

RELIABILITY ANALYSIS OF
THE SNUPPS
AUXILIARY FEEDWATER SYSTEM

May 1981

8106090 644

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
	SUMMARY	
1.0	INTRODUCTION	1-1
	1.1 Background	1-1
	1.2 Objective	1-1
	1.3 Scope	1-2
	1.4 General Approach	1-2
	1.5 Assumptions and Criteria	1-3
2.0	SYSTEM DESCRIPTION	2-1
	2.1 Introduction	2-1
	2.2 Component Description	2-1
	2.3 Emergency Operation	2-2
	2.4 Power Sources	2-3
	2.5 Information Available to the Operator	2-5
	2.6 Technical Specifications	2-6
3.0	METHODOLOGY	3-1
	3.1 Systems Review/Study Bounds	3-1
	3.2 Fault Trees	3-1
	3.3 Minimal Cut-Sets	3-2
	3.4 Fault Tree Quantification	3-2
	3.5 Importance Evaluation	3-2
	3.6 Common Cause Failure	3-3
	3.7 Interfacing Systems Failures	3-3
4.0	COMMON CAUSE FAILURE EVALUATION	4-1
5.0	RESULTS OF THE RELIABILITY EVALUATION	5-1
	5.1 AFW System Reliability	5-1
	5.2 Importance Evaluation	5-3
	5.3 Dominant Failure Modes	5-10
	5.4 Interfacing Systems	5-11
6.0	CONCLUSIONS/RECOMMENDATIONS	6-1
7.0	REFERENCES	7-1
	Appendix A: Fault Trees	A-1
	Appendix B: Failure Data - Basic Event Probabilities	B-1
	Appendix C: Minimal Cut Sets	C-1

LIST OF TABLES

<u>Table</u>		<u>Page</u>
B-1	Component-Basic Event Failure Probabilities	B-6
B-2	Composite Basic Event Probabilities - Options A, B, and C	B-9
C-1	AFWS Fault Tree Reduced to 9 Three-Event Cut-Sets	C-2
C-2	Significant Minimal Cut-Sets: Option A	C-3
C-3	Significant Minimal Cut-Sets: Option B	C-5
C-4	Significant Minimal Cut-Sets: Option C	C-7

LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
1-1	Basic Tasks of SNUPPS AFWS Reliability Study	1-4
2-1	Auxiliary Feedwater System P&ID	2-9
2-2	Auxiliary Feedwater Pump Turbine P&ID	2-10
2-3	Main Single Line Diagram of AC Power System	2-11
2-4	Main Single Line Diagram of DC Power System	2-12
5-1	Qualitative Comparison of the Reliability Characteristics for AFWS Designs in Plants Using the Westinghouse NSSS (including SNUPPS)	5-5
5-2	Quantification of the Reliability Characteristics of the SNUPPS AFWS for Various Options	5-6
5-3	Importance of Selected Events for Option A	5-7
5-4	Importance of Selected Events for Option B	5-8
5-5	Importance of Selected Events for Option C	5-9

Summary

The NRC has requested all pending operating license applicants with nuclear steam supply systems (NSSS) designed by Westinghouse and Combustion Engineering to assess the reliability of their auxiliary feedwater system (Reference 5). As a part of the response to this request, a reliability evaluation was made of the auxiliary feedwater system (AFWS) as designed for SNUPPS. This report presents the results of that reliability evaluation.

The primary objective of the study was to evaluate the reliability of the AFWS for SNUPPS using an approach which would yield results that could be compared to those obtained by the NRC analyses for Westinghouse NSSS as reported by NUREG-0611. A secondary objective of the study was to identify any dominant component failures or other faults affecting system reliability. In a manner similar to that reported in NUREG-0611, AFWS reliability was evaluated for three cases:

1) Loss of Main Feedwater (LMFW) with reactor trip, 2) Loss of Main Feedwater coincident with loss of offsite power (LMFW/LOOP), and 3) Loss of Main Feedwater accompanied by a total loss of all AC power (LMFW/LOAC). For each case, system unreliability was assessed through the construction and analysis of fault trees.

The results of the study indicated that the reliability ranking of the SNUPPS AFWS, compared to conditional reliabilities as defined and reported for Westinghouse plants in NUREG-0611, is in the 10^{-4} to 10^{-5} range for a loss of main feedwater transient, in the 10^{-4} to 10^{-5} range for a loss of main feedwater coupled with a loss of offsite power transient, and in the 10^{-1} to 10^{-2} range for the unlikely transient of a loss of main feedwater coincident with a total loss of both onsite and offsite AC power.

1.0 Introduction

1.1 Background

This report presents the results of a reliability study for the SNUPPS auxiliary feedwater system (AFWS) in a form compatible with information contained in NUREG-0611. The approach followed in this study was based on the information available in the initiating request (Reference 5) and information provided by the NRC to analysts performing AFWS reliability studies.

1.2 Objectives

- o To perform a reliability analysis to determine the relative reliability of the SNUPPS auxiliary feedwater system (AFWS). To facilitate a meaningful comparison with NRC analyses, the initiating events given in NUREG-0611 were used, as well as similar assumptions, reliability data, and evaluation techniques.
- o To identify the dominant failure modes of the SNUPPS AFWS.
- o To examine in more detail than treated in NUREG-0611, the possible contributions of single point vulnerabilities, common causes, human error, and test/maintenance outages to AFWS unavailability.

1.3 Scope

Three initiating event scenarios were analyzed:

Case 1: Loss of main feedwater (LMFW)

Case 2: Loss of main feedwater coincident with loss
of offsite power (LMFW/LOOP)

Case 3: Loss of main feedwater coincident with loss
of all AC power (LMFW/LOAC)

The existence of the above scenarios was considered a priori and an evaluation of their probability of occurrence was considered to be outside the bounds of this study.

Consistent with NUREG-0611, low probability common cause factors such as flood, fire, earthquake, sabotage or high energy line breaks were not considered.

1.4 General Approach

The principal technique used in this study was the construction and analysis of fault trees which represent the failure logic of the AFWS. The deductive logic used in evaluating the relative reliability of the AFWS is based on the Boolean logic associated with fault trees. The fault trees representing the SNUPPS auxiliary feedwater system can be found in Appendix A. The fault trees were resolved into a list of cut sets to identify the failure modes, and failure rate data were inserted to evaluate system unreliability. Although failure data (see Appendix B) were taken primarily from NUREG-0611 (Reference 4), secondary sources of failure data were the LER Summaries (References 6 and 7), WASH-1400 (Reference 11) and NPRDS (Reference 12).

The degree of development of the fault tree was consistent with the reliability assessment goals and data available in NUREG-0611, and was limited to a point estimate of AFWS unavailability on demand. For the purposes of this study, unavailability is synonymous with unreliability and both terms may be found in this report. Although an uncertainty analysis was not performed, the importance of certain failure modes and the interrelationship between and significance of hardware failures, test/maintenance outages, and human errors were examined (see Section 5.2). The sensitivity to human error was examined for three levels of human error (Options A, B, and C); the three options are defined in Appendix B.

Figure 1-1 is a flow chart of the basic tasks in the study. Each of these steps is discussed in more detail in Section 3.

1.5 Assumptions

Assumptions were consistent with information supplied in NUREG-0611 and by the NRC Staff to industry analysts performing reliability studies for other plants. The assumptions assure that the SNUPPS reliability evaluation will give results comparable to those obtained by the NRC for plants evaluated in NUREG-0611. However, all the sensitivity evaluations, common cause evaluations and importance evaluations were based on a slightly more conservative assumption for onsite AC power availability (i.e., potential failure of either diesel generator was assumed). The specific assumptions used in the evaluation are:

1. Mission Success Criteria

The success criteria is a minimum flow of 470 GPM delivered within one minute to at least two steam generators following a loss of main feed-water. This is a conservative criteria specified to assure adequate heat removal for a worse case. This criteria is the basis of the top event in the SNUPPS AFWS fault tree as presented in Appendix A. Since this quantitative evaluation of system reliability is a point estimate and since each AFWS pump is sized to provide at least 470 gpm to two steam generators, the top event can be simplified to no flow to more than 2 out of 4 steam generators.

2. Hardware and Human Error Failure Data

The failure data was taken primarily from NUREG-0611 and assumed valid and directly applicable to the evaluation of basic events in this study. In a few instances failure data was taken from WASH-1400 (Appendix III) and the LER Summaries. The actual data used is presented in Appendix B.

3. Test and Maintenance Outage Contribution

The calculational approach along with the outage mean duration data presented in Table III-2 of NUREG-0611 was used in this study. Test and maintenance outages were consistent with the Standard Technical Specifications (Reference 8).

A more detailed discussion of the treatment of T&M outages is presented in Appendix B.

4. Power Availability

- o DC and battery-backed AC were assumed available with a probability of 1.0.
- o For comparison with the NUREG-0611 results, one diesel generator was assumed available with a probability of 1.0 and the other diesel generator fails with a probability of .04/demand. However, all sensitivity evaluations, common cause evaluations and importance evaluations were based on the potential failure of either diesel generator with a probability of .04/demand.

5. Sample and Test Lines

Sample and test lines were not considered as significant flow diversion and/or leakage paths in the development of fault trees used in the study.

6. Passive Piping Components

All piping components (i.e., section of pipes, flanges, reducers, etc.) were assumed available with a probability of 1.0 and were not considered in the fault tree development. However, the effects on system unreliability of pipe breaks in non-

seismic/non-Q interfacing systems were examined (see Section 5.4).

7. Degraded Component Failures

Degraded failures were not considered in the analysis, that is, components were assumed to operate properly or were treated as a total failure. Assumptions regarding component status, partial-capacity performance, and time-dependent (delayed) failures are made conservatively. That is, component failures will occur instantaneously and completely.

8. Coupling of Human Errors

Coupled human errors for test and maintenance were considered through the selection of the appropriate data for human acts and errors as supplied by the NRC in NUREG-0611. For a more detailed discussion of the human error treatment, see Appendix B.

9. Technical Specifications

Since plant technical specifications are not available at this time, the Standard Technical Specifications (Reference 8) were assumed.

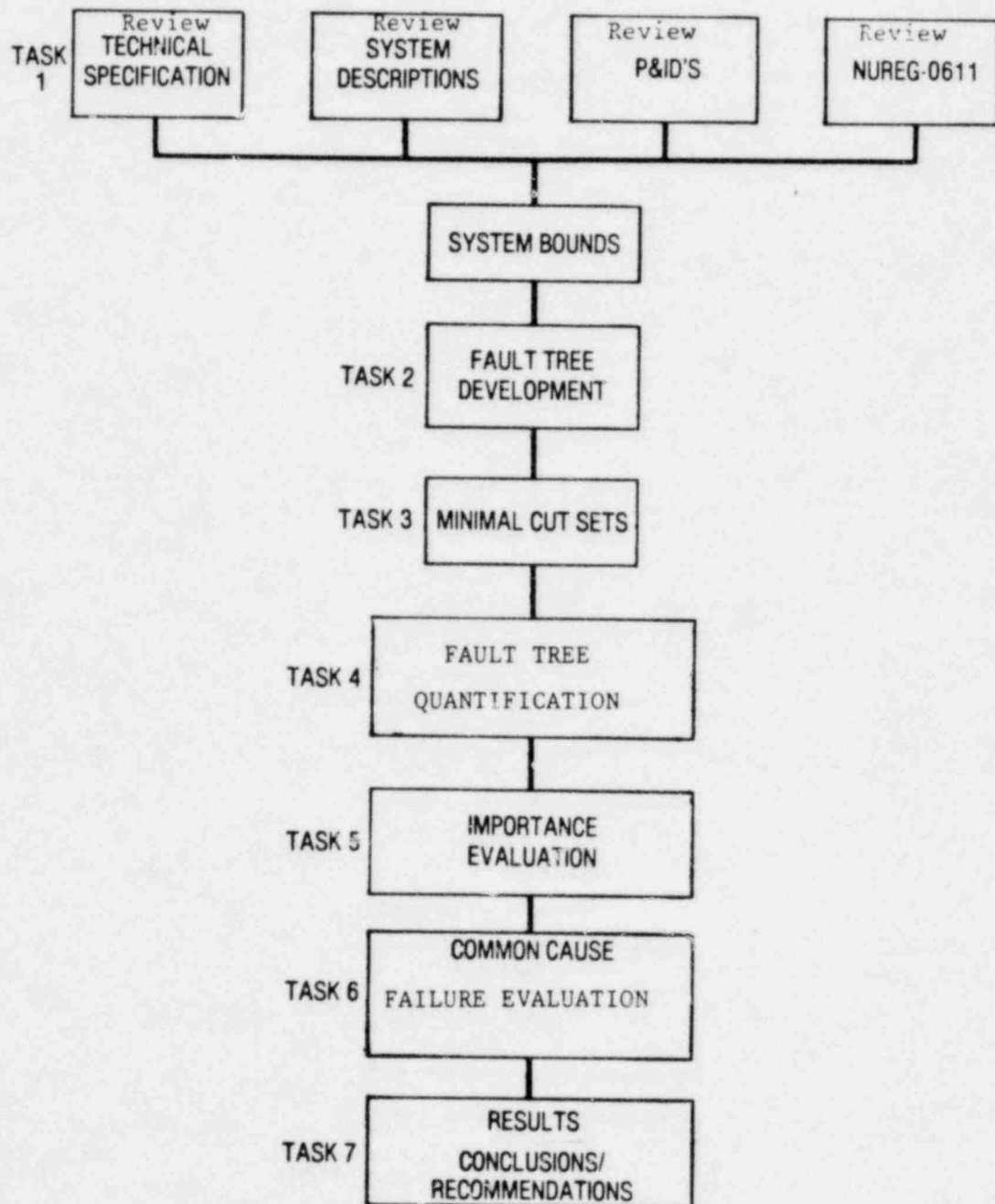


Figure 1-1

2.0 System Description

2.1 Introduction

The following paragraphs describing the SNUPPS AFWS summarize the more extensive description given in the SNUPPS FSAR (Reference 3).

Figure 2-1 is a flow diagram of the SNUPPS AFWS. The SNUPPS Auxiliary Feedwater System consists of two motor-driven pumps, one steam turbine-driven pump, and associate piping, valves, instruments, and controls as shown in Figure 2-1. Figure 2-2 shows the piping and instrumentation for the steam turbine.

Each motor-driven auxiliary feedwater pump will supply 100 percent of the feedwater flow required for removal of the reactor decay heat. The turbine-driven pump is sized to supply up to twice the capacity of a motor-driven pump.

Normally, water to the AFW pumps is supplied from the condensate storage tank (CST). However, two redundant safety-related backup sources of water from the essential service water system (ESWS) are provided. Should the CST water supply to the pump suction be disrupted, the system will automatically switch from the CST to the ESWS on low pump suction pressure.

2.2 Component Description

Motor-Driven Pumps: These two auxiliary feedwater pumps are driven by AC-powered electric motors supplied with power from independent Class 1E switchgear buses. The pumps are horizontal centrifugal units.

Turbine-Driven Pump: The pump is a horizontal centrifugal unit. The pump bearings are cooled by the pumped fluid. Turbine bearing lube oil is circulated by an integral shaft-driven pump. Power for all controls, valve operators, and other support systems is independent of AC power sources.

Steam supply piping to the turbine is taken from two of the four main steam lines between the containment penetrations and the main steam isolation valves. Each of the steam supply lines to the turbine is equipped with air-operated globe bypass valve to keep the line warm. The steam line is kept warm to prevent the accumulation of condensate which might produce a waterhammer in the line. The air-operated globe valves are equipped with DC-powered solenoid valves. These steam supply lines join to form a header which leads to the turbine via a normally closed, DC motor-operated mechanical trip and throttle valve. De-energizing one of the redundant control solenoids will vent air from the "fail open" valve operators allowing these isolation valves to open and admit steam to the TDP. The steam is supplied by steam generators B and C.

