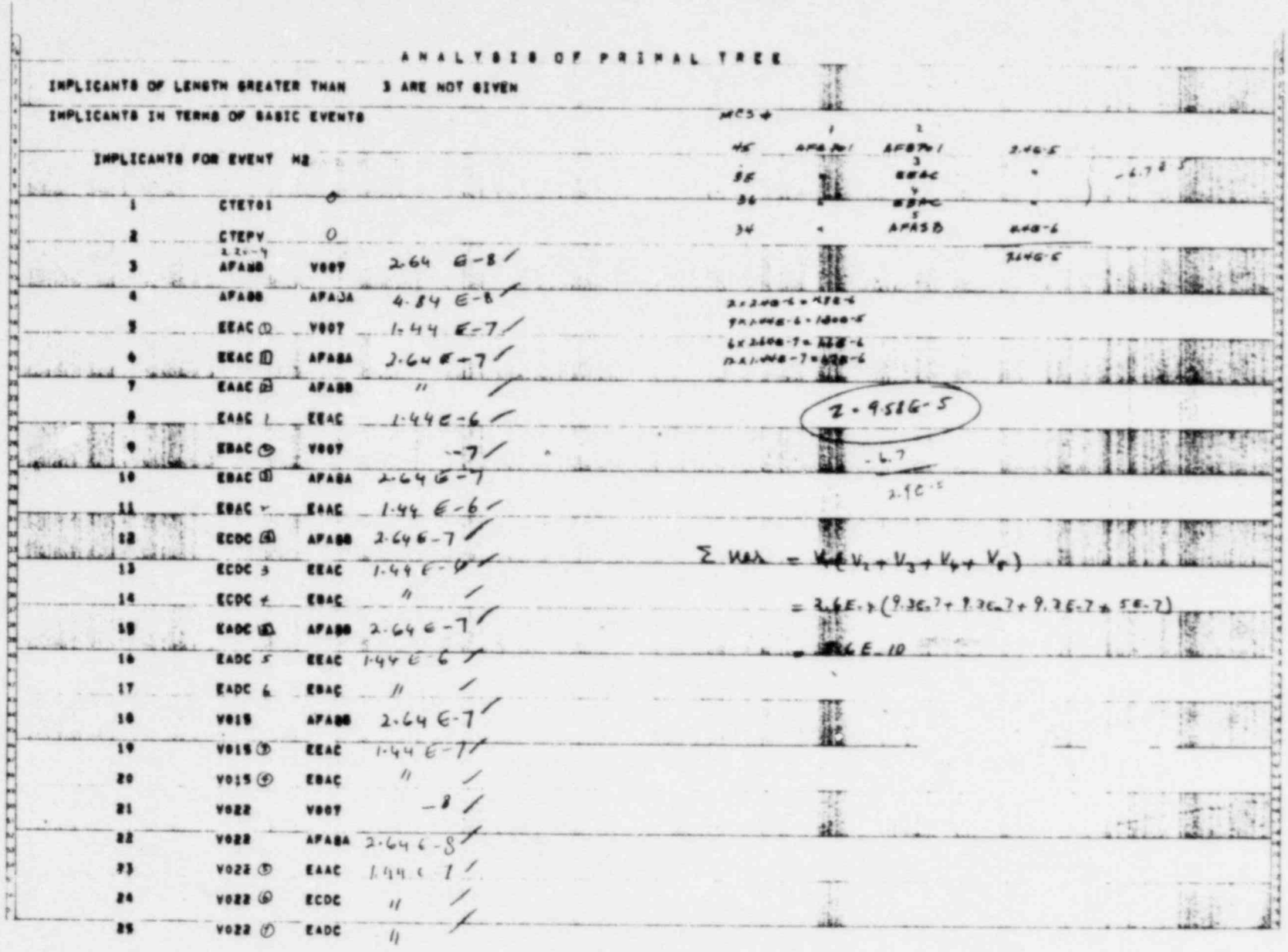
56	AB	V015	
57	AB	AFAP01	
58	V007	UV172	UV175
59	V653	V007	UV172
60	V693	V007	UV172
61	UV135	V007	UV172
62	UV130	V007	UV175
63	UV130	V653	V007
64	UV130	V693	V007
65	UV130	UV135	V007
66	AFABA	UV172	UV175
67	AFABA	V653	UV172
68	AFABA	V693	UV172
69	AFABA	UV135	UV172
70	AFABA	UV130	UV175
71	AFABA	UV130	V653
72	AFABA	UV130	V693
73	AFABA	UV130	UV135
74	ECDC	UV172	UV175
75	ECDC	V653	UV172
76	ECDC	V693	UV172
77	ECDC	UV135	UV172
78	ECDC	UV130	UV175
79	ECDC	UV130	V653
80	ECDC	UV130	V693
81	ECDC	UV130	UV135
82	EADC	UV172	UV175
83	EADC	V653	UV172
84	EADC	V693	UV172
85	EADC	UV135	UV172

