NUREG/CR-3511/1 of 2
SAND83-2086/1 of 2
AN, RG
Printed March 1984

Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant

Volume 1. Main Report

Arthur C. Payne, Jr., Principal Investigator

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-76DP00789

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-3511/1 of 2
SAND83-2086/1 of 2
AN, RG

INTERIM RELIABILITY EVALUATION PROGRAM:

ANALYSIS OF THE CALVERT CLIFFS UNIT 1 NUCLEAR POWER PLANT

VOLUME 1

MAIN REPORT

MARCH 1984

A. C. Payne, Jr.
D. W. Stack
N. L. Brisbin
S. W. Hatch
Sandia National Laboratories

S. H. McAhren
Remote Sensing, Inc.

B. Atefi
W. L. Ferrell
W. S. Galyean
A. A. Garcia
J. E. Kelly
M. Modarres
M. Raeisinia
Science Applications, Inc.

M. I. Roush
University of Maryland

S. M. Davis
D. R. Lasher
P. D. O'Reilly
U. S. Nuclear Regulatory Commission

J. J. O'Neill
Evaluation Associates, Inc.

S. M. Davis
R. N. Hunt
Baltimore Gas & Electric Co.

S. Lainoff
J. Held
Energy, Inc.

Sandia National Laboratories
Albuquerque, New Mexico 87185
Operated By
Sandia Corporation
for the
U. S. Department of Energy

Prepared for
Division of Risk Analysis
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1241

TABLE OF CONTENTS

VOLUME 1 - MAIN REPORT — Page

Executive Summary ES-1

Summary S-1

Chapter 1 - Introduction. 1-1

1.1 IREP Overview. 1-1
1.2 Calvert Cliffs Unit 1 Analysis Team Makeup 1-2

Chapter 2 - GENERAL METHODOLOGY 2-1

2.1 Information Base 2-1
2.2 Methodology. 2-2

Chapter 3 - Plant Design. 3-1

3.1 Basic Information 3-1
3.2 Plant Functions 3-1
3.2.1 LOCA Mitigating Functions 3-1
3.2.2 Transient Mitigating Functions 3-4
3.3 System Dependencies 3-5

Chapter 4 - Initiating Events 4-1

4.1 Introduction 4-1
4.2 Initiating Events Chosen for Calvert Cliffs Unit 1 4-1
4.2.1 LOCA Initiating Events 4-2
4.2.2 Transient Initiating Events 4-3
4.2.2.1 Service Water System Analysis 4-4
4.2.2.2 Emergency AC Power Bus Analysis. . . . 4-5
4.2.2.3 Emergency DC Power Bus Analysis. . . . 4-5
4.2.2.4 Instrument Air System Analysis 4-6
4.2.2.5 Component Cooling Water System Analysis 4-6
4.2.2.6 Salt Water System Analysis 4-7
4.2.2.7 Heating and Ventilation System Analysis 4-8
4.3 Description of the Calvert Cliffs Unit 1 Initiating Events 4-8

Chapter 5 - Accident Sequence Delineation 5-1

5.1 Introduction 5-1
5.2 CC-1 Functional Event Trees 5-1
5.2.1 LOCA Functional Event Trees 5-1
5.2.1.1 Large LOCA Functional Dependencies . 5-1
5.2.1.2 Small and Small-Small LOCA Functional Dependencies. 5-3

TABLE OF CONTENTS (Continued)

	Page
5.2.1.3 LOCA Functional Accident Sequence Descriptions	5-4
5.2.2 Transient Functional Event Tree	5-9
5.2.2.1 Transient Functional Dependencies. .	5-9
5.2.2.2 Transient Functional Accident Sequence Descriptions	5-10
5.3 CC-1 Systemic Event Trees	5-12
Chapter 6 - Systems Analysis.	6-1
6.0 Introduction	6-1
6.1 Methodology and General Assumptions	6-1
6.2 Safety Injection Tanks (SITs)	6-2
6.3 Low Pressure Safety Injection/Recirculation System (LPSI/R)	6-4
6.4 Containment Air Recirculation and Cooling System (CARCS)	6-6
6.5 Containment Spray/Shutdown Heat Exchanger System (CSS/SDHX)	6-7
6.6 High Pressure Safety Injection/Recirculation System (HPSI/R)	6-9
6.7 Reactor Protection System (RPS)	6-11
6.8 Power Conversion and Secondary Steam Relief Systems (PCS)	6-13
6.9 Auxiliary Feedwater System (AFW)	6-14
6.10 Power Operated Relief Valves (PORV)	6-16
6.11 Chemical and Volume Control System (CVCS)	6-18
6.12 Code Safety Valves (SRV)	6-19
6.13 Electrical Power System (Emerg. AC and DC Systems) .	6-20
6.14 Engineered Safety Features Actuation System (ESFAS)	6-22
6.15 Service Water System (SRWS)	6-26
6.16 Component Cooling Water System (CCWS)	6-29
6.17 Salt Water System (SWS)	6-31
6.18 Heating and Ventilation	6-34
6.18.1 Description (Diesel Generator Room Ventilation System).	6-34
6.18.2 Description (ECCS Pump Room Cooling)	6-34
Chapter 7 - Accident Sequence Quantifications	7-1
7.1 Introduction	7-1
7.2 Screening Quantification	7-2
7.3 Final Quantification	7-6
7.4 Example Calculation	7-7

TABLE OF CONTENTS (Continued)

Page

Chapter 8 - Results 8-1

8.1 Dominant Accident Sequences. 8-1
8.1.1 ATWS(PSF) 8-3
8.1.2 $T_{DC}L$ - Sequence T_{DC}-82 8-6
8.1.3 S_2H - Sequence S_2-50 8-9
8.1.4 S_2FH - Sequence S_2-52 8-15
8.1.5 T_2L - Sequence T_2-82 8-20
8.1.6 T_4KU - Sequence T_4-173 8-22
8.1.7 T_4ML - Sequence T_4-147 8-26
8.1.8 T_1Q-D"CC'- Sequence T_1-81-65 8-29
8.1.9 T_1L - Sequence T_1-82 8-34
8.1.10 Station Blackout 8-41
8.1.11 T_4KQ - Sequence T_4-152 8-43
8.1.12 T_3KU - Sequence T_3-139 8-45
8.1.13 T_3KQ - Sequence T_3-118 8-47
8.1.14 T_3ML - Sequence T_3-113 8-48
8.1.15 S_2D" - Sequence S_2-59 8-51
8.1.16 T_1LCC' - Sequence T_1-85 8-52
8.2 Containment Response and Determination of Release Categories 8-58
8.3 Sensitivities 8-60
8.4 Limitations of the IREP Methodology and Analysis and Future Uses of the Models 8-66
8.4.1 Application of Results 8-67
8.4.2 Conclusions on the Applications of PREP . . . 8-70

References. R-1

ACKNOWLEDGEMENT

The efforts of the Quality Assurance Review Team which periodically reviewed the conduct of the work and provided technical guidance are acknowledged. This team consisted of:

David D. Carlson, Sandia National Laboratories
Jack W. Hickman, Sandia National Laboratories
Gregory J. Kolb, Sandia National Laboratories
Joseph A. Murphy, U. S. Nuclear Regulatory Commission
Kenneth Murphy, U. S. Nuclear Regulatory Commission
Jonathan Young, Energy, Inc.

In the area of human factors, we wish to thank Barbara Bell of Battelle Columbus Laboratories and Dwight Miller of Sandia National Laboratories for guiding the team in the human error calculations.

The authors also would like to thank Emily Preston, Vickie Black and Robin Cassell for their help in typing this report.

Executive Summary

This report presents the results of the analysis of Calvert Cliffs Unit 1 Nuclear Power Plant. The analysis was performed as part of the Interim Reliability Evaluation Program (IREP). Two of the IREP objectives are addressed by this analysis. They are (1) the identification of those accident sequences which can be expected to dominate the risk related to the operation of Calvert Cliffs Unit 1, and (2) the development of system models that can be used for future, more extensive probabilistic risk assessments of Calvert Cliffs Unit 1.

The analysis used fault tree and event tree models as the primary tools to evaluate the risk due to a core melt at Calvert Cliffs. Core melt sequences initiated by one of three break-size LOCAs or one of six categories of transients were evaluated, and the dominant (i.e., highest frequency) sequences were further analyzed to estimate the magnitude and frequency of radionuclide release. The accident sequences were then placed into the release categories defined in the Reactor Safety Study [11].

The most significant sequences contributing to the core melt frequency are (1) Anticipated Transients Without Scram (ATWS) (33% of the total core melt frequency), (2) Small-small LOCAs (i.e., 1.9" to 3" in diameter) with makeup system failure in the recirculation phase (20% of the total core melt frequency), (3) the loss of a DC bus followed by failure of secondary heat removal (16% of the total core melt frequency), and (4) Loss of Offsite Power following by failure of secondary heat removal or a stuck open relief valve (12% of the total core melt frequency).

Insights were developed concerning the importance of plant design features. For example, several single failures were identified in the systems called upon to mitigate accidents and in their support systems. Support systems, e.g., AC/DC power, room cooling and service water, were modeled in detail and found to be important contributors to risk. The analysis led to the identification of key components/events, that contribute most to the core melt frequency.

Similar insights were developed concerning plant operations. Operator errors made during the course of accidents were found to be significant. Some changes to plant procedures could be made based on this analysis in order to take greater advantage of possible operator actions. Operator recovery actions were very important in preventing or mitigating accidents. Test and maintenance contributions were, in general, small; however, maintenance of several key components was found to be a significant contributor to particular sequences.

The estimated core melt frequency for Calvert Cliffs Unit 1 (CC-1) is similar to the values predicted by probabilistic risk assessments of other pressurized water reactors.

Summary

This section summarizes the Calvert Cliffs Unit 1 dominant accident sequences, engineering insights gained via the analysis, changes to the design and operation of the plant as the result of this study and sensitivity analyses done on the dominant sequences. These topics are briefly discussed below. A more detailed discussion can be found in Chapter 8. While a PRA has already been done on Calvert Cliffs Unit 2 [9], a detailed comparison of the differences between the two analysis is not made here. The reader is referred to the paper referenced below for such a comparison.*

Dominant Accident Sequences

Accident sequences are combinations of system failures following an initiating event such as a LOCA, which lead to some mode of containment failure. Sequences which were determined to lead to core melt were examined and quantified. Those core melt sequences which had an initial frequency greater than 1.0E-6/yr were then recalculated, considering recovery actions, and a new sequence frequency was derived. (For a detailed discussion of this application of recovery to each sequence, see the recovery discussions in Chapter 8 and Appendix C.) Those sequences which still had a frequency greater than 1.0E-6/yr were considered to be the dominant contributors to core melt (see Table S-1). These sequences were further analyzed to determine the probability of containment failure by five different mechanisms: in-vessel steam explosion (α), containment leakage (β), hydrogen burning (γ), overpressurization (δ), and basemat meltthrough (ϵ). The dominant accident sequences were then assigned to release categories, and the results are presented in Table S-2 and Figure S-1. (Release categories define the severity of the post core melt radioactive material release from containment. Category 1 is the most severe and Category 7 is the least severe.)

Sequence ATWS(PSF)**

This sequence is an anticipated transient without scram (ATWS) followed by reduced secondary heat removal capacity (i.e., either power conversion system (PCS) in a runback mode and/or auxiliary feedwater (AFW)). The resulting imbalance

*G. J. Kolb and A. C. Payne, Jr., Sandia National Laboratories "A Review and Analysis of Insights from Plant Transients as gained from the Interim Reliability Evaluation Program," Proceedings of the ANS Topical Meeting on Anticipated and Abnormal Transients in Light Water Reactors, Jackson, Wy. September 26-29, 1983 (to be published).

**See the sensitivity analysis involving the sequence in Section 8.3.

between the energy production and removal rates leads to the heatup of the primary system and an increase in system pressure. Primary system failure (PSF) is assessed to occur and result in core melt if the pressure exceeds the service level C (3200 psia) limit. Such pressures can result in system damage severe enough to make continued reactor core cooling highly questionable. For instance, core melt can result from a LOCA induced by the overpressure with simultaneous failure of all LOCA mitigating systems. Containment failure is predicted to occur, most likely, by hydrogen burn and/or overpressure.

Because this sequence is driven by phenomenological considerations, it was not explicitly modeled on the event trees and an independent calculation of its frequency was done. The resulting estimate is 2.8E-5/yr., and it contributes 20% of the total core melt frequency. (A detailed discussion of the calculation is presented in Chapter 8.)

Sequence T_{DC}-82 ($T_{DC}L$)

In this sequence, a failure of DC bus 11 (T_{DC}) results in a trip of units 1 and 2 and failure of the PCS and the AFW motor-driven pump #13 with degradation of the safety systems. The plant scrams successfully, but AFW (L) subsequently fails. The Containment Air Recirculation and Cooling System (CARCs) and the Containment Spray System, Injection (CSSI) succeed and cool the containment. As a result of the lack of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to the low head of the HPSI pumps and the uncertainty as to whether or not the pressure could be reduced enough for the HPSI pumps to be able to inject water, [24, 25]. Recent calculations done by EG&G for the Station Blackout Program [26] indicate that approximately 86 minutes is available to start an AFW pump in order to prevent core uncovery. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The sequence frequency is estimated as 2.1E-5/yr and contributes 16% of the total core melt frequency. The dominant contributors to this sequence are single failures in the AFW turbine-driven pump #11 train combined with failure of the operator to start the locked-out turbine-driven AFW pump #12.

Sequence S_2-50 (S_2H)

In this sequence, a Small-small LOCA (S_2) occurs followed by successful scram and operation of AFW and High Pressure Safety Injection (HPSI) providing both secondary heat removal and primary system makeup. When the Refueling Water Tank (RWT) depletes and switchover to recirculation occurs (anywhere from 4 to 12 hours into the transient depending on the size of the leak), High Pressure Safety Recirculation (HPSR) (H) fails.

Due to the lack of primary makeup, the core then uncovers and core melt ensues. CARCS and the Containment Spray System, Recirculation (CSSR) succeed and cool the containment. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The sequence frequency is estimated as 1.4E-5/yr and contributes 11% of the total core melt frequency. The dominant contributors to this sequence are of two types: (1) failures of HPSR pump #13 combined with failures of room cooling to the other two HPSR pumps (they are in the same room and failure of room cooling results both pumps failing) or (2) failures of the Component Cooling Water (CCW) system or Salt Water System (SWS) resulting in loss of pump seal cooling and failure of all HPSR pumps.

Sequence S_2-52 (S_2FH)

In this sequence, a Small-small LOCA (S_2) occurs and is followed by successful scram and operation of AFW and HPSI providing both secondary heat removal and makeup. When the RWT depletes and switchover to recirculation occurs (anywhere from 4 to 12 hours into the accident), HPSR (H) and CSSR (F) fail. Due to the lack of primary makeup, the core then uncovers and core melt ensues. CARCS succeeds and cools the containment. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The sequence frequency is estimated as 1.1E-5/yr. and contributes 9% of the total core melt frequency. The dominant contributors to this sequence are failures in each train of room cooling to the two Engineered Safety Features (ESF) pump rooms. These result in failure of all HPSR and CSSR pumps.

Sequence T_2-82 (T_2L)

In this sequence, a loss of PCS (T_2) occurs and is followed by a loss of AFW(L). The reactor has scrammed and CARC and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for use of feed and bleed due to information presented in References 23 and 24. Recent calculations done by EG&G for the Station Blackout program [26] indicate that 86 minutes is available to start an AFW pump in order to prevent core uncovery. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The frequency of this sequence is estimated to be 7.1E-6/yr, and it contributes 6% of the total core melt frequency. The dominant contributors to this sequence are (1) failure of the common suction line valve resulting in failure of all operating AFW pumps combined with failure of the operator to

realign the AFW suction to an alternate supply and start the locked-out turbine-driven AFW pump, and (2) double failures of both operating AFW pumps combined with failure of the operator to start the locked-out turbine-driven AFW pump.

Sequence T_4-173 (T_4KU)

This sequence is a T_4 (all other) transient followed by a failure to scram (K) and failure of emergency boration (U). The reactor vessel has survived the initial pressure transient due to an assessed Power Conversion System (PCS) runback. CE analyses [21] and the NRC analysis in support of the ATWS rule [22] state that greater than 10 minutes are available for the operator to initiate emergency boration. In this study, we have assessed that, if the operator fails to start shutting the reactor down within 20-30 minutes, core melt will result. Containment failure is predicted to occur, most likely, by hydrogen burn and/or overpressure.

This sequence frequency is estimated as 6.7E-6/yr and contributes 5% of the total core melt frequency. The dominant contributor to this sequence is common mode failure of the Reactor Protection system to insert any control rods combined with failure of the operator to initiate emergency boration.

Sequence T_4-147 (T_4ML)

In this sequence, a T_4 (all other) transient occurs and is followed by a loss of PCS (M) and AFW (L). The reactor has scrammed and CARC and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to information presented in References 23 and 24. Recent calculations done by EG&G for the Station Blackout program [26] indicate that 86 minutes are available to start an AFW pump in order to prevent core uncovery. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The sequence frequency is estimated as 6.3E-6/yr and contributes 5% of the total core melt frequency. The dominant contributor to this sequence is failure of 120 VAC inverter #11 (which fails PCS and results in failure to actuate the motor-driven AFW pump) combined with various single failures of the AFW turbine-driven pump and failure of the operator to manually actuate the motor-driven pump from the control room.

Sequence T_1-81-65 (T_1Q-D"CC')

This sequence is a loss of offsite power (T_1) followed by a transient-induced LOCA(Q). AFW works but HPSI (D"), CSSI(C') and CARCS(C) fail. Due to the lack of primary system makeup, the core uncovers in about 1 hour (see the EG&G Station

Blackout Analysis [26]) and core melt ensues. Containment failure is predicted to be, most likely, by overpressure.

The frequency of this sequence is estimated to be 5.3E-6/yr and contributes 4% of the total core melt frequency. The dominant contributors to this sequence are various failures of AC power train A combined with failures of AC power train B. The resulting lack of AC power fails all core and containment cooling systems except the turbine-driven AFW pump.

Sequence T_1-82 (T_1L)

This sequence is initiated by a loss of offsite power (T_1) followed by failure of AFW (L). The plant scrams successfully and CARCS and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to the information presented in References 24 and 25. Recent calculations done by EG&G for the Station Blackout program [26] indicate that approximately 86 minutes is available to start an AFW pump in order to prevent core uncovery. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The sequence frequency is estimated as 4.9E-6/yr and contributes 4% of the total core melt frequency. The dominant contributors to this sequence are failure of the AFW motor-driven pump due to failures of train A of onsite AC power combined with failure of the AFW turbine-driven pump #11 and failure of the operator to start the locked-out turbine-driven AFW pump #12 and failure to restore offsite power in order to restart the motor-driven AFW pump.

Sequence Blackout

The Blackout sequence was not modeled explicitly on the event trees. This sequence is a new sequence identified by the Station Blackout Program [17]. The usual sequence modeled in most PRAs is loss of offsite power followed by loss of all onsite AC power and immediate failure of AFW due to hardware or DC power faults (see sequence T_1-85). While this usual sequence was identified in the Station Blackout Program and in this study as a dominant sequence, it was not as likely as the Blackout sequence. The Blackout sequence consists of a loss of offsite power followed by the loss of all onsite AC power and successful operation of the AFW system until battery depletion occurs some four hours into the accident (offsite and onsite AC not being recovered). Since all decay heat removal systems are failed, heatup and boiloff of the primary inventory occurs followed by core melt. Containment failure is predicted to be, most likely, by overpressure. No containment heat removal systems are operable due to the failure of AC power.

The sequence frequency is estimated to be 4.4E-6/yr and contributes 3% of the total core melt frequency. The dominant contributors to this sequence are various combinations of diesel generator and support system failures for train A and B emergency power combined with failure to recover offsite power and initiate cooling and makeup within six hours.

Sequence T_4-152 (T_4KQ)

In this sequence, a T_4 (all others) transient occurs and is followed by failure to scram and an induced LOCA due to a stuck open relief valve (Q). The PCS is assessed to have run back and the primary system has survived the initial pressure transient. The operator then successfully initiates emergency boration. Due to the estimated high initial rate of coolant loss and the low rate of pressure reduction, core uncovery and melt occurs before successful HPSI coolant injection. Injection is prevented by system pressure remaining above the HPSI shutoff head of 1275 psia. This situation is unique to the Calvert Cliffs design because of the low shutoff head of the pumps. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

This sequence frequency is estimated as 4.3E-6/yr and contributes 3% of the total core melt frequency. The single contributor to this sequence is failure to scram combined with failure of a relief valve to reclose.

Sequence T_3-139 (T_3KU)

This sequence is a T_3 (requires primary pressure relief) transient followed by a failure to scram (K) and failure of emergency boration(U). The primary system has survived the initial pressure transient due to a runback of the PCS as a result of the initiator. CE analyses [21] and NRC analysis in support of the ATWS rule [22] state that greater than 10 minutes are available for the operator to initiate emergency boration. In this study, we have assessed that, if the operator fails to start shutting the reactor down within 20-30 minutes, then core melt will result. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

This sequence frequency is estimated as 3.7E-6/yr and contributes 3% of the total core melt frequency. The dominant contributor to this sequence is a common mode failure of the Reactor Protection System to insert any control rods combined with failure of the operator to initiate emergency boration.

Sequence T_3-118 (T_3KQ)

In this sequence, we have a T_3 (requires primary pressure relief) transient followed by failure to scram and an

induced LOCA due to a stuck open relief valve (Q). The PCS has runback due to the initiator and the primary system has survived the initial pressure transient. The operator then successfully initiates emergency boration. Due to the estimated high initial rate of coolant loss and the low rate of pressure reduction, core uncovery and melt occurs before successful HPSI coolant injection. Injection is prevented by system pressure remaining above the HPSI shutoff head of 1275 psia. This situation is unique to the Calvert Cliffs design because of the low shutoff head of the pumps. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

This sequence frequency is estimated to be 2.3E-6/yr and contributes 2% of the total core melt frequency. The single contributor to this sequence is failure to scram combined with failure of a relief valve to reclose.

Sequence T_3-113 (T_3ML)

In this sequence, we have a T_3 (requires primary pressure relief) transient followed by a loss of PCS (M) and AFW (L). The reactor has scrammed and CARCS and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to information presented in References 24 and 25. Recent calculations done by EG&G for the Station Blackout program [26] indicate that 86 minutes are available to start an AFW pump in order to prevent core uncovery. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The sequence frequency is estimated as 1.7E-6/yr and contributes 1% of the total core melt frequency. The dominant contributor to this sequence is failure of 120 VAC inverter #11 (which results in failure of the PCS and failure to actuate the motor-driven AFW pump) combined with various single failures of the AFW turbine-driven pump and failure of the operator to manually actuate the motor-driven AFW pump from the control room.

Sequence S_2-59 (S_2D")

In this sequence, we have a Small-small LOCA (S_2), successful scram and secondary heat removal via the AFW system. However, HPSI (D") fails and we have no makeup in the injection phase. This initiator can be broken up into two parts: (1) reactor coolant pump seal LOCAs (IE=2E-2/yr) and (2) other Small-small LOCAs (IE=1E-3/yr). The other Small-small LOCA portion of the sequence is negligible (1E-3/yr initiating event * 1.3E-4 failure of HPSI = 1.3E-7/yr). Work done by EG&G for

the Station Blackout program [26] indicates that, for a leak of the maximum expected reactor coolant pump seal LOCA (<500 gpm) with secondary cooling available, approximately three hours is available to isolate the leak or start primary makeup. Containment sprays (CSSI) and fans (CARCS) are successful. Containment failure is predicted to be, most likely, by hydrogen burn and/or overpressure.

The frequency of this sequence is estimated to be 1.6E-6/yr and contributes 1% of the total core melt frequency. The dominant contributors to this sequence are failure of either of the two valves in the common minimum flow recirculation line. These values are common to all HPSI, LPSI, and CSS pumps. For the Small-small LOCA case, if these valves should fail closed, the HPSI pumps were assessed as failing. This is because the slow drop in primary pressure from 1600 to 1275 psi would result in pump heat up and failure due to pumping against dead head for a significant period of time (i.e., greater than 10 minutes).

Sequence T_1-85 (T_1LCC')

In this sequence, we have a loss of offsite power (T_1) followed by failure of AFW(L), CSSI(C), and CARCS(C'). The plant has scrammed successfully, but due to the lack of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to information presented in References 2 and 25. Recent calculations done by EG&G for Station the Blackout program [26] indicate that 86 minutes are available to start an AFW pump in order to prevent core uncovery. Containment failure is predicted to be, most likely, by overpressure.

The sequence frequency is estimated as 1.0E-6/yr and contributes 1% of the total core melt frequency. The dominant contributors to this sequence are of two types: (1) Maintenance of two feedwater valves which fails delivery of water to the S/G's from both turbine-driven AFW pumps combined with failure of both emergency AC power trains and no recovery of offsite power or (2) various single failures of the turbine-driven pump #11 combined with failures of both emergency AC power trains and failure of the operator to start the locked-out turbine-driven AFW pump #12 and no recovery of offsite power.

Engineering Insights

Insights from the analysis were at three levels. The first level was overall insights on plant core melt frequency. The second level was insights into the particular causes of each dominant sequence. The third level was insights into the specific causes of failure in individual systems which did not affect overall risk.

Overall Engineering Insights

The total core melt frequency for Calvert Cliffs was estimated to be 1.3E-4/yr and consisted almost entirely of sequences with frequencies greater than 1E-6/yr. This estimate is similar to estimates made for other light water reactors in other probabilistic risk assessments.