Both the air-operated (AOV) and motor-operated (MOV) flow control valves (FCV) are normally open. The AOVs are fail-open and the motor-operated FCVs fail as is. Half of the valves (4 valves) are powered from Class IE Load Group 1 and the other 4 valves are powered from Class IE Load Group 4 (see Figure 2-1).

2.3 Emergency Operation

The AFWS is designed for automatic actuation in the event of an emergency. Any one of the following conditions will automatically start both motor-driven pumps:

- A. Two out of four low-low level signals in any one steam generator.
- B. Trip of both main feedwater pumps.
- C. Safeguards sequence signal (initiated by safety injection signal).
- D. Class 1E bus loss of voltage sequence signal.

The turbine-driven pump is automatically actuated on either of the following signals:

- A. Two out of four low-low level signals in any two steam generators.
-
- B. Under voltage conditions on any two out of four reactor coolant pump feeder potential transformer cubicles.

Additionally, the AFWS is capable of remote-manual actuation.

In case of failure of the CST water supply, the normally closed, motor-operated butterfly valves from the ESWS are automatically opened on low suction header pressure.

2.4 Power Sources

Each SNUPPS unit is provided with a Class IE AC and DC power system.

The Class IE AC system distributes power at 4.16 kv, 480v, 208/120v, and 120 v to all safety-related loads. The Class IE AC system (see Figure 2-3) consists of the following features:

Power Supply Feeders:

Each Class IE 4.16 kv load group (two in each unit) is supplied by a separate preferred power supply feeders and one diesel generator (standby) supply feeder. Each 4.16 kv bus supplies motor loads and 4.0 kv/480 v load center transformers with their associated 480 v buses.

Bus Arrangement:

The Class IE AC system is divided into two redundant load groups per unit (load groups 1 and 2). For each unit, each AC load group consists of a 4.16 kv bus, two 480 v load centers, 480 v motor control center, and lower voltage AC supplies.

No provisions exist for automatically connecting one Class IE load group to another redundant Class IE load group or automatically transferring loads between load group.

The Class IE switchgear, load centers, and motor control centers for the redundant load groups are located in separate rooms of the control building to ensure physical separation.

Although the power distribution system is described in some detail, the failure of breakers and buses was not explicitly treated in the reliability evaluation.

Instrumentation and Control:

The DC control supplies for switchgear breaker operation are separate and independent so that Class IE DC load group 1 supplies Class IE load group 1 switchgear. The battery chargers for DC load group 1 are fed from the same load group switchgear. Class IE DC load group 2 supplies Class IE AC load group 2 switchgear.

Diesel Generators:

The standby power supply for each safety-related load group consists of one diesel generator complete with its accessories and fuel storage and transfer systems. One diesel generator is connected exclusively to a single 4.16 kv safety feature bus of a load group. The diesel generators are housed in separate rooms of a seismic Category I structure which ensures physical separation for fire and missile protection. Power and control cables for the diesel generators and associated switchgear are routed to maintain physical separation.

2.4.1 Vital Instrument AC Power Supply

Four independent Class IE 120v AC vital instrument power supplies are provided to supply the four channels of protection systems and reactor control systems. Each vital instrument AC power supply consists of one

inverter, one distribution bus, and one manual transfer switch. Each inverter is supplied by a Class IE battery system.

2.4.2 Class IE DC Power System

The Class IE DC system provides DC electric power to the Class IE DC loads and for control and switching of the Class IE systems. Physical separation, electrical isolation, and redundancy are provided to comply with the requirements of IEEE-308. The four Class IE DC subsystems are shown in Figure 2-4. Subsystems 1 and 4 provide control power for AC Load Groups 1 and 2, respectively. Each Class IE DC power subsystem consists of one 125v battery, one battery charger, one inverter, and distribution switchboards.

The Class IE batteries, chargers, and DC switch gear of each separate group are located in separate rooms of the seismic Category I control building. Chargers and DC switchgear are in separate rooms for the batteries.

2.5 Information Available to Operator

In addition to control room instrumentation showing the water level and pressure in individual steam generators, the operator is provided with the following information relating to the auxiliary feedwater system:

<u>Indication/Control</u>	<u>Control Room</u>	<u>Local</u> ⁽¹⁾	<u>Control Room Alarm</u>
Condensate storage tank suction MOV valve position	X	X	
ESW suction MOV valve position	X	X	
Condensate storage tank level	X	X	X
Condensate storage tank suction header pressure	X		
Low pump suction pressure	X	X	X
Low pump discharge pressure	X	X	X
Pump flow control valve operation	X	X	
Pump flow control valve position	X	X	
Auxiliary feedwater flow	X	X	

<u>Indication/Control</u>	<u>Control Room</u>	<u>Local</u> ⁽¹⁾	<u>Control Room Alarm</u>
Auxiliary feedwater pump turbine trip & throttle valve position	X	X	
Auxiliary feedwater pump turbine speed	X	X	
Auxiliary feedwater pump turbine low lube oil pressure			X
Auxiliary feedwater pump turbine high lube oil temperature			X

(1) Local control here means the auxiliary shutdown panel.

2.6 Technical Specifications

A review of the Standard Technical Specifications (Reference 8) indicates that for power, start-up, or hot standby plant status the limiting condition of the AFWS for plant operation include:

1. At least three independent auxiliary feedwater pumps and associated flow paths shall be operable with:

- a. Two motor-driven AFW pumps, each capable of being powered from separate emergency buses, and,
- b. One turbine-driven AFW pump capable of being powered from an operable steam supply system.

2. Action

- a. With one auxiliary feedwater pump inoperable, restore at least three AFW pumps (two capable of being powered from separate emergency buses and one capable of being powered by an operable steam supply system) to an OPERABLE status within 72 hours or be in at least HOT STANDBY condition within the next 6 hours and in a HOT SHUTDOWN within the following 6 hours.

- b. With two auxiliary feedwater pumps inoperable, be in at least HOT STANDBY within 6 hours and in HOT SHUTDOWN within the following 6 hours.
- c. With three auxiliary feedwater pumps inoperable, immediately initiate corrective action to restore at least one auxiliary feedwater pump to OPERABLE status as soon as possible.

To satisfy specified surveillance requirements, each auxiliary feedwater pump shall be demonstrated OPERABLE:

- 1. At least once per 31 days by:
 - a. Verifying that each motor-driven pump develops a discharge pressure of greater than or equal to (later) psig at a flow of greater than or equal to (later) gpm.
 - b. Verifying that the steam turbine-driven pump develops a discharge pressure of greater than or equal to (later) psig at a flow of greater than or equal to (later) gpm when the secondary steam supply pressure is greater than (later) psig.
 - c. Verifying that each non-automatic valve in the flow path that is not locked, sealed, or otherwise secured in position, is in its correct position.
 - d. Verifying that each automatic valve in the flow path is in the fully open position whenever the auxiliary feedwater system is placed in automatic control or when above 10 percent of RATED THERMAL POWER.
- 2. At least once per 18 months during shutdown by:
 - a. Verifying that each motor-driven pump starts automatically upon receipt of each of the following test signals:

1. Loss of both main feedwater pumps.
 2. Safety injection signal.
 3. Two out of four low-low level signals in any one steam generator.
 4. Class IE bus loss of voltage sequence signal.
- b. Verifying that the steam turbine-driven pump starts automatically upon receipt of each of the following test signals:
1. Undervoltage conditions on any two out of four reactor coolant pump feeder potential transformer cubicles.
 2. Two out of four low-low level signals in any two steam generators.
- c. Verifying that the valve in the suction line of each auxiliary feedwater pump from the Essential Service Water System automatically actuates to its full open position on a low suction pressure test signal.

DOCUMENT/ PAGE PULLED

ANO. 8106090 644

NO. OF PAGES 1

REASON

☐ PAGE ILLEGIBLE

☐ HARD COPY FILED AT PDR CF

OTHER _____

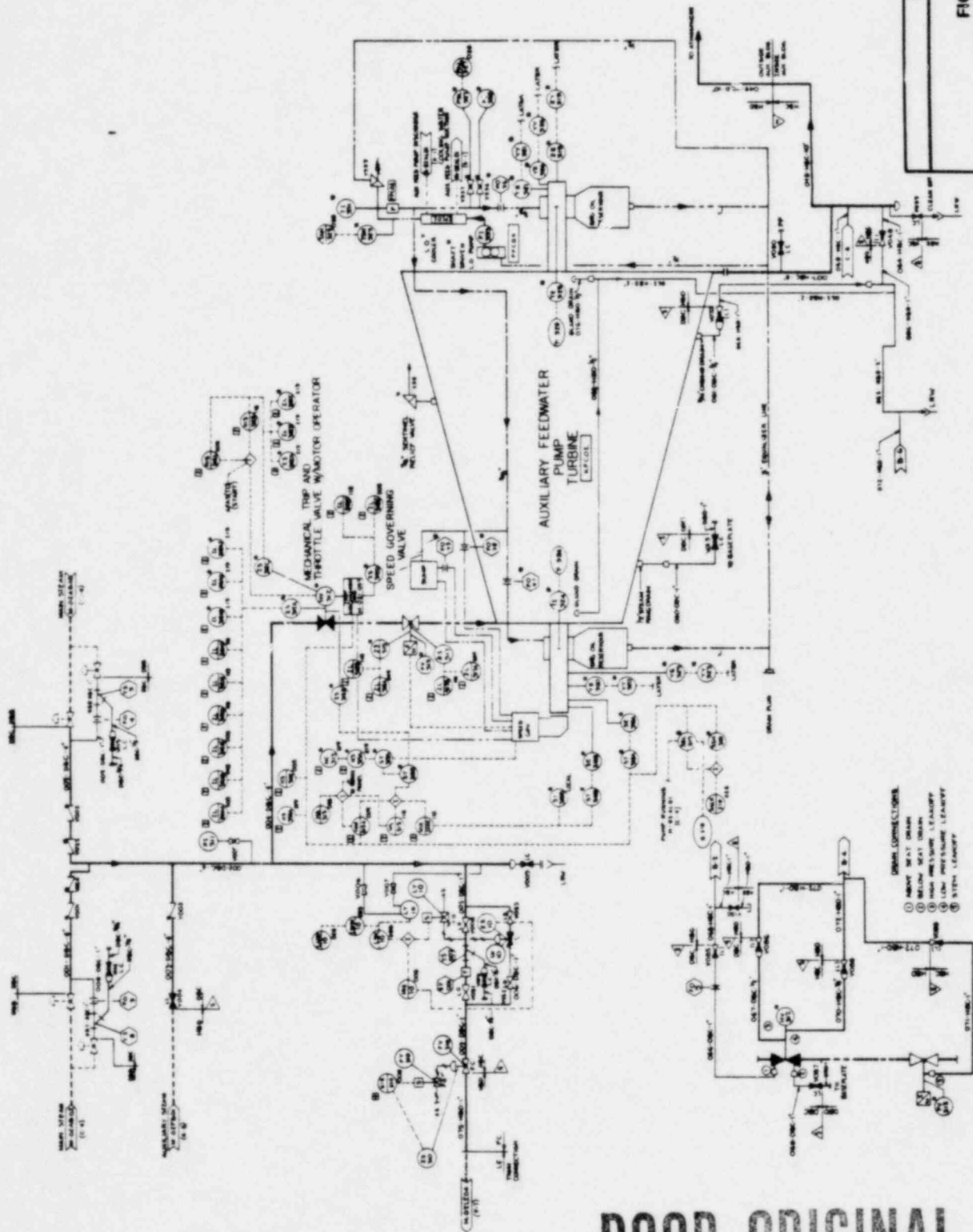
☐ BETTER COPY REQUESTED ON 1/1/1

☐ PAGE TOO LARGE TO FILM

☒ HARD COPY FILED AT PDR CF

OTHER _____

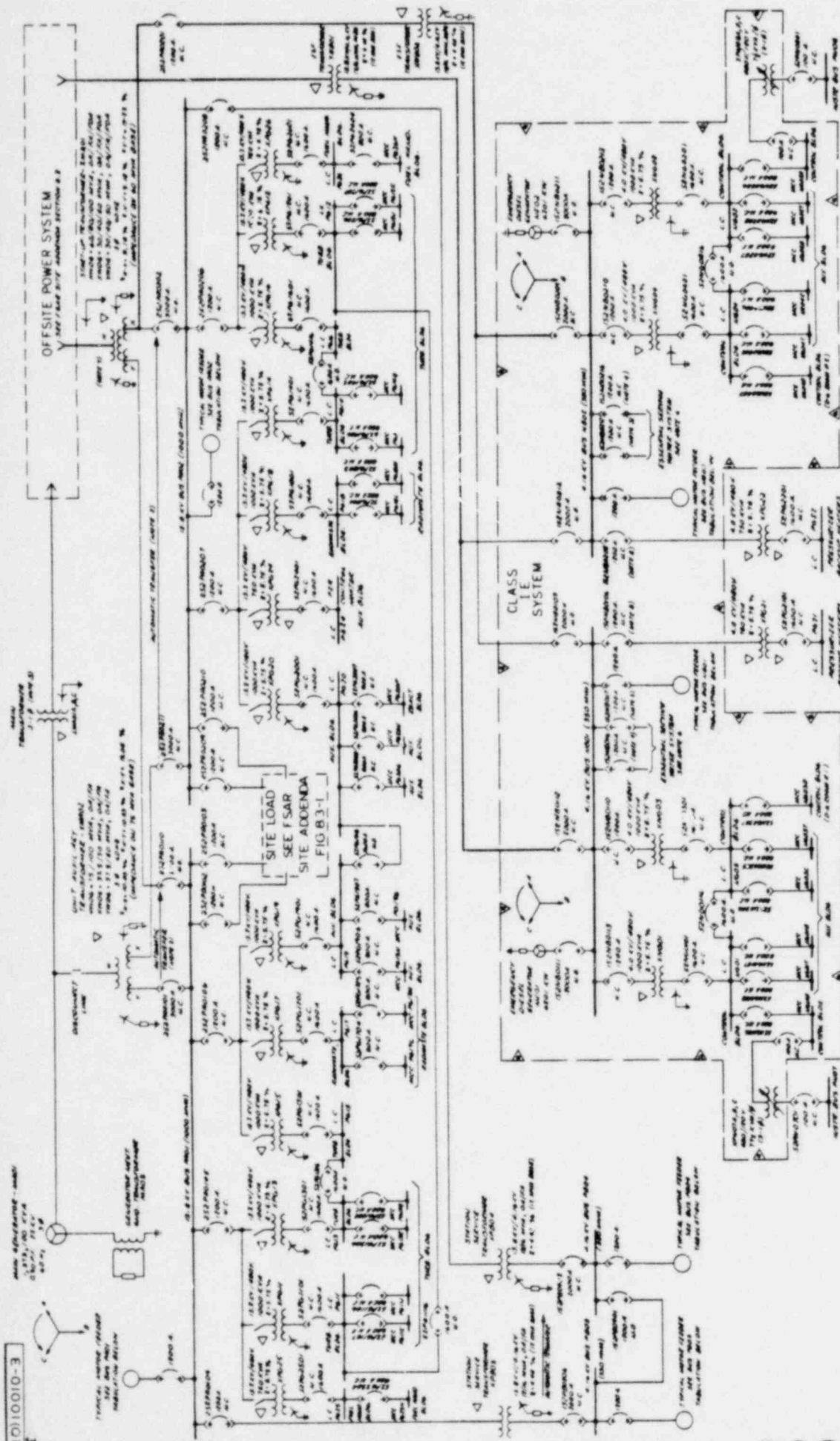
☒ FILMED ON APERTURE CARD NO 8106090644



SNUPPS

FIGURE 2-2
AUXILIARY FEEDWATER
PUMP TURBINE
(M-02FC02-6)