1.4E-6

634 Minimal Cut Sets

Table I-5

CASES 1, 2 AND 2A LMFW TRAIN 3 OUT (Sheet 1 of 2)



ANALYSIS OF PRIMAL TREE

IMPLICANTS OF LENGTH GREATER THAN 3 ARE NOT GIVEN

IMPLICANTS IN TERMS OF BASIC EVENTS

IMPLICANTS FOR EVENT H2

1	CTET01	0	
2	CTEPV	0	
3	APAMB	V007	2.64 E-8
4	APABB	APAJA	4.84 E-8
5	EEAC ①	V007	1.44 E-7
6	EEAC ①	APABA	2.64 E-7
7	EAAC ②	APABB	"
8	EAAC 1	EEAC	1.44 E-6
9	EBAC ③	V007	-7
10	EBAC ③	APABA	2.64 E-7
11	EBAC 2	EAAC	1.44 E-6
12	ECDC ④	APABB	2.64 E-7
13	ECDC 3	EEAC	1.44 E-6
14	ECDC 4	EBAC	"
15	EADC ⑤	APABB	2.64 E-7
16	EADC 5	EEAC	1.44 E-6
17	EADC 6	EBAC	"
18	V015	APABB	2.64 E-7
19	V015 ③	EEAC	1.44 E-7
20	V015 ④	EBAC	"
21	V022	V007	-8
22	V022	APABA	2.64 E-8
23	V022 ⑤	EAAC	1.44 E-7
24	V022 ⑥	ECDC	"
25	V022 ⑦	EADC	"