The following general classes of accident sequences were found to contribute the most to the Calvert Cliffs core melt frequency:

1. Anticipated Transients Without Scram (ATWS) contributed 33% of the core melt frequency.

2. Small-small LOCAs (S_2) contributed 20% of the core melt frequency.

3. The special transient initiator T_{DC} (loss of DC bus 11) contributed 16% of the core melt frequency.

4. Loss of Offsite Power transients (T_1) contributed 12% of the core melt frequency.

5. Loss of the Power Conversion System (PCS) transients (T_2) contributed 6% of the core melt frequency (not including the ATWS sequences).

6. All other transients (T_4) contributed 5% of the core melt frequency (not including the ATWS sequences).

7. Transients requiring pressure relief (T_3) contributed 1% of the core melt frequency (not including the ATWS sequences).

Dominant Sequence Engineering Insights

In addition to determining the overall results and significance of analysis as described above, it was important also to determine the reasons why these items were significant. Carefu. examination of the dominant contributors to the dominant sequences revealed certain insights, of which the most important are summarized below.

1. A review of the dominant and near dominant sequences shows that 12% of the total core melt frequency involves operator errors committed during the course of an accident. Almost all of this is from failure to initiate emergency boration after an ATWS.

2. A review of the dominant sequences, both before and after recovery was applied, reveals that operator recovery actions play a very important role in reducing the frequency of various accidents. Overall, operator recovery reduced the CC-1 core melt frequency by approximately a factor of 10.

3. Failures in support systems were found to be important contributors to the total core melt frequency. In particular, failure of Component Cooling Water (CCW) pump seal cooling which fails Emergency Core Cooling System (ECCS) pumps and Shutdown Heat Removal in the recirculation phase of an accident, Salt Water (SWS) ECCS pump room cooling which fails ECCS pumps in the recirculation phase, and diesel generator (DG) room cooling which fails emergency AC power were found to be important. Together these contribute to 20% of the total core melt frequency.

4. In one support system, a special transient initiating event was identified that also was found to contribute significantly to the total core melt frequency. This event was failure of 125 VDC bus #11 and resulted in the second most frequent sequence.

5. Several single failures were identified in front-line and support systems. These were the dominant contributors to some accident sequences.

    o For Small-small LOCAs, the failure of either of two valves in the common minimum flow recirculation line for all the ECCS pumps could result in heatup and failure of the HPSI and LPSI pumps as a result of pumping against dead head. This contributes to 1% of the total core melt frequency.

    o Two common modes were found in the Component Cooling Water System. First, failure of a single valve in the return line from all the HPSI and LPSI pump coolers would fail all HPSI and LPSI pumps in the recirculation phase. Second, since only one CCW heat exchanger is usually in operation, various single failures in this heat exchanger train or in its corresponding salt water train will fail all of CCW unless the operator actuates the other heat exchanger. These contribute to 3% of the total core melt frequency.

    o All auxiliary feedwater pumps take suction from the condensate storage tank through a common header. Failure of the valve in this line could

result in failure of all operating AFW pumps before the operator could stop the pumps. Because of the new AFW design where one turbine-driven pump will be locked out, the operator has the ability to realign the pump suction to an alternate tank and start the undamaged pump. In addition, the locked-out turbine-driven pump gives added recovery potential for almost all other AFW failures and significantly reduced the frequencies of many of the dominant accident sequences. This contributes 2% of the total core melt frequency.

6. The unavailability of CC-1 systems due to test and maintenance outages was found, generally, to be small compared to other system faults. Test unavailabilities were small because most systems are not taken out of service during test. Many have auto-actuation signals which realign the systems to their safety position in case of an accident. For those systems which are taken out of service, test personnel are, in general, in contact with control room operators and could quickly restore the system given an accident situation. A review of the maintenance logs showed that the frequency at which active components are taken out of service for unscheduled maintenance is small. This is primarily because it is plant policy not to do periodic maintenance on safety systems when the plant is during power. Preventive maintenance on these systems is conducted at during scheduled shutdowns.

7. Safety system and component unavailabilities caused by the failure of personnel to realign valves and circuit breakers to their safeguards position after test or maintenance activities were generally small compared to other faults. There are two basic reasons for this: (1) most safety system components have alignment verification indication in the control room and are verified during each shift using a check list, and (2) the component tagging procedure require operators to perform redundant checks on components following test and maintenance.

8. The HPSI pumps have a low shutoff head (~1275 psia) and successful primary makeup or operation in a "feed and bleed" mode to remove decay heat is not thought to be possible for sequences where secondary heat removal has failed or a failure to scram has occurred. The ability to "feed and bleed" would affect most of the ATWS and loss of secondary heat removal sequences and would significantly reduce the total core melt frequency.

System Reliability Engineering Insights

During the early stages of the study, some discoveries were made of specific items which affected the reliability of individual systems. These were important to individual system reliability; but, when the systems were analyzed together, it turned out that these items did not contribute significantly to risk. Since this is the case, modifications to solve these "problems" would not significantly reduce risk. However, they are, nonetheless, interesting, if only to illustrate the type of things which can be found by a detailed probabilistic analysis. Some of these insights are summarized below (the reader should refer to the system descriptions in Appendix B for more discussion of these and other insights):

- The Power Operated Relief Valves are powered from two separate AC buses, but both require actuation of relays powered by the same DC bus to allow AC power to reach the valves.

- The Low Pressure Safety Injection System is automatically shutdown in the recirculation phase of a LOCA. This is because the High Pressure Safety Injection System is designed to draw directly from the containment sump in the recirculation mode and is the preferred system. The low pressure system can be used but, depending on the way in which the recirculation signal was generated, some complicated operator actions might be involved.

- The swing pumps in the Service and Salt Water Systems are aligned electrically to one train and mechanically to the other train. On failure of the operating pump in a subsystem, the swing pump does not automatically supply backup to that subsystem.

Plant Modifications

The utility has not yet made any changes to procedures or hardware directly as a result of this study. Several insights developed during the course of the study are currently being looked at by the utility to determine their significance and if any changes may be warranted. After the study is completed, the utility intends to use all the models developed to help analyze the effects of proposed modifications on plant risk. The insights the utility is currently examining are:

- For long term loss of offsite power, a 69 KV line which connects to the neighboring grid could be used to supply the necessary AC power to both units. The utility is re-examining the procedure for its use in light of the importance of loss of offsite power to plant risk.

o The utility intends to use the motor-driven AFW pumps for crossfeeding the units in instances where the AFW system on one unit has failed. Some insights discovered as a result of this study which relate to this, as yet unwritten, procedure are (1) since the feedwater valves are normally open, starting the motor-driven pump on the operating unit will inject cold water into that unit's steam generators (this is significant because the operators might be reluctant to initiate crossfeeding without specific instructions), and (2) for loss of offsite power situations failure of a diesel generator (which has a relatively high failure rate) may preclude the motor-driven pump on the other unit from operating so the recovery potential will be limited by the DG unavailability. In the second case, the importance of being able to use the locked-out turbine-driven AFW pump is increased.

Uncertainty and Sensitivity

The techniques for performing data uncertainty analysis are in the process of being improved, and it was decided to use the Calvert Cliffs IREP study to test the improved techniques. Therefore, a data uncertainty analysis is not presented in this report, but will be published later in a separate volume.

A sensitivity analysis is reported in Section 8.3 and covers the following items:

(1) HPSI pumps requirement for seal and room cooling for Small-small LOCAs.

(2) Crossfeeding AFW from the other unit.

(3) The ability to perform primary system "Feed and Bleed".

(4) ATWS (i) Service level "C" vs. "D."

(ii) Pressure equilibrating below the relief valve set point for an extended time after failure to borate.

(iii) Pressure decreasing enough with a stuck open PORV to have successful primary makeup before core uncovery.

(iv) Various Probabilities of unfavorable MTC.

(v) Various Probabilities of failure to scram.

Table S.1

Final Calvert Cliffs Dominant Accident Sequences
(after recovery)

SEQUENCE	DESCRIPTION	IREP FREQUENCY BEFORE RECOVERY (/YR)	IREP FREQUENCY AFTER RECOVERY (/YR)	% TOTAL CM FREQUENCY
ATWS(PSF)	----	2.8E-5	2.8E-5	20
T_{DC}-82	$T_{DC}L$	4.9E-4	2.1E-5	16
S_2-50	S_2H	5.1E-5	1.4E-5	11
S_2-52	S_2FH	5.7E-5	1.1E-5	9
T_2-82	T_2L	1.8E-4	7.1E-6	6
T_4-173	T_4KU	6.7E-6	6.7E-6	5
T_4-147	T_4ML	3.4E-4	6.3E-6	5
T_1-81-65	T_1Q-D"CC'	1.3E-5	5.3E-6	4
T_1-82	T_1L	2.4E-5	4.9E-6	4
Blackout	----	2.4E-4	4.4E-6	3
T_4-152	T_4KQ	4.3E-6	4.3E-6	3
T_3-139	T_3KU	3.7E-6	3.7E-6	3
T_3-118	T_3KQ	2.3E-6	2.3E-6	2
T_3-113	T_3ML	8.5E-5	1.7E-6	1
S_2-59	S_2D"	2.8E-6	1.6E-6	1
T_1-85	T_1LCC'	5.9E-5	1.0E-6	1
Sequences below cutoff	----	----	7.8E-6	6
Total	----	----	1.3E-4	100

Table S.1 (Cont.)

Legend Used in Tables S.1, and S.2

<u>Initiating Events</u>

S_2 = Small-small LOCA (1.9" in dia.)

T_1 = Loss of Offsite Power

T_2 = Loss of PCS

T_3 = Transients requiring primary relief

T_4 = All other transients

T_{DC} = Loss of 125 VDC bus 11

<u>System Failures</u>

D" = High Pressure Safety Injection

F = Containment Spray System (Recirculation)

H = High Pressure Safety Recirculation System

K = Reactor Protection System

L = Auxiliary Feedwater System

M = Power Conversion System

Q = Relief valves fail to reclose

U = Chemical Volume and Control System

C = Containment Air Recirculation and Cooling System

C' = Containment Spray System (Injection)

<u>Containment Failure Modes</u>

α = Vessel steam explosion

β = Leakage

γ = Hydrogen burning

δ = Overpressure

δ' = Delayed overpressure

ϵ = Basemat meltthrough

Table S.2

Calvert Cliffs Unit-1 Dominant Accident Sequence
Frequencies by Release Category

Sequence	Release Category 1	2	3	4	5	6	7
ATWS (PSF)	α=2.8E-9	--	γ+δ=2.0E-5	--	β=2.0E-7	--	ε=8.4E-6
$T_{DC}L$	α=2.1E-9	--	γ+δ=1.5E-5	--	β=1.5E-7	--	ε=6.3E-6
S_2H	α=1.4E-7	--	γ+δ=9.8E-6	--	β=9.8E-8	--	ε=4.2E-6
S_2FH	α=1.1E-7	γ+δ=7.7E-6	--	β=7.7E-8	--	ε=3.3E-6	--
T_2L	α=7.1E-10	--	γ+δ=5.0E-6	--	β=5.0E-8	--	ε=2.1E-6
T_4KU	α=6.7E-10	--	γ+δ=4.7E-6	--	β=4.7E-8	--	ε=2.0E-6
T_4ML	α=6.3E-10	--	γ+δ=4.4E-6	--	β=4.4E-8	--	ε=1.9E-6
T_1Q-D"CC'	α=5.3E-10	δ=4.2E-6	δ'=1.1E-6	β=3.7E-8	--	--	--
T_1L	α=4.9E-10	--	γ+δ=3.4E-6	--	β=3.4E-8	--	ε=1.5E-6
Blackout	α=4.4E-10	δ=3.5E-6	δ'=8.8E-7	β=3.1E-8	--	--	--
T_4KQ	α=4.3E-10	--	γ+δ=3.0E-6	--	β=3.0E-8	--	ε=1.3E-6
T_3KU	α=3.7E-10	--	γ+δ=2.6E-6	--	β=2.6E-8	--	ε=1.1E-6
T_3KQ	α=2.3E-10	--	γ+δ=1.6E-6	--	β=1.6E-8	--	ε=6.9E-7
T_3ML	α=1.7E-10	--	γ+δ=1.2E-6	--	β=1.2E-8	--	ε=5.1E-7
S_2D"	α=1.6E-10	--	γ+δ=1.1E-6	--	β=1.1E-8	--	ε=4.8E-7
T_1LCC'	α=1.0E-10	δ=8.0E-7	δ'=8.0E-7	β=7.0E-9	--	--	--
Category Total	2.6E-7	2.0E-5	7.5E-5	1.5E-7	7.2E-7	3.3E-6	3.1E-5

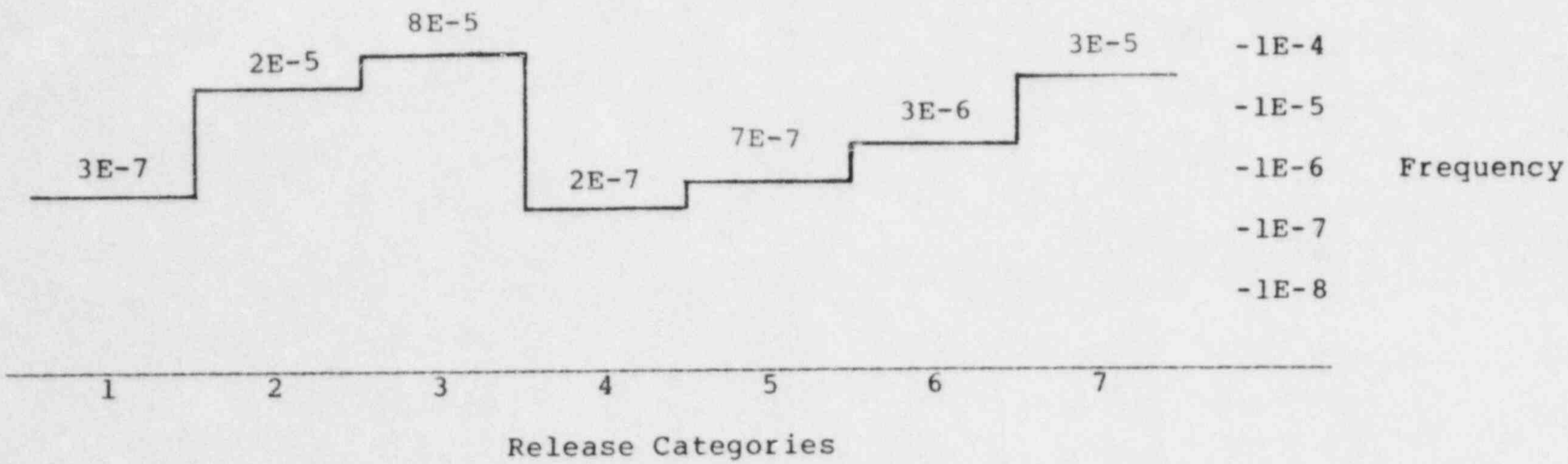


Figure S-1 Calvert Cliffs Unit-1 Histogram of Release Category Frequencies

CHAPTER 1

INTRODUCTION

1.1 IREP Overview

Probabilistic safety analysis and risk assessment techniques are widely believed to offer powerful tools for the safety design and safety evaluation of nuclear power plants. Past attempts to apply such techniques to commercial nuclear plants have provided useful catalogues of accident sequences, identified many strengths and weaknesses in the design and operation of the plants, provided insights into the importance of accident contributors, and provided estimates of the likelihood of serious accidents. Recent evidence tends to suggest that plant-to-plant differences in design and operation may give rise to significant differences in the likelihood and/or course of accidents. Therefore, the extensive application of these safety analysis techniques to many reactor plants appears to be desirable. This need is reflected in the TMI Action Plan (NUREG-0660) [1] in which the Interim Reliability Evaluation Program (IREP) is identified as a high priority effort leading to the systematic risk assessment of all reactors by other PRA programs (Section II.C).

The Interim Reliability Evaluation Program is intended to apply probabilistic risk analysis techniques to five nuclear power plants and to develop procedures adequate for the consistent analysis of all plants with the following specific objectives: (1) identify -- in a preliminary way -- those accident sequences that dominate the contribution to the public health and safety risks originating in nuclear power plant accidents; (2) develop a foundation for subsequent, more intensive, applications of probabilistic safety analysis or risk assessment on the subject plants; (3) expand the cadre of experienced practitioners of risk assessment methods within the NRC and the nuclear power industry; and (4) evolve procedures codifying the competent use of these techniques for use in the extension of IREP to all domestic light water reactor plants.

Phase I of the IREP study consisted of a reliability analysis of the Crystal River Unit 3 facility. A report on that effort has been published (NUREG/CR-2515)[2]. Using methodological insights gained from the Crystal River Study, the Phase II IREP studies were initiated in September 1980. The Phase II studies consist of analyses of four plants:

1. Browns Ferry Unit 1, by a team composed of personnel from EG&G, Idaho and Energy, Inc.

2. Arkansas Nuclear One Unit 1, by a team composed of personnel from Sandia National Laboratories, Science Applications, Inc. (SAI), and Arkansas Power and Light Company.

3. Calvert Cliffs Unit 1 (CC-1), by a team composed of personnel from Sandia National Laboratories, Energy, Inc., Science Applications, Inc., Evaluation Associates, Baltimore Gas and Electric, and NRC.

4. Millstone Unit 1, by a team composed of personnel from Science Applications, Inc., Northeast Utilities, and NRC.

Responsibility for overall technical management of the study rested with Sandia National Laboratories. Periodic reviews to assure the quality of the product were conducted by Sandia National Laboratories and NRC personnel not directly involved with the work of any one team, with the assistance of Energy, Inc.

This report is one of a series of four reporting the results of these Phase II studies. A separate report, the IREP Procedures Guide [3], has been issued detailing procedures for conducting future analyses of the same scope and breadth as these four studies, and detailing the technical and methodological insights and nuclear safety perspectives gained from this activity.

The reader is cautioned that while it is our opinion that these studies represent the state-of-the-art given their scope, they are incomplete. External events (earthquakes, fires, etc.) are not included, and the assignment of accident sequences to release categories was performed in a subjective manner with limited plant-specific calculations. Thus, this portion of the study relied heavily on analyses performed previously on similar facilities. Other limitations are discussed in detail in Chapter 8. While accident sequence and release category frequencies were quantified, they are of value primarily in comparative analyses, and the absolute values determined should not be used without a clear appreciation of their inherent uncertainties. The principal product obtained is the integrated engineering logic presented in the plant and system models and insights into plant features contributing significantly to risk, not the specific values computed for accident frequencies.

1.2 Calvert Cliffs Unit 1 Analysis Team Makeup

The team was comprised of 21 individuals from Sandia National Laboratories, Remote Sensing, Inc., Energy, Inc., Science Applications, Inc., Evaluation Associates, Inc., Baltimore Gas and Electric Co., University of Maryland, and the

U. S. Nuclear Regulatory Commission. Four members worked full time, while the remaining 19 contributed on a part-time basis, either part-time for all or part of the study, or full time for a portion of the study. Sandia National Laboratories was responsible for team leadership. The team members had varying degrees of risk analysis experience. Some had little or no experience, while others had participated in studies such as the Reactor Safety Study Methodology Applications Program, the Crystal River Study, the Station Blackout Program, Ringals II Safety Study, and the Reactor Safety Study.

Sixteen of the twenty-one members were systems analysts. They were responsible for construction of the event tree and fault tree models which were utilized in determining the most frequent core melt accident sequences.

Three of the members were computer specialists. One of these was responsible for manipulation and debugging of the computerized fault tree models. The remaining two were responsible for running the SETS code [4]. SETS operates on the system fault tree models and performs the Boolean algebra necessary to determine the most frequent core melt accident sequences.

Although no team members were human factors specialists, the Calvert team did have access to the services of two human factors specialists. Each team member was responsible for the initial evaluation of human factors effects on each system. This included the evaluation of operational and emergency procedures, and test and maintenance procedures and their effects on the plant response to LOCA and transient initiators. Once the dominant human interactions were identified using conservative initial values, a detailed human reliability analysis using the techniques presented in NUREG/CR-1278[5] was performed.

Finally, two team members, provided by Baltimore Gas and Electric, acted to provide information concerning plant operations. Their familiarity with the plant design and operation helped facilitate modeling of the plant systems and operator response.

CHAPTER 2

IREP METHODOLOGY

To provide guidance for the IREP analyses and to aid consistency among the four IREP teams, procedures for the analysis were developed. Since these procedures had never been used in their entirety, it was recognized that some flexibility in approach would be necessary. Nevertheless, the four teams generally followed the same approach, which is described below. A more detailed description can be found in the IREP Procedures Guide [3].

2.1 Information Base

The IREP analysis of a plant represents an integrated plant systems analyses. Detailed analyses were performed of those systems required to respond to a variety of initiating events (i.e., front-line systems) and of those systems supporting the responding systems. The analyses included unavailabilities during test and maintenance activities, human errors which could arise in restoring the systems to operability following test and maintenance and in response to accident situations, and a thorough investigation of support system faults which could affect operations of more than one front-line system.

To perform the IREP analysis, considerable and, in some instances very detailed, information was obtained from the plant. The sources of information used in the analysis are listed in Table 2.1.

The Final Safety Analysis Report (FSAR)[6] and plant system descriptions and drawings provided the basic information base for the analysis. This was supplemented by information contained in other studies of the plants (where available) and by more detailed information in support of particular aspects of the analysis.

To identify initiating events and initiating event frequencies, EPRI NP-2230, "ATWS: A Reappraisal - Part 3, Frequency of Anticipated Transients,"[7] was used as the basic source. Additional insight was obtained through reviewing Licensee Event Reports (LERs) for the plant and for plants of similar design. To identify the systems needed to respond to an accident and their success criteria, the FSAR was used. In some instances, documentation from the plant, Nuclear Steam Supply System (NSSS) vendor or other reports was obtained suggesting and supporting the use of less stringent success criteria.

To construct the fault tree models, more detailed drawings were obtained, particularly for electrical systems and control and actuation circuitry. Test, maintenance, and emergency procedures were reviewed to identify potential human errors to be included in the plant models.

Data for quantifying the fault trees was a mixture of generic and plant specific data. Basic hardware failure rate data was initially obtained from a modified WASH 1400 data base [8] assembled by the NRC. Later, a generic data base, given in the IREP procedures guide [3], was developed and used in the Calvert Cliffs study. For particular components, plant specific failure data obtained from plant logs was used. Plant specific test and maintenance frequencies were obtained from plant logs and used in the analysis. Data for human error rates was obtained from NUREG/CR-1278.[5]

In addition to the above documentation, the utility personnel participating in the study served as contacts with the plant to obtain more information when needed. Each team visited its plant to view particular equipment and to discuss questions with plant personnel. The utilities also reviewed periodic reports to ensure accuracy of information.

2.2 Methodology

The IREP analyses consisted of eight tasks:

1. Plant familiarization
2. Event tree construction
3. Systems analysis
4. Human reliability and procedural analysis
5. Data development
6. Accident sequence evaluation
7. Containment analysis
8. Interpretation and analysis of results.

The relationships among these tasks are illustrated in Figure 2-1. Each is discussed briefly below.

2.2.1 Plant Familiarization

The initial task of the analysis involved the analysts' becoming familiar with the plant. This began by identifying those functions which must be performed to prevent core melt or to mitigate its consequences. By reviewing the FSAR and other documentation, the systems which perform these functions, termed "front-line systems," were identified.

Initiating events for consideration in the analysis were determined from EPRI NP-2230 and a review of LERs. These were grouped according to the systems which must respond to the

event. Loss-of-coolant accidents (LOCAs) were generally grouped into three or four groups. This grouping tended to be by size of LOCA since mitigating requirements generally depend on the size of the break. Transients fell into three to six groups. The grouping often reflected equipment lost as a result of the initiating event.

For each initiating event grouping, the criteria for successful system operation to mitigate the accident were determined. This information was usually found in the FSAR. Utility, NSSS vendor calculations and other reports sometimes indicated that the FSAR criteria were too conservative. Where appropriate documentation existed, the IREP teams used the more realistic criteria.

A final activity during the plant familiarization tasks was the identification of system dependencies. Systems which support the front-line systems were identified; dependencies among various support systems were also noted.

Upon completion of the plant familiarization task, the following information had been developed:

1. The necessary functions to prevent core melt or to mitigate its consequence;

2. The systems which perform these functions (front-line systems);

3. The generic initiating events included in the analysis and grouped according to mitigating requirements;

4. The systems required to respond to each initiating event group and the criteria for system success; and

5. Dependencies between front-line and support systems and support systems with other support systems.

This task set the groundwork for construction of the models used in the study. The systems to be analyzed were identified, and the number of and headings for event trees were defined.

2.2.2 Event Tree Construction

The accident sequences to be analyzed in IREP were delineated by event trees. Functional event trees were constructed to clarify functional dependencies. From these and information developed in the plant familiarization activity, systemic event trees were constructed. Sequences delineated on the systemic trees were analyzed in the study.

In general, separate systemic event trees were constructed for each initiating event group. Each event tree had a different structure since the initiating events were grouped according to mitigating requirements. Different mitigating requirements result in different tree structure. Headings for the event trees correspond to the systems responding to the initiating event. Only front-line systems appear on the trees. Most identified system dependencies and dependencies arising from phenomenological aspects of the accident are reflected in the tree structure.

2.2.3 Systems Analysis

Fault tree models were constructed for each front-line system. Support system fault trees were constructed to model the particular interfaces with the front line systems. In general, different fault tree modeling techniques were used by the different IREP teams. The approach used in The Calvert Cliffs Unit 1 analysis is discussed in Chapter 6. Top events for the front-line system fault trees correspond to the success criteria defined in the plant familiarization task.

The fault trees were developed to the component level. Component faults which affected only the particular component were grouped as "local faults." Faults which could affect multiple components, generally those faults associated with support systems, were further developed. The level of detail in the fault trees generally corresponded to the detail of available data.

In addition to hardware faults, the fault trees included unavailability due to test and maintenance, human errors associated with failing to restore components to their operable state following test and maintenance, and human errors associated with accident responses. The human reliability analysis is discussed in the next section.