POOR ORIGINAL



Rev. 1
9/80

SNUPPS

FIGURE 2-3

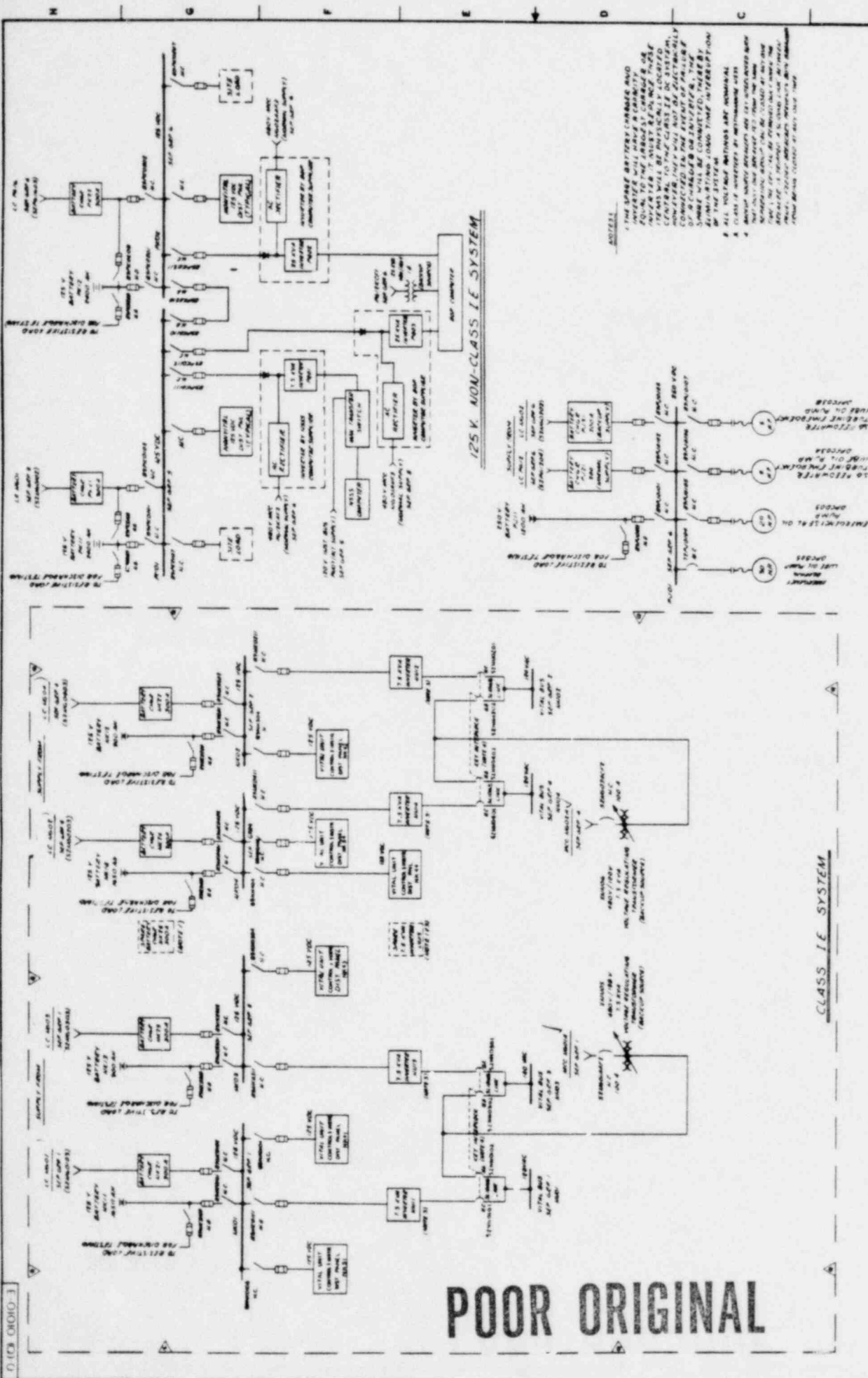
MAIN SINGLE LINE DIAGRAM

(E-01001-3)

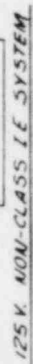
1. OFFSITE POWER SYSTEM IS DESCRIBED IN SNUPPS, E-01001-1.
2. CLASS 1E SYSTEM IS DESCRIBED IN SNUPPS, E-01001-2.
3. SITE LOAD IS DESCRIBED IN SNUPPS, E-01001-3.
4. THIS DIAGRAM IS A SUMMARY OF THE MAIN SINGLE LINE DIAGRAM.
5. THIS DIAGRAM IS A SUMMARY OF THE MAIN SINGLE LINE DIAGRAM.
6. THIS DIAGRAM IS A SUMMARY OF THE MAIN SINGLE LINE DIAGRAM.
7. THIS DIAGRAM IS A SUMMARY OF THE MAIN SINGLE LINE DIAGRAM.
8. THIS DIAGRAM IS A SUMMARY OF THE MAIN SINGLE LINE DIAGRAM.
9. THIS DIAGRAM IS A SUMMARY OF THE MAIN SINGLE LINE DIAGRAM.
10. THIS DIAGRAM IS A SUMMARY OF THE MAIN SINGLE LINE DIAGRAM.

DESCRIPTION	UNIT	REMARKS
13.8 kV BUS	1	13.8 kV BUS
4.16 kV BUS	1	4.16 kV BUS
120 V BUS	1	120 V BUS
240 V BUS	1	240 V BUS
480 V BUS	1	480 V BUS
600 V BUS	1	600 V BUS
720 V BUS	1	720 V BUS
840 V BUS	1	840 V BUS
960 V BUS	1	960 V BUS
1080 V BUS	1	1080 V BUS
1200 V BUS	1	1200 V BUS
1320 V BUS	1	1320 V BUS
1440 V BUS	1	1440 V BUS
1560 V BUS	1	1560 V BUS
1680 V BUS	1	1680 V BUS
1800 V BUS	1	1800 V BUS
1920 V BUS	1	1920 V BUS
2040 V BUS	1	2040 V BUS
2160 V BUS	1	2160 V BUS
2280 V BUS	1	2280 V BUS
2400 V BUS	1	2400 V BUS
2520 V BUS	1	2520 V BUS
2640 V BUS	1	2640 V BUS
2760 V BUS	1	2760 V BUS
2880 V BUS	1	2880 V BUS
3000 V BUS	1	3000 V BUS

POOR ORIGINAL



250 V. NON-CLASS I'E SYSTEM



4507499 0

[illegible][illegible]

SNUPPS

FIGURE 2-4
DC MAIN SINGLE
LINE DIAGRAM
(E-01010-1)

3.0 Methodology

In this section the actual step-by-step procedure followed in performing the AFWS reliability study will be presented.

3.1 System Review/Study Bounds

In this first step the various drawings, P&ID's and schematics representing the SNUPPS AFWS were examined along with the FSAR and systems descriptions. Special attention was given to identifying the following:

1. Instrumentation systems required for success.
2. Fluid systems connected directly or indirectly to the AFWS.
3. HVAC systems required and their power sources.
4. The power sources of each of the components.
5. Any obvious single point vulnerabilities.

The reliability information described in Appendix III of NUREG-0611 was then appraised and AFWS studies performed for other facilities were reviewed. Since plant technical specifications did not exist when the study was initiated, the applicable requirements from the Standard Technical Specification (Reference 8) were assumed. Additionally, a review was made of the LER Summaries and NPRDS data to select failure data for some of the events not identified in the NUREG-0611 data base (see Appendix B).

Based on the above information, the bounds of the study were set, level of resolution decided upon, and the assumptions stated, to form the foundation for the subsequent analysis.

3.2 Fault Trees

The fault trees were constructed (see Appendix A). In constructing the trees an effort was made to minimize the number of events explicitly identified

on the tree. This was accomplished by combining many of the basic events, which would be found under a single OR -gate, into a single composite basic event (CBE) (see Appendix B). In this way, a tree containing a manageable number of events was constructed which preserved the fault propagation within and between systems. When coalescing basic events into composite events, it was important to ensure that no event appearing in a composite event may appear elsewhere in the tree, unless the entire composite event recurs as a unit.

3.3 Minimal Cut-Sets

The fault tree was evaluated down to the level of composite basic events and the "subtrees" 77, 88 and 99; the "subtrees" are indicated by the transfer symbols on the fault trees presented in Appendix A. Coalescing the basic events into composite basic events results in a significant reduction in the number of cut-sets generated and required to be truncated. It was possible to reduce the resulting 2916 Boolean Indicated Cut-Sets (BICS) down to 9 three-event cut-sets (see Appendix C). Finally, the minimal cut-sets representing the "subtree-events" 77, 88 and 99 were substituted to resolve the fault tree to the level of composite basic events. These BICS were the basis of the subsequent quantification of the system.

3.4 Fault Tree Quantification

During this phase of the study, the BICS were processed in conjunction with the various event probabilities as defined in Appendix B. The probability of the top event was calculated by the following conservative first order approximation:

$$P(\text{TOP}) = 1 - \prod [1 - P(\text{ith cut set})]$$

3.5 Importance Evaluation

To identify the dominant failure modes of the SNUPPS AFWS, the importance of various events and groups of events was computed. The Importance of event E, I_E , is the probability that event E is contributing to the top

event failure, given the top event is failed (Reference 14). To perform the actual computation of the Importance, it was necessary to inspect the cut-sets of the various cases for events of interest and then to sum the probabilities. Finally, to obtain the Importance, the total probability of the selected cut-sets is divided by the top event probability.

The actual Importances for the various cases and options are presented in Section 5.2. In that section, the Importance of some of the events are further categorized. Testing is distinguished from maintenance, actuation failure from hardware failure, and human error is distinguished from hardware faults. In Figures 5-3, 5-4, 5-5, the relative Importance of various events is displayed on bar charts.

3.6 Common Cause Failure

The evaluation of common cause failures was approached in two phases. In the first phase those areas which historically have been associated with common cause failures, i.e., diesel generators, common location of components belonging to different trains were examined. In addition to examining P&IDs and other drawings, extensive examination was made of the SNUPPS model (a completely detailed one-sixteenth scale model). It was concluded that human error was the only significant secondary cause and that other secondary causes, such as grit, temperature, manufacture, vibration, etc., would be insignificant in comparison. In the second phase, an attempt was made to quantify the effect and importance of the human error induced common cause failures. A more detailed discussion of the common cause failure evaluation is given in Section 4.

3.7 Interfacing Systems Failures

Finally, the effects on system reliability of expanding the bounds of the study to include two interfacing systems were examined. Because of their potential for diverting large portions of the water required by the steam generators, the main feedwater system and the service water system were the two interfacing systems examined. For the main feedwater system, the failure mode considered was failure of the main feedwater isolation valve coincident

with pipe break (i.e., $P = 1.0$) in the feedwater system. The failure treated in the service water system was failure of the redundant service water isolation valves coincident with an assumed pipe break. A discussion and the results of this evaluation can be found in Section 5.4.

4.0 Common Cause Failure Evaluation

The evaluation of potential common cause failures (CCF) was broken into two parts. The first part was an initial screening in which P&IDs, systems descriptions, and the SNUPPS Model were examined for items which generally are associated with common cause failures, i.e., diesel generators, common location of pumps and valves belonging to different trains. Due to the high degree of separation, the initial screening did not identify any potential for secondary causes, such as, grit, vibration, stress, temperatures. The only potential secondary causes which could be identified were common manufacture and human error during test and maintenance. The former was not considered to be a significant cause because any gross manufacturing errors would be expected to be found in the pre-operational testing and any subtle common manufacturing defects would most likely appear as an increase in the random failure rate. Therefore, human error was the only secondary cause likely to be significant which could be explicitly identified and could be conservatively quantified based on the information provided in NUREG-0611.

4.1 Hardware

Diesel Generators:

Significant redundancy and separation of systems supporting the diesel generators was verified; separate fuel tanks, fuel lines, air intakes, exhausts, etc. Two potential common causes always associated with DGs are extreme low temperature and contaminated fuel. Potential failure from the first cause is greatly decreased for SNUPPS because the air intakes are within the DG rooms and the fuel tanks are located below the frostline; also, the fuel lines drain back to the fuel tanks, so they are dry when not in use. The problem with contaminated fuel is reduced by the presence of many filters and strainers throughout the fuel system with pressure differential switches and indicators. Also, the standard technical specifications require the diesel generators be tested at least once per 31 days.

Essential Service Water System:

Redundancy and separation of the ESWS was verified. An area of concern with the ESWS was the potential for debris blocking the ESWS intake. However, it was concluded that the large quantities of debris necessary to produce substantial blockage could not be generated. Problems with ice cover are eliminated by taking water from substantially below the surface and by the addition of warming water.

Pump and Valves:

The pumps and valves of the three AFWS trains are located in distinct rooms and valve compartment.

HVAC:

Each MDP train has a separate ventilation system operating from the same Class IE load group as the pump/valve room it serves. Since the TDP must operate with a complete loss of AC power, the TDP and associated controls are qualified to operate without ventilation. Tests will be performed to demonstrate that pump room ambient conditions (e.g., temperature, humidity) do not exceed environmental qualification limits for equipment in the AFWS.

Electrical Equipment:

All Class IE AC and DC equipment (e.g., load centers, MCC, etc.) are located in separate rooms to ensure physical separation.

4.2 Human Error

Next, common cause failures associated with human error were investigated. Any redundant systems or components which also contained manual valves were considered prime candidates. All the CCFs treated were associated with mispositioning the locked open manual valves that must be periodically closed for test and maintenance. There was no CCF quantified for the actual test

and maintenance of components but, a consistent error by an individual performing test and maintenance on all three trains could hypothetically disable the entire AFWS. The following events were identified:

	<u>Events</u>
1. Loss of steam from SG B and SG C (to the TDP)	44 45
2. Loss of ESWS train A and ESWS train B	41 42
3. Loss of discharge valves V031, V043, and V055	20 21 22

All of these events have human error contributions (i.e., manual valves) for option B and C. Options A, B, And C are defined in Appendix B. The top event probabilities and Importances were constructed as cut-sets containing these events to various degrees. The implicit assumption in these quantifications was that the events are statistically independent; that is, no statistical coupling exists between the events. This is a lower bound estimate. One could obtain an upper bound by assuming complete coupling within the event sets given above. This is equivalent to assigning a single event probability to the coincident occurrence of two events. That is, if the operator neglects to re-open one manual discharge valve, he would also neglect to re-open the corresponding valve in the other train.