MCS #

45	1 APABB	2 AFABB		2.46-5
35		3 EEAC		-6.7 E-5
36		4 EBAC		
34		5 AFASB		2.46-6
				7.46-6

2 x 2.46-6 = 4.92-6
9 x 1.46-6 = 1.3e-5
6 x 2.64-7 = 1.58-6
12 x 1.46-7 = 1.78-6

Σ = 9.58E-5

-6.7

2.9E-5

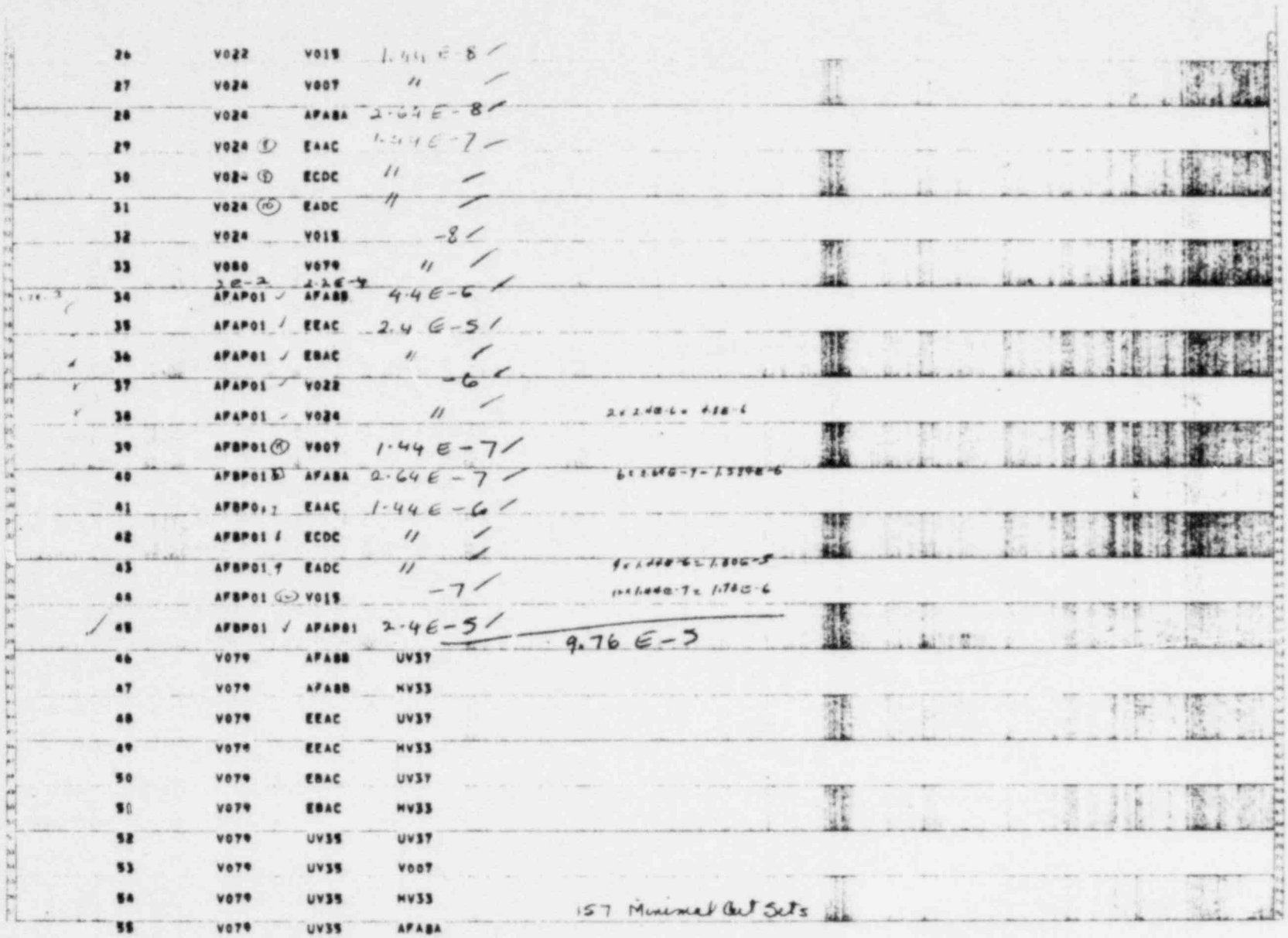
$\Sigma \text{MCS} = V_1(V_2 + V_3 + V_4 + V_5)$

$= 2.6E-7 (9.3E-7 + 9.3E-7 + 9.3E-7 + 5E-7)$

$= 9.6 E-10$

Table I-5

CASES 1, 2 AND 2A LMFW TRAIN 3 OUT (Sheet 2 of 2)