The detailed development contained in the system fault trees facilitated identification of hardware, test and maintenance, and human error faults which could cause multiple component failures. These classes of common mode failures were explicitly modeled in the fault trees. Other potential common mode failures such as environmental conditions or manufacturing defects were not considered in the study.

2.2.4 Human Reliability and Procedural Analysis

Test, maintenance, and emergency procedures were reviewed to determine potential human errors. Human errors associated with failing to restore a system to its operable state following test and maintenance were included explicitly in the fault trees. Potential operator errors in response to an accident

were included in a limited way. The emergency procedures expected to be used in response to each accident sequence were reviewed to identify actions expected to be performed. Incorrect performance and omission of the actions were postulated and included in the model. The investigation, however, was limited to those actions expected to be performed, rather than postulating all actions an operator might take.

2.2.5 Data Development

A modified WASH-1400 [8] data base was used for quantification of hardware faults. However, for Calvert Cliffs, when the IREP generic data base [3] was developed, the basic data were changed to reflect the updated recommendations. In some instances, plant specific data was used instead. Test and maintenance intervals and durations were obtained, where possible, from discussions with plant personnel and from reviewing plant logs. Estimated upper values were chosen for human error rates for initial calculations. For those human errors which appeared in potentially dominant accident sequences, detailed analyses were performed with the assistance of human factors specialists. This approach to human error quantification permitted more efficient utilization of limited human factors expertise.

2.2.6 Accident Sequence Evaluation

For each accident sequence, a frequency was calculated. This was performed by logically combining the initiating event and the system successes and failures to develop combinations of failures (cut sets) which could result in the accident sequence. Frequencies assigned to the initiating events, and probabilities assigned to each failure, were combined to generate a frequency for each sequence.

The evaluation process was an iterative one. Initial calculations used generic data and upper bound human error rates. From these initial calculations, a collection of potentially dominant accident sequences was chosen. These were chosen based on a certain frequency below which none of the sequences were expected to contribute significantly.

The potentially dominant sequences were examined more closely to ensure that the probabilities chosen were as accurate as they could be and to develop better human error rate estimates. The potential for recovery actions which could terminate the sequence was then evaluated and the sequence frequencies where recalculated. These more refined calculations resulted in a list of dominant accident sequences.

2.2.7 Containment Analysis

Each potential accident sequence was evaluated by Battelle Columbus Laboratories (BCL) to determine the expected mechanism of containment failure, the associated probability of failure, and to characterize the potential radioactive release. This analysis was quite limited in nature, relying primarily on insights developed from similar analyses in the past [9], but supplemented by further calculations where necessary.

2.2.8 Interpretation and Analysis of Results

The dominant accident sequences in terms of risk (the highest frequency sequences in the most severe release categories) were examined to draw engineering insights of interest from the analysis. Those plant vulnerabilities and failure modes contributing most significantly to risk were identified. These constitute the principal results of the study.

Table 2.1. Information Sources for IREP

- o Final Safety Analysis Report [6]
- o System description and plant drawings
- o Other probabilistic analyses of the plant [9]
- o EPRI/NP-2230, "ATWS: A Reappraisal -- Part 3: Frequency of Anticipated Transients" [7]
- o Licensee Event Reports for the plant and similar plants
- o System performance documentation
- o Electrical one-line drawings
- o Control and actuation circuitry drawings
- o Test and maintenance procedures
- o Emergency procedures
- o A generic data base [3], [8]
- o Plant logs
- o "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications" (NUREG/CR-1278)[5]
- o Plant visits
- o Discussions with and review by plant personnel

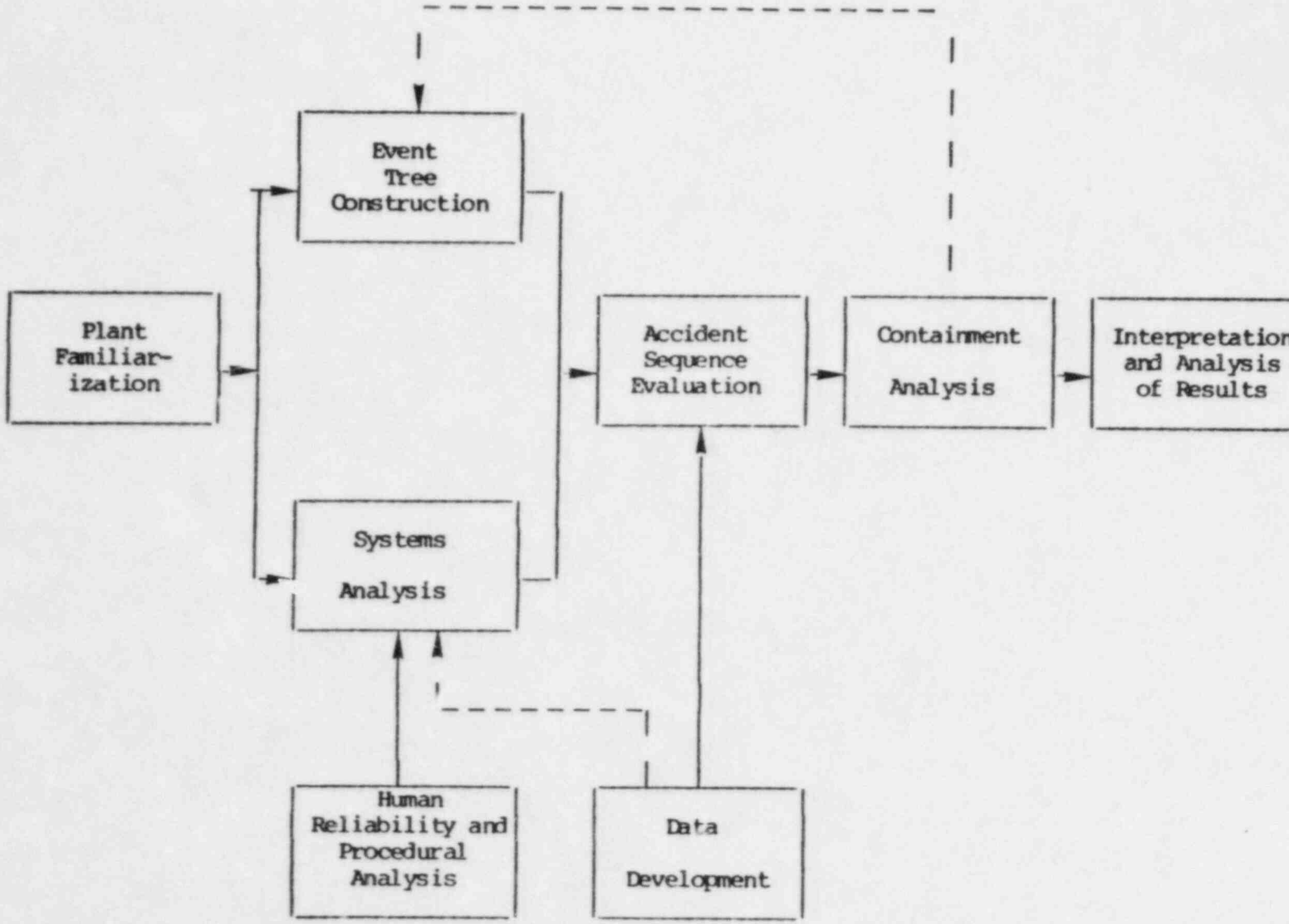


Figure 2-1 IREP Methodology

CHAPTER 3

PLANT DESIGN

3.1 Basic Information

Calvert Cliffs Nuclear Power Plant-Unit 1 (CC-1) is the first unit of a two unit plant owned and operated by Baltimore Gas and Electric Company (BG&E). Bechtel Power Corporation was the architect-engineer, and Combustion Engineering, Incorporated (CE) was the reactor supplier. The operating license for CC-1 was issued by the Nuclear Regulatory Commission (NRC) in September, 1974. Commercial operation started in May, 1975. The CC-1 plant is located on the western shore of the Chesapeake Bay in Calvert Cliffs County, Maryland, about 10 miles southeast of the town of Prince Fredrick.

3.2 Plant Functions

The plant functions required to ensure safe shutdown following a transient initiator are different from those required following a LOCA initiator. The important functions required to place the reactor in a safe condition following a LOCA are (1) Reactor Subcriticality, (2) Reactor Heat Removal, (3) Containment Atmospheric Heat Removal, and (4) Containment Radioactivity Removal. In addition to the four functions listed above for LOCAs, transients require two other functions: (1) Primary System Relief, and (2) Reactor Coolant System Integrity. In the case where failure of a function leads to core melt, success or partial success of other functions may still result in significant mitigation of the accident consequences.

Outlined in this section is a description of each of the plant functions listed above, including the plant systems that can be used to fulfill each of these functions. The response of the plant functions to LOCA and transient initiators is presented in Chapter 5 of this report. Tables 3.1 and 3.2 contain listings of the required plant functions following a LOCA or a transient, respectively, and the systems that can perform each function. The systems used to perform the mitigating functions are more thoroughly described in Chapter 6 and Appendix B.

3.2.1 LOCA Mitigating Functions

3.2.1.1 Reactor Subcriticality (RESC)

This function is necessary in order to decrease the power output of the core to the decay heat level. At this level, decay heat only, the emergency core cooling and containment cooling systems have sufficient capacity to remove the energy from the primary system and prevent core melt.

For Large LOCAs (i.e., breaks greater than 4.3" in diameter), the reactor is rendered subcritical due to core voiding caused by the LOCA and subsequent reflooding of the core by borated water from the emergency core cooling systems. For Small and Small-small LOCAs (i.e., breaks from 1.9" to 4.3" and .3" to 1.9" in diameter, respectively), it is necessary to use the Reactor Protection System (RPS) to perform the function of Reactor Subcriticality. This is done by inserting the shutdown rods into the reactor core immediately following a LOCA signal.

3.2.1.2 Reactor Heat Removal(REHR)

The systems used for reactor heat removal during LOCAs are intended to both replace the coolant lost during the LOCA and to remove the residual decay heat from the core. This protects the core from uncovery, heat up, and subsequent core melt. This function is generally divided into two phases: 1) Injection -- where makeup water is drawn from the Refueling Water Tank (RWT), and 2) Recirculation -- where the makeup water is drawn from the containment sump.

In the injection phase, water is pumped from the RWT by the High Pressure Safety Injection (HPSI) System and the Low Pressure Safety Injection (LPSI) System. These systems are actuated on decreasing primary system pressure (at 1600 psia) or on increasing containment pressure (at 2.8 psig) by a safety injection signal and begin injecting water into the core at about 1275 psia and 200 psig, respectively. The HPSI system consists of three high-pressure pumps which draw water directly from the RWT and inject it into the four primary loop cold legs. The LPSI consists of two low-pressure pumps which also draw directly from the RWT and inject into the four primary loop cold legs. For large LOCAs, the LPSI system operates in conjunction with the Safety Injection Tanks (SIT) System to keep the core covered and cool. The SIT system consists of four pressurized tanks which supply additional water during the initial phase of the LOCA when the primary pressure reaches 200 psig. For Small LOCAs, the HPSI system can perform this function alone. For Small-small LOCAs, the HPSI system must be used in conjunction with the Auxiliary Feedwater (AFW) System. This is because additional heat removal is necessary to decrease the primary system pressure to below the shutoff head of the HPSI pumps (about 1275 psia). The AFW system consists of two turbine-driven pumps and one motor-driven pump which draw water from the Condensate Storage Tank (CST) and inject it into the Steam Generators (SGs). The water in the SGs absorbs heat from the primary system and boils off, venting to the atmosphere.

In the recirculation phase, either the High Pressure Safety Recirculation (HPSR) System (for all LOCA sizes) or the Low Pressure Recirculation (LPSR) System (for Large LOCAs only) can perform the Reactor Heat Removal function. However, at Calvert Cliffs, the HPSR system is the preferred system. This is because the LPSI system is designed to shutoff on switchover to the recirculation phase and requires operation action to restart. These systems are really the HPSI and LPSI systems realigned to draw water from the containment sump when the water level in the RWT reaches a low level.

3.2.1.3 Containment Atmospheric Heat Removal (CNHR)

During the injection and recirculation phases following a LOCA, steam emitted through the break will cause the containment pressure to increase. If the steam is not condensed, the containment would fail due to overpressure within several hours.

In the injection phase, two systems can perform this function: (1) the Containment Spray System (Injection) (CSSI) which consists of two pumps that draw cold water from the RWT and spray it into the containment atmosphere in order to condense the steam; or (2) the Containment Air Recirculation and Cooling System (CARCS) which consists of four fans which cool the containment atmosphere using heat exchangers which reject the heat to the environment. Both these systems are actuated on high containment pressure (at 4 psig).

In the recirculation phase, the CARCS can continue to perform this function without any realignments; however, the CSSI must be aligned to draw water from the sump similar to the HPSI and LPSI systems. In this mode, the CSSI is called Containment Spray System (Recirculation) and denoted CSSR. However, since the CSSR system is drawing hot water from the sump, it would no longer be effective unless there was some way of cooling the water before it was sprayed into the containment. This is done using the Shutdown Heat Exchangers (SDHX) System which consists of two heat exchangers in the CSSR spray lines that cool the spray before it is injected into the containment.

3.2.1.4 Containment Radioactivity Removal (CNRR)

After a LOCA has occurred, some method needs to be used to remove the radioactive material released into the containment atmosphere through the break. The CSSI and CSSR perform this function in the injection and recirculation phases, respectively. By spraying water into the containment atmosphere, the radioactive material can be scrubbed out of the atmosphere into the water where it can later be processed.

Both this function and the Containment Heat Removal function, previously discussed, can also mitigate the consequences of accidents which proceed to core melt.

3.2.2 Transient Mitigating Functions

3.2.2.1 Reactor Subcriticality (RESC)

The Reactor Subcriticality function for a transient is the same as that for a LOCA. However, in addition to the Reactor Protection System (RPS), the Chemical Volume and Control System (CVCS) can also be used to shut down the reactor. The CVCS consists of three pumps which can inject a concentrated boric acid solution directly into the primary, resulting in reactor shutdown within a few minutes.

3.2.2.2 Reactor Heat Removal (REHR)

The systems used for reactor heat removal during a transient must keep the core cool by removing the decay heat. Primary makeup is not necessary, unless a transient-induced LOCA occurs; in which case the appropriate LOCA systems must be used.

Two systems can perform the REHR function for transients. The Power Conversion System (PCS) and the Auxiliary Feedwater (AFW) System. The PCS is normally used for decay heat removal. The system consists of the Main Feedwater (MFW) and Condensate Systems (CS) which deliver water to the steam generators via three motor-driven condensate pumps, three motor-driven condensate booster pumps and two turbine-driven main feedwater pumps. The steam is removed by the Secondary Steam Relief (SSR) System to the atmosphere or back to the main condensor via the turbine bypass valves. If the PCS should be unavailable, then the Auxiliary Feedwater (AFW) System can be used to remove the decay heat. The AFW system consists of two turbine-driven pumps and one motor-driven pump which draw water from the CST and deliver it to the steam generators.

3.2.2.3 Primary System Relief (PSR)

Following some severe transients, the surge capacity of the pressurizer may not be sufficient to prevent a pressure increase from rupturing the reactor coolant system. In particular, for all transients in which the Reactor Protection System (RPS) fails, a pressure spike is assumed to rupture the primary system and lead to an unmitigatable LOCA unless primary system pressure relief occurs. This relief is accomplished in all cases by using the two Safety Relief Valves (SRVs) and two Power Operated Relief Valves (PORVs).

3.2.2.4 Reactor Coolant System Integrity (RCSI)

For those transients where Primary System Relief was required or the relief valves may have been demanded but relief was not required to mitigate the accident, all the relief

valves which opened must reclose when the pressure subsides or a transient-induced LOCA may result (equivalent to a Small-small LOCA).

3.2.2.5 Containment Heat Removal (CNHR)

The function and systems used are identical to the LOCA function described in section 3.2.1.3.

3.2.2.6 Containment Radioactivity Removal (CNRR)

The function and systems used are identical to the LOCA function described in section 3.2.1.4.

3.3 System Dependencies

The systems described in section 3.2, which directly perform the accident mitigating functions are called "front-line" systems. In order to (1) identify special initiating events (discussed in Chapter 4), (2) to adequately model systems to include potential common mode failures, and (3) to establish a complete list of systems which need to be modeled; the system dependencies between front-line systems, between front-line and support systems, and between support systems were identified. This was done by looking at each major component in each front-line system one at a time to determine what kind of support requirements it had and where it got the support from. This was then repeated for each component in the support systems which were identified, and the process was continued until all obvious dependencies were identified. The results of this process are shown in the Failure Mode and Effects Analyses (FMEAs) done for each system in Appendix B. A summary of these dependencies is shown in Tables 3.3 and 3.4.

Several systems at Calvert Cliffs are either shared between units 1 and 2 or have connections with similar systems on the other unit. The two systems which are shared are the emergency AC and DC power systems and these are modeled explicitly in this analysis to include all components which can affect unit 1. Also, if a failure of a unit 2 component could affect a unit 1 component (e.g. Diesel Generator 21 failure on unit 2 could require diesel generator 12, which is a swing diesel, to be diverted to unit 2), the event was modeled on unit 1's fault trees. Those connections which increased the reliability of a system on a particular unit were not modeled explicitly on the fault trees since they usually required some operator action and were better treated in the recovery analysis or were judged not to be significant.

A description of each support system can be found in the appropriate section of Chapter 6 and Appendix B.

TABLE 3.1

CC-1 LOCA FUNCTION/SYSTEM INDFX

LOCA Function	System(s)
Reactor Subcriticality (RESC)	a) Reactor Protection System (RPS)
Reactor Heat Removal (injection phase) (REHR)	a) High Pressure Safety Injection System (HPSI) with/ without Auxiliary Feedwater System (AFW)
	b) Safety Injection Tanks (SIT)
	c) Low Pressure Safety Injection (LPSI)
Containment Atmospheric Heat Removal (CNHR) (injection phase)	a) Containment Spray System, Injection (CSSI)
	b) Containment Air Recirculation and Cooling System (CARCS)
Containment Radioactivity Removal (CNRR) (injection phase)	a) Containment Spray System, Injection (CSSI)
Reactor Heat Removal (REHR) (recirculation phase)	a) High Pressure Safety Recirculation System (HPSR)
	b) Low Pressure Safety Recirculation System (LPSR)
Containment Heat Removal (CNHR)(recirculation phase)	a) Containment Spray System, Recirculation (CSSR) and Shutdown Cooling Heat Exchangers (SDHX)
	b) Containment Air Recirculation and Cooling System (CARCS)
Containment Radioactivity Removal (CNRR) (recirculation phase)	a) Containment Spray System, Recirculation (CSSR)

TABLE 3.2

CC-1 TRANSIENT FUNCTION/SYSTEM INDEX

Transient Function	System(s)
Reactor Subcriticality (RESC)	a) Reactor Protection System (RPS) b) Chemical Volume and Control System (CVCS)
Reactor Heat Removal (REHR)	a) Power Conversion System (PCS) (i.e.,, Main Feedwater (MFW) and secondary steam relief (SSR) or turbine bypass) b) Auxiliary Feedwater System (AFW) and secondary steam relief (SSR)
Primary System Relief (PSR)	a) Safety Relief Valves (SRVs) and Power Operated Relief Valves (PORVs) open
Reactor Coolant System Integrity (RCSI)	a) Safety Relief Valves (SRVs) and Power Operated Relief Valves (PORVs) close
Containment Heat Removal	a) Containment Spray System, Injection (CSSI) b) Containment and Cooling System (CARCS)
Containment Radioactivity Removal (CNRR)	a) Containment Spray System, Injection (CSSI)

TABLE 3.3

FRONT-LINE SYSTEM VS SUPPORT SYSTEM DEPENDENCIES

Front-line System*	Support System**								
	Offsite AC	ESFAS	Emerg. AC	DC	CCW	SRW	SWS	RMCL	Air
RPS									
CVCS	X	X	X	X					
SIT									
LPSI/R	X	X	X	X	X			X	
HPSI/R	X	X	X	X	X			X	
CSSI/R	X	X	X	X	X			X	
CARCS	X	X	X			X			
PCS	X	X		X		X			X
AFW	X	X	X	X					
SDHX	X	X	X	X	X				
SRV									
PORV	X		X	X					

*The front-line systems are:

RPS = Reactor Protection System
CVCS = Chemical Volume and Control System
SIT = Safety Injection Tanks
LPSI/R = Low Pressure Safety Injection/Recirculation System
HPSI/R = High Pressure Safety Injection/Recirculation System
CSSI/R = Containment Spray System Injection/Recirculation System
CARCS = Containment Air Recirculation and Cooling System
PCS = Power Conversion System
AFW = Auxiliary Feedwater System
SDHX = Shutdown Cooling Heat Exchanger System
SRV = Safety Relief Valves
PORV = Power Operated Relief Valves

**The support systems are defined on the next page.

TABLE 3.4

SUPPORT SYSTEM VS SUPPORT SYSTEM DEPENDENCIES

Support System*	Support System								
	Offsite AC	ESFAS	Emerg. AC	DC	CCW	SRW	SWS	RMCL	Air
Offsite AC	-								
ESFAS		-		X					
Emergency AC		X	-	X		X			
DC	X		X	-					
CCW	X	X	X	X	-		X		
SRW	X	X	X	X		-	X		
SWS	X	X	X	X			-		X
RMCL	X		X				X	-	
AIR	X		X	X		X			-

*The support systems are:

Offsite AC	=	Offsite AC Power
ESFAS	=	Engineered Safety Features Actuation Systems
Emer. AC	=	Emergency AC Power System
DC	=	125 VDC Power System
CCW	=	Component Cooling Water System
SRW	=	Service Water System
SWS	=	Salt Water System
RMCL	=	Diesel Generator or ECCS Pump Room Cooling Systems
AIR	=	Instrument Air, Plant Air, or N_2 Systems.

CHAPTER 4

INITIATING EVENTS

4.1 Introduction

The use of event tree methodology in the probabilistic risk assessment of Calvert Cliffs Unit 1 (CC-1) requires that accident initiating events be defined. These initiating events represent the starting points of many different accident sequences and delineate the initial conditions for these sequences.

This chapter will describe which initiating events were chosen for the CC-1 analysis, how they were grouped, and how they were quantified. The end product of the chapter is a list of the CC-1 initiating events and is described in Section 4.3.

4.2 Initiating Events Chosen for Calvert Cliffs Unit 1

Two general types of initiating events have been considered for the CC-1 analysis: loss of coolant accidents (LOCAs) and transients.

In order to determine the specific types of LOCA and transient initiating events to be studied, a failure mode and effects analysis (FMEA) was performed on the RCS piping and front-line systems and their support subsystems which are operating when the reactor is at power.

The RCS FMEA consisted of postulating different size RCS breaks and break locations to determine if different combinations of plant systems were required to mitigate the LOCA. Those breaks with similar front-line system mitigating requirements were placed in the same group. For example, LOCAs at CC-1 were divided into three categories ranging from small pump seal ruptures to large RCS pipe breaks. The LOCA initiating events for CC-1 are described in Section 4.2.1.

The FMEA performed to identify transients consisted of postulating a <u>single</u> fault in a normally operating system or subsystem and studying the plant response to that fault. For each postulated fault, the following questions were asked:

1. Does the fault lead to a reactor trip?

2. If the reactor trips, is the reliability of the front line systems and their support systems which must respond to the trip affected? If so, how?

Throughout the FMEA, EPRI NP-2230, "Frequency of Anticipated Transients," [7], provided guidance in choosing the general types of system faults to be considered.

A fault was only considered to be important if the answer to the first question was yes. If the reactor did not trip, it was assumed that the fault would be detected and corrected before a reactor trip from some other cause occurred. The faults that did cause a reactor trip were then grouped. Those which affected the reliability of the systems in a similar manner were placed in the same group. For example, CC-1 transients were split into six groups. Some of these groups were loss of offsite power, loss of the Power Conversion System, loss of a DC bus, etc. The CC-1 transient initiating events are described in Section 4.2.2.

4.2.1 LOCA Initiating Events

A number of LOCA break size ranges were determined for CC-1. Each LOCA break size range defines a unique set of emergency core cooling requirements for the injection or recirculation phase of a loss of coolant accident. Table 4.1 presents the different LOCA sizes and the appropriate success criteria for various plant functions. The emergency core cooling success criteria and LOCA break size ranges were determined by information from the plant FSAR [6], NUREG-0635 [10], and the Calvert Cliffs RSSMAP Study [9].

The initiating event frequencies for each LOCA break size range were calculated using RSS [11] data. Two basic assumptions were made in the calculation of the CC-1 LOCA frequencies. The first assumption was that the total frequency of random LOCAs at CC-1 was the same as that identified for the RSS plants. It was also assumed that the probability distribution over each RSS break range was constant. This assumption allowed uniform probability distributions to be generated for each RSS LOCA break size range. These probability distributions were then integrated over the CC-1 break ranges to produce CC-1 specific LOCA initiating event frequencies. The RSS and CC-1 LOCA break size ranges, frequencies and an example calculation, are given in Table 4.2.

One CC-1 LOCA break size range has an additional initiating event frequency contribution that is not included in the RSS data. For the smallest CC-1 LOCA break range (.3 to 1.9 inches equivalent diameter), a .02 frequency was assessed for certain types of reactor coolant pump seal ruptures. The RSS data only includes data on random pipe failures and therefore does not cover this type of LOCA. The .02 number overshadows the random failure contribution for this break size range. The pump seal information was obtained from an NRC memo on the subject [12].

It can be noted that no LOCAs smaller than 0.3 inch equivalent diameter were analyzed. It was ascertained that breaks of this magnitude could be mitigated by normally operating makeup systems.