However, in this study the only effect examined was that of using the values given in NUREG-0611 for the coupling of human errors. These values represent less coupling than mentioned in the preceeding paragraph. The information presented in Table III-2 of NUREG-0611 implies a coupling factor of .2 and .3 for options B and C, respectively. This approach is consistent with WASH-1400 in which the mean of an assumed log-normal distribution of values between the statistically independent case and the complete coupling case was assumed. For example, for events 44 and 45, the human error probability component for option B is 5×10^{-3} and the hardware failure probability is 2×10^{-3} ; then, the following values can be assigned to the coincident occurrence of events 44 and 45 based on the degree of statistical coupling:

$$\text{Statistically Independent: } (2 \times 10^{-3} + 5 \times 10^{-3})(2 \times 10^{-3} + 5 \times 10^{-3}) = 4.9 \times 10^{-5}$$

$$\text{Complete Coupling: } (1)(2 \times 10^{-3} + 5 \times 10^{-3}) = 7.0 \times 10^{-3}$$

$$\text{Partial Coupling: } (2 \times 10^{-3} + .2)(2 \times 10^{-3} + 5 \times 10^{-3}) = 1.4 \times 10^{-3}$$

The approach was to select those () sets (≤ 4 events) containing the coincident occurrence of the events of interest. Then, the procedure was to recalculate the cut-set and total probability using the method described in the preceding paragraph.

5.0 Results of the Reliability Evaluation

5.1 AFW System Reliability

5.1.1 Qualitative Evaluation

Figure 5-1 is a reproduction of the reliability characteristics chart presented in NUREG-0611 for AFW designs in plants using the Westinghouse NSSS with a row added which presents the results of a qualitative evaluation of the SNUPPS AFWS reliability. The intent of the figure is to show the relative reliability ranking of the SNUPPS AFWS for each of the three cases studied and to compare these results to those obtained by the NRC. This qualitative evaluation is included to complement the results of the quantitative analysis which are discussed in the next section. The qualitative evaluation described below was performed by comparing the SNUPPS AFWS design to similar designs evaluated in NUREG-0611. The NUREG-0611 plants characterized by high reliability were used as a reference in performing the following qualitative evaluation:

In characterizing the reliability of AFW systems NUREG-0611 generally implies that the following traits exist for specific reliability ratings:

1. Loss of Main Feedwater (SNUPPS - High Reliability Characterization)

<u>Low Reliability</u>	<u>Medium Reliability</u>	<u>High Reliability</u>
a. Manual System Actuation	a. Auto actuation with manual backup	a. Auto actuation with manual backup
b. Two-pump system	b. Single point vulnerabilities may be present	b. No single point vulnerabilities present
c. Single point vulnerabilities present	c. Technical specifications permit unlimited outage time	c. High system redundancy
d. Technical specifications permit unlimited outage time for system maintenance, test, etc		d. Low reliance on operator action (human error)

The NUREG-0611 plants used in this study are classified in the high reliability range for this transient. Generally, the system consists of three AFW pumps (two motor and one steam) and is actuated automatically when required.

2. Loss of Main Feedwater with Loss of Offsite Power
(SNUPPS - High Reliability Characterization)

The reliability classification of a specific plant under this transient is basically the same as for the previous LOFW event. The major difference being that onsite AC power sources are now accounted for and the system evaluated for the possible degradation of onsite AC power (i.e., loss of one of two diesel generators).

3. Loss of Main Feedwater with Loss of All AC Power
(SNUPPS - High Reliability Characterization)

Low and medium reliability classifications under this event are generally due to systems having strong AC power dependencies in the steam turbine driven pump train. Such dependencies may include lube oil cooling, AC power to steam turbine admission valves, or air-operated valves which fail closed on loss of air. Those systems characterized as having a relatively high reliability generally are automatically actuated and have no potentially degrading AC power dependencies.

In comparing the SNUPPS AFWS to the NUREG-0611 plants which have a high reliability characterization, the SNUPPS design has a similar reliability in that the turbine pump train has no AC dependencies in order to function normally.

5.1.2 Quantitative Evaluation

Figure 5-2 presents the SNUPPS AFWS reliability characteristics based on the quantitative evaluation. This quantitative evaluation encompassed not only a computation of relative reliability for comparison with NUREG-0611 but also an examination of the sensitivity of the AFWS reliability to various assumptions concerning human error and diesel generator availability. The "base" case for making a comparison with NUREG-0611 is Option A (i.e., no explicit human errors) with only one diesel generator capable of failure (i.e. row 1). In rows 3, 4, and 5, the effects of various levels of human error (i.e., Options A, B, and C) coupled with the potential failure of either diesel generator are presented.

Rows 6 through 11 of Figure 5-2 present the AFWS reliability characteristics for human error induced common cause failures in the identified systems. As indicated in rows 6 through 9, the inadvertent closing of both manual valves in the steam lines to the turbine-driven pump has a minimal effect on the system reliability while failure of the essential service water system (ESWS) due to mispositioning manual valves has a significant impact only for Class 1. Finally, it is clear from the results indicated in rows 10 and 11 that the inadvertent closing of the manual discharge valves in two AFW trains produces the lowest system reliability of all the options presented.

5.2 Importance Evaluation of Events (Reference 14)

Calculating the Importance values for events or groups of events permits quantification of the dominant and potentially dominant failure modes of the system.

$$\text{Importance } (I_E) = \frac{\sum P_k(E)}{P(\text{TOP})}$$

where,

$P(\text{TOP})$ - Probability of the Top Event (AFWS failure) for a particular case/option.

$\sum P_k(E)$ - Summation of probabilities of k minimal cut-sets which contributes to the Top Event and which contain the event E .

Importance (I_E) - The Importance of event E , I_E , is the probability, that event E is contributing to the top event failure.

The method used to compute the Importances was to first select the cut-sets containing events of interest and then to calculate the total probability of the selected cut-sets. Finally, to obtain the Importance, this $\sum P_k(E)$ for the selected cut-sets was divided by the $P(\text{TOP})$. The relative Importance for the events of interest are displayed on bar-charts in Figures 5-3, 5-4, 5-5.

Although the various events shown on the figures were presented on the fault trees given in Appendix A and were described in more detail in Appendix B, a brief description is given below:

- o Test and Maintenance: Unavailability due to test and maintenance outages except for test and maintenance of the diesels.
- o Actuation Failure: An actuation failure probability of 7×10^{-3} per demand per AFWS train.
- o Pump Failure: Represents all failure modes other than actuation failure.
- o Human Error: This category includes all those events (excluding event 26: CST Isolation Valve) which have human error as one of the contributors to the composite basic event probability and is associated with mispositioning of manual valves.
- o Throttle/Governor Valve: Control faults and plugging in the turbine-driven pump's throttle valve or speed governor valve.
- o Diesel Generator: The failure of the diesels consists of failure on demand, as well as, test and maintenance outage for the diesels.
- o CST Isolation Valve: This item includes human error for failure to maintain the valve locked opened in addition to a small plugging probability. The plugging contribution is so negligible in relation to the other events that for Option A (i.e., no human error), Figure 5-3, the bar-chart shows a line representing a negligible Importance.

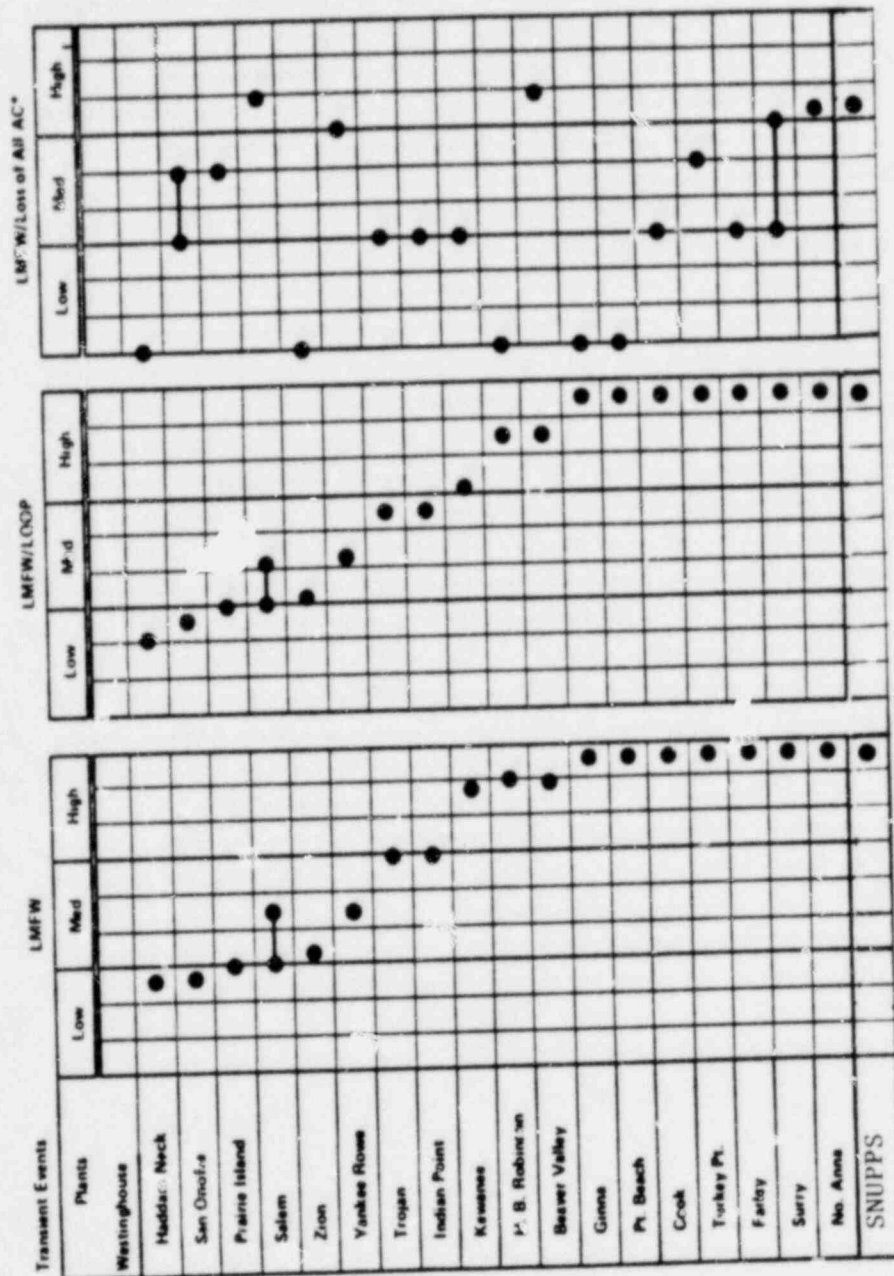


Figure 5-1. Qualitative Comparison of the Reliability Characteristics for APUS Regions in Plants Using the Westinghouse NSSS (including SNUPPS)

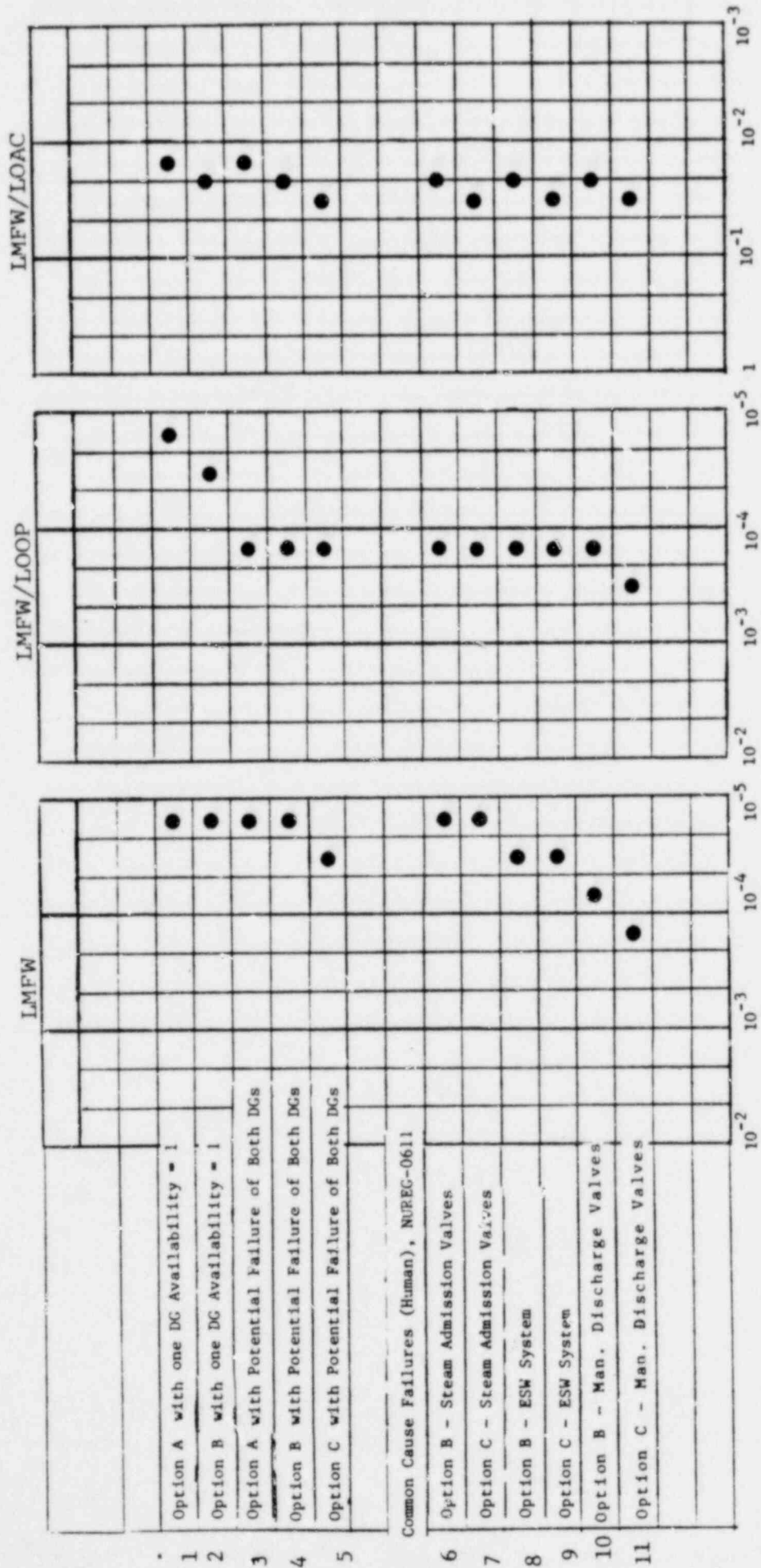


Figure 5-2. Quantification of the Reliability Characteristics of the SNUPPS AFWS for Various Options