26	V022	V015	1.44 E-8
27	V024	V007	〃
28	V024	AFABA	2.64 E-8
29	V024 (5)	EAAC	1.44 E-7
30	V024 (5)	ECDC	〃
31	V024 (16)	EADC	〃
32	V024	V015	-8
33	V080	V079	〃
34	AFAP01	AFABB	4.4 E-6
35	AFAP01	EEAC	2.4 E-5
36	AFAP01	EBAC	〃
37	AFAP01	V022	-6
38	AFAP01	V024	〃
39	AFBP01 (4)	V007	1.44 E-7
40	AFBP01 (5)	AFABA	2.64 E-7
41	AFBP01	EAAC	1.44 E-6
42	AFBP01	ECDC	〃
43	AFBP01	EADC	〃
44	AFBP01 (15)	V015	-7
45	AFBP01	AFAP01	2.4 E-5
46	V079	AFABB	UV37
47	V079	AFABB	HV33
48	V079	EEAC	UV37
49	V079	EEAC	HV33
50	V079	EBAC	UV37
51	V079	EBAC	HV33
52	V079	UV35	UV37
53	V079	UV35	V007
54	V079	UV35	HV33
55	V079	UV35	AFABA

9.76 E-5

157 Minimal Cut Sets

k. The total statistically independent AFS unavailability due to T or M is the sum of f (1.1E-5) + h (2.5E-5) + j (7.5E-7) equal to 3.7E-5.

2. T or M Common Cause Estimate = 4.0E-5.

Potential Common Cause (CC) was assumed only to occur in the three main branches of the tree. No CC was assumed between the three main branches. CC factors from Section 4.1.6 were utilized as applicable to the hardware/operator portion of the tree.

e'. Common cause factor of 1.8E-4 was selected for the trains 2 & 3 because the two trains were assumed to be similar including the pump. This added to the independent Q (1.4E-3) is 1.6E-3.

f'. Train 1 out and Trains 2 & 3 fail with CC = 1.2E-5. This is the product of Train 1 unavailability (7.8E-3) and Trains 2 & 3 fails with CC (1.6E-3) = 1.2E-5.

g'. CC factor of 1.1E-4 was selected for Trains 1 & 3 because all components were assumed similar except the pumps. This added to 3.3E-3 = 3.4E-3.

h'. Train 2 out and Trains 1 & 3 fails with CC = 2.6E-5. This is the product of (7.8E-3) and 3.4E-3 = 2.6E-5.

i'. CC factor of 1.1E-4 was selected for Trains 1 & 2 because all components were assumed similar except the pumps. This added to 9.6E-5 = 2.1E-4.

j'. Train 3 out and Trains 1 & 3 fails with CC = 1.6E-6. This is the product of (7.8E-3) and (2.1E-4) = 1.6E-6.

k'. The total AFS unavailability due to T or M with independence and CC is the sum of f' (1.2E-5) + h' (2.6E-5) and j' (1.6E-6) equal to 4.0E-5.

C. Human Error - Figure I-2

The human error, which was considered, was forgetting to reclose the pump full flow test valve after it was opened and forgetting to reopen the pump discharge manual maintenance valve after a pump failure and maintenance action.

1. Independent estimate = 1.3E-4

   a. Test valve open = 1.0

      Full flow pump test requires the flow by-pass valve to be fully opened. All pumps were assumed to be tested on a monthly basis, thus the likelyhood of this valve to be opened is 1.0.

   b. For the turbine pump, the demand failure rate is assessed at 2E-2, thus, conservatively, the maintenance valve will be closed monthly at a likelyhood of 2E-2 due to a failure.

   c. Similar to "b", the electric pump demand failure rate is assessed at 1.2E-3, thus its maintenance valve will be closed monthly at a likelyhood of 1.2E-3 due to a failure.

d. The human error of "fail to reclose or reopen" a valve without position indicators in the control room was taken from NUREG 0635 and was assessed at 2.7E-2.

e. Train 1 out for human error = 2.75E-2.