A final comment should be made concerning the LOCA initiating events analyzed for Calvert Cliffs Unit 1. The interfacing systems LOCA, which was found to be important to risk in other PRAs (e.g., Surry in the RSS and Oconee in the RSSMAP) was not found to be a significant accident sequence at CC-1. The interfacing systems LOCA assumes either: (1) a failure of a series of check valves and motor-operated valves in one of the low pressure injection lines; or (2) failure of two locked closed motor-operated valves in the shutdown cooling suction line. Both of these allow high pressure RCS water to enter the low pressure piping outside containment and a pipe rupture to occur. A core melt would ensue because the core cooling systems are not designed to mitigate a LOCA outside containment. The probability of this event was found to be low (less than 1E-7 per reactor year) because of the number of valves in series which would have to fail and the placement of relief valves which would alert the operators to this event, thus increasing the recovery potential. The RSSMAP Calvert Cliffs PRA [9] provides a more detailed analysis of the interfacing systems LOCA at the Calvert Cliffs' plant.

4.2.2 Transient Initiating Events

A number of transient initiating events were identified for CC-1. The success criteria for front-line systems which function to mitigate transient initiated accidents are given in Table 4.3.

Four types of transient initiating events which do not involve specific component failures and which were quantified using industry data were analyzed for CC-1. These are:

1. Loss of Offsite Power (T_1); this event was defined as a total loss of offsite power to both units at the site.

2. Events which totally interrupt the Power Conversion System (T_2) (not caused by a loss of offsite power).

3. Transients requiring RCS pressure relief (T_3). These are transients which do not affect front-line systems significantly but are severe enough to require primary system pressure relief to terminate the accident successfully.

4. Transients requiring shutdown, but which do not affect front-line systems significantly (T_4). These transients do not require primary pressure relief to successfully terminate the accident.

The source used to define and quantify these transient designations was EPRI NP-2230 [7]. This report presents and analyzes events at nuclear plants which have lead to fast reactor shutdowns (scrams). A list of the PWR transients defined in the EPRI document is given in Table 4.4. Table 4.5 shows how the EPRI transient categories were grouped together to quantify the four transient types listed above. The numbers used are the generic values for all plants at all power levels. These numbers were compared to Calvert Cliffs Unit 1 plant specific data for 26-110% power trips and found not to be statistically different. Calvert Cliffs has a higher than average number of trips from high power. Table 4.6 shows the EPRI NP-2230 categories not used in the CC-1 initiating event analysis.

Two normally operating support systems were identified at CC-1 whose failure would cause a reactor shutdown and also degrade safety systems required post trip or affect recovery actions. These support system failures were identified by the performance of a FMEA (described in Section 4.2) on all normally operating support systems. These support systems are listed in Table 4.7.

In the following sections, the normally operating support systems which were reviewed in depth are discussed. The components identified as possible initiating events are included in the list of initiating events described in Section 4.3.

4.2.2.1 Service Water System Analysis

The Service Water System (SRWS) at CC-1 consists of two trains, each of which contains a motor-driven pump and heat exchanger, and is designed to remove heat from various plant components. Refer to Appendix B.15 for a more detailed discussion of the SRWS.

Several component failures in the SRWS were identified as possible initiating events. During normal operation, train number 12 supplies water to the main feedwater pump lube oil coolers and the condensate booster pump lube oil coolers. If flow through train number 12 were abruptly stopped, all lube oil cooling to these pumps would be lost. Given this situation, a reactor trip would be expected due to a main feedwater trip or operator action. The CC-1 Abnormal Operating Procedure (AOP-3) for a loss-of-service water event indicates that the operator would trip the plant when high pump and turbine temperatures are measured.

Given that SRWS train number 12 fails and that the reactor is tripped, main feedwater would be lost, auxiliary feedwater would be demanded, and a number of safety related systems would be degraded. The safety systems affected by SRWS train number 12 are Containment Air Coolers numbers 13 and 14 and emergency

diesel number 12. For this reason, single failures of SRWS have been analyzed as initiating events.

The failures of SRWS train Number 12 considered in the quantification of this initiating event are the manual inlet and outlet valves (SRW 127 and SRW 128) for SRWS heat exchanger number 12. Refer to Figure 6-26. Other single faults of train number 12 are feasible, but are more likely to be recovered.

The initiating event frequency for these service water failures was taken from the IREP quantification guide. A frequency of 8.8E-4 per year was assessed for each fault based on the plug standby failure rate for manual valves (1E-7 x 8760 hrs.). Therefore, the total initiating event frequency for this event is 1.8E-3. It is acknowledged that an operating failure rate rather than a standby failure should be used and may be different than the assigned value. However, this frequency is similar to the frequency used for this event in the Zion and Indian Point PRAs [13] which was calculated using a different method. The initiating event representation used in this analysis for this SRW fault is T_{SRW}.

4.2.2.2 Emergency AC Power Bus Analysis

The Emergency AC Power System provides AC power to several front-line/support systems which may be required to operate after an initiating event. (Refer to AC power discussion in Section 6.13 and Appendix B.13).

A FMEA was performed on each emergency AC bus to determine the effects of the bus shorting to ground. No emergency AC buses were identified which would cause a reactor trip and degrade front-line systems if lost. This was due to the fact that there were no balance-of-plant dependencies on the safety-related AC buses.

4.2.2.3 Emergency DC Power Bus Analysis

The analysis of the four DC power trains was very similar to that done for the AC buses. Failure of either of two DC buses (Numbers 11 and 21) were identified as causing a plant trip and degrading the safety systems. We will describe the failure of bus 11.

If bus 11 fails, one half of all safety systems which are not already running will be affected (i.e., AFW, HPSI, LPSI, CSSI). Those systems which are running would not be affected. A plant trip results when 120 VAC bus 11 fails as a result of DC bus 11 failing. Failure of 120 VAC bus 11 results in failure of: (1) a SG level control, (2) various instrumentation; and (3) a SGFP recirculation line valve and may result in a plant trip due to (1) low SG level; (2) inability to control SG level in auto requiring manual control which is ineffective; or (3) SGFP trip on low suction pressure.

The effects of DC bus 21 failing are not as severe as DC bus 11. Failure of bus 11 fails the motor-driven AFW pump; failure of bus 21 does not. Also, failure of bus 21 prevents the PORVs from opening which reduces the chances of a transient-induced LOCA.

The initiating event frequency for a single bus is taken to be 1.8E-2/yr. from NSAC data done for the Oconee PRA*. Since only bus 11 was quantified, an initiating event frequency of 3.6E-2 was used in order to envelope the failure of bus 21. This data looks at bus failure as an initiating event <u>not</u> as an independent failure (i.e., includes independent failures 1E-8/yr. x 8760 per year = 8.76 E-5 = 9E-5/yr. and random human interactions, etc.). The initiating event representation used in this analysis for DC bus 11 failure is T_{DC}.

4.2.2.4 Instrument Air System Analysis

The Instrument Air System (IAS) provides process air to many plant components, mainly air-operated control valves. The analysis of this system indicated that the only front-line or support system which would degrade or fail on loss of the IAS is the Power Conversion System. The reason for this is that most safety system components which interface with the IAS fail safe on loss of instrument air. The only valves where failure could affect a safety system is failure of the SRW and CCW heat exchanger valves in the SWS. However, this is a failure only if it occurs concurrently with a Large LOCA or Small LOCA, not for Small-small LOCAs or transients. Because these valves have a separate and redundant, seismically qualified air supply; this failure was judged to be negligible. Total loss of the IAS would lead to an immediate reactor trip as per Emergency Operating Procedure Number 14. However, since instrument air only affects main feedwater for transient initiators, its failure was considered as part of the T_2 initiating event. For this reason, no instrument air faults were analyzed as specific initiating events.

4.2.2.5 Component Cooling Water Analysis

The Component Cooling Water System (CCWS) is a closed cooling system which provides cooling to various safety and non-safety components not cooled by the SRWS.

Two failures of the CCWS were found to lead to reactor trip. The first is the failure of a valve in the CCWS line cooling the reactor coolant pump seal and lube oil coolers.

---

*Ref: Telephone conversation between G. J. Kolb, Sandia National Laboratories and G. J. Boyd, Technology for Energy Corporation.

However, since this failure would not degrade the ability of the CCWS to perform its safety functions, no special initiating event needed to be defined.

The second failure was a large rupture in a segment of the CCW piping which would result in a complete loss of water so fast that operator action could not prevent the complete draining of the system. An example of such a segment is the cross-tie piping between loops. This would result in a plant trip due to loss of cooling to both the reactor coolant pump seals and the lube oil coolers.

This event was judged initially to lead to a reactor coolant pump seal LOCA and to simultaneously fail the HPSI and LPSI pumps due to a lack of pump seal cooling. However, this was felt to be much too conservative for the following reasons. First, in discussions with the NRC, the CE Owner's Group [14] presented evidence to show that reactor coolant pump seal leaks due to a loss of seal cooling are not likely to occur due to the design of their pumps which have three full system pressure seals (which are cooled by the Component Cooling Water System) and then a controlled 10 gpm leakoff back to the Volume Control Tank or another full system pressure seal to the containment. Second, a recent assessment done by BG&E* showed no need for any LPSI or HPSI pump seal cooling in the injection mode and only after two hours in the recirculation phase following a Large LOCA. Because of the long time to get to recirculation (~10 hours)for a Small-small LOCA of this size: (1) the heat loads will be much less and the pump would likely last significantly longer than two hours in the recirculation mode; and (2) the operator could isolate the leak in the component cooling system and refill it. For the above reasons, this event was judged to be negligible and not considered further.

4.2.2.6 Salt Water System Analysis

The Salt Water System (SWS) is a two train system, each with its own dedicated pump. The SWS provides secondary cooling for the SRWS and CCWS and cooling for the ECCS pump room coolers and the circulating water pump seals.

No single fault was identified in the SWS which would require a rapid reactor trip and degrade safety systems. A partial loss of SWS due to a single failure could cause a slow heatup of the SRWS and CCWS which, if left untended, could cause trouble. However, the time for the heatup to occur is long (of the order of one hour), and it has been assumed that a safe condition could be achieved.

---

*Ref: Discussions with Niall Hunt and other BG&E engineers.

4.2.2.7 Heating and Ventilation System Analysis

The heating and ventilation systems which were reviewed are the Diesel Generator Room Ventilation System and the ECCS Pump Room Air Coolers. No failure within these systems was identified which could cause a reactor trip. Therefore, no special initiating event associated with these systems was applicable.

4.3 Description of the Calvert Cliffs Unit 1 Initiating Events

The accident initiating events used in the CC-1 analysis are those discussed in the previous sections and are summarized in Table 4.8. When the initiating events are combined with the appropriate system fault and success trees, unique CC-1 accident sequences are produced. An alternate way to display the CC-1 initiating events is with a fault tree. This is done in Figure 4-1.

The initiating events define the initial conditions for accident sequences and may, in themselves, affect the availability of front line systems. The dependencies found between the CC-1 initiating events and the mitigating systems are either modeled explicitly on the system fault trees or are shown by the difference in system success criteria in Tables 4.1 and 4.3 for the different initiating events. They are also shown in the system dependency Tables 3.3 and 3.4 in Chapter 3.

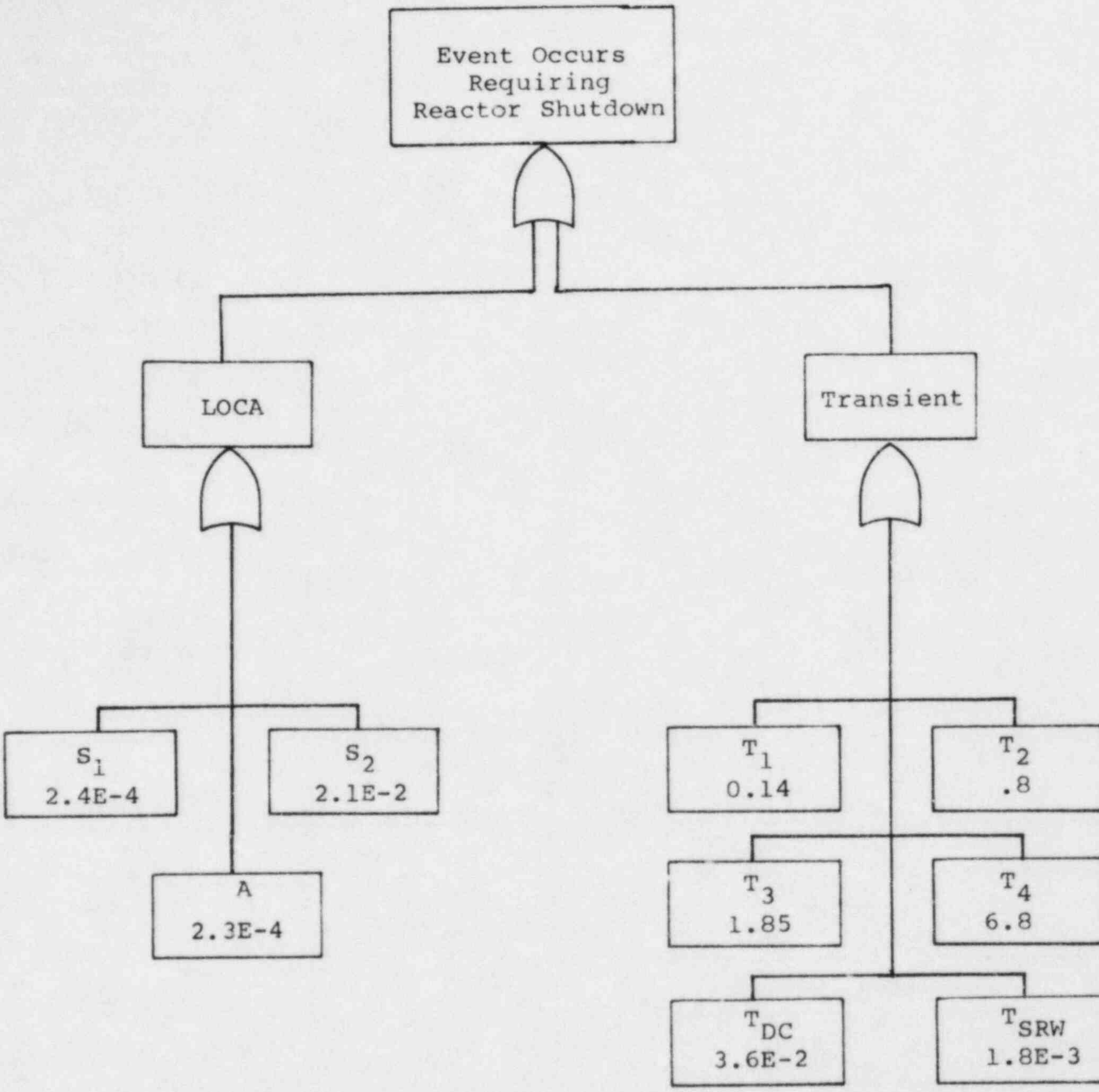


Figure 4-1. Calvert Cliffs Unit 1 Initiating Event Fault Tree

Table 4.1

LOCA EVENT DEFINITION AND MITIGATING SYSTEMS SUCCESS CRITERIA FOR CALVERT CLIFFS UNIT 1

LOCA Size[1]	Mitigating Function[2]						
	Reactor Subcriticality (RESC)	Injection Phase			Recirculation Phase		
		Reactor Heat Removal (REHR)	Containment Atmospheric Heat Removal (CNHR)	Containment Radioactivity Removal (CNRR)[3]	Reactor Heat Removal (REHR)	Containment Heat Removal (CNHR)	Containment Radioactivity Removal (CNRR)[3]
Small-Small .3"<D*≤1.9"	RPS	1/3 HPSI AND SSR AND 1/2 AFW	1/2 CSSI OR 1/4 CARC[4]	1/2 CSSI	1/3 HPSR	1/2 CSSR with 1/2 SDHX OR 1/4 CARC	1/2 CSSR
Small 1.9"<D*≤4.3"	RPS SSR	1/3 HPSI	1/2 CSSI OR 1/4 CARC[4]	1/2 CSSI	1/3 HPSR	1/2 CSSR with 1/2 SDHX OR 1/4 CARC	1/2 CSSR
Large D*<4.3"	None Required[5]	3/4 SITs AND 1/2 LPSI	1/2 CSSI OR 1/4 CARC	1/2 CSSI	1/3 HPSR	1/2 CSSR with 1/2 SDHX OR 1/4 CARC	1/2 CSSR

TABLE 4.1 NOTES

1. D* = Equivalent diameter of break in inches.

2. Mitigating functions are performed by mitigating systems. Mitigating systems success criteria are defined as follows:

RPS	=	Reactor Protection System. One half of the control element assemblies (CEAs) insert.
3/4 SITs	=	Safety Injection Tanks. 3 of 4 SIT trains (not connected to the failed loop) operate.
1/3 HPSI	=	High Pressure Safety Injection. 1 of 3 HPSI pump trains operates with 1 of 4 safety injection headers (not connected to the failed loop).
1/3 HPSR	=	High Pressure Safety Recirculation. 1 of 3 HPSR pump trains operates with 1 of 4 safety injection headers (not connected to the failed loop).
1/2 LPSI	=	Low Pressure Safety Injection. 1 of 2 LPSI pump trains operates with 1 of 4 safety injection headers (not connected to the failed loop).
1/2 LPSR	=	Low Pressure Safety Recirculation. 1 of 2 LPSR pump trains operates with 1 of 4 safety injection headers (not connected to the failed loop).
SSR	=	Secondary Steam Relief. 2 of 2 atmospheric dump valves dump steam directly to the outside atmosphere, <u>OR</u> 1 of 16 steam generator safety valves dumps steam directly to the outside atmosphere.
1/2 AFW	=	Auxiliary Feedwater. 1 of 2 steam generators supplied by 1 of 2 AFW pump trains.

TABLE 4.1 NOTES (continued)

1/2 CSSI	=	Containment Spray System Injection. 1 of 2 CSSI pump trains operates.
1/2 CSSR	=	Containment Spray System Recirculation. 1 of 2 pump trains operates.
1/2 SDHX	=	Shutdown Cooling Heat Exchanger. 1 of 2 SDHXs (associated with the operating CSSR pump train) provides cooling.
1/4 CARC	=	Containment Air Recirculation and Cooling. 1 of 4 fan cooler trains operates.

3. The function of containment radioactivity removal is not required if reactor heat removal and containment heat removal have been successful. However, the severity of the offsite radiological consequences of any sequence which ends in core melt or containment failure will be affected by the success or failure of the containment radioactivity removal function in the injection and/or recirculation phase, depending on the timing of core melt and/or containment failure.

4. The function of containment heat removal may not be required for LOCA breaks with D* $\leq$4.3 inches, providing the reactor heat removal function in the injection phase and the reactor subcriticality function have been successful. However, if either the reactor heat removal function in the injection phase or the reactor subcriticality function has not been successful, then the consequence will be core melt, but the severity of the offsite radiological consequences will be affected by the success or failure of the containment heat removal function in the injection phase.

5. The reactor subcriticality function is not dependent on the successful operation of mitigating systems for LOCA breaks with D* >4.3 inches. The reactor is automatically rendered subcritical due to core voiding during the blowdown phase and is maintained subcritical during the subsequent core reflood by borated water from the Safety Injection System (SIS). It is assumed that the probability of injection of inadequately borated water from the Refueling Water Tank (RWT) into the core is insignificant.

Table 4.2

Comparison of RSS and Calvert Cliffs Unit 1 LOCA Frequencies

Reactor Safety Study		Calvert Cliffs Unit 1	
LOCA Break[1] Size Range	Frequency	LOCA Break[1,2] Size Range	Frequency
S_2 = .5 to 2 inches	1.0E-3	S_2 = .3 to 1.9 inches	2.1E-2
S_1 = 2 to 6 inches	3.0E-4	S_1 = 1.9 to 4.3 inches	2.4E-4
A = 6 inches and larger	1.0E-4	A = 4.3 inches and larger	2.3E-4

[1]Equivalent diameter in inches.
[2]S_2 LOCA includes RCS pump seal leak contribution.

<u>Sample Calculation</u>

For the RSS S_2 LOCA, $\int_{.5}^{2} P_{S2}\, dx = 1.0E-3$

Similarly, for the RSS S_1 LOCA, $\int_{2}^{6} P_{S1}\, dx = 3.0E-4$

Assume that the distributions are uniform probability distributions. Therefore, the normalizing constants P_{S1} = 7.5E-5 and P_{S2} = 6.67E-4. Now, integrate these distributions over Calvert Cliff's S_1 LOCA break size range to obtain its frequency:

$$\int_{1.9}^{2} P_{S2}\, dx + \int_{2}^{4.3} P_{S1}\, dx = 2.4E-4$$

Table 4.3

Transient Event Definition and Mitigating Systems Success Criteria for Calvert Cliffs Unit 1

Transient	Mitigating Functions[1]					
	Reactor Subcriticality (RESC)	Reactor Heat Removal (REHR)	Primary System Relief (PSR)	Reactor Coolant System Integrety (RCSI)	Containment Heat Removal (CNHR)	Containment Radioactivity Removal (CNRR)
Loss of Offsite Power(T_1) or Loss of Power Conversion System (T_2)	RPS OR 2/3 CVCS	SSR AND 1/2 AFW	With RPS Success: None With RPS Failure: 4/4 SRV Open With RPS & CVCS Failure: None Effective[3]	With RPS Success: 2/4 reclose[2] With RPS Failure: 4/4 reclose	1/4 CARC OR 1/2 CSSI	1/2 CSSI
Transients Requiring RCS Pressure Relief (T_3)	RPS OR 2/3 CVCS	1/2 MFW (PCS) OR 1/2 AFW	With RPS Success: 2/4 SRV Open With RPS Failure: 4/4 SRV Open With RPS & CVCS Failure: None Effective[3]	With RPS Success: 4/4 reclose[2] With RPS Failure: 4/4 reclose	1/4 CARC OR 1/2 CSSI	1/2 CSSI
Remaining Transients Requiring Reactor Trip (T_4)	RPS OR 2/3 CVCS	1/2 MFW (PCS) (1/1 MFW for Loss of One MFW Train) OR 1/2 AFW	With RPS Success: None With RPS Failure: 4/4 SRV Open With RPS & CVCS Failure: None Effective[3]	With RPS Success: 2/4 reclose[2] With RPS Failure: 4/4 reclose	1/4 CARC OR 1/2 CSSI	1/2 CSSI

TABLE 4.3 NOTES

1. Success Criteria for Transient Systems from Appendix A:

PCS:		1 of 2 MFW pump trains
	and	1 of 3 condensate booster pump trains
	and	1 of 3 condensate pump trains
	and	interconnecting valves, etc.
	and	1 of 2 steam generators
SSRS:		1 of 4 turbine bypass valves
	or	2 of 2 atmospheric dump valves
	or	1 of 16 steam generator safety valves
SRVs open:		2 of 4 relief valves, where there are 2 PORVs, 2 SRVs
		4 of 4 with RPS failure
AFWS:		2 of 4 branches at 200 gpm each or 1 of 4 branches at 400 gpm (at least 400 gpm required)
	to	1 of 2 steam generators
	from	1 of 1 motor driven pumps at 450 gpm each
	or	1 of 1 turbine driven pumps at 700 gpm each
CARCS:		1 of 4 fan units and SRW subsystem
CSS:		1 of 2 pumps
RPS:		One-half of the control rod assemblies (CEAs) insert
CVCS:		1 of 2 boric acid pumps
	and	2 of 3 charging pumps
	and	1 of 2 injection paths

2. For T_1 and T_2 transients, a probabilistic demand of the PORVs will occur. If so, the two PORVs will open and must reclose. If these do not open, the SRVs will not be demanded. For T_3 transients, a probabilistic demand of the relief valves may also occur; however, as all four valves may be demanded, all four must reclose.

3. For transients with reactor subcriticality failure, pressure relief through the relief valves is not effective in mitigating the accident and preventing core melt.