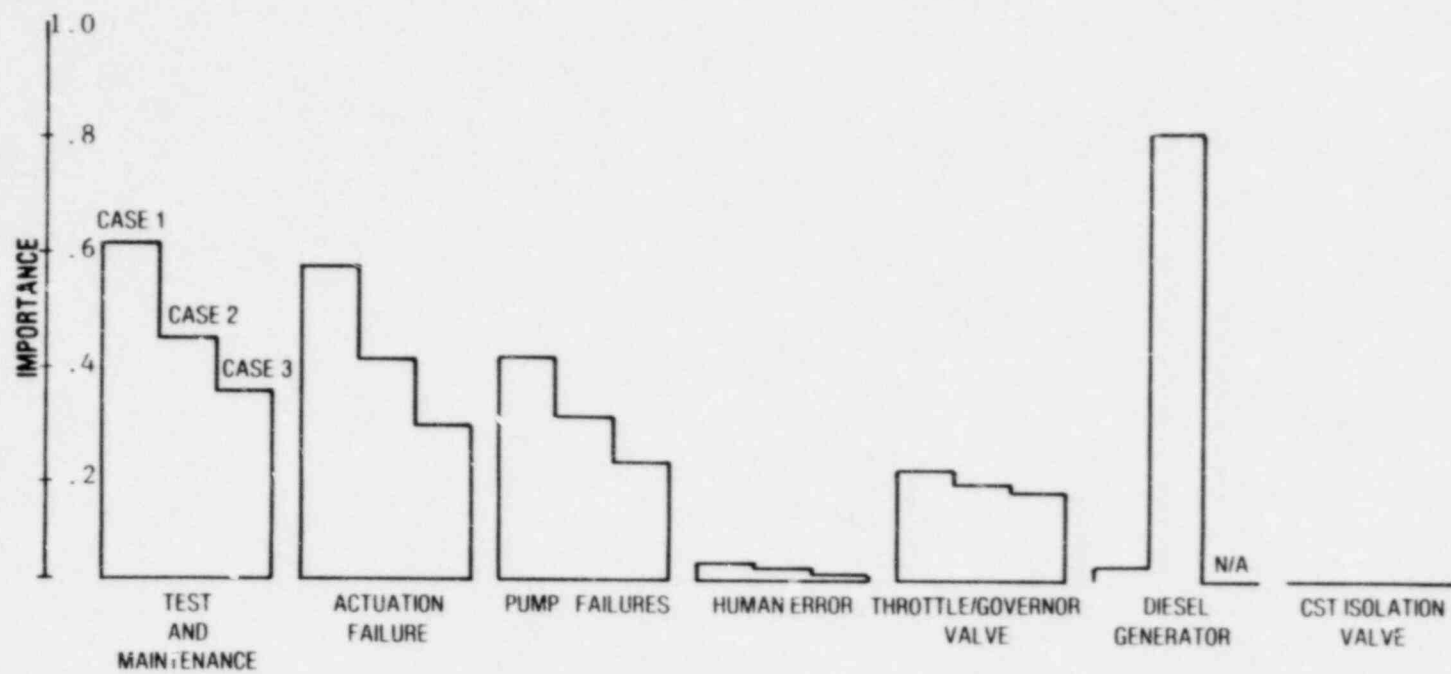


Figure 5-3: Importance of Selected Events for Option A

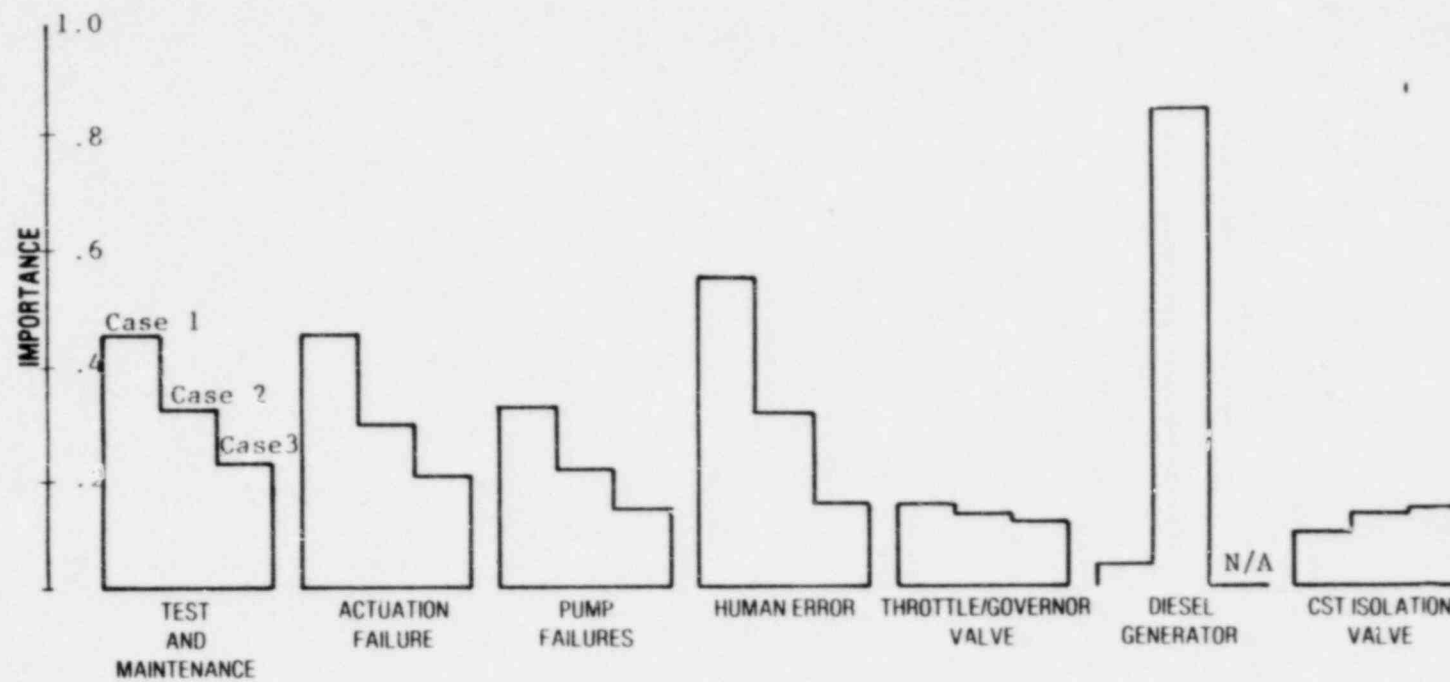


Figure 5-4. Importance of Selected Events for Option B

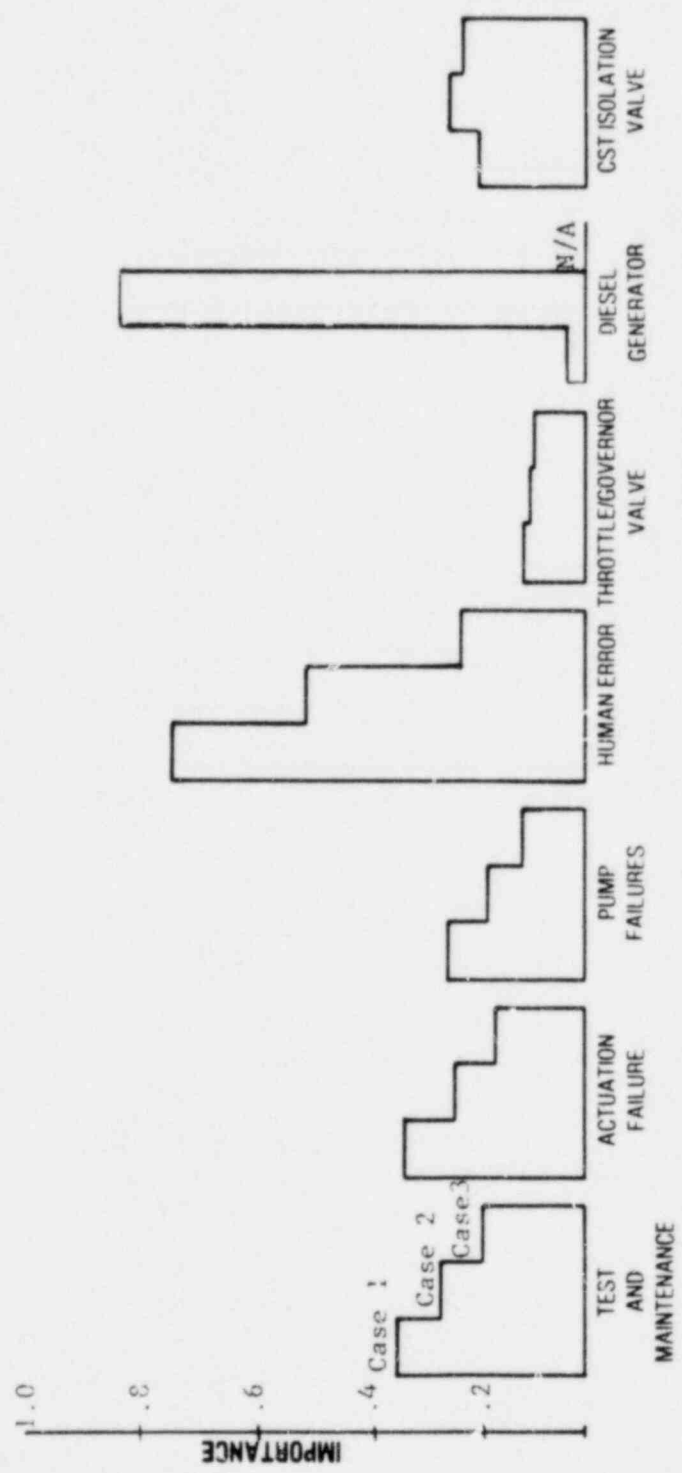


Figure 5-5. Importance of Selected Events for Option C

5.2 Dominant Failure Modes

Loss of Main Feedwater (with offsite power available):

The resulting unavailability of the AFWS for this scenario is in the upper interval of the 10^{-4} to 10^{-5} range. The system unavailability during this transient is dominated by several combinations of three event cut-sets. These include test and maintenance outages and hardware failures in various combinations along with failure of the CST isolation valve and the ESWS. This conclusion is supported by the Importances indicated in Figure 5-3, 5-4 and 5-5.

Test and maintenance outages of the motor-driven pump and turbine-driven pump are based on monthly pump tests, as well as a mean maintenance duration based on 72 hours of allowable inoperability. The hardware failures of the MDP trains include pump failure, in-line valve failures and control signal failure to the pumps. Additionally, human errors, which consisted of failures to maintain manual valves (in-line) in an open position during operation, were modelled for various probabilities, as discussed in Appendix B.

The turbine-driven pump was modelled in the same manner as the MDPs except that valve failures in the steam supply lines were included in the model.

Loss of Main Feedwater (with loss of offsite AC power):

Generally, the dominant failure contributors for this scenario are the same as in the previous transient except that failure of a motor-driven pump can result from the potential failure of the associated diesel-generator train. The resulting unavailability for this scenario is in the upper interval of the 10^{-4} to 10^{-5} range when one diesel generator is assumed available with a probability of 1.0. However, as can be seen in the third row of Figure 5-2, the results are sensitive to the failure probabilities assigned to the diesel generators.

Loss of Main Feedwater (with loss of all AC power):

The unavailability of AFWS for this scenario lies in the 10^{-1} to 10^{-2} range. Since in this scenario loss of both onsite and offsite AC power is postulated to occur, the AFWS is reduced to the single turbine-driven

pump train. The unavailability of the TDP train is dominated by five single events: test and maintenance, failure of the TDP, discharge valve left closed (human error), CST isolation valve left closed (human error), and failure of the steam supply throttle or speed governor valves. If a coupling of human error is assumed for the manual valves in the steam supply lines (i.e., a common cause failure), then failure of the steam supply becomes a sixth dominant failure mode.

As indicated by Figures 5-3, 5-4 and 5-5, the failure modes are approximately equal in Importance.

5.4 Interfacing Systems Failures

Main Feedwater System: The main feedwater isolation valves (FWIV) prevent the auxiliary feedwater from being diverted into the non-seismic/non-Q main feedwater system. A failure probability of 3×10^{-4} /demand was assigned to these valves. The inclusion of FWIV failures increases the failure probabilities assigned to events 9 through 12 from 2×10^{-4} to 5×10^{-4} . The effect of including this failure mode was to increase the failure probability for Case 1, Option A by 20% but did not change the reliability ranking as shown in row 1 of Figure 5-2. The effect for all other cases was less than 5%.

Service Water System: Including the failure of the redundant service water isolation valves had negligible impact on the AFWS reliability.

6.0 Conclusions/Recommendations

The results of this AFWS reliability study indicate that, on both a qualitative and quantitative basis, the SNUPPS auxiliary feedwater system has a high relative reliability. Although there were no significant hardware related weaknesses in the system, some of the human error potential could be reduced by implementation of the following recommendations:

- o Staggered Test and Maintenance for the driver-pumps and associated valves.
- o A strong procedure for checking the status of Locked Opened valves, particularly, the CST isolation valve and the pump-discharge valves.
- o There should be an LCO on the outage duration for any train of the essential service water system.

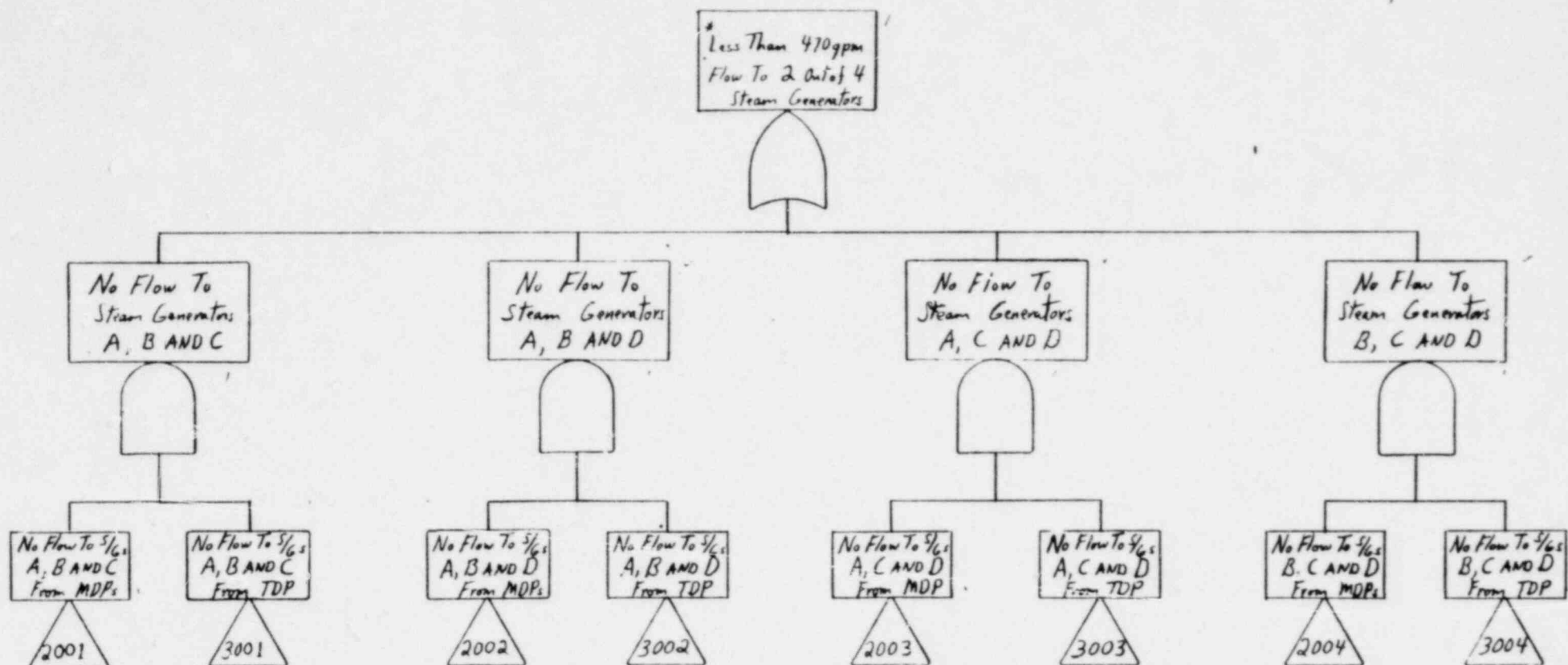
7.0 References

1. "Steam Systems Design Manual," Westinghouse (Project Information Package) Revision 2, August 1973
2. "Steam Systems Design Manual," Westinghouse (Standard Information Package, 10-1) Revision 3
3. SNUPPS-FSAR: Chapter 10, Section 10.4.9; Chapter 7, Chapter 8, Chapter 9, Section 9.2.1.2 (Figure 9.2-12, CST)
4. NUREG-0611, Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Westinghouse-Designed Operating Plants, January 1980, USNRC
5. March 10, 1980 Letter to All Pending Operating License Applicants from USNRC (Division of Project Management); Auxiliary Feedwater Systems
6. NUREG/CR-1362, "Data Summaries of Licensee Event Reports of Diesel Generators at U. S. Commercial Nuclear Power Plants; January 1, 1976 to December 31, 1978," March 1980, prepared by EG&G Idaho, Inc.
7. NUREG/CR-1363, Volume 1, "Data Summaries of Licensee Event Reports of Valves at U. S. Commercial Nuclear Power Plants; January 1, 1976 to December 31, 1978," June 1980, prepared by EG&G Idaho, Inc.
8. NUREG-0452, Revision 3, "Standard Technical Specifications for Westinghouse Pressurized Water Reactors," USNRC, Fall 1980
9. SNUPPS-FSAR: Figures 8.3-1, -2, -3 (Schematics E-01001-3, E-01005-4, E-01010-1) - Class 1E AC and DC System