The likelyhood of train 1 to be unavailable is the product of the likelyhood to open the test valve and to close the maintenance valve (1.02) times the human error failure probability (2.7E-2) equal to 2.75E-2.

f. Train 2 or 3 out for human error = 2.7E-2

The likelyhood of train 2 or 3 to be unavailable is the product of the likelyhood to open the test valve or to close the maintenance valve (1.001) times the human error failure probability (2.7E-2) equal to 2.7E-2.

g. Trains 2 & 3 Fails = 1.4E-3

Same as T & M, B.1.e.

h. Train 1 out and Trains 2 & 3 fails = 3.9E-5

This is the product of Train 1 unavailable due to human error (2.75E-2) and Trains 2 & 3 fails (1.4E-3) equal to 3.9E-5.

i. Trains 1 & 3 Fails = 3.3E-3

Same as T & M B.1.g.

j. Train 2 out and Trains 1 & 3 fails = 8.9E-5

This is the product of Train 2 out due to human error (2.7E-2) and Trains 1 & 3 fails (3.3E-3) equal to 8.9E-5

k. Trains 1 & 2 Fails = 9.6E-5

Same as T & M B.1.g.

l. Train 3 out and Trains 1 & 2 fails = 2.6E-6

This is the product of Train 3 out for human error (2.7E-2) and Trains 2 & 3 fails (9.6E-5) equal to 2.6E-6.

m. AFS Statistical Independent Unavailable Due to Human Error (1.3E-4) is the sum of h (3.9E-5) + j (8.9E-5) + m (2.6E-6).

2. Human Error Common Cause estimate = 8.7E-4

Potential Common Cause (CC) was assumed to occur in the three main branches of the tree. In addition, a potential CC between the three main branches of the tree was assumed to exist in that the operator may forget to reclose or reopen valves after test or maintenance on all three main branches.

g'. Common cause factor of 1.8E-4 was selected for the same reason as T or M CC B.2.e'. This added to the independent Q (1.4E-3) is 1.6E-3.

h'. Train 1 out and Trains 2 & 3 fail with CC = 4.4E-5.

This is the product of Train 1 unavailability (2.75E-2) and Trains 2 & 3 fails with CC (1.6E-3) = 4.4E-5.

i'. CC factor of 1.1E-4 was selected for trains 1 & 3 for the same reason as T or M CC B.2.g'. This added to the independent Q (3.3E-3) is 3.4E-3.

j'. Train 2 out and Trains 1 & 3 fail with CC = 9.2E-5.

This is the product of Train 2 unavailability (2.7E-2) and Trains 1 & 3 fails with CC (3.4E-3) = 9.2E-5.

k'. CC factor of 1.1E-4 was selected for trains 1 & 2. For the same reason as T or M CC B.2.i'. This added to the independent Q(9.6E-5) is 2.1E-4.

m'. Train 3 out and Trains 1 & 2 fails with CC = 5.6E-6

This is the product of Train 3 unavailability (2.7E-2) and Trains 1 & 2 fail with CC (2.1E-4) = 5.6E-6

n'. The total AFS unavailability due to human error with independence and CC in the three main branches is the sum of

h' (4.4E-5) + j' (9.2E-5) + m' (5.6E-6) equal to 1.4E-4.

n". The CC factor between the three main branches was assessed to be human error failure probability (2.7E-2) times the common cause β-factor (2.7E-2) equal to 7.3E-4. This added to the independent failure (1.3E-4) equal to 8.7E-4.

D. Total Failure Probability per demand - Table I-1

1. Independent = 2.0E-4

The total statistical independent failure probability is the sum of the hardware/operator error (3.7E-5) and T & M (3.7E-5) and human error (1.3E-4) equal to 2.0E-4.

2. Common Cause = 1.1E-3

Total CC failure probability is the sum of hardware/operator error (1.5E-4) and T & M (4.0E-5) and human error (1.1E-3) equal to 1.1E-3.