Table 4.4

Transients Identified in EPRI NP-2230

1	Loss of RCS Flow (1 Loop)
2	Uncontrolled Rod Withdrawal
3	CRDM Problems and/or Rod Drop
4	Leakage from Control Rods
5	Leakage in Primary System
6	Low Pressurizer Pressure
7	Pressurizer Leakage
8	High Pressurizer Pressure
9	Inadvertent Safety Injection Signal
10	Containment Pressure Problems
11	CVCS Malfunction-Boron Dilution
12	Pressure/Temperature/Power Imbalance-Rod Position Error
13	Startup of Inactive Coolant Pump
14	Total Loss of RCS Flow
15	Loss or Reduction in Feedwater Flow (1 Loop)
16	Total Loss of Feedwater Flow (All Loops)
17	Full or Partial Closure of MSIV (1 Loop)
18	Closure of All MSIV
19	Increase in Feedwater Flow (1 Loop)
20	Increase in Feedwater Flow (All Loops)
21	Feedwater Flow Instability-Operator Error
22	Feedwater Flow Instability-Misc. Mechanical Causes
23	Loss of Condensate Pump (1 Loop)
24	Loss of Condensate Pumps (All Loops)
25	Loss of Condenser Vacuum
26	Steam Generator Leakage
27	Condenser Leakage
28	Misc. Leakage in Secondary System
29	Sudden Opening of Steam Relief Valves
30	Loss of Circulating Water
31	Loss of Component Cooling
32	Loss of Service Water Systems
33	Turbine Trip, Throttle Valve Closure, EHC Problems
34	Generator Trip or Generator Caused Faults
35	Total Loss of Offsite Power
36	Pressurizer Spray Failure
37	Loss of Power to Necessary Plant Systems
38	Spurious Trips-Cause Unknown
39	Auto Trip-No Transient Condition
40	Manual Trip-No Transient Condition
41	Fire Within Plant

Table 4.5

Grouped EPRI NP-2230 Transient Events Causing Reactor Shutdown at Calvert Cliffs Unit 1

Transient Designator	Transient Description	Applicable EPRI NP-2230 Transients	EPRI NP-2230 Frequency Per Reactor Year	Total Frequency Per Reactor Year
T_1	Total Loss of Offsite Power	#35) Total Loss of Offsite Power	0.14	0.14
T_2	Total Interruption of the Power Conversion System (Main Feed-water)	#16) Total Loss of Main Feedwater Flow	0.15	0.80
		#18) Closure of all MSIVs	0.03	
		#21&22) Feedwater Flow Instability	0.36	
		#24) Loss of All Condensate Pumps	0.00	
		#25) Loss of Condenser Vacuum	0.20	
		#30) Loss of Circulating Water	0.06	
T_3	Transients Requiring RCS Pressure Relief	#33) Turbine Trip or Throttle Valve Closure	1.38	1.85
		#34) Generator Trip or Generator Caused Faults	0.38	
		#37) Loss of Power to Necessary Plant Systems	0.09	
T_4	Other Transients Requiring Reactor Shutdown Which Do Not Significantly Affect Front Line Systems	#1) Loss of RCS Flow in One Loop	0.39	6.8
		#3) CRDM Problems, Rod Drop	0.65	
		#6) Low Pressurizer Pressure	0.03	
		#8) High Pressurizer Pressure	0.03	
		#9) Inadvertent Safety Injection Signal	0.06	

Table 4.5 (Continued)

Grouped EPRI NP-2230 Transient Events Causing Reactor Shutdown at Calvert Cliffs Unit 1

Transient Designator	Transient Description	Applicable EPRI NP-2230 Transients	EPRI NP-2230 Frequency Per Reactor Year	Total Frequency Per Reactor Year
		#11) CVCS Malfunction-Boron Dilution	0.04	
		#12) Pressure/Temperature/Power Imbalance	0.16	
		#14) Total Loss of RCS Flow	0.03	
		#15) Loss or Reduction in Main Feedwater (1 Loop)	1.88	
		#17) Full or Partial Closure of One MSIV	0.23	
		#19) Increase in Main Feedwater Flow in One Loops	0.69	
		#20) Increase in Main Feedwater Flow in All Loops	0.01	
		#23) Loss of Condensate Pump (1 Loop)	0.08	
		#27) Condenser Leakage	0.05	
		#28) Leakage in Secondary System	0.08	
		#29) Sudden Opening of Steam Relief Valves	0.04	
		#36) Pressurizer Spray Failure	0.04	
		#38) Spurious Trips-Cause Unknown	0.14	
		#39) Auto Trip-No Transient Condition	1.55	
		#40) Manual Trip-No Transient Condition	0.62	

Table 4.6

EPRI NP-2230 Transients Not Used in CC #1 Initiating Event Analysis

EPRI NP-2230 Transient	Comments
#2) Uncontrolled Rod Withdrawal	All control rods are out at high power
#4) Leakage from Control Rods #5) Leakage in Primary System #7) Pressurizer Leakage	For leak rates > 132 gpm, those transients are considered to be LOCAs For leak rates < 132 gpm charging pumps supply makeup. Normal shutdown occurs, no reactor trip required
#10) Containment Pressure Problems	It is assumed only LOCAs will cause this condition
#13) Startup of Inactive RCS Pump	All pumps will be on at full power
#26) Steam Generator Leakage	Normal shutdown is assumed possible
#41) Fire Within Plant	Outside scope of IREP

Table 4.7

Support Systems Reviewed in the Calvert Cliffs
Initiating Event Analysis

The following systems were reviewed to identify possible failures which could act as an accident initiator:

Service Water System

Emergency AC Power System

Emergency DC Power System

Instrument Air System

Component Cooling Water System

Salt Water System

Heating and Ventilation Systems

Table 4.8

Initiating Events Used in the Calvert Cliffs #1 Analysis

Designator	Initiating Evert Description	Frequency Per Reactor Year
S_2	LOCA with a .3 to 1.9 inch equivalent diameter break	$2.1x10^{-2}$
S_1	LOCA with a 1.9 to 4.3 inch equivalent diameter break	$2.4x10^{-4}$
A	LOCA with an equivalent diameter break greater than 4.3 inches	$2.3x10^{-4}$
T_1	Loss of offsite power transient	$1.4x10^{-1}$
T_2	Transient initiated by a total interruption of main feedwater	0.8
T_3	Transients requiring RCS pressure relief	1.85
T_4	Other transients requiring reactor shutdown which do not significantly affect front line system	6.8
T_{SRW}	Failure of SRWS Train #12	1.8E-3
T_{DC}	Failure of DC Bus 11	3.6E-2

CHAPTER 5

ACCIDENT SEQUENCE DELINEATION

5.1 Introduction

The type of accidents of concern for the CC-1 IREP study are the core meltdown accidents initiated by the LOCAs and transients defined in Chapter 4. It is the goal of the study to quantify the frequency of these core meltdown accidents and to estimate their severity expressed in terms of radioactive material released from containment. The severity of a core melt accident depends on the initiating event, on which plant safety functions/systems succeeded or failed during the accident, and on the approximate time at which they failed, i.e. the accident sequence.

Event trees are the logic models from which accident sequences are derived. Two types of event trees were constructed to delineate the accident sequences. First, the functional event trees which interrelate the initiating event and the plant safety function failures and results in functional accident sequences. Second, the systemic event trees which interrelate the initiating event and the safety system failures and results in the system accident sequences. The CC-1 functional event trees are described in section 5.2. The CC-1 systemic event trees are briefly described in section 5.3. A more detailed discussion of these can be found in Appendix A.

5.2 CC-1 Functional Event Trees

5.2.1 LOCA Functional Event Trees

The CC-1 LOCA functional event trees are depicted in Figures 5-1 and 5-2. These trees were constructed by (1) making the plant LOCA functions described in Section 3.2.1 the event tree headings; (2) placing the event tree headings in the approximate chronological order they would be expected to be called upon following a LOCA; and (3) incorporating the functional interdependencies into the event tree structure. The interdependencies were incorporated into the event tree structure by removing success/failure decision branches at the appropriate places in the tree.

5.2.1.1 Large LOCA Functional Dependencies

The following dependencies were incorporated into the Large LOCA functional event tree:

1. The Reactor Subcriticality (RESC) function is not required for successful mitigation of a Large LOCA. Voiding of the core in the initial phase of the accident and subsequent reflooding of the core with borated water from the Emergency Core Cooling Systems (ECCS) will render the reactor subcritical. This affects all sequences (1 - 15).

2. The failure of the Reactor Heat Removal (REHR) function in the injection phase precludes success of REHR (recirculation) since some of the same systems are used in the recirculation phase and the dominant failure modes in injection are expected to fail the systems in recirculation also. In addition REHR (recirculation) success will not prevent core melt and is not expected to significantly affect the accident consequences. This affects sequences 9 - 15.

3. The failure of the Containment Atmospheric Heat Removal (CNHR) function in the injection phase precludes success of CNHR (Recirculation) and Containment Radioactivity Removal (CNRR) in both the injection and recirculation phases. The systems used for these functions are the same as those used in CNHR (injection) and the dominant failure modes in CNHR (injection) are expected to fail the systems in any other mode of operation. Also, REHR (recirculation) is assumed to have failed since CNHR (injection) failure will result in containment failure before the recirculation phase is reached. Upon failure, the containment would undergo rapid depressurization. This would cause the superheated water in the sump to partially flash to steam and boil vigorously. The pumps which provide cooling and radioactivity removal during the recirculation phase are assumed to fail due to the pumping of two-phase water. This affects sequences 8 and 15. It should be noted that in sequence 8, containment failure occurs before core melt.

4. The failure of the Containment Radioactivity Removal (CNRR) function in the injection phase precludes successful CNRR (recirculation) since the same system is used in both phases and the dominant failure modes in the injection phase are expected to fail the system in recirculation also. This affects sequences 13 and 14.

5. Successful Reactor Heat Removal (REHR) and Containment Atmospheric Heat Removal (CNRR) in the injection phase prevent a core melt in the injection phase. A

decision branch is not made for Containment Radioactivity Removal (CNRR) in the injection phase for non-core melts since the success of th's function would not significantly affect accident consequences. This affects sequences 1 - 7.

6. Successful Reactor Heat Removal (REHR) and Containment Atmospheric Heat Removal (CNRR) in both the injection and recirculation phase lead to a safe situation. A decision branch is not made for Containment Radioactivity Removal (CNRR) in recirculation since success of this function would not significantly affect accident consequences. This affects sequence 1 only.

5.2.1.2 Small and Small-small LOCA Functional Dependencies

The following dependencies were incorporated into the Small and Small-small LOCA functional event tree:

1. Upon failure of the Reactor Subcriticality (RESC) function, sequences 30-36 were assumed to lead to core melt. This is not an unreasonable assumption since the turbine may not trip for some time and the power level and pressure may remain high for an extended period of time, thereby, preventing successful primary makeup. In the case with successful scram, reactor pressure drops relatively slowly. The higher amount of energy in the primary in the case with unsuccessful scram should result in even slower decreases in reactor pressure and increased likelihood of core uncovery without some operator recovery actions within a short time.

2. The failure of the Reactor Heat Removal (REHR) function in the injection phase precludes success of REHR in the recirculation phase for the same reasons as in (2) for the Large LOCA case. This affects sequences 23 - 29.

3. The failure of the Containment Atmospheric Heat Removal (CNHR) function precludes success of CNHR (recirculation) and Containment Radioactivity Removal (CNRR) in both the injection and recirculation phases for the same reasons as in (3) for the Large LOCA case. This affects sequences 29 and 36.

4. The failure of the Containment Radioactivity Removal (CNRR) function in the injection phase precludes success of CNRR in the recirculation phase for the same

reasons as in (4) for the Large LOCA case. This affects sequences 27, 28, 34 and 35.

5. Successful Reactor Subcriticality (RESC) and Reactor Heat Removal (REHR) in injection prevent a core melt in the injection phase. A decision branch is not made for Containment Atmospheric Heat Removal (CNHR) or Containment Radioactivity Removal (CNRR) in the injection phase since success of these function would not significantly affect accident consequences. This affects sequences 16 - 22.

6. Successful Reactor Heat Removal (REHR) in injection and recirculation phases and Containment Atmospheric Heat Removal (CNHR) in the recirculation phase prevent core melt and lead to a safe situation. A decision branch is not made for Containment Radioactivity Removal (CNRR) in recirculation for the same reason as in (6) for the Large LOCA case. This affects sequence 16 only.

5.2.1.3 LOCA Functional Accident Sequence Descriptions

The following sections will discuss the sequences shown on the LOCA functional event trees.

5.2.1.3.1 Sequence 1

This sequence is a Large LOCA followed by successful operation of the Reactor Heat Removal and Containment Heat Removal functions. The result is a safe outcome.

5.2.1.3.2 Sequence 2

This sequence is a Large LOCA with successful reactor heat removal in both the injection and recirculation phases. Containment heat removal is successful in injection but fails in recirculation. This results in containment failure by overpressure and subsequent failure of all safety systems leading to core melt. The containment radioactivity removal function works to reduce the initial radioactive release but is not effective after the containment fails.

5.2.1.3.3 Sequence 3

This sequence is similar to sequence 2 except that containment radioactivity removal has also failed. This will increase the initial radioactive release.

5.2.1.3.4 Sequence 4

This is a Large LOCA with successful reactor and containment heat removal in the injection phase. Reactor heat removal

fails in the recirculation phase and core melt occurs. Containment heat and radioactivity removal continue to work. Containment failure by meltthrough is most likely, although long-term overpressure failure due to non-condensables is possible.

5.2.1.3.5 Sequence 5

This sequence is similar to sequence 4 except that containment radioactivity removal fails which may result in higher radioactive releases.

5.2.1.3.6 Sequence 6

This sequence is a Large LOCA with successful reactor and containment heat removal in the injection phase. Reactor and containment heat removal fail in recirculation resulting in core melt. Containment radioactivity removal functions to reduce the radioactive release. The most likely containment failure mode is by overpressure.

5.2.1.3.7 Sequence 7

This sequence is similar to sequence 6 except that both containment heat and radioactivity removal fail. This results in higher radioactive releases.

5.2.1.3.8 Sequence 8

This sequence is a Large LOCA followed by successful reactor heat removal. Containment heat removal fails in the injection phase. The subsequent containment failure due to overpressure results in the failure of all core cooling systems and core melt.

5.2.1.3.9 Sequence 9

This sequence is a Large LOCA followed by failure of the reactor heat removal function resulting in core melt. The containment heat and radioactivity removal functions work and containment failure by meltthrough is most likely, although long-term overpressure failure caused by non-condensables is possible.

5.2.1.3.10 Sequence 10

This sequence is similar to sequence 9 except that containment radioactivity removal fails. This may result in higher releases.

5.2.1.3.11 Sequence 11

This sequence is a Large LOCA followed by failure of reactor heat removal resulting in core melt. The containment heat removal function works in injection but fails in recirculation leading to containment failure by overpressure. The containment radioactivity function works to mitigate the release.

5.2.1.3.12 Sequence 12

This sequence is similar to sequence 11 except that the containment radioactivity removal function also fails in recirculation leading to increased radioactive releases.

5.2.1.3.13 Sequence 13

This sequence is a Large LOCA followed by failure of reactor heat removal and containment radioactivity removal. Core melt occurs but the containment heat removal function works. Containment failure by meltthrough is most likely, although long-term overpressure failure due to non-condensables is possible.

5.2.1.3.14 Sequence 14

This sequence is similar to sequence 14 except that containment heat removal fails in recirculation. Containment failure by overpressure is most likely.

5.2.1.3.15 Sequence 15

This sequence is a Large LOCA followed by failure of all functions. The core melts and containment failure by overpressure is most likely.

5.2.1.3.16 Sequence 16

This sequence is a Small (S_1) or Small-small (S_2) LOCA followed by successful operation of all functions. The result is a safe outcome.

5.2.1.3.17 Sequence 17

This sequence is a S_1 or S_2 LOCA with successful reactor subcriticality, reactor heat removal and containment radioactivity removal. Containment heat removal fails in recirculation resulting in containment failure due to overpressure and subsequent failure of reactor heat removal and core melt.

5.2.1.3.18 Sequence 18

This sequence is similar to sequence 17 except that containment radioactivity removal fails leading to increased releases.

5.2.1.3.19 Sequence 19

This sequence is a S_1 or S_2 LOCA with successful reactor subcriticality and reactor and containment heat removal in the injection phase. Reactor heat removal fails in recirculation leading to core melt. The most likely containment failure mode is by meltthrough, although long-term overpressure failure due to non-condensables is possible.

5.2.1.3.20 Sequence 20

This sequence is similar to sequence 19 except that the containment radioactivity removal function fails in recirculation leading to higher releases.

5.2.1.3.21 Sequence 21

This sequence is similar to sequence 19 except that the containment heat removal function also fails in recirculation. The most likely containment failure mode is overpressure.

5.2.1.3.22 Sequence 22

This sequence is similar to sequence 21 except that both the containment heat and radioactivity removal functions have failed in recirculation. This results in increased radioactive releases.

5.2.1.3.23 Sequence 23

This sequence is a S_1 or S_2 LOCA with successful reactor subcriticality. Reactor heat removal fails in the injection phase resulting in core melt. Containment heat and radioactivity removal work and containment failure by meltthrough is most likely, although long-term overpressure failure due to non-condensables is possible.

5.2.1.3.24 Sequence 24

This sequence is similar to sequence 23 except that containment radioactivity removal fails in recirculation resulting in higher releases.

5.2.1.3.25 Sequence 25

This sequence is a S_1 or S_2 LOCA with successful reactor subcriticality. Reactor heat removal fails in the injection

phase resulting in core melt. Containment heat and radioactivity removal work in injection but containment heat removal fails in recirculation resulting in containment failure by overpressure.

5.2.1.3.26 Sequence 26

This sequence is similar to sequence 25 except that containment radioactivity removal also fails in recirculation resulting in higher radioactive releases.

5.2.1.3.27 Sequence 27

This sequence is a S_1 or S_2 LOCA followed by successful reactor subcriticality. Reactor heat removal and containment radioactivity removal fail in injection and core melt occurs. Containment heat removal works and containment failure by meltthrough is most likely, although long-term overpressure failure due to non-condensables is possible.

5.2.1.3.28 Sequence 28

This sequence is similar to sequence 27 except that containment heat removal fails in recirculation. The most likely containment failure mode is now overpressure.

5.2.1.3.29 Sequence 29

This sequence is a S_1 or S_2 LOCA followed by successful reactor subcriticality. Reactor and containment heat removal fail in injection resulting in core melt and containment failure by overpressure.

5.2.1.3.30 Sequence 30

This sequence is a S_1 or S_2 LOCA followed by failure of reactor subcriticality and core melt. Containment heat and radioactivity removal work and containment failure by meltthrough is most likely, although long-term overpressure failure due to non-condensables is possible.

5.2.1.3.31 Sequence 31

This sequence is similar to sequence 30 except that containment radioactivity removal fails in recirculation resulting in higher releases.

5.2.1.3.32 Sequence 32

This sequence is a S_1 or S_2 LOCA followed by failure of reactor subcriticality and core melt. Containment heat removal works in the injection phase but fails in the

recirculation phase leading to containment failure by overpressure. Containment radioactivity removal works to mitigate the release.

5.2.1.3.33 Sequence 33

This is similar to sequence 32 except that containment radioactivity removal also fails leading to higher radioactive releases.

5.2.1.3.34 Sequence 34

This is similar to sequence 31 except that containment radioactivity removal fails in injection instead of recirculation.

5.2.1.3.35 Sequence 35

This sequence is similar to sequence 32 except that containment radioactivity removal fails in injection instead of recirculation.

5.2.1.3.36 Sequence 36

This sequence is a S_1 or S_2 LOCA followed by failure of reactor subcriticality and containment heat removal. Core melt occurs followed by failure of containment by overpressure.

5.2.2 Transient Functional Event Tree

The CC-1 transient functional event tree is depicted in Figure 5-3. This tree was constructed in the same way as the LOCA functional trees.

5.2.2.1 Transient Functional Dependencies

The following dependencies were incorporated into the transient functional event tree:

1. Upon failure of the Reactor Subcriticality (RESC) function, sequences 11-13 were assessed to lead to core melt. Following a severe pressure transient, reactor power will equilibrate at the heat removal rate (i.e., either main feedwater and auxiliary feedwater at about 10% or just auxiliary feedwater at about 5%). Current analyses of these accidents by CE and the NRC only go out to 20 minutes. The accident progression beyond this point is uncertain, and they are assessed to result in core melt if the operator fails to inject boron by 20-30 minutes (see discussion of TKU sequences in Chapter 8 and the

sensitivity analysis in Section 8.3 for a more detailed discussion of the thermal-hydraulics). No choice is given for Primary System Relief (PSR) Reactor Coolant System Integrity (RCSI) and Reactor Heat Removal (REHR) functions since the sequences lead to core melt and their operation is moot.

2. The failure of the Reactor Heat Removal (REHR) function results in core melt and makes successful Primary System Relief (PSR) and Reactor Coolant System Integrity (RCSI) moot. This affects sequences 8 - 10.

3. The failure of the Primary System Relief (PSR) function (if required) makes successful Reactor Coolant System Integrity (RCSI) moot since the resulting pressure transient is assumed to result in an unmitigatable LOCA. This affects sequences 5 - 7.

4. The failure of the Containment Atmospheric Heat Removal (CNHR) function precludes successful Containment Radioactivity Removal (CNRR) since the system used for CNRR is also used for CNHR. This affects sequences 4, 7 and 10.

5. The success of Reactor Subcriticality (RESC), Reactor Heat Removal (REHR), Primary System Relief (PSR) and Reactor Coolant System Integrity (RCSI) lead to a safe situation. A decision branch is not given for either Containment Atmospheric Heat Removal (CNHR) or Containment Radioactivity Removal (CNRR) since they would not significantly affect the consequences. This affects sequence 1 only.

5.2.2.2 Transient Functional Accident Sequence Descriptions

The following sections will discuss the sequences shown on the transient functional event tree.

5.2.2.2.1 Sequence 1

In this sequence, all functions work as expected. The reactor is rendered subcritical, decay heat is removed, primary system relief works (if required), and RCS integrity is maintained. As a result, there is no need for containment heat or radioactivity removal. The sequence has a safe outcome.

5.2.2.2.2 Sequence 2

In this sequence, the reactor is rendered subcritical and decay heat is removed. But after successful primary system pressure relief, the relief valves fail to reclose resulting in

a Small-small LOCA. The containment functions succeed and this sequence transfers to the appropriate Small-small LOCA sequences.

5.2.2.2.3 Sequence 3

This sequence is similar to sequence 2 except that the containment radioactivity removal function fails. This sequence also results in a Small-small LOCA and transfers to the appropriate Small-small LOCA sequences.

5.2.2.2.4 Sequence 4

This sequence is similar to sequence 2 except that containment heat and radioactivity removal fail. The sequence transfers to the appropriate Small-small LOCA sequences.

5.2.2.2.5 Sequence 5

In this sequence, the reactor is rendered subcritical, decay heat is removed, but primary system pressure relief fails (if required) and is assumed to result in an unmitigatable LOCA. This results in a core melt. All containment functions work to mitigate the accident and meltthrough is the most likely containment failure mode, although long-term overpressure failure due to non-condensables is possible.

5.2.2.2.6 Sequence 6

This sequence is similar to sequence 5 except that the containment radioactivity removal function has failed. This may increase the radioactive release compared to sequence 5.

5.2.2.2.7 Sequence 7

This sequence is similar to sequence 5 except that all containment heat and radioactivity removal functions have failed. This makes containment failure by overpressure most likely and results in higher radioactive releases.

5.2.2.2.8 Sequence 8

In this sequence, the reactor is rendered subcritical but reactor heat removal fails. This results in core melt. The containment heat and radioactivity removal functions are successful and meltthrough is the most likely containment failure mode, although long-term overpressure failure due to non-condensables is possible.

5.2.2.2.9 Sequence 9

This sequence is similar to sequence 8 except that the containment radioactivity removal function has failed. This may increase the radioactive release compared to sequence 8.

5.2.2.2.10 Sequence 10

This sequence is similar to sequence 8 except that all containment heat and radioactivity removal functions have failed. This makes containment failure by overpressure most likely and results in higher radioactive releases.

5.2.2.2.11 Sequence 11

In this sequence, the reactor is not made subcritical. The containment heat and radioactivity removal functions succeed and containment failure by overpressure is most likely.

5.2.2.2.12 Sequence 12

This sequence is similar to sequence 11 except that the containment radioactivity removal function has failed. This increases the radioactive release compared to sequence 11.

5.2.2.2.13 Sequence 13

This sequence is similar to sequence 11 except that the containment heat removal and radioactive release functions have failed. This increases the likelihood of containment failure by overpressure.

5.3 CC-1 Systemic Event Trees

There were three LOCA and four transient systemic event trees constructed to represent the plant front-line system response to the 3 LOCAs, the 4 transients, and 2 special initiating events defined in Chapter 4. A total of seven systemic trees were drawn using the same method as for the functional, trees but using systems instead of functions for the event tree headings. This many systemic trees were required in order to represent all of the different sets of system success criteria required for the various initiators or the interdependencies between systems which may also vary with initiator. The seven systemic trees are shown in Figures 5-4 to 5-10.

The definitions for the events depicted on the seven systemic event trees are listed in Table 5.1 and the notes for each tree in Tables 5.2 - 5.5. The reader should refer to Appendix A for a detailed discussion of these event trees and the system interdependencies.