10. System Description, "Auxiliary Feedwater System";
M-00AL(Q), Revision 3 (SNUPPS)
11. Reactor Safety Study, WASH-1400 (October 1975); Appendix III
- (Failure Data) and Appendix IV (Common Cause Failure)
12. NUREG/CR-1635, "Nuclear Plant Reliability Data System 1979
Annual Reports of Cumulative System and Component
Reliability," September 1980, prepared by Southwest
Research Institute
13. NUREG/CR-1464 (ORNL), "Review of Nuclear Power Plant Offsite
Power Source Reliability and Related Recommended Changes
to the NRC Rules and Regulations," May 1980
14. NUREG-0492, Fault Tree Handbook, USNRC, January 1981

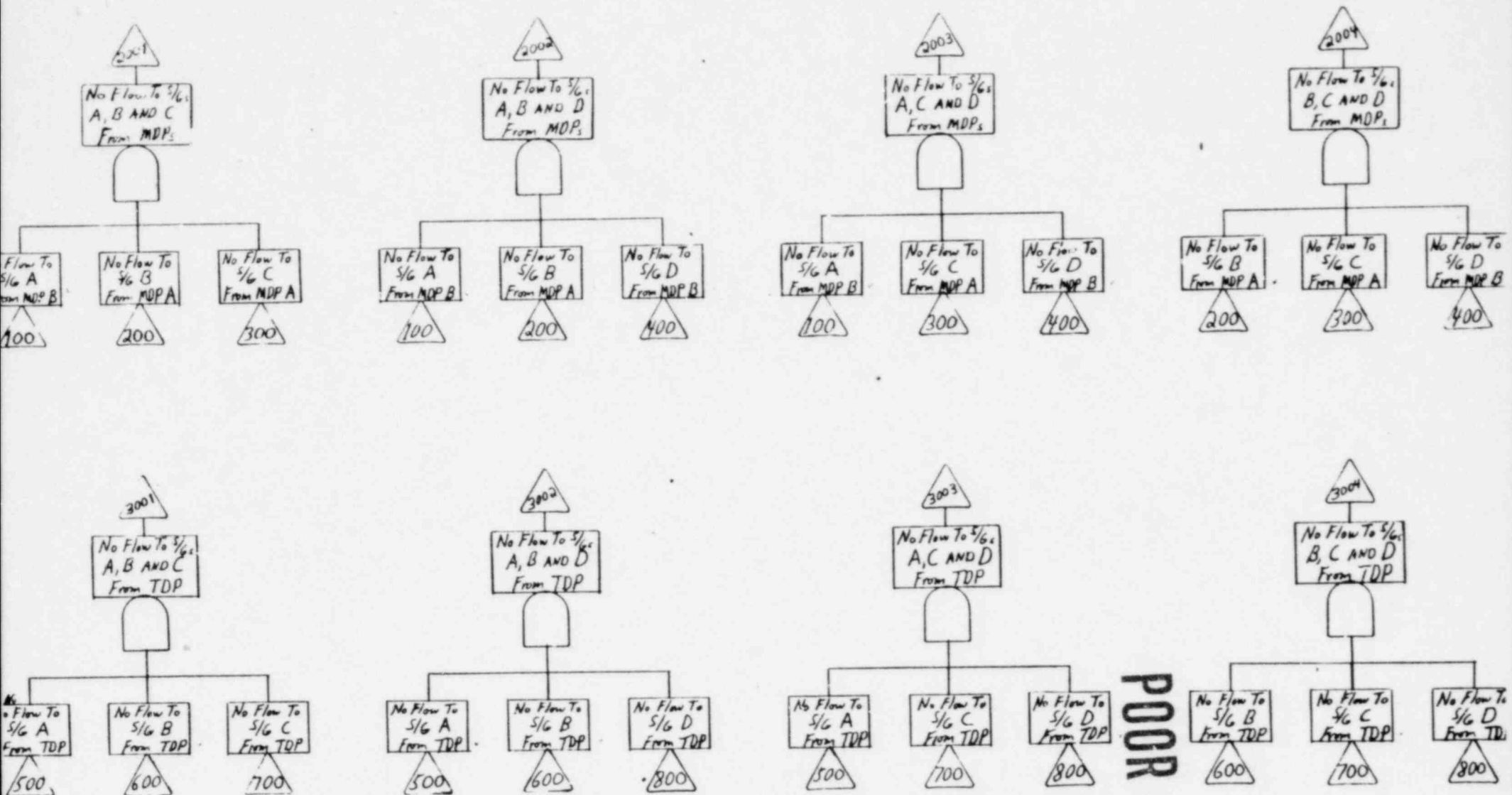
A P P E N D I X A

FAULT TREES

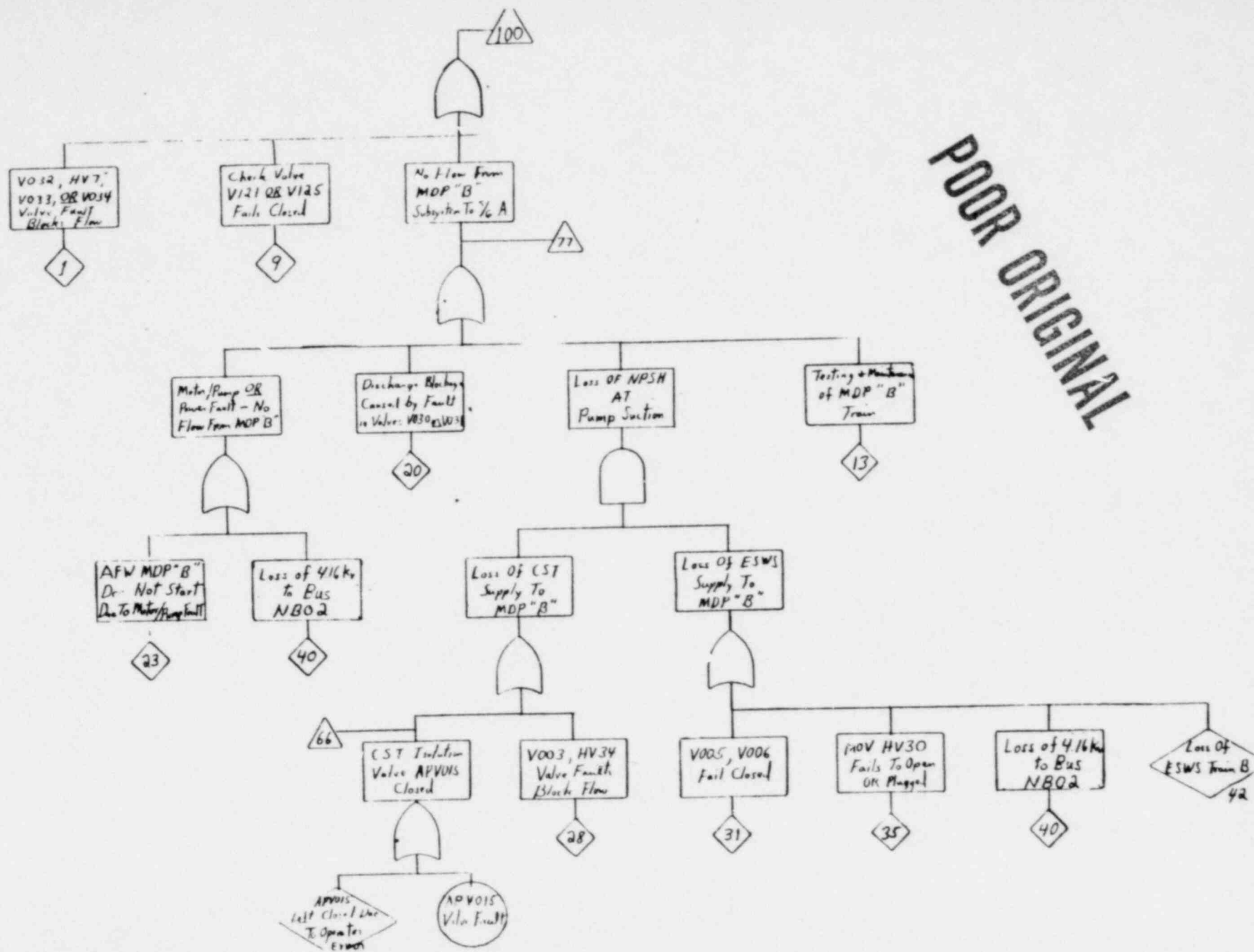


POOR ORIGINAL

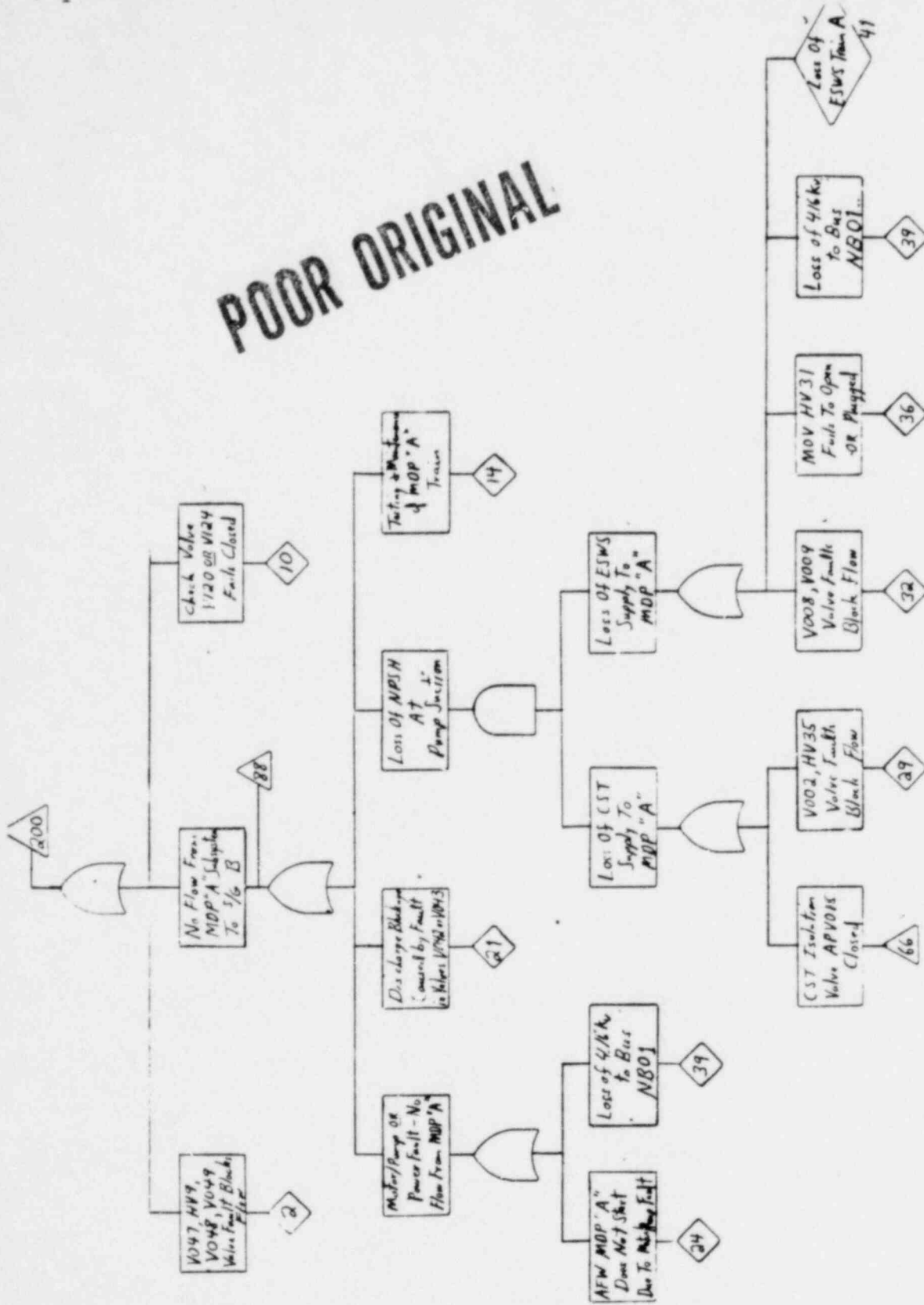
Actually modified as Zero flow to 2 out of 4
 within one minute because no credit taken for
 initial failures, i.e. a component was "on or off".



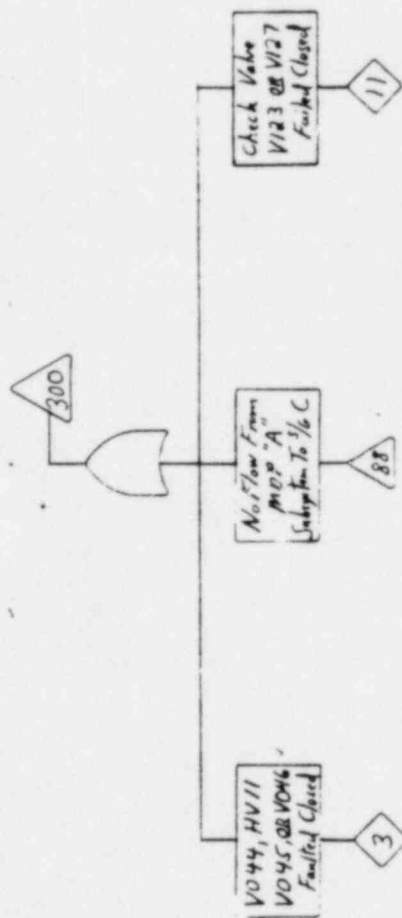
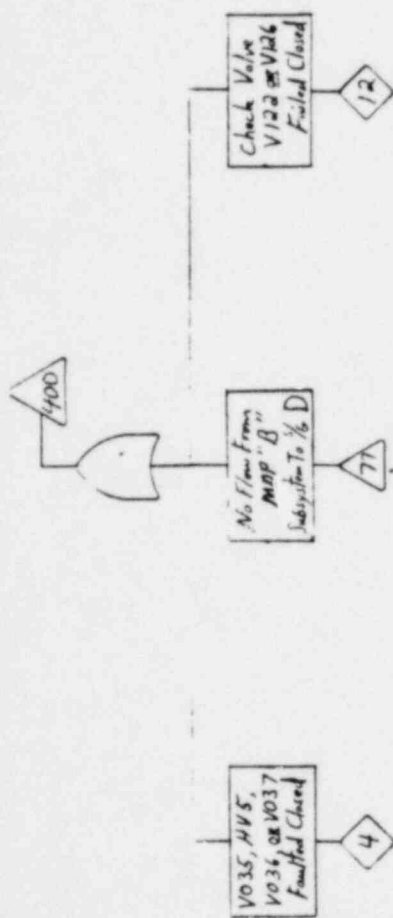
POOR ORIGINAL