E. Unavailibility (A) per year - assume 3 LMFW/year. Table I-1

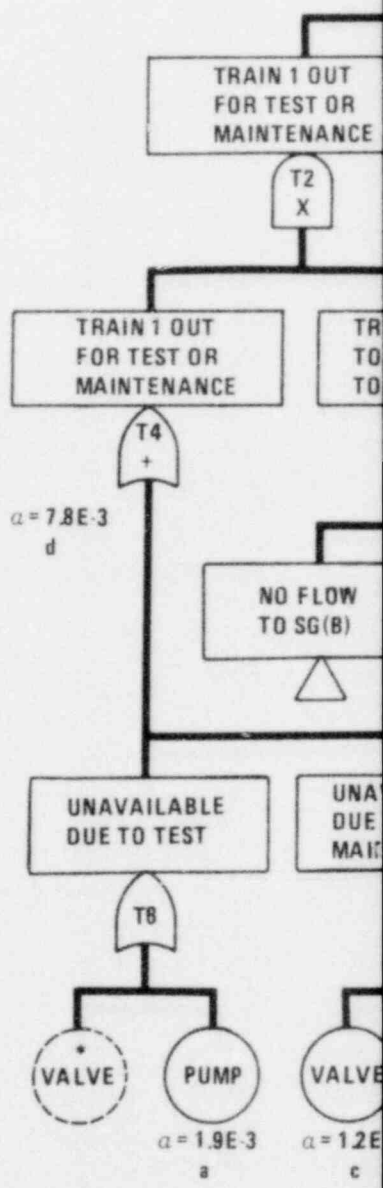
1. Independent = 6.0E-4

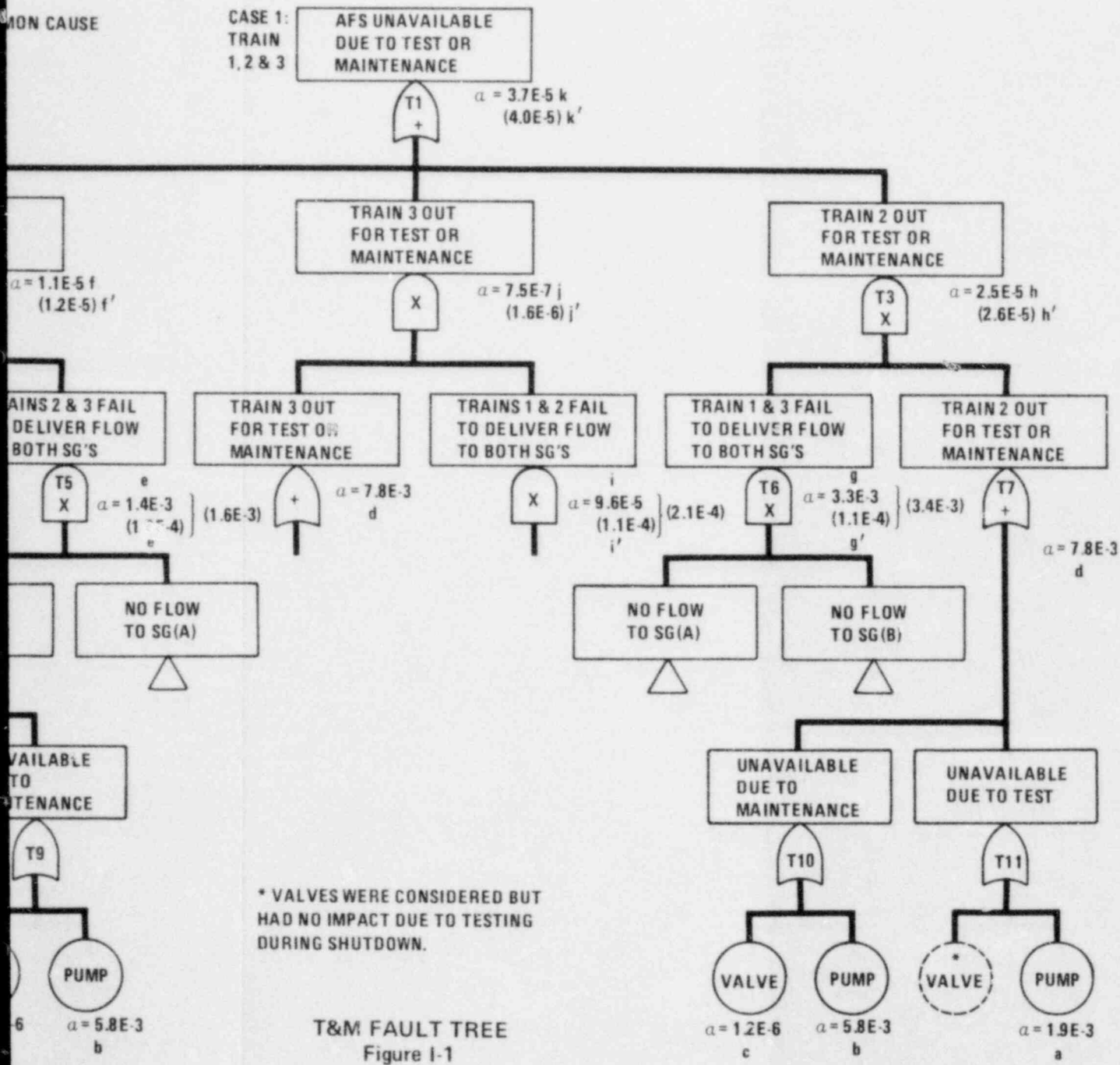
The total statistical independent failure probability per demand (2.0E-4) times the demand per year (3) equal to 6.0E-4.