Figure 5-1 Large LOCA (A) Functional Event Tree

Initiating Event	Mitigating Functions Response							Sequence	Result
Large LOCA	Reactor Sub-criticality	Injection Phase			Recirculation Phase				
		Reactor Heat Removal	Contain-ment Atmos-pheric Heat Removal	Contain-ment Radio-Activity Removal	Reactor Heat Removal	Contain-ment Atmos-pheric Heat Removal	Contain-ment Radio-Activity Removal		
A	RESC	REHR	CNHR	CNRR	REHR	CNHR	CNRR		

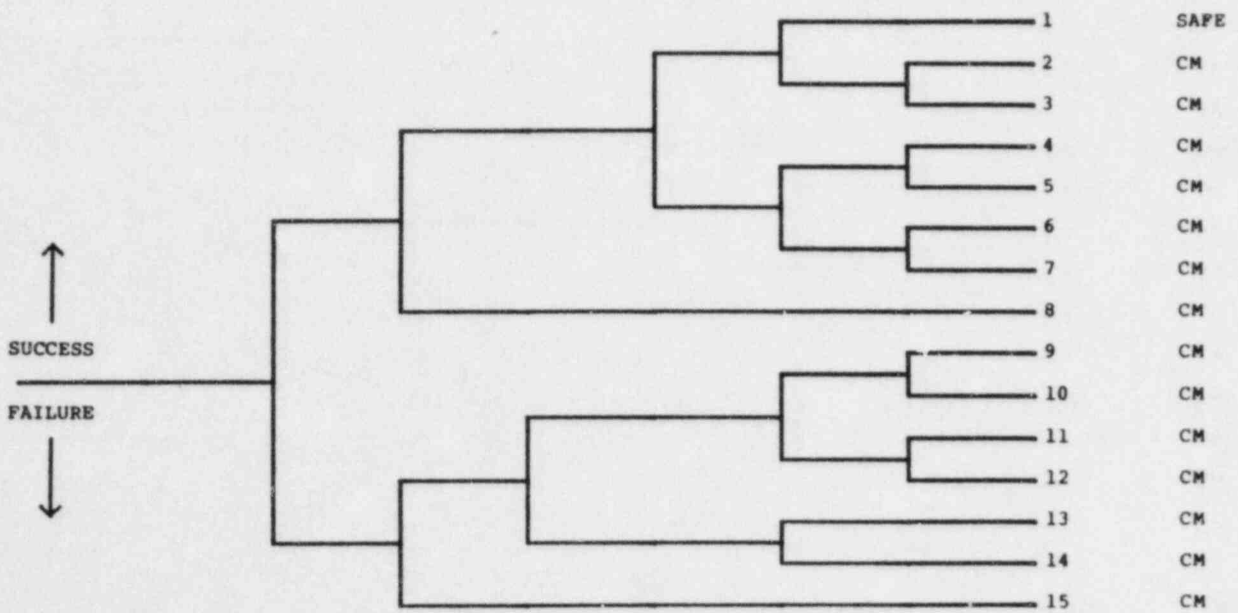


Figure 5-2 Small or Small-Small LOCA (S_1 or S_2) Functional Event Tree

Initiating Event	Mitigating Functions Response							Sequence	Result
		Injection Phase			Recirculation Phase				
Small or Small-Small LOCA	Reactor Sub-criticality	Reactor Heat Removal	Containment Atmospheric Heat Removal	Containment Radio-Activity Removal	Reactor Heat Removal	Containment Atmospheric Heat Removal	Containment Radio-Activity Removal		
S_1 or S_2	RESC	REHR	CNHR	CNRR	REHR	CNHR	CNRR		

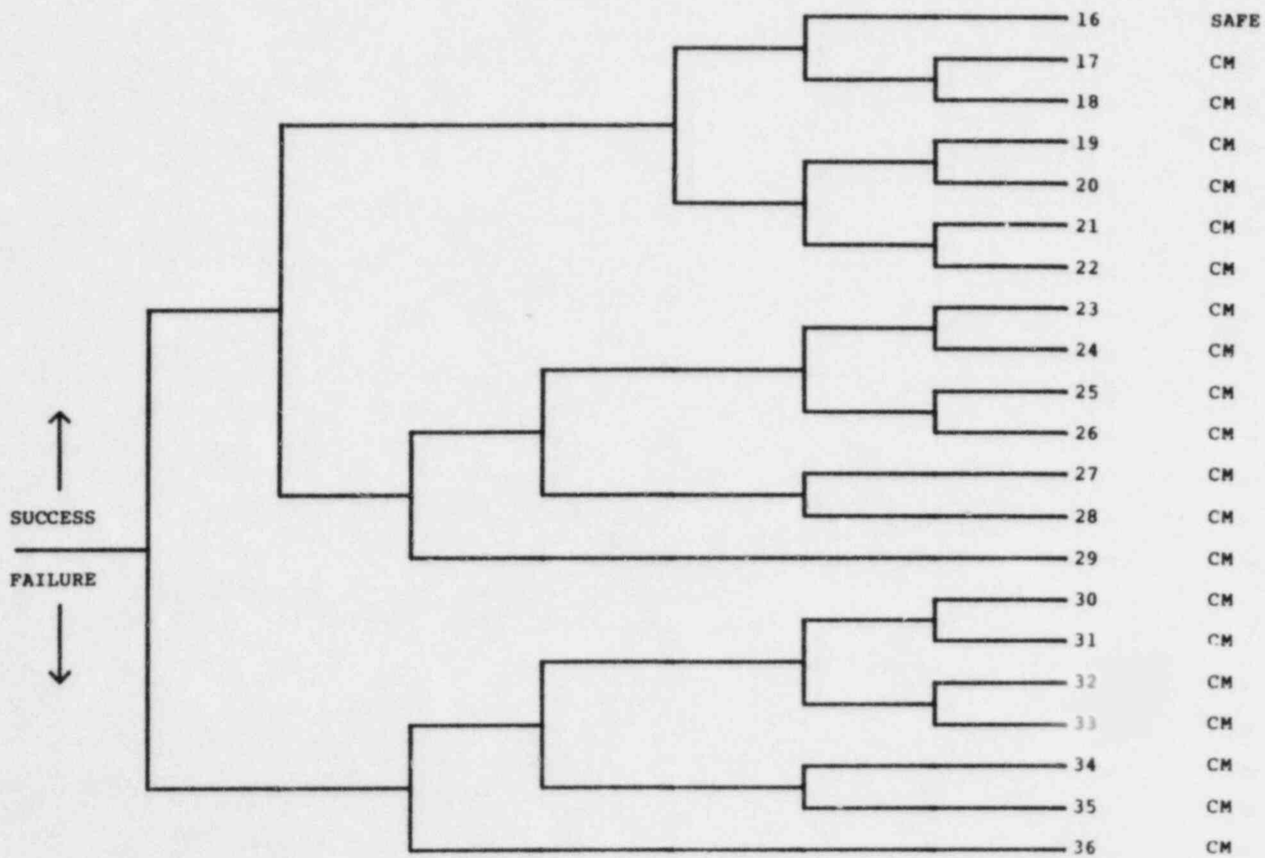
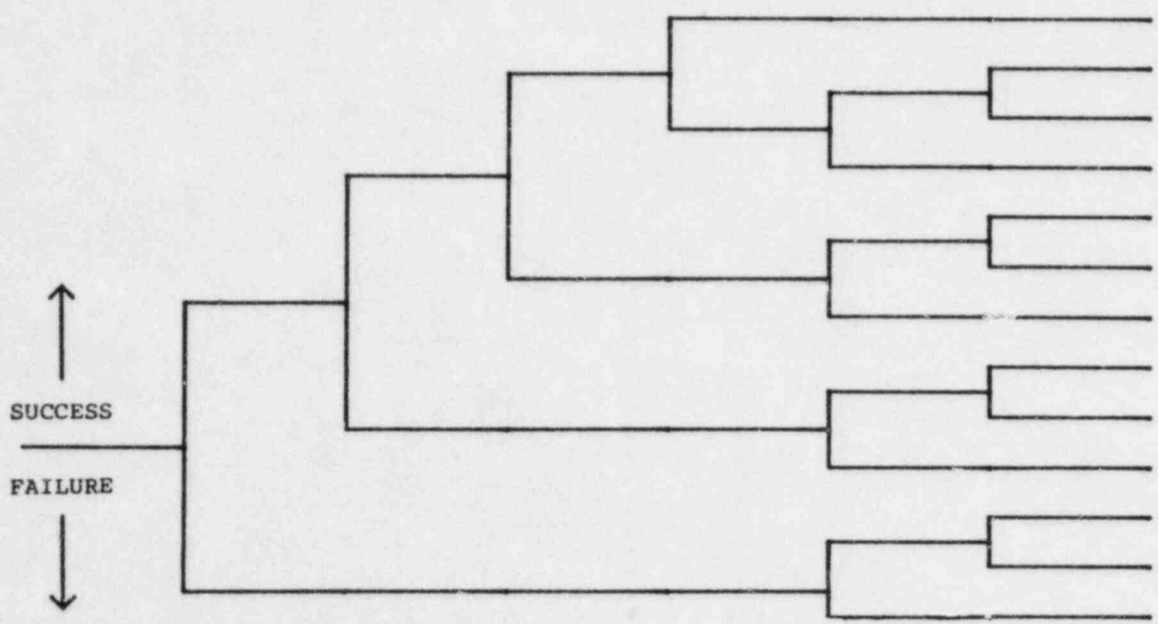


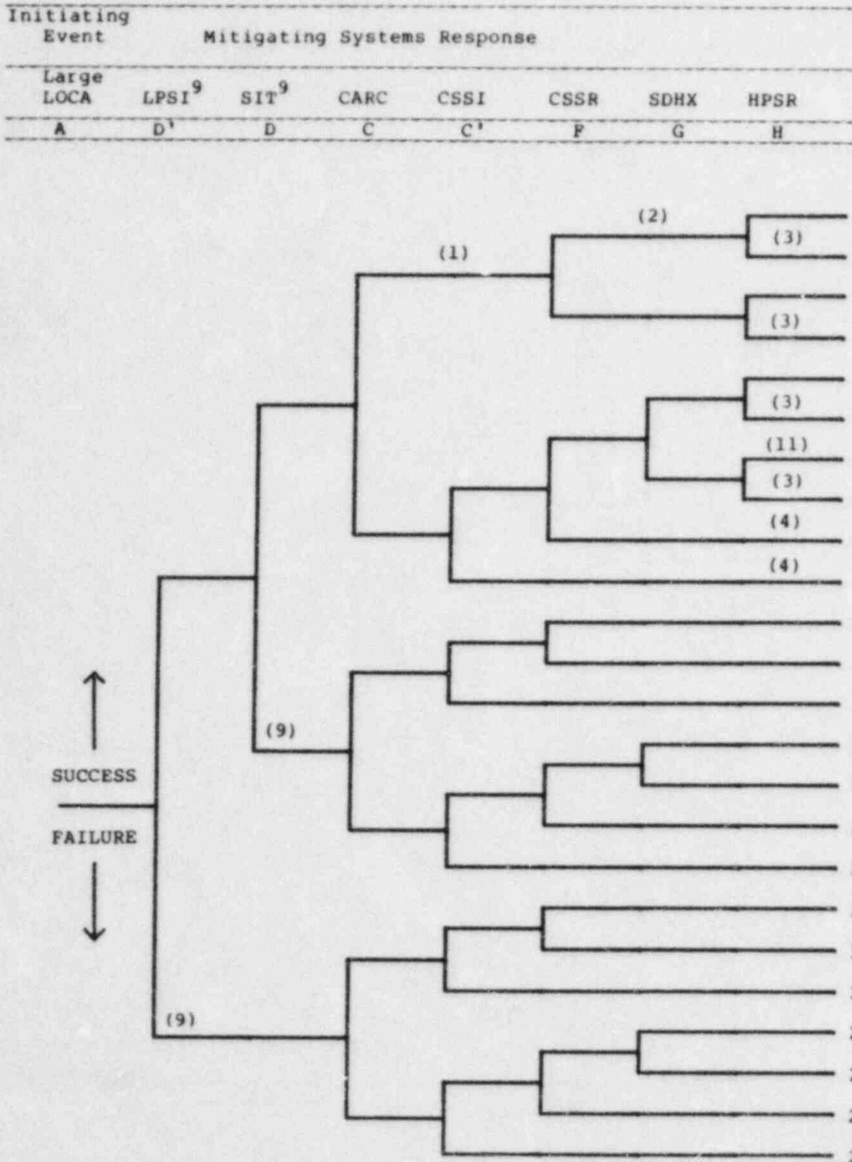
Figure 5-3 Transient T_1, T_2, T_3, T_4 Functional Event Tree

Initiating Event	Mitigating Function Response						Sequence	Result
Transient	Reactor Subcriticality	Reactor Heat Removal	Primary System Relief	Reactor Coolant System Integrity	Contain-ment Atmos-pheric Heat Removal	Contain-ment Radio-Activity Removal		
T	RESC	REHR	PSR	RCSI	CNHR	CNRR		



Sequence	Result
1	SAFE
2	LOCA and/or CM
3	LOCA and/or CM
4	LOCA and/or CM
5	CM
6	CM
7	CM
8	CM
9	CM
10	CM
11	CM
12	CM
13	CM

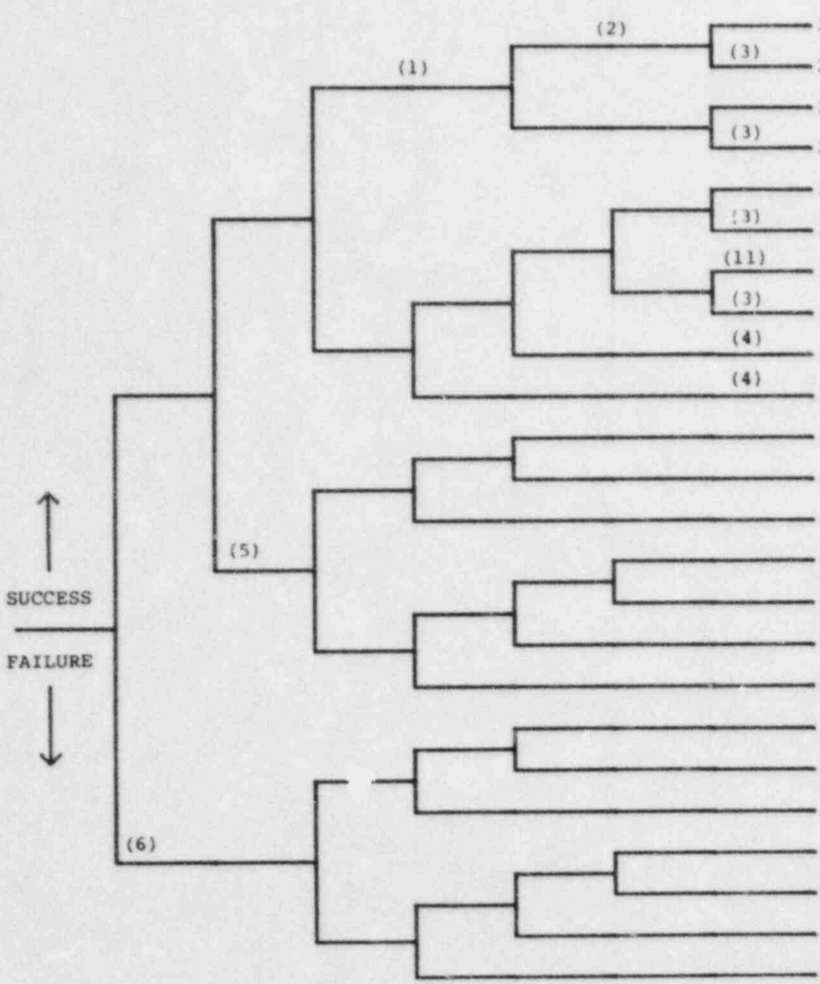
Figure 5-4 Large LOCA (A) Systemic Event Tree



Sequence No.	Sequence Designator	REHR INJ	REHR REC	CNHR INJ	CNHR REC	CNRR INJ	CNRR REC	RCS Status	NOTES
1	A							SAFE	1,2
2	AH		x					CM	1,2,3
3	AF							SAFE	1
4	AFH		x				x	CM	1,3
5	AC							SAFE	
6	ACH		x					CM	3
7	ACG		x		x			CM	11
8	ACGH		x		x			CM	3
9	ACF		x		x		x	CM	4
10	ACC'		x	x		x		CM	4
11	AD	x						CM	9
12	ADF	x					x	CM	9
13	ADC'	x				x		CM	9
14	ADC	x						CM	9
15	ADCG	x			x			CM	9
16	ADCF	x			x		x	CM	9
17	ADCC'	x		x		x		CM	9
18	AD'	x						CM	9
19	AD'F	x					x	CM	9
20	AD'C'	x				x		CM	9
21	AD'C	x						CM	9
22	AD'CG	x			x			CM	9
23	AD'CF	x			x		x	CM	9
24	AD'CC'	x		x		x		CM	9

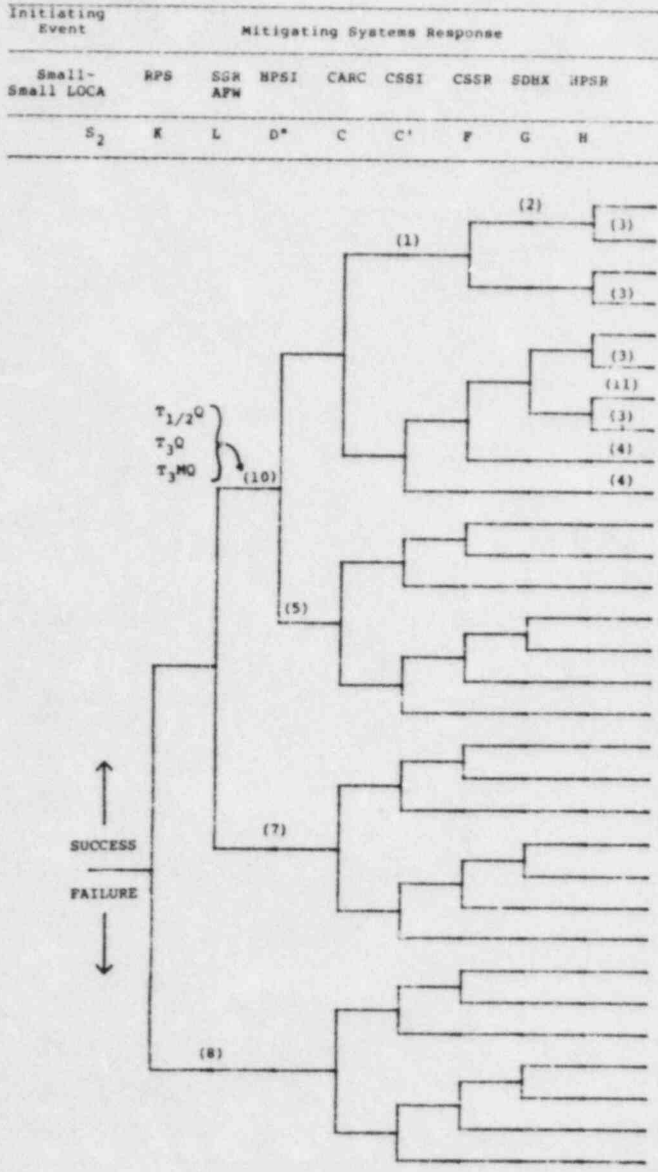
Figure 5-5 Small LOCA (S_1) Systemic Event Tree

Initiating Event	Mitigating Systems Response						
Small LOCA	RPS	HPSI	CARC	CSSI	CSSR	SDHX	HPSR
S_1	K	D"	C	C'	F	G	H



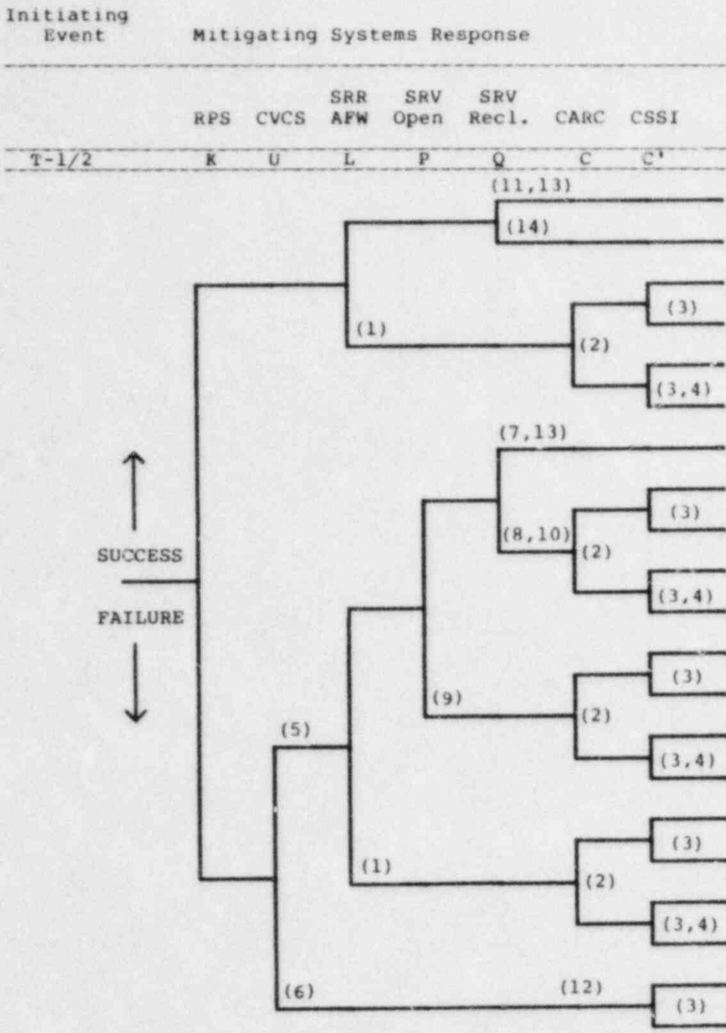
Sequence No.	Sequence Designator	RESC	REHR INJ	REHR REC	CNHR INJ	CNHR REC	CNRR INJ	CNRR REC	RCS Status	NOTES
25	S_1								SAFE	1,2
26	S_1H			x					CM	1,2,3
27	S_1F								SAFE	1
28	S_1FH			x				x	CM	1,3
29	S_1C								SAFE	
30	S_1CH			x					CM	3
31	S_1CG			x		x			CM	11
32	S_1CGH			x		x			CM	3
33	S_1CF			x		x		x	CM	4
34	S_1CC'			x	x		x		CM	4
35	$S_1D"$		x						CM	5
36	$S_1D"F$		x					x	CM	5
37	$S_1D"C'$		x				x		CM	5
38	$S_1D"C$		x						CM	5
39	$S_1D"CG$		x			x			CM	5
40	$S_1D"CF$		x			x		x	CM	5
41	$S_1D"CC'$		x		x		x		CM	5
42	S_1K	x							CM	6
43	S_1KF	x						x	CM	6
44	S_1KC'	x					x		CM	6
45	S_1KC	x							CM	6
46	S_1KCG	x				x			CM	6
47	S_1KCF	x				x		x	CM	6
48	S_1KCC'	x			x		x		CM	6

Figure 5-6 Small-Small LOCA (S_2) Systemic Event Tree



Sequence No.	Sequence Designator	RESC	REHR INJ	REHR REC	CNHR INJ	CNHR REC	CNRR INJ	CNRR REC	RCS Status	NOTES
49	S_2								SAFE	1,2,10
50	S_2H			x					CM	1,2,3,10
51	S_2F								SAFE	1,10
52	S_2FH			x				x	CM	1,3,10
53	S_2C								SAFE	10
54	S_2CH			x					CM	3,10
55	S_2CG			x		x			CM	11,10
56	S_2CGH			x		x			CM	3,10
57	S_2CF			x		x		x	CM	4,10
58	S_2CC'			x	x		x		CM	4,10
59	S_2D^*		x						CM	5,10
60	S_2D^*F		x					x	CM	5,10
61	S_2D^*C'		x				x		CM	5,10
62	S_2D^*C		x						CM	5,10
63	S_2D^*CG		x			x			CM	5,10
64	S_2D^*CF		x			x		x	CM	5,10
65	S_2D^*CC'		x		x		x		CM	5,10
66	S_2L		x						CM	7
67	S_2LF		x					x	CM	7
68	S_2LC'		x				x		CM	7
69	S_2LC		x						CM	7
70	S_2LCG		x			x			CM	7
71	S_2LCF		x			x		x	CM	7
72	S_2LCC'		x		x		x		CM	7
73	S_2K	x							CM	8
74	S_2KF	x						x	CM	8
75	S_2KC'	x					x		CM	6
76	S_2KC	x							CM	8
77	S_2KCG	x				x			CM	8
78	S_2KCF	x				x		x	CM	8
79	S_2KCC'	x			x		x		CM	8

Figure 5-7 Loss of Offsite Power (T_1) Loss of PCS (T_2), Loss of a DC Bus (T_{DC}) and Loss of Service Water (T_{SRW}) Systemic Event Tree

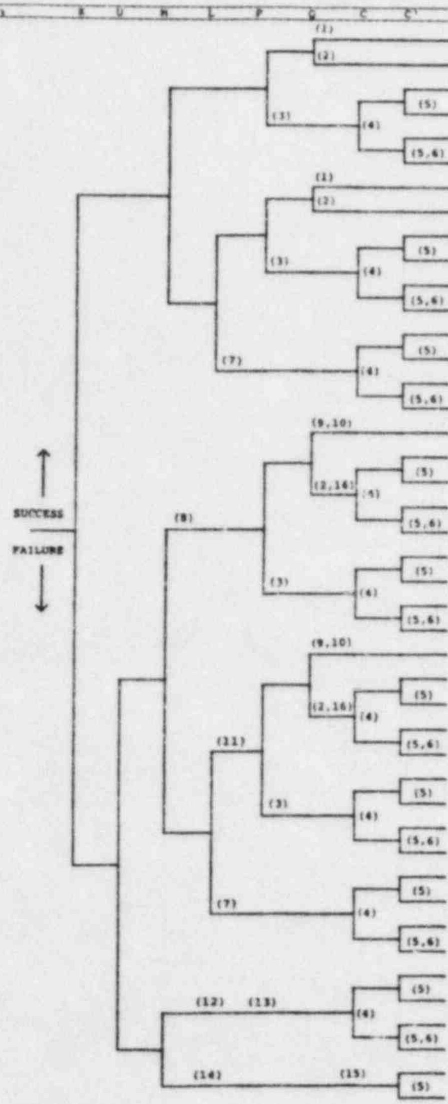


Sequence No.	Sequence Designator	RESC	REHR	RCSI	PSR	CNHR	CNRR	RCS Status	NOTES
80	T-1/2							SAFE	11,13
81	T-1/2 Q			x				LOCA	14
82	T-1/2 L		x					CM	1,2
83	T-1/2 LC'		x				x	CM	1,2,3
84	T-1/2 LC		x					CM	1,2
85	T-1/2 LCC'		x			x	x	CM	1,2,3,4
86	T-1/2 K							SAFE	5,7,13
87	T-1/2 KQ			x				LOCA,CM	2,5,8,10
88	T-1/2 KQC'			x			x	LOCA,CM	2,3,5,8,10
89	T-1/2 KQC			x				LOCA,CM	2,5,8,10
90	T-1/2 KQCC'			x		x	x	LOCA,CM	2,3,4,5,8,10
91	T-1/2 KP				x			CM	2,5,9
92	T-1/2 KPC'				x		x	CM	2,3,5,9
93	T-1/2 KPC				x			CM	2,5,9
94	T-1/2 KPCC'				x	x	x	CM	2,3,4,5,9
95	T-1/2 KL		x					CM	1,2,5
96	T-1/2 KLC'		x				x	CM	1,2,3,5
97	T-1/2 KLC		x					CM	1,2,5
98	T-1/2 KLCC'		x			x	x	CM	1,2,3,4,5
99	T-1/2 KU	x				x		CM	6,12
100	T-1/2 KUC'	x				x	x	CM	3,6,12