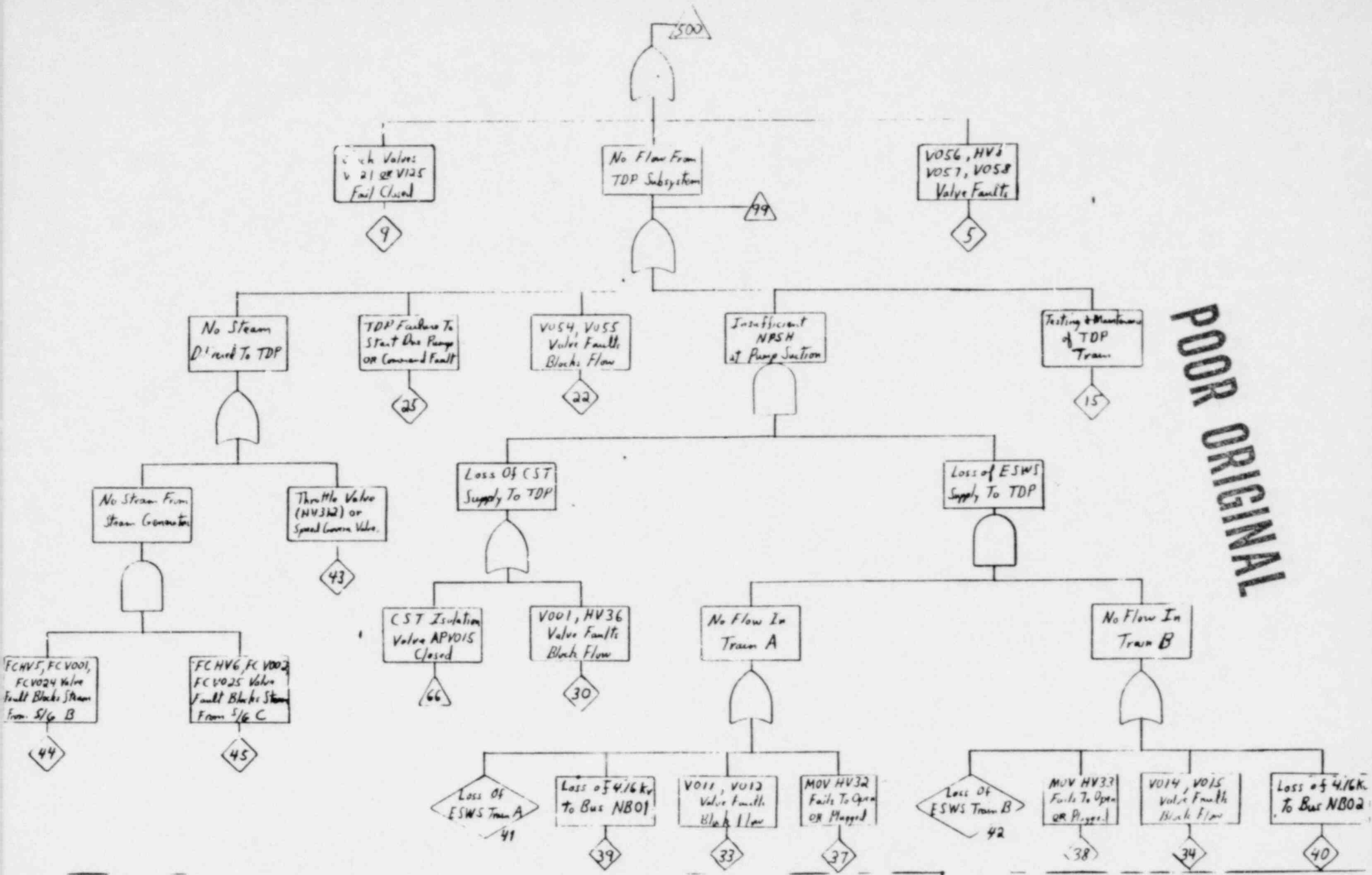


POOR ORIGINAL

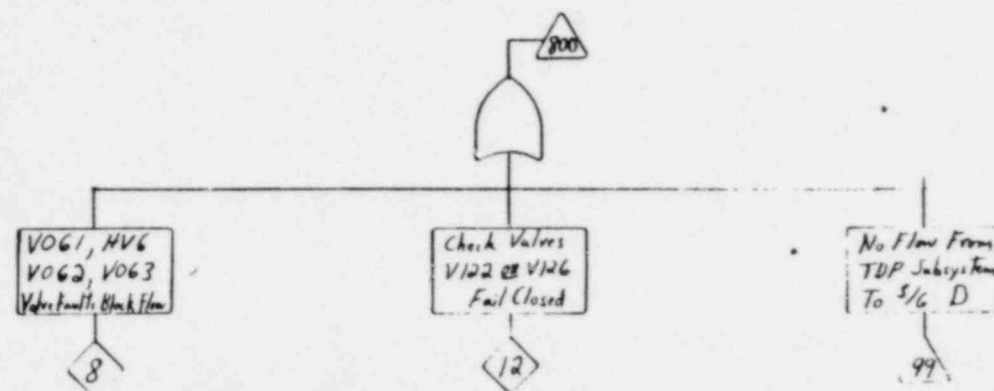
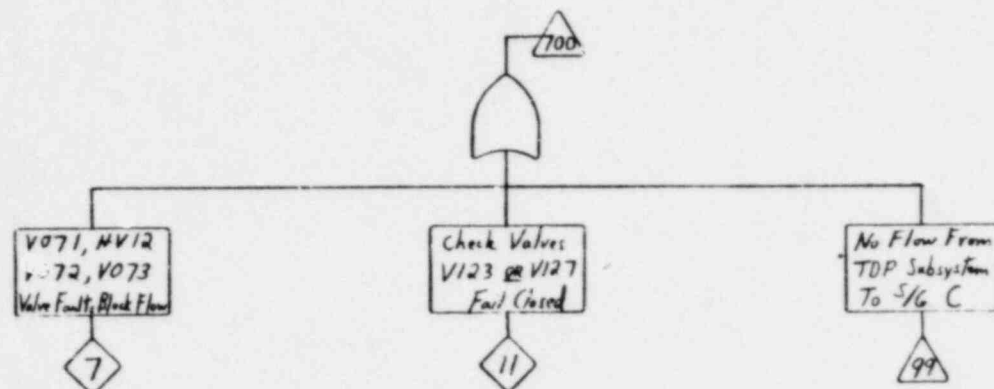
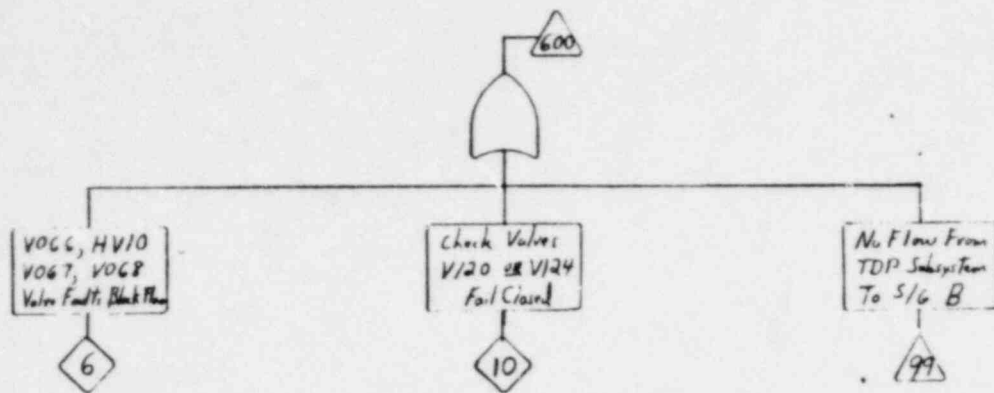


POOR ORIGINAL





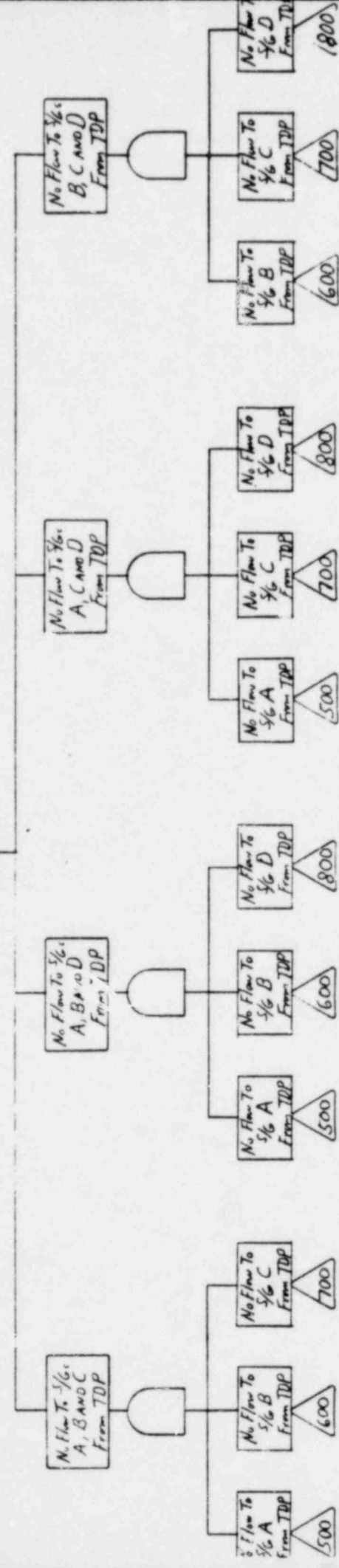
POOR ORIGINAL



POOR ORIGINAL

Case 3

Let there be 4/10 gpm Flow to
2 out of 4 5/16 s within 2 min
from the Tubing Drive Pump



POOR ORIGINAL

APPENDIX B

Failure Data - Basic Event Probabilities

Hardware

The failure data used in this study are presented in Table B-1. Unless otherwise indicated all failure data were taken directly from NUREG-0611. One item, "Flow Element/Runout Protection Fault," is explained in the following paragraph.

The MDP runout protection system consists of a feedback from flow elements FE1, FE2, FE3, FE4 to NOV's HV5, HV7, HV9 and HV11, respectively. Since the valves are normally open, there would strictly speaking, be no need to include a control circuit failure for these valves; i.e., loss of power or control signal would leave the valves as is--open. However, the introduction of a feedback from the flow elements to the valve positioner permits a spurious closing of the valve; any plugging of the flow element could be interpreted as a high flow past the element. Therefore, for Events 1 through 4, an additional basic event probability of $5 \times 10^{-4*}$ was inserted. Other failure modes (circuits, loss of local power) were not considered because the failures would likely result in a 0 amp input to the valve positioner which maintains the valve in the full open state. Finally, it should be noted that even if a higher failure probability was assigned to the flow element (e.g., 10^{-3}) the impact would be negligible because these valve failures are not significant contributors to the Top Event probability.

Human Error

The sensitivity of the AFWS reliability to human error was examined for three levels of assumed pre-accident human error. Since the AFWS is

*This probability was chosen by a conservative extrapolation of the 3×10^{-4} probability estimated in WASH-1400 for plugging of a flow orifice.

automatically actuated, no effort was made to quantify post-accident operator error. This treatment of human error was limited to mispositioning manual and motor-operated valves and was based on the human error probabilities given in NUREG-0611 which are reproduced in Table B-1; the three levels or options of human error are summarized below:

- o Option A: These probabilities contain no explicit human error; i.e., the failures are strictly hardware failures.
- o Option B: These probabilities include human error for failure to position manual and motor operated valves properly; this option assumes double check and walk-around procedures for manual valves. Note: This applies only to the locked opened valves in the AFWS flow path (i.e., from water supply to steam generators).
- o Option C: This option is similar to Option B except that no valve position checking is assumed and, therefore, a higher human error probability is assigned.

The probabilities given in Table III-2 of NUREG-0611 were treated as unconditional probabilities; that is, the values were not decreased by the probability of maintenance (i.e., .22). Based on the system's assumed test and maintenance requirements, human error was not included for all manual valves (See the T & M section of Appendix B). Also, pre-accident mispositioning of valves in interfacing systems was not treated. For example, if the manual valves on the line carrying diesel generator jacket cooling water were closed, the diesel generator would fail after several minutes. However, since the assumed diesel generator failure probability is relatively large, that particular human error would not make a significant impact on the system reliability.

Test and Maintenance

The approach presented in NUREG-0611 was used along with the testing frequencies given in the Standard Technical Specifications for Westinghouse PWRs (Reference 8).

Testing and maintenance activities which remove components and/or systems from service can be significant contributors to the overall AFWS unavailability. The most common forms of valve maintenance performed during power operation are packing adjustments and repairs to MOV and AOV control circuits and operators. Nearly all these maintenance activities are performed with the valve in the failsafe position during the maintenance interval. Therefore, maintenance of MOVs and AOVs was not considered to be a contributor to valve unavailability. Check valves and manual valves are expected to require very little maintenance. The low test and maintenance impact on this part of the AFWS was the basis for not including a human error contributor to unavailability for the manual valves in the individual S/G flow paths (i.e., fore and aft of the MOVs and AOVs). Although T & M contributions were not treated for the valves associated with the branch flowpaths to a specific steam generator, the unavailability due to testing and maintenance of the pump sub-systems was treated.

In the sub-system part of the fault-tree, T & M was treated as a distinct composite basic event. Since the T & M unavailability was higher for the pump-driver than the valves in each train, only the pump-driver unavailability was considered. Essentially the pump unavailability was considered to be synonymous with "pump sub-system" unavailability. The probabilities for the events (i.e., 13, 14 and 15) were determined using the methods described in NUREG-0611 as follows:

Test

$$(\text{Unavailability/demand}) Q_{\text{Test}} = \frac{(\text{hrs / test}) (\text{number of tests per year})}{*7008 \text{ hrs./yr.}}$$

* Assumes the plant is in a functional mode only 80% of the year.

Q_{Test} will be calculated using the default hrs./test (t_a)* from NUREG-0611 and the number of tests per year based on the technical specifications:

<u>Component</u>	<u>Hrs./Test</u>	<u>Tests/Year</u>	<u>Q_{Test}</u>
-			
Pumps	1.4	12	2.4×10^{-3}
Diesels	1.4	12	2.4×10^{-3}

Maintenance

$$(\text{Unavailability/demand}) Q_{\text{Maint.}} = \frac{.22 (\text{Hrs./Maintenance Action})}{720}$$

Q_{Maint} will be based on the most conservative value for hrs/maintenance action.

<u>Component</u>	<u>Hrs./Maintenance Action</u>	<u>$Q_{\text{Maint.}}$</u>
Pumps	19	5.8×10^{-3}
Diesels	21	6.4×10^{-3}

* Standard Technical Specifications requires testing pumps and valves in the AFWS monthly.

Additionally, it was assumed that coincident test and/or maintenance of components of more than one AFW pump and its associated flow paths, while the reactor is at full power, is in violation of the plant technical specifications; therefore, minimum cut sets containing such coincident basic events are treated as not being credible and are discarded in the quantitative evaluation.