2. Common Cause = 3.3E-3

Total CC failure probability per demand (1.1E-3) times the demand per year (3) equal to 3.3E-3.

( ) COMI

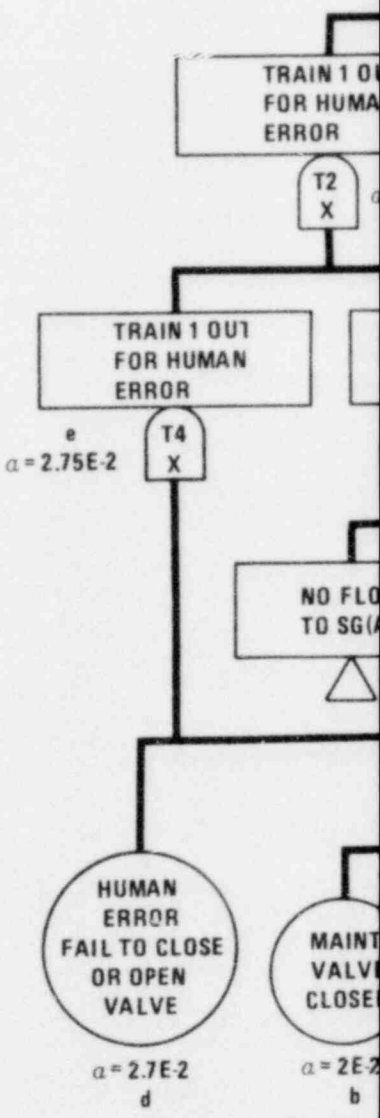

TRAIN 1 OUT
FOR TEST OR
MAINTENANCE
T2
X
TRAIN 1 OUT
FOR TEST OR
MAINTENANCE
T4
+
α = 7.8E-3
d
NO FLOW
TO SG(B)
UNAVAILABLE
DUE TO TEST
T8
VALVE
PUMP
α = 1.9E-3
a
VALVE
α = 1.2E
c