Functional Failures: RESC, REHR, RCSI, PSR, CNHR, CNRR

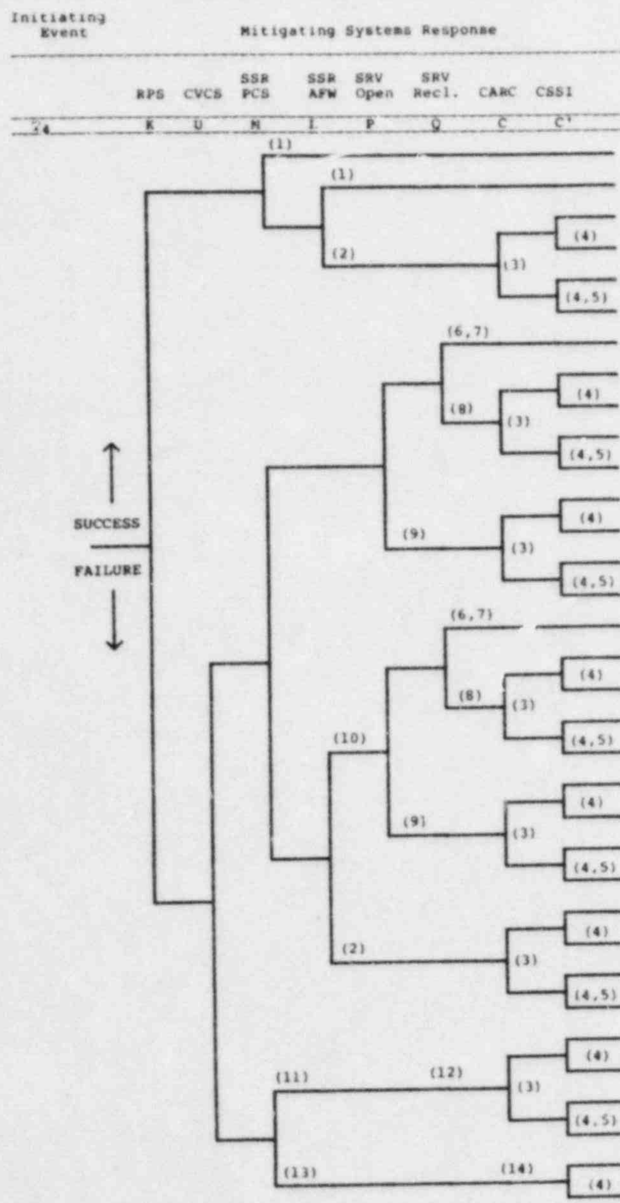
Figure 5-8 Transients Requiring Primary System Relief (T_3) Systemic Event Tree

Initiating Event	Mitigating Systems Response							
	RPS	CVCS	SSR PCS	SSR APW	SRV Op.	SRV Recl.	CARC	CSSI
T_3	K	U	M	L	P	Q	C	C'



Sequence No.	Designator	RESC	REHR	RCSI	PSR	CHRR	CHRR	RCS Status	NOTES
101	T_3							SAFE	1
102	T_3 Q			x				LOCA	2
103	T_3 P				x			CM	3,4
104	T_3 PC'				x		x	CM	3,4,5
105	T_3 PC				x			CM	3,4
106	T_3 PCC'				x	x	x	CM	3,4,5,6
107	T_3 M							SAFE	1
108	T_3 MQ			x				LOCA	2
109	T_3 MP				x			CM	3,4
110	T_3 MPC'				x		x	CM	3,4,5
111	T_3 MPC				x			CM	3,4
112	T_3 MPCC'				x	x	x	CM	3,4,5,6
113	T_3 ML		x					CM	4,7
114	T_3 MLC'		x				x	CM	4,5,7
115	T_3 MLC		x					CM	4,7
116	T_3 MLCC'		x			x	x	CM	4,5, 6,7
117	T_3 K							SAFE	8,9,10
118	T_3 KQ			x				LOCA,CM	2,8,4,16
119	T_3 KQC'			x			x	LOCA,CM	2,8,4,5,16
120	T_3 KQC			x				LOCA,CM	2,8,4,16
121	T_3 KQCC'			x		x	x	LOCA,CM	2,8,4,5,6,16
122	T_3 KP				x			CM	3,8,4
123	T_3 KPC'				x		x	CM	3,8,4,5
124	T_3 KPC				x			CM	3,8,4
125	T_3 KPCC'				x	x	x	CM	3,8,4,5,6
126	T_3 KM							SAFE	9,10,11
127	T_3 KMQ			x				LOCA,CM	2,4,11,16
128	T_3 KMQC'			x			x	LOCA,CM	2,4,5,11,16
129	T_3 KMQC			x				LOCA,CM	2,4,11,16
130	T_3 KMQCC'			x		x	x	LOCA,CM	2,4,5,6,11,16
131	T_3 KMP				x	x		CM	3,4,11
132	T_3 KMPC'				x	x	x	CM	3,4,5,11
133	T_3 KMPC				x	x		CM	3,4,11
134	T_3 KMPCC'				x	x	x	CM	3,4,5,6,11
135	T_3 KML		x					CM	4,7
136	T_3 KMLC'		x				x	CM	4,5,7
137	T_3 KMLC		x					CM	4,7
138	T_3 KMLCC'		x			x	x	CM	4,5,6,7
139	T_3 KU	x	x					CM	4,12,13
140	T_3 KUC'	x	x				x	CM	4,5,12,13
141	T_3 KUC	x	x			x		CM	4,12,13
142	T_3 KUCC'	x	x			x	x	CM	4,5,6,12,13
143	T_3 KUM	x	x			x		CM	14,15
144	T_3 KUMC'	x	x			x	x	CM	14,15,5

Figure 5-9 Remaining Transients Requiring Reactor Trip (T_4) Systemic Event Tree



Sequence No.	Designator	RESC	RENR	RCSI	PSR	CNHF	CNRR	RCS Status	NOTES
145	T_4							SAFE	1
146	T_4 M							SAFE	1
147	T_4 ML		x					CM	2,3
148	T_4 MLC'		x				x	CM	2,3,4
149	T_4 MLC		x					CM	2,3
150	T_4 MLCC'		x			x	x	CM	2,3,4,5
151	T_4 K							SAFE	6,7
152	T_4 KQ			x				LOCA,CM	3,8
153	T_4 KQC'			x			x	LOCA,CM	3,4,8
154	T_4 KQC			x				LOCA,CM	3,8
155	T_4 KQCC'			x		x	x	LOCA,CM	3,4,5,8
156	T_4 KP				x			CM	3,9
157	T_4 KPC'				x		x	CM	3,4,9
158	T_4 KPC				x			CM	3,9
159	T_4 KPCC'				x	x	x	CM	3,4,5,9
160	T_4 KM							SAFE	6,7,10
161	T_4 KMQ			x				LOCA,CM	3,8,9,10
162	T_4 KMQC'			x			x	LOCA,CM	3,4,8,10
163	T_4 KMQC			x				LOCA,CM	3,8,10
164	T_4 KMQCC'			x		x	x	LOCA,CM	3,4,5,8,10
165	T_4 KMP				x			CM	3,9,10
166	T_4 KMPC'				x		x	CM	3,4,9,10
167	T_4 KMPC				x			CM	3,9,10
168	T_4 KMPCC'				x	x	x	CM	3,4,5,9,10
169	T_4 KML		x					CM	2,3
170	T_4 KMLC'		x				x	CM	2,3,4
171	T_4 KMLC		x					CM	2,3
172	T_4 KMLCC'		x			x	x	CM	2,3,4,5
173	T_4 KU	x	x					CM	3,11,12
174	T_4 KUC'	x	x				x	CM	3,4,11,12
175	T_4 KUC	x	x					CM	3,11,12
176	T_4 KUCC'	x	x			x	x	CM	3,4,5,11,12
177	T_4 KUM	x	x			x		CM	13,14
178	T_4 KUMC'	x	x			x	x	CM	4,13,14

Table 5.1

Event Definitions For Systemic Event Trees

1. Initiators

Large LOCA	A breach of the RCS greater than 4.3" in diameter.
Small LOCA	A breach of the RCS greater than 1.9" but less than or equal to 4.3" in diameter.
Small-small LOCA	A breach of the RCS greater than .3" but less than or equal to 1.9" in diameter.
T_1	Shutdowns initiated by loss of Offsite Power.
T_2	Shutdowns initiated by loss of the Power Conversion system (other than due to T_1)
T_3	Shutdowns initiated by transients which require primary system relief.
T_4	Shutdowns initiated by all other transients.
T_{DC}	Shutdowns initiated by failure of DC bus 11.
T_{SRW}	Shutdowns initiated by failure of SRW train 12.

2. Systems

RPS	Reactor Protection System
CVCS	Chemical Volume and Control System
SIT	Safety Injection Tanks System
LPSI	Low Pressure Safety Injection System
HPSI/R	High Pressure Safety Injection/ Recirculation System
CSSI/R	Containment Spray System, Injection/ Recirculation
SDHX	Shutdown Heat Exchanger System

Table 5.1 (cont.)

Event Definitions For Systemic Event Trees

CARC	Containment Air Recirculation and Cooling System
SSR AFW	Auxiliary Feedwater and Secondary Steam Relief System
SRV Open	Safety relief valves open
SRV Recl.	Safety relief valves reclose
SSR PCS	Power Conversion System and Secondary Steam Relief

Table 5.2

Notes for LOCA Systemic Event Trees

1. CSSI is not required, because CARC performs the containment heat removal function during the injection phase, and because containment radioactivity removal is not needed until after core melt, which occurs during the recirculation phase if at all.

2. SDHX is not required because: (1) CARC performs the containment heat removal function, (2) the combined operation of CARC and HPSR can perform the reactor heat removal function, and (3) CSSR performs the containment radioactivity removal function independent of SDHX.

3. Core melt occurs early in the recirculation phase because of loss of core makeup due to failure of HPSR.

4. HPSR will eventually fail due to failure of containment systems.

5. Core melt occurs during the injection phase due to failure of HPSI.

6. Core melt occurs during the injection phase due to failure of RPS. Primary pressure will not drop below the HPSI shut-off head in time to prevent core uncovery and melt since the turbine will not trip for an extended period of time and reactor power and pressure will remain high.

7. HPSI success/failure states are not given in sequences where SSR-AFW has failed, because RCS pressure is assumed not to drop below the HPSI pump shut-off head of 1275 psia.

8. With failure of RPS, RCS pressure is assumed not to drop below the HPSI pump shut-off head of 1275 psia in time to prevent core uncovery and subsequent core melt since the turbine will not trip for an extended period of time and reactor power and pressure will remain high.

9. Even though SIT is expected to operate before LPSI, LPSI appears first on the event tree because failure of LPSI precludes any significant effect of SIT success or failure on the core melt consequences whereas if SIT fails LPSI can still significantly affect the consequences.

10. Sequences $T_{1/2}Q$-, T_3Q-, and T_3MQ- are transferred to the S_2 tree in locations where RPS has succeeded and SSR-AFW has succeeded.

11. Core melt occurs late in the recirculation phase because HPSR fails due to failure of heat sink.

Table 5.3

Transients $T_1/T_2/T_{DC}$ and T_{SRW} Event Tree Notes

1. Failure of SSR/AFW to remove sufficient heat from the reactor coolant system after a Loss of Offsite Power (LOSP) or Loss of Power Conversion System (PCS) will result in core melt.

2. For all accidents leading to core melt, the consequences may be mitigated by containment atmospheric heat and radioactivity removal. Therefore, the operational response decisions for CARC and CSSI appears in these cases.

3. Failure of CSSI results in failure to remove radioactivity from the containment atmosphere.

4. Failure of CSSI when CARC has also failed results in complete loss of containment atmospheric heat removal and potential containment overpressure rupture.

5. Successful CVCS operation after failure of RPS will make the reactor subcritical with no side effects due to pressure spikes (see the discussion of the ATWS(PSF) sequence in Chapter 8). It is assumed that the SRVs will be challenged when the RPS fails.

6. Failure of CVCS and RPS constitutes failure to reach subcriticality. Reactor power will equilibrate at the AFW heat removal rate of about 5% after a severe pressure transient and substantial loss of primary inventory.

7. Due to failure of RPS but successful shutdown of the reactor by CVCS, the opening and reclosing of the SRVs is required. It is assumed that the excess pressure will not rupture the RCS and that the core will remain intact (see the discussion of the ATWS(PSF) sequence in Chapter 8).

8. Failure to reclose any one of the SRVs after RPS failure will result in a Small-small LOCA and subsequent core melt since the resulting high equilibrium primary pressure will prevent successful primary makeup for an extended period of time due to the low HPSI pump shut-off head.

9. Failure of SRVs to open is assumed to result in RCS overpressure and subsequent loss of RCS integrity and core melt.

10. CVCS will provide successful reactor shutdown but will not provide successful coolant makeup.

Table 5.3 (cont.)

Transients $T_1/T_2/T_{DC}$ and T_{SRW} Event Tree Notes

11. Successful recovery does not require operation of the PORVs or Code Safeties when RPS succeeds, as described in NUREG-0635 for a realistic treatment of loss of feedwater transients. However, since there is a chance that a PORV may be opened, the SRV RECLOSE success would be required.

12. Sequences with failure of CARCS and/or CSSI are probabilistically negligible. CSSI was chosen so that both containment heat removal and radioactivity removal are successful.

13. It is assumed that successful recovery from a T_1 or T_2 transient would result from successful RPS, SSR, AFW, and SRV RECLOSE (if SRV's demanded). However, in the event that RPS fails, successful recovery requires PORV and code safety operation.

14. Failure to reclose a PORV after RPS success would result in a Small-small LOCA. The success of this sequence depends on LOCA mitigating systems success.

Table 5.4

Transient T_3 Event Tree Notes

1. Successful opening and reclosing of the PORVs with the reactor subcritical and adequate reactor heat removal will ensure a safe recovery. The RCS coolant loss through the PORVs will be retained by the reactor coolant drain tank.

2. Failure to reclose one of the PORVs will lead to a Small-small LOCA.

3. Failure to open any of the primary system pressure relief valves is assumed to result in RCS overpressure and subsequent loss of RCS integrity and core melt.

4. For all accidents leading to core melt, the consequences may be mitigated by containment overpressure suppression and adequate containment atmospheric heat removal, which is carried out by CARC and/or CSSI.

5. Failure of CSSI results in a reduced capability to remove radioactivity from the containment atmosphere.

6. Failure of CSSI when CARC has also failed results in complete loss of containment atmospheric heat removal and potential containment overpressure rupture.

7. Failure of SSR/AFW after failure of SSR/PCS will result core melt due to insufficient reactor heat removal.

8. The initiator involves a turbine trip which will cause the PCS to run back to a 5% flow level.

9. Due to the failure of RPS, the shutdown of the reactor is carried out by operation of CVCS, and the opening of the PORVs and Code Safeties can be expected. It is assumed that the excess pressure will not rupture the RCS and that the core will remain intact (see discussion of the ATWS(PSF) sequence in Chapter 8).

10. Success of CVCS after failure of RPS is assumed to provide the additional needed coolant inventory provided the SRVs reclose.

11. Failure of RPS followed by failure of SSR/PCS would leave only SSR/AFW to remove heat from a reactor that is undergoing a slow shutdown. Safe recovery, even with pressure relief, may be less certain than for the PCS success sequence.

Table 5.4 (cont.)

Transient T_3 Event Tree Notes

12. The initiator involves a turbine trip which runs back PCS flow to 5%.

13. With PCS flow at 5% and AFW flow at 5%, the excess energy in the core upon failure to scram will make the RCS pressure equilibrate near the RCS safety valve setpoints after a moderately severe pressure transient and substantial loss of primary inventory.

14. Failure of SSR/PCS with the reactor still critical would leave only SSR/AFW to remove heat. Reactor power will equilibrate at the AFW heat removal rate of about 5% after a severe pressure transient and substantial loss of primary inventory.

15. Sequences with failure of CARCS and/or CSSI are probabilistically negligible. CSSI was chosen so that both containment heat removal and radioactivity removal are successful.

16. Transient-induced LOCAs following failure to trip the reactor but successful shutdown by CVCS are assumed to result in core melt because the pressure will equilibrate above the HPSI pump shut-off head for an extended period of time.

17. Core melt sequences are distinguished from each other due to timing of core melt and subsequent radionuclide release to the containment.

Table 5.5

Transient T_4 Event Tree Notes

1. Successful recovery from a T_4 event is assumed to be achieved by tripping the reactor and removing reactor heat.

2. Failure of SSR/AFW after failure of SSR/PCS will result in core melt due to insufficient reactor heat removal.

3. For all accidents leading to core melt, the consequences may be mitigated by containment overpressure suppression and adequate containment atmospheric heat removal, which is carried out by CARC and/or CSSI.

4. Failure of CSSI results in a reduced capability to remove radioactivity from the containment atmosphere.

5. Failure of CSSI when CARC has also failed results in complete loss of containment atmospheric heat removal and potential containment overpressure rupture.

6. Due to the failure of RPS but successful shutdown of the reactor carried out by operation of CVCS, the opening of the PORVs and code safeties can be expected. It is assumed that the excess pressure will not rupture the RCS and that the core will remain intact (see the discussion of the ATWS(PSF) sequence in Chapter 8).

7. Success of CVCS after failure of RPS is assumed to provide the additional needed coolant inventory provided the SRVs reclose.

8. Failure to reclose one or both of the PORVs after RPS failure will lead to a Small-small LOCA and subsequent core melt, since the pressure will equilibrate above the HPSI pump shut-off head for an extended period of time.

9. Failure to open any of the primary system pressure relief valves would lead to RCS overpressure and rupture. This event is assumed to lead to a loss of RCS integrity and subsequent core melt.

10. Failure of RPS followed by failure of SSR/PCS would leave only SSR/AFW to remove heat from a reactor that is undergoing a slow shutdown. Safe recovery, even with pressure relief, may be less certain than for the PCS success sequence.

Table 5.5 (cont.)

Transient T_4 Event Tree Notes

11. Failure to shutdown the reactor would allow the PCS to remove heat at a power level greater than or equal to 5%. Should turbine trip or MSIV closure occur after the T_4 initiator, the PCS would runback to 5%. This is expected to occur in about 50% of the cases.

12. With PCS flow at 5% and AFW flow at 5%, the excess energy in the core upon failure to scram will make the RCS pressure equilibrate near the RCS safety valve setpoints after a moderately severe pressure transient and substantial loss of primary inventory.

13. Failure of SSR/PCS with the reactor still critical would leave only SSR/AFW to remove heat, reactor power will equilibrate at the AFW heat removal rate of about 5% after a severe pressure transient and substantial loss of primary inventory.

14. Sequences with failure of CARCS and/or CSSI are probabilistically negligible. CSSI was chosen so that both containment heat removal and radioactivity removal are successful.

CHAPTER 6

SYSTEMS ANALYSIS

6.0 Introduction

The probabilistic risk assessment of CC-1 necessitated a thorough comprehension of the systems at the plant which could be used to mitigate the effects of a LOCA or transient. This chapter briefly presents the methodology and several assumptions used in this task. Furthermore, summaries of the systems, both front-line and support, are given. Detailed system descriptions and fault trees are presented in Appendix B.

6.1 Methodology and General Assumptions

The methodology used in the CC-1 systems analysis is that presented in SAND82-0963, "Modular Fault Tree Analysis Procedures Guide." [15]. The methodology presented in the report is a modular logic approach to the development of detailed fault tree models for the various systems studied.

Fault tree models were constructed for all systems described in this section, with the exception of the RPS (Section 6.7), the PCS (Section 6.8), PORVs (Section 6.10), and the Code Safety Valves (Section 6.12). These systems were either evaluated using operating experience and/or were modeled using simple Boolean failure equations.

The fault trees were constructed using a modular approach. This involved developing a simplified energy flow diagram of the system to be analyzed. Each node on the diagram was noted and the system segment between nodes was assigned a reference letter. Pipe segment fault tree modules were selected for each component between nodes on the diagram and component fault tree modules were selected for each component in the system segments. The component modules tie in the support systems required for the component to successfully function. These modules were joined together to form the system fault trees.

Some basic assumptions were established to formulate guidelines for the failure modes to be considered in the fault trees. These assumptions are as follows:

1. System fault events which could also be accident initiators (e.g., LOCA events, LOSP) were explicitly included as appropriate in each system fault tree.

2. Only single passive failures which can fail the <u>entire</u> system were included in each system fault tree unless the passive failure was an accident initiator.

3. Flow diversion paths were considered as potential system failure modes for fluid delivery systems. However, each potential diversion path was only included on the fault tree if it could result in failure of the system and its likelihood was comparable or greater than other system faults.

4. Spurious control faults of components after successful initial operation were only considered in those cases where the component is expected to receive an additional signal during the course of the accident to readjust or change its operating state.

5. Operator errors of commission which misposition valves or fail other components in response to the accident were only included for those components which are specifically identified in procedures as requiring operator manipulation.

6. Consideration of operator action as a successful operating mode for systems was only done in those cases where a written procedure for system operation exists which specifies the required operator actions. That is, operator recovery actions are not explicitly considered in the fault tree, but are treated following the screening calculations for accident sequence frequencies. "Verify" statements in procedures are treated as recovery operations.

7. Mispositioning of valves prior to the accident was not considered in those cases where valve position is indicated in the control room and monitored shiftly. Nor was it considered if the valves receive an automatic signal to return to their operable state under accident conditions.

6.2 Safety Injection Tanks (SITs)

6.2.1 Description

Four SITs are available to flood the core with borated water immediately following a large break LOCA. They are designed to minimize core damage until the safety injection pumps can provide adequate water for core cooling. Each tank is pressurized with nitrogen at 200 psig and contains a minimum water volume of 8,300 gallons with a minimum boron concentration of 1,720 ppm. This concentration is sufficient to render the reactor subcritical with all rods withdrawn at $60^{o}F$.

The SITs are self-contained, self-actuating, and passive in nature. Each tank is connected to the RCS at one of the reactor inlets (cold legs). Two check valves, held closed by

RCS pressure, provide isolation during normal operation. The tanks can be isolated by motor-operated valves during plant shutdown and depressurization. Figure 6-1 is a simplified diagram of the SITs. The SITs are not dependent on any support systems.

In the case of the large break LOCA, RCS pressure will fall below the SIT pressure, the check valves will open and the tank contents will empty into the RCS. This action requires no actuation signal or outside power source. Three of the four tanks provide sufficient water to cover the core following a Design Basis Accident (DBA), assuming the contents of one of the four tanks spilled through the break.

6.2.2 Fault Tree Top Event

From the above success criteria, the fault tree top event is defined as "One SIT train (not connected to the failed loop) fails to function." Since operation of the SITs requires RCS pressure to drop below 200 psig, this fault tree is an input only to the large break LOCA systemic event tree.

6.2.3 Assumptions

The following assumptions were made during the fault tree construction of the SIT system.

1. Misposition faults for the normally locked-open motor-operated valves have been neglected since their position is checked shiftly.

2. Test and maintenance actions are not allowed due to technical specification requirements.

3. Faults related to tank pressure, level, and boron concentration have been neglected since pressure and level are alarmed and checked every shift and boron concentration is checked monthly and after each makeup.

4. A Large LOCA is assumed to occur in the loop to which injection line 11A is connected and to fail that SIT tank by dumping its contents on the floor.

6.2.4 Qualitative Insights

No unusual characteristics were identified for this system.

6.3 Low Pressure Safety Injection/Recirculation System (LPSI/R)

6.3.1 Description

The Low Pressure Safety Injection/Recirculation (LPSI/R) System injects borated water from the RWT into the RCS with a design flow of 3,000 gpm at a head of 350 ft. The LPSI/R System provides core cooling water during the injection phase of a large break LOCA.

The LPSI/R System can also be aligned to take suction from the containment sump and maintain a borated water cover over the core for extended periods of time in the recirculation phase of the large break LOCA; however, since this requires operator action and it is not the preferred system (HPSR is preferred), operation in the recirculation mode was treated as a recovery action.

The LPSI/R System consists of two pumps taking suction from separate RWT discharge headers and discharging to a common header. This header splits into four parallel injection lines to the RCS. The RWT discharge header is common for the LPSI/R System, the HPSI/R System, and the CSS/SDHX System. The injection lines pipe segments just prior to the cold legs are common for the LPSI/R System, the HPSI/R System, and the SITs. Also, the pump recirculation lines from the LPSI/R, HPSI/R and CSS/SDHX systems back to the RWT all share a common portion. Figure 6-2 is a simplified diagram of the system and Figure 6-3 shows the support systems required to operate the system.

Upon receipt of a SIAS, the two pumps will start and four injection line motor-operated valves will open. When RCS pressure drops below 200 psig, the LPSI/R will begin to deliver flow to the cold legs.

At a low level in the RWT, the automatic Recirculation Actuation Signal (RAS) will shutdown the LPSI/R pumps. The pumps cannot be restarted until this signal is cleared. There are complications involved in the process of clearing an automatic RAS signal. Thus, should HPSI/R fail in the recirculation phase of the Large LOCA, the operator can not easily restart the LPSI/R pumps to proceed with the cooldown.

6.3.2 Fault Tree Top Event

A fault tree was only drawn for the injection phase of a Large LOCA. LPSI/R operation during recirculation was treated as a recovery action. The fault tree top event for the LPSI/R is defined as "Failure to deliver the flow of one out of two LPSI/R pumps to one of four safety injection headers."

6.3.3 Assumptions

The following assumptions were made during the fault tree construction of the LPSI/R system:

1. RWT water temperature was assumed to be above 45°F and thus failure of the RWT due to freezing was not considered.

2. No significant flow diversion paths to the connecting ESF systems were identified.

3. Unavailability due to test events for pumps and MOVs was neglected since all affected components receive ESFAS signals to go to their safety states.

4. Failure to restore events for MOVs and/or their breakers were neglected since all LPSI/R MOVs get ESFAS signals to actuate and their positions are checked shiftly.

5. A large break LOCA is assumed to occur in the loop to which injection line 11A is connected and fail that line by dumping its contents on the floor.