TABLE B-1

Component-Basic Event Failure Probabilities

<u>Component or Basic Event</u>	<u>Failure Probability (on demand)</u>
Local Fault in MOV:	
- Mechanical	1×10^{-3}
- Plugging	1×10^{-4}
- Control ("Command") Circuit, <u>local</u>	2×10^{-3}
Local Fault in AOV:	
- Mechanical	3×10^{-4}
- Control Circuit	1.3×10^{-3} (Table 8, Reference 7)
- Plugging	1×10^{-4}
Check Valve (Plugging)	1×10^{-4}
Manual Valve (Plugging)	1×10^{-4}
Local Fault in MDP or TDP	
- Mechanical	1×10^{-3}
- Control Circuit	4×10^{-3}
MDP or TDP: Down for Maintenance	5.8×10^{-3} (conservatively assumes 19 hrs. per interval)
Down for Testing	2.4×10^{-3} (12 tests/year @ 1.4 hrs. per test)
Manual Valve Left Closed (Operator Error)	5×10^{-3} (Option B) 1×10^{-2} (Option C)
Actuation Logic (Failure to transmit a start signal to AFWS)	7×10^{-3} /train
Loss of Offsite Power	1×10^{-2} (based on an examination of Reference 16)

Table B-1 (continued)

<u>Component or Basic Event</u>	<u>Failure Probability (on demand)</u>
Diesel Generator	
- Fails to start	4×10^{-2} (Reference 6)
- Test and Maintenance	8.8×10^{-3}
Flow Element/Runout Protection	5×10^{-4}

Composite Basic Events

Table B-2 presents the probabilities assigned to each composite basic event (CBE) indicated on the AFWS fault tree (see Appendix A). Since the same probabilities apply to many valves which perform similar functions but are located in different trains or branches, a generic notation has been used. For example, CBEs 9, 10, 11 and 12 are included under one heading, "Check Valves V12X or V12Y Fails Closed" and is interpreted as:

CBE 9: Check Valve V121 or V125 Fails Closed

CBE 10: Check Valve V120 or V124 Fails Closed

CBE 11: Check Valve V123 or V127 Fails Closed

CBE 12: Check Valve V122 or V126 Fails Closed

The various contributions (i.e., basic events) are then listed. So that information in Table B-2 can be easily understood without reference to the fault trees, a description of each composite basic event (CBE) is listed below:

CBE 1 through 8: VOXX, VOYY, VOZZ, HVXX Valve Fault Blocks Flow

CBE 8 through 12: Check Valve V12X or V12Y Fails Closed

CBE 13, 14 and 15: Test and Maintenance of MDP "B", MDP "A", and
TDP AFW Trains

CBE 20, 21 and 22: Discharge Blockage Caused by Fault in Valves VOXX
or VOYY

CBE 23 and 24: AFW MDP "X" Does Not Start Due to Motor/Pump Fault

CBE 25: TDP Does Not Start Due to Turbine/Pump Fault

CBE 26: Isolation Valve APV015 Inadvertently Left Closed
(Operator Error)

CBE 27: APV015 - Valve Fault

CBE 28, 29 and 30: VOXX, HVYY Valve Fault Blocks Flow

CBE 31 through 34: VOXX, VOYY Valve Fault Blocks Flow

CBE 35 through 38: MOV HVXX Fails to Open or Plugged

CBE 38 and 40: Loss of 4.16 KV to Bus NBOX

CBE 41 and 42: Loss of ESWS Train A (B)

CBE 43: Throttle Valve or Speed Governor Valve Faults

CBE 44: FCHV5, FCV001 FCV024, FCV085 Valve Faults Block
Steam from S/G B

CBE 45: FCHV6, FCV002, FCV024, FCV087 Valve Faults Block
Steam from S/G C

TABLE B-2

		Probability of Failure (On Demand)		
		Option A	Option B	Option C
<u>Composite Basic Events 1 through 8</u>				
Valves VOXX; Plug		1.0E-04		
Valves VOZZ; Plug		1.0E-04		
Valves VOYY; Check Valve Fails Closed		1.0E-04	4.0E-04	4.0E-04
Valves HVX; Plug		1.0E-04		
Flow Element	Events 5-8	--	--	--
	Events 1-4	5.0E-04	5.0E-04	5.0E-04
Human Error - Valve HVX		--	5.0E-04	5.0E-04
Total Probability	Events 1-4	9.0E-04	1.4E-03	1.4E-03
	Events 5-8	4.0E-04	9.0E-04	9.0E-04
<u>Composite Basic Events 9 through 12</u>				
V12X; Fails Closed		1.0E-04	1.0E-04	1.0E-04
V12Y; Fails Closed		1.0E-04	1.0E-04	1.0E-04
Total Probability		2.0E-04	2.0E-04	2.0E-04
<u>Composite Basic Events 13, 14 and 15</u>				
Testing (Manual Discharge Valves Closed)		2.4E-03		
Maintenance of MDPs (TDP) and Associated Valves		5.8E-03	N/C*	N/C
Total Probability		8.2E-03	8.2E-03	8.2E-03
<u>Composite Basic Events 20, 21 and 22</u>				
Check Valve VOXX; Fails Closed		1.0E-04		
Manual Valve VOYY; Plug		1.0E-04	2.0E-04	2.0E-04
Human Error - Manual Valve VOYY		--	5.0E-03	1.0E-02
Total Probability		2.0E-04	5.2E-03	1.02E-02

* N/C indicates No Change from Option A for the group of basic events.

TABLE B-2 (continued)

	Probability of Failure (On Demand)		
	Option A	Option B	Option C
<u>Composite Basic Events 23, 24 and 25</u>			
Mechanical Fault	1.0E-03		
Control Circuit Fault	4.0E-03	N/C	N/C
Actuation Failure	7.0E-03		
Total Probability	1.2E-02	1.2E-02	1.2E-02
<u>Basic Event 26</u>			
CST Valve APV015 <u>Left</u> Closed	--	5.0E-03	1.0E-02
<u>Basic Event 27</u>			
CST Valve APV015 Plugged	1.0E-04	1.0E-04	1.0E-04
<u>Composite Basic Events 28, 29 and 30</u>			
Check Valve V00X; Fails Closed	1.0E-04	N/C	N/C
MOV HVYY; Plug	1.0E-04		
Human Error; MOV Left Closed	--	5.0E-04	5.0E-04
Total Probability	2.0E-04	7.0E-04	7.0E-04
<u>Composite Basic Events 31 through 34</u>			
Check Valve VOYY; Fails Closed	1.0E-04	1.0E-04	1.0E-04
Manual Valve VOXX; Plug	1.0E-04	1.0E-04	1.0E-04
Human Error - Manual Valve VOXX <u>Left</u> Closed	--	5.0E-03	1.0E-02
Total Probability	2.0E-04	5.2E-03	1.02E-02
<u>Composite Basic Events 35 through 38</u>			
Mechanical	1.0E-03		
Plug	1.0E-04	N/C	N/C
Control Circuit Failure	2.0E-03		
Total Probability	3.1E-03	3.1E-03	3.1E-03

TABLE B-2 (continued)

Basic Events 39 and 40

Events 39 and 40 represent the unavailability of Offsite AC power and Onsite AC (diesel generators) for the two Class IE buses:

$$A \text{ (unavailability of AC power)} = A_{DG} \cdot A \text{ (offsite AC)}$$

where:

$$\begin{aligned} A_{DG} \text{ (Diesel Generator Unavailability)} &= (\text{Probability of failure on demand}) + \\ &\quad (\text{Test and Maintenance Outage}) \\ &= .04 + .0088 = 4.088\text{E-}02 \end{aligned}$$

For comparison with NUREG-0611, $P(39) = 0.0$ and:

$$\text{Case 1: } P(40) = (4.088\text{E-}02) (.01) = 4.088\text{E-}04$$

$$\text{Case 2: } P(40) = 4.088\text{E-}02 (1)$$

For all the sensitivity, Importance and common cause evaluations:

$$\text{Case 1: } P(40) = P(39) = 4.088\text{E-}04$$

$$\text{Case 2: } P(40) = P(39) = 4.088\text{E-}02$$

$$\text{Case 3: } P(40) = P(39) = 1.0$$

Note: These probabilities overstate the impact of testing since the ESFAS will override any testing. Also, the diesel generator may already be running and only needs to be sequenced onto the safety loads.

TABLE B-2 (continued)

		<u>Probability of Failure (On Demand)</u>		
		<u>Option A</u>	<u>Option B</u>	<u>Option C</u>
<u>Composite Basic Events 41 and 42</u>				
ESW Motor/Pump; Mechanical Failure		1.0E-03		
Check Valve EFV00X; Fails Closed		1.0E-04	N/C	N/C
Control Fault (Local)		4.0E-03		
Manual Valves (EFV00X, EFV10X, EFV10Y)	(3x)	1.0E-04		
Human Error: Manual Valves (3x)		--	1.5E-02	3.0E-02
Total Probability		5.4E-03	2.04E-02	3.54E-02
<u>Composite Basic Event 43</u>				
Throttle Valve; Control Fault		2.0E-03		
Speed Governor Valve; Control Fault		2.0E-03	N/C	N/C
Plug (either valve)		2.0E-04		
Total Probability		4.2E-03	4.2E-03	4.2E-03
<u>Composite Basic Event 44</u>				
Check Valves FCV001, FCV024; Fail Closed	(2x)	1.0E-04		
Manual Valve FCV085; Plug		1.0E-04		
AOV FCHV5; Mechanical		3.0E-04	N/C	N/C
Control Circuit (Local)		1.3E-03		
Plug		1.0E-04		
Human Error; Manual Valve FCV085		--	5.0E-03	1.0E-02
Total Probability		2.0E-03	7.0E-03	1.2E-02
<u>Composite Basic Event 45</u>				
Same Probabilities as CBE 44				

APPENDIX C

Minimal Cut-Sets

This appendix presents a tabulation of the significant minimal cut-sets for each case and option. The cut-sets are listed in approximately descending order of probability. The total probability associated with these cut-sets represents at least 90% of the Top Event probability; therefore, the additional cut-sets were not listed. It is evident, from a review of these cut-sets, that failure of the pumps or actuation failure (Events 23, 24, 25), test and maintenance outages (Events 13, 14, 15), discharge valves closed or faulted (Events 20, 21, 22) and loss of power (Event 40) are dominant failure modes.

Table C-1 gives the SNUPP-3 AFWS fault tree reduced to 9 three-event cut-sets. The "events" 77, 88 and 99 represent the "subtrees" 77, 88 and 99 (see Appendix A). The fault tree was completely resolved to the level of composite basic events by substitution of the minimal cut-sets representing the subtrees. Tables C-2, C-3 and C-4 list the resulting cut-sets by option for Case 1, Case 2 and Case 3. All the events making up the cut-sets were previously defined in Appendix B.

TABLE C-1

AFWS Fault Tree Reduced to 9 Three-Event Cut-Sets

-

77	88	99
1	88	99
2	77	99
3	77	99
4	88	99
9	88	99
10	77	99
11	77	99
12	88	99

TABLE C-2

Significant Minimal Cut-Sets: Option A

<u>Case 1</u>			<u>Case 2</u>			<u>Case 3</u>
23	24	25	24	25	40	25
13	24	25	14	25	40	15
14	23	25	15	24	40	15
15	23	24	24	40	43	43
23	24	43	23	24	25	22
14	23	43	14	40	43	30
13	24	43	15	23	24	27
2	23	25	14	23	25	
3	23	25	13	24	25	
1	24	25	23	24	43	
4	24	25	3	25	40	
2	13	25	2	25	40	
3	15	23	13	24	43	
3	13	25	14	23	43	
1	15	24	3	15	40	
1	14	25	2	15	40	
4	15	24	2	40	43	
4	14	25	3	40	43	
2	15	23	4	24	25	
23	25	39	3	23	25	
24	25	40	2	23	25	
13	25	39	1	24	25	
15	24	40	11	25	40	
14	25	40	22	24	40	
15	23	39	10	25	40	
4	24	43	21	25	40	
1	24	43	3	13	25	
2	23	43	2	13	25	
3	23	43	1	15	24	
3	13	43	1	14	25	
2	13	43	4	15	24	
1	14	43	4	14	25	
4	14	43	2	15	23	

TABLE C-2 (continued)

<u>Case 1</u>			<u>Case 2</u>			<u>Case 3</u>		
9	24	25	3	15	23			
12	24	25	15	21	40			
20	24	25	14	22	40			
21	23	25	10	15	40			
10	23	25	11	15	40			
11	23	25	3	23	43			
22	23	24	1	24	43			
23	39	43	4	24	43			
24	40	43	2	23	43			
13	22	24	21	40	43			
14	22	23	11	40	43			
9	15	24	10	40	43			
13	21	25	1	14	43			
9	14	25	2	13	43			
10	15	23	3	13	43			
14	20	25	4	14	43			
12	15	24	9	24	25			
12	14	25	22	23	24			
11	15	23	10	23	25			
15	20	24	11	23	25			

TABLE C-3

Significant Minimal Cut-Sets: Option B

<u>Case 1</u>			<u>Case 2</u>			<u>Case 3</u>	
23	24	25	24	25	40	25	
13	24	25	14	25	40	15	
14	23	25	15	24	40	22	
15	23	24	22	24	40	26	
22	23	24	21	25	40	43	
20	24	25	26	40	41	30	
21	23	25	24	40	43	27	
23	24	43	14	22	40	44	45
15	20	24	15	21	40		
13	21	25	23	24	25		
14	20	25	14	40	43		
15	21	23	21	22	40		
13	22	24	15	23	24		
14	22	23	13	24	25		
26	41	42	14	23	25		
13	24	43	21	40	43		
14	23	43	3	25	40		
21	22	23	2	25	40		
20	22	24	20	24	25		
20	21	25	21	23	25		
20	24	43	22	23	24		
21	23	43	23	24	43		
13	21	22	2	15	40		
15	20	21	3	15	40		
14	20	22	14	20	25		
3	23	25	15	21	23		
1	24	25	13	22	24		
4	24	25	14	22	23		
2	23	25	15	20	24		
14	20	43	13	21	25		
13	21	43	26	41	42		
20	21	22	14	23	43		
1	14	25	13	24	43		
3	15	23	2	22	40		
			3	22	40		

TABLE C-3 (continued)

<u>Case 1</u>		
4	15	24
2	15	23
4	14	25
3	13	25
2	13	25
1	15	24
20	21	43
3	22	23
3	20	25
1	22	24
1	21	25
4	22	24
4	21	25
2	22	23
2	20	25

TABLE C-4

Significant Minimal Cut-Sets: Option C

<u>Case 1</u>			<u>Case 2</u>			<u>Case 3</u>	
26	41	42	26	40	41	25	
23	24	25	24	25	40	22	
21	23	25	21	25	40	15	
22	23	24	22	24	40	26	
20	24	25	21	22	40	43	
20	22	24	15	24	40	30	
20	21	25	14	25	40	27	
21	22	23	14	22	40	44	45
15	23	24	15	21	40		
13	24	25	24	40	43		
14	23	25	26	41	42		
20	21	22	21	40	43		
14	22	23	23	24	25		
13	22	24	14	40	43		
15	21	23	20	24	25		
13	21	25	22	23	24		
15	20	24	21	23	25		
14	20	25	20	22	24		
15	20	21	21	22	23		
13	21	22	20	21	25		
14	20	22	13	24	25		
23	24	43	14	23	25		
21	23	43	15	23	24		
20	24	43	20	21	22		
20	21	43	13	21	25		
13	24	43	15	20	24		
14	23	43	14	22	23		
14	20	43	14	20	25		
13	21	43	15	21	23		
4	24	25	13	22	24		
2	23	25					
3	23	25					

TABLE C-4 (continued)

<u>Case 1</u>		
1	24	25
3	22	23
4	22	24
4	21	25
3	20	25
2	20	25
1	22	24
1	21	25
2	22	23
3	20	22
4	21	22
2	20	22
1	21	22
1	14	25
3	15	23
1	15	24
2	15	23
4	15	24
3	13	25
2	13	25