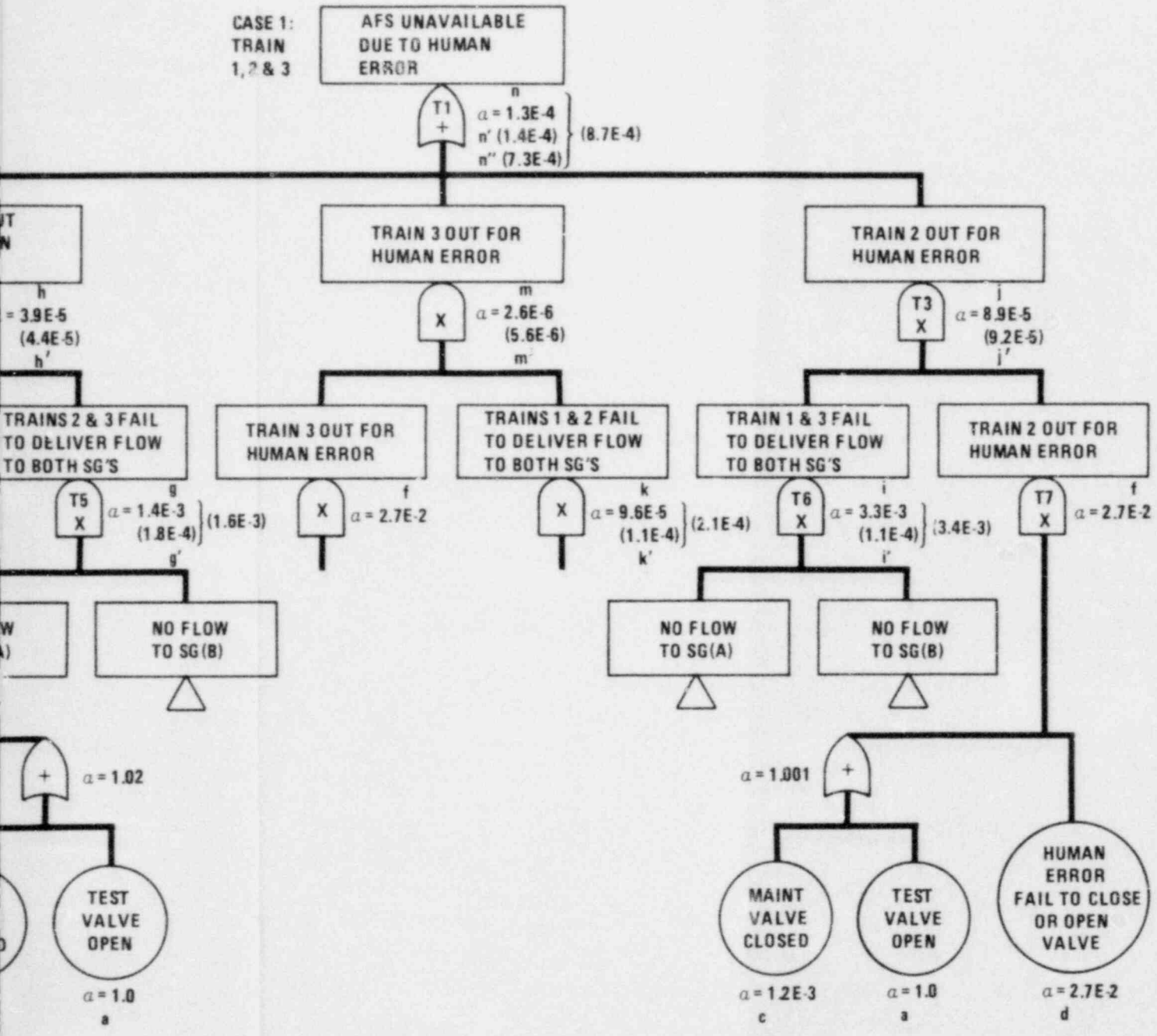


* VALVES WERE CONSIDERED BUT HAD NO IMPACT DUE TO TESTING DURING SHUTDOWN.

T&M FAULT TREE
Figure I-1

( ) COMMON CAUSE





HUMAN ERROR FAULT TREE
Figure I-2