6.3.4 Qualitative Insights (LPSI/R)

Some qualitative insights gained at the system level are presented below. Quantitative evaluation shows that these insights are insignificant to risk (see Appendix C).

1. Failure of a single air-operated valve leads to system failure (CV-306). This is a low probability event since the valve is locked-open, deenergized and position checked every 12 hours.

2. The event tree for the Large LOCA does not take credit for the Low Pressure Safety Recirculation (LPSR) system should the High Pressure Safety Recirculation (HPSR) system fail. To use the LPSR, the pumps must be manually started since the RAS will have tripped them. RAS may be initiated manually or automatically. Procedures exist directing the operator to manually initiate RAS when the refueling water tank reaches a level of four feet. If this occurs, the RAS can be reset manually and the LPSI pumps started manually. If manual RAS does not occur, it will occur automatically when the refueling water tank reaches a level of 2.5 feet. In this case, the LPSI pumps cannot be started until the RAS is reset. RAS cannot be reset until the water level is increased in the Refueling Water Tank or the RAS logic interlock is defeated.

6.4 Containment Air Recirculation and Cooling System (CARCS)

6.4.1 Description

The Containment Air Recirculation and Cooling System (CARCS) consists of four fan/cooler units supplying cooled, recirculation air to the containment and to the RCS components via ducts in the containment. The fans are driven by two-speed motors which are supplied by 480 VAC buses. Fans 11 and 12 are fed by Load Group A, fans 13 and 14 are fed by Load Group B. The fans draw air over the cooling units which are supplied by the Service Water System (SRWS). Coolers 11 and 12 are supplied by SRW Subsystem 11, Coolers 13 and 14 are supplied by Subsystem 12. Figure 6-4 is a simplified diagram of the fans and Figure 6-5 shows the coolers. Figure 6-6 is a dependency diagram showing the support systems required for successful operation of CARCS.

CARCS is normally operating with three of four fan coolers at high speed and reduced SRW flow. Upon receipt of a Containment Spray Actuation Signal (CSAS), all four fans start in slow speed, and outlet valves open to increase SRW flow through the coolers. In addition, should containment temperature rise above 140^{o}F, fusible links will melt and dropout plates open. This bypasses the normal ductwork, allowing a free air flow should the ducts collapse during a LOCA. For all classes of LOCA, CARCS succeeds if one of four units is operating with the fan in slow speed and full SRW flow through the cooler.

6.4.2 Fault Tree Top Event

From the above success criteria, the CARCS fault tree top event is "Failure of CARCS to Cool Containment with one of four Fan Coolers".

6.4.3 Assumptions

The following assumptions were made during fault tree construction of CARCS:

1. The only air flow paths considered in the fault tree are those that are rated for a normal air flow of 55,000 cfm.

2. For the Large LOCA case, the steam/vapor atmosphere would overload the fan motors if they remained in HIGH speed. Therefore, the fan is assumed to fail if it doesn't receive a CSAS to switch to SLOW speed.

3. Three of four fans are normally running. Fan 13 is assumed to be in standby and requires CSAS actuation for any size LOCA.

4. Collapse of the ducts due to a pressure differential in the early stages of the LOCA is considered a credible event. This event was modeled as "local fault of duct" and a value of 0.1 was assessed for this event in a LOCA environment.

5. In duct segment AF1 (see Figure 6-4), failure of any damper is assumed to fail the whole segment.

6. No credit has been given for unusual success criteria of CARCS (i.e., all four fans in slow speed with normal SRW flow through each cooler).

7. Operation of CARCS was assumed to be impeded in a core melt environment. High aerosol loading could reduce the heat removal efficiency or fail the system. A probability of 0.1 was assessed for "Inadequate Heat Removal" in CARCS heat exchanger in a core melt environment.

6.4.4 Qualitative Insights

No unusual system dependencies or characteristics were identified for this system.

6.5 Containment Spray/Shutdown Heat Exchanger System (CSS/SDHX)

6.5.1 Description

The Containment Spray/Shutdown Heat Exchanger System (CSS)/SDHX) performs two functions following an accident. First, it limits the containment pressure and temperature following a LOCA or transient-induced accident, thus reducing the possibility of a breach of containment and leakage of airborne radioactivity to the outside environment. Second, it reduces the amount of radioactive material in the containment atmosphere so that even in the event of containment failure a reduced amount of radioactivity would be released.

The CSS/SDHX system sprays cooled, borated water into the containment atmosphere. During the injection phase, borated water is supplied by the RWT. During the recirculation phase, suction for the CSS/SDHX system pumps is taken from the containment sump. In both phases, the water is pumped through the shutdown cooling heat exchangers and then through spray nozzles and into the containment atmosphere. The spray nozzles are

located in the dome of the containment and arranged in headers to give complete spray coverage at the containment horizontal cross-section area. The CSS/SDHX system consists of two electric motor-driven pumps, the two shutdown cooling heat exchangers, two spray headers and nozzles, and associated piping, valves and instrumentation. The capacity of each containment spray pump is such that it can limit the containment pressure to less than its design value following a LOCA without needing CARCS operation. The CSS/SDHX system and CARCS provide the same function and thus are redundant. Figure 6-7 is a simplified diagram of the system and Figure 6-8 shows the support systems required for successful operation of the CSS/SDHX system.

The CSS/SDHX system pumps are started on a Containment Spray Actuation Signal (CSAS), while the spray header isolation valve receives a SIAS signal to open. Also, a RAS signal will open the two containment sump valves in the recirculation phase.

In the injection phase, both the Containment Heat and Radioactivity Removal functions are performed simultaneously and this mode of operation is performed by the Containment Spray System (Injection) and denoted by CSSI. In the recirculation phase, if the shutdown cooling heat exchangers do not remove heat, then the system can still reduce the containment airborne radiation levels by spraying hot water into the containment atmosphere. In this mode the system is called the Containment Spray System (Recirculation) and denoted CSSR. If the shutdown heat exchangers are working, then both the Containment Heat and Radioactivity Removal functions can be performed. In this mode of operation, the system is called the Shutdown Heat Exchanger System and denoted SDHX.

6.5.2 Fault Tree Top Event

Three fault trees were constructed, one for the injection phase (CSSI) and two for the recirculation phase (CSSR and SDHX). Both CSS trains must fail in order to achieve system failure. The fault tree top events for CSSI/R are defined as "Failure to provide water from 1 of 2 CSS pumps through 1 of 2 headers in the Injection/Recirculation phase." The fault tree top event for SDHX is defined as "Failure to provide containment cooling through 1 of 2 shutdown heat exchangers."

6.5.3 Assumptions

A list of system-specific assumptions made during the CSS/SDHX fault tree analysis is provided below:

1. The minimum flow recirculation line does not constitute a significant path of diversion.

2. Lines to the LPSI/R and HPSI/R headers were not modeled in the fault tree as paths of diversion since significant diversion will not occur.

3. Failure of the operator to close the RWT outlet valves after recirculation has begun (RAS opened the containment sump valves and suction is being taken from the sump) will not cause the pumps to cavitate since the spray pumps are at an elevation (-15 ft.) lower than both the RWT (45 ft.) and the containment sump (10 ft.) and there is sufficient net positive suction head for continued pump operation.

4. Operation in a post-core melt environment is assumed. While core melt debris thrown into the sump could fail this system, one of the factors, pipe insulation, is not of the type identified as possibly leading to pump failure.

6.5.4 Qualitative Insights

No unusual system dependencies or characteristics were identified for this system.

6.6 High Pressure Safety Injection/Recirculation System (HPSI/R)

6.6.1 Description

The High Pressure Safety Injection/Recirculation (HPSI/R) System injects borated water from the RWT into the RCS at discharge pressures up to 1,275 psia. The HPSI/R System provides core cooling for Small and Small-small LOCAs when the RCS does not depressurize sufficiently to allow injection via the LPSI/R System before core damage occurs.

The HPSI/R System can also be aligned to take suction from the containment sump and maintain a borated water cover over the core for extended periods of time following any size LOCA.

The HPSI/R System consists of three pumps drawing from the RWT suction headers and injecting into the RCS cold legs via two trains of four injection headers each. Upon receipt of a SIAS, eight HPSI/R MOVs open and two of the three pumps start. At least 400,000 gallons of borated water are available in the RWT for safety injection and containment spray. When this water supply reaches a low level, a RAS is generated. This opens two containment sump MOVs and the HPSI/R System now begins to recirculate sump water that has spilled through the break.

The sump water can be cooled before recirculation to the core by passing it through two shutdown cooling heat exchangers and directing it to the HPSI/R suction header. This reconfiguration can be performed from the control room by the operator, but has not been credited in our analysis. Figure 6-9 is a simplified diagram of the system and Figure 6-10 shows the support systems required to operate the HPSI/R System in both modes.

In both the injection and recirculation phase, all three pumps must fail and both trains must be unavailable for system failure. These criteria cover all classes of LOCA except the large break. As mentioned previously, the HPSI/R System was not considered essential for mitigating a Large LOCA during the injection phase, only during the recirculation phase. The HPSI/R System shares the RWT and containment sump suction headers with the LPSI/R and CSS/SDHX.

6.6.2 Fault Tree Top Event

Two fault trees were drawn, one for the injection phase and one for the recirculation phase. The HPSR fault tree includes all events in the HPSI fault tree in addition to events of the recirculation phase. The fault tree top event for the HPSI/R System is defined as "HPSI/R fails to provide at least 1 pump flow through 1 of 4 headers."

6.6.3 Assumptions

A list of system-specific assumptions made during the HPSI/R fault tree analysis is provided below:

1. No significant flow diversions to other ESF systems were found.

2. Unavailability due to test events for pumps and valves has been neglected since all pumps and values receive ESFAS signals to go to their safety states.

3. Cavitation of the pump in the recirculation phase (due to non-closing of the RWT valves) has been neglected since sufficient NPSH exists for continued pump operation.

4. The minimum flow recirculation line was neglected as a diversion path but failure in the closed position was assumed to fail the HPSI pumps during Small-small LOCAs due to the pumps low shutoff head and the slow decrease in the primary pressure.

5. No immediate operator actions were modeled except operator failure to actuate RAS. All other actions were treated as recovery actions.

6. Failure to restore events for MOVs and their breakers have been neglected since all MOVs get ESFAS signals to go to their safety states and are position checked shiftly.

7. RAS actuation logic has been modeled to include both automatic and manual initiation (ESFAS fault tree).

6.6.4 Qualitative Insights (HPSI/R)

A qualitative insight gained at the system level is presented below. Quantitative evaluation shows that this insight is significant to risk (see Chapter 8).

All HPSI/R, LPSI/R and CSS pump minimum flow recirculation lines join together in a common portion which contains two normally open motor-operated valves. On initiation of HPSI following a Small-small LOCA by an SIAS signal failure of one of these valves in a closed position would result in failure of both LPSI pumps and all three HPSI pumps due to the slow decrease in primary system pressure and the fact that the pumps are pumping against dead head for a significant period of time. The CSS pumps would not fail since they only start on a CSAS signal which is expected to occur either simultaneously with or after the SIAS signal which opens the CSS spray header valves, thereby negating the need for recirculation flow in their case.

6.7 Reactor Protection System (RPS)

6.7.1 Description

The Reactor Protection System (RPS) provides the initiating signals and means of rapid insertion of the CEAs into the reactor core when process and plant conditions deviate from the limits established to protect the NSSS.

The RPS continuously monitors all critical NSSS and plant conditions and processes the information to provide reactor trip initiation when each of the following functions are determined to be beyond their allowable limits:

1. Power Level
2. Rate of Change of Power
3. Reactor Coolant Flow
4. Steam Generator Water Level
5. Steam Generator Steam Pressure

6. Pressurizer Pressure
7. Thermal Margin (DNBR)
8. Loss of Load
9. Containment Pressure
10. Axial Power Distribution.

A simplified functional diagram of the RPS is shown in Figure 6-11 to assist in the understanding of the following sequence of events which take place during a reactor trip.

1. The magnitude of the measured signal is compared to a given preset level. If the allowable deviation from the preset level is exceeded, a channel trip signal for that function is generated and transmitted to the logic matrices.

2. The logic matrices identify two coincident channel trips from any group of four measurement channels monitoring a protective parameter.

3. Upon identification of the 2 out of 4 channel trips, the coincidence logics generate four trip signals to two Control Element Drive Mechanism (CEDM) power supplies.

4. Interruption of the power to the two CEDM power supplies removes power from each CEDM hold coil and allows the spring loaded CEDM holding latch to release and cause the individual CEAs to enter the reactor core.

5. Given failure of the auto-trip system, an independent manual trip can be initiated to interrupt power to the two CEDM power supplies.

The only system providing support to the RPS is the Electric Power System. However, a loss of electric power will result in a reactor trip. Thus, the RPS is a completely independent system.

6.7.2 Fault Tree Top Event

A simple fault tree was developed for the RPS. It was determined that at full power, a reactor scram will be successful if at least one CEDM power supply bus deenergizes to cause approximately half of the CEAs to enter the core. The RPS fault tree was not used in the quantification and sequence evaluation process. It is believed that a reliability calculation based on operating experience would provide a more realistic estimate of RPS failure. (See Appendix C for a discussion of the quantification of all undeveloped events.)

6.8 Power Conversion and Secondary Steam Relief Systems (PCS & SSR)

6.8.1 Description

The Power Conversion (PCS) and Secondary Steam Relief System (SSRS) at CC-1 consist of the Main Feedwater and Condensate System (MFWCS), the steam generators (SG), and the SSRS.

The MFWCS is designed to transfer feedwater (condensate) from the condenser hotwell to the steam generators. During this operation, this system raises the feedwater temperature and pressure and controls its chemical composition.

The two steam generators at CC-1 are shell heat exchangers with reactor coolant on the tube side and secondary system water on the shell side. They transfer the heat generated in the RCS to the SSRS. The Main Steam System (MSS) transfers steam from the steam generators via turbine throttle stop valves, the reheaters, and the turbine-driven pumps to the turbine building. The steam is used here to drive the turbine generator and produce electricity. The MSS also controls the pressure on the secondary side of the steam generators by means of the turbine bypass valves, atmospheric dump valves, or steam generator safety valves (high pressure) and main steam isolation valves (MSIVs) (low pressure).

Figures 6-12, 6-13, and 6-14 show simplified diagrams of the MFWCS, the steam generator, and the SSRS, respectively.

The PCS will operate successfully to provide 5% full MFW flow to the steam generators if one train (one MFW pump, one condensate booster pump, one condensate pump, and the associated valves and piping) of the MFWCS remains in operation during the transient. One out of two steam generators functioning successfully is sufficient to remove the decay heat level of 5% full power from the RCS. The SSRS can remove 5% full power main steam flow successfully in several ways:

1. One out of four turbine bypass valves must open to relieve steam to the condenser, or

2. Two out of two atmospheric steam dump valves must open to relieve steam to the atmosphere, or

3. One out of 16 steam generator safety valves must open to relieve steam to the atmosphere.

The PCS depends upon a number of interfacing systems to successfully fulfill its design function. Figures 6-15 and 6-16 show dependency diagrams for the PCS and SSRS, respectively.

6.8.2 Fault Tree Top Event

The success criteria for the PCS is to supply at least 5% of full flow to one of two steam generators via one operable train of feedwater pumps (one condensate, one condensate booster and one main feedwater pump and associated valves and piping). Datailed fault trees were not developed for the PCS. Instead a Boolean failure equation was written directly from knowledge of the support system dependencies and all other faults were grouped as local faults and quantified using CC-1 operating experience. (See Appendix C for a discussion of the quantification and the Boolean equation of PCS.)

6.8.3 Qualitative Insights

The qualitative insights presented below were gained at the system level. Quantitative evaluation showed that two of these insights were significant to risk (see Chapter 8).

1. The failure of either of two 125 VDC buses were found to lead to a trip of the PCS and result in a subsequent reactor trip while simultaneously degrading the responding safety systems. These events were treated as a special initiating event and are discussed in Chapter 4 in more detail. These events were found to contribute significantly to risk (see the discussion of sequence $T_{DC}L$ in Chapter 8).

2. The failure of a SRW valve was found to lead to a trip of the PCS and result in a subsequent reactor trip while simultaneously degrading the responding safety systems. This event was treated as a special initiating event and is discussed in Chapter 4 in more detail. It found not to contribute significantly to risk.

3. Following a T_4 transient with failure to scram, the PCS was assessed to runback resulting in an ATWS sequence with inadequate heat removal. Accident sequences resulting from this series of events were found to contribute significantly to risk (see Chapter 8).

6.9 <u>Auxiliary Feedwater System (AFWS)</u>

6.9.1 Description

The purpose of the Auxiliary Feedwater System (AFWS) is to supply feedwater to the steam generators for evaporation to provide for the removal of decay heat and to cool the primary system to 300°F at which point shutdown cooling is initiated. The AFWS is used whenever the PCS is not available.

The system consists of a pair of steam turbine-driven feed pumps (one of which is locked-out) connected in parallel with a motor-driven feed pump. Each of the three pumps has sufficient capacity to provide the required flow to the steam generators. The only source of AFWS water modeled in this study is Condensate Storage Tank (CST) #12, a seismically qualified, missile and tornado-proof tank. There are two other CSTs which could supply water to the AFWS which are non-seismic. Manual action is required to realign the AFW to take suction from these tanks. Credit for these tanks was treated in the recovery analysis.

The two turbine-driven pumps are located in the auxiliary feed pump room and discharge into a common header to individual feedlines to the two steam generators. Flow in each feedline is controlled to regulate automatically at 200 gpm per feedline. The motor-driven pump discharges through a separate pair of feedlines to the steam generators, again with flow related to 200 gpm per feedline. The motor-driven pump, located in the service water heat exchanger room receives motive power from the 4kV bus 11. The turbine-driven pumps receive steam from either steam generator #11 or #12, and are capable of operating as long as the steam pressure exceeds 50 psig.

Successful operation of the AFWS is defined as the supply of a sufficient flow of feedwater to the steam generators so they will perform their function. The AFWS supplies water through four branches with flow controlled to 200 gpm in each branch. By neglecting the consideration of partial success in any branch, the total AFWS flow need only be considered for various values from 0 to 800 gpm in multiples of 200 gpm. Successful operation involves providing a flow rate of at least 400 gpm, starting within about 86 minutes after termination of PCS.

Figure 6-17 is a simplified diagram of the system and Figure 6-18 is a dependency diagram showing the support systems required for successful operation of AFWS.

6.9.2 Fault Tree Top Event

Based on the success criteria described above, the top event for the AFWS fault tree is defined as "Failure to provide at least 400 gpm to one or both steam generators." (This is equivalent to flow from at least one pump through at least two of four headers.)

6.9.3 Assumptions

A list of system-specific assumptions made during the AFWS fault tree analysis is provided below.

1. Ongoing design modifications of the CC-1 AFWS have been modeled in this study. These modifications include the addition of the motor-driven pump to the two turbine-driven pumps of AFWS and the locking-out of turbine-driven pump #12. The use of this locked-out turbine-driven pump as a recovery factor significantly reduced the frequencies of some of the dominant accident sequences. These modifications are scheduled to be made during the November 1983 outage at Unit 1 and have already been made at Unit 2.

2. Although a manual capability exists, via manual realignment, to supply water to the suction of the AFW pumps from CST #11, this capability was considered as a recovery action and was not modeled on the fault tree.

3. Although the capability exists, via operator action, to utilize AFW pump #23 from Unit 2 to provide water to steam generators #11 or #12, this capability was also considered as a recovery action and not modeled on the fault tree.

4. The capability exists, via manual action, to open a flow path to bypass any one of the throttling valves and provide water to a steam generator in case of failure of a throttling valve. This capability was also considered as a recovery action and not modeled on the fault tree.

6.9.4 Qualitative Insights

The qualitative insight presented below is gained at the system level. Quantitative evaluation showed that this insight is significant to risk (see Chapter 8).

There is a manual valve (AFW-161) in the AFWS, between the Condensate Storage Tank and the pump suction, that will disable the system if it fails to remain open. Recovery is possible by either (1) manually realigning the AFWS to the alternative CST #11 and starting the locked-out turbine pump, or (2) cross-feeding from Unit 2's AFWS.

6.10 Power Operated Relief Valves (PORVs)

6.10.1 Description

CC-1 is equipped with two PORVs located on the pressurizer. The PORVs are a type of electromatic relief valve. These valves are pilot-actuated, reverse-seated relief valves that use primary system pressure as the motive force to open and close the valve. When the pressure in the primary system

exceeds that of the valve setpoint, the pilot valve's solenoid is energized. Each solenoid is powered from a 480 VAC bus: ERV 402 from MCC-114R and ERV404 from MCC-104R. Both PORVs require DC bus 21 (load group B) to actuate a relay to allow AC power to energize the solenoids. The energizing of the solenoid causes its plunger to actuate an operating lever which in turn opens the pilot valve. The opening of the pilot valve vents the main valve's pressure chamber, resulting in a pressure differential across the main valve disc, thereby causing the valve to open and permit the discharge of the primary fluid at full rated flow. Conversely, when the pressure in the primary system drops below the valve's setpoint, the solenoid is deenergized. When the solenoid is deenergized, the pilot valve closes and steam is trapped in the chamber above the main valve disc. The trapped steam builds up pressure and forces the main valve's disc down on its seat, thereby closing the PORV. During power operation, the PORVs are actuated whenever the RPS's high primary pressure trip is actuated by two or more of the four channel logic system. The PORVs are actuated by the same bistable trip units which actuate reactor trip on high RCS pressure. Figure 6-19 is a dependency diagram showing the support systems required for successful operation of the PORVs.

There are normally open motor-operated valves upstream of the PORVs. These block valves can isolate the PORVs if seat leakage becomes excessive or the valve fails to reclose. They are powered from the opposite 480 VAC bus as their respective PORV.

The setpoint pressure for the PORVs is 2385 psig and the relieving capacity is 153,000 lb./hour.

For Small-small LOCAs and transients where the PCS and AFWS have failed, the "Feed and Bleed" method of core cooling can be initiated, the PORVs are blocked open by removing a bistable; however, this is a complicated operator action and is not in the procedures. Also, there is insufficient analysis to determine whether the PORVs are capable of relieving sufficient pressure to allow the high pressure injection system to function due to the low shutoff head of the HPSI pumps and, at this time, engineering judgement has concluded that this is not a viable mode of operation. For these reasons, "Feed and Bleed" has not been modeled in this study.

Instead of constructing a fault tree for failure of the PORVs to open on demand and to reclose when required, operating experience was used to quantify these events. A Boolean equation was written for the PORVs failing to open and included their AC and DC support system dependencies. A probability of 1E-5 per demand per valve was used for the hardware failure of a PORV to open. The failure probability for a PORV to reclose was found to be 2E-2 per demand per valve. If the PORVs do not

reclose, there is a 1E-2 probability from the recovery model that the operator fails to observe the failure to reclose. If he does observe the failure he can close the block valves if power is available. The probability of a block valve failing to close is 1E-3. A more detailed discussion of the PORV Boolean equation and its quantification can be found in Appendix C.

6.11 Chemical and Volume Control System (CVCS)

6.11.1 Description

The Chemical and Volume Control System (CVCS) provides several major functions during startup, normal operation, emergency operation, and shutdown of the reactor. The RCS boron concentration is normally controlled by the makeup portion of the CVCS. However, there are occasions when it is necessary to borate at a rate that exceeds the normal, maximum capability of the makeup system. In these situations, the CVCS is initiated either by a SIAS or manually to rapidly inject concentrated boric acid into the RCS. Of concern here are the situations where the CVCS can be initiated only manually (i.e., following ATWS).

Two boric acid storage tanks and two boric acid pumps are provided to supply boric acid to the RCS cold legs 11A and 12B during the emergency injection phase of the CVCS operation. A batching tank is provided for convenience in preparing boric acid for makeup to the storage tanks. The two boric acid pumps are started either manually or on a SIAS. For emergency boration a boric acid direct feed valve MOV-514 is provided. This is a motor-operated valve which comes off the common boric acid pump discharge and supplies concentrated boric acid directly to the charging pump suction header. This valve may be opened by either a SIAS or a handswitch on the control panel.

Figure 6-20 is a simplified diagram of the CVCS and Figure 6-21 is a dependency diagram showing the support systems required for system operation. (Dependency on SIAS is not considered here.)

The CVCS fault tree was constructed using a success criteria of 1 out of 2 boric acid pumps providing concentrated boric acid to 2 out of 3 charging pumps for injection into the RCS.

6.11.2 Fault Tree Top Event

Based on the success criteria discussed before, the CVCS fault tree top event was defined as "CVCS fails to provide 2 out of 3 charging pump flow to the reactor core."

6.11.3 Assumptions

A list of major assumptions made during the CVCS fault tree analysis is provided below.

1. No credit was given for automatic actuation of the systems since it is believed that there will not be a SIAS signal generated in the transient event tree sequence where there is a requirement for the CVCS.

2. Credit was not given for use of gravity feed lines, since the action required to open the MOVs on these lines is not mentioned in the emergency boration procedure EOP-13.

3. No credit was given for using the RWT as another source of boron. According to EOP-13, the RWT is used only in cases where the operator notices a low level in the boric acid storage tanks. Since failure of the boric acid tanks is a low probability event, this does not significantly affect system reliability.

4. Two out of three charging pumps were assumed to provide sufficient flow based on the information obtained from the technical specifications and EOP-13.

5. The makeup stop motor-operated valve 512 has not been modeled in the fault tree. This valve should be closed by the operator during emergency boration, but failure to close the valve would not lead to system failure, and at most (if makeup pumps are running and MOV-501 is open) could dilute the boric acid flow.

6. It is assumed that one charging pump is running at all times. Hence, faults of components in the segments associated with the operating pump have been ignored in the fault tree analysis, since these segments are assumed to be operational at the time of the accident.

6.11.4 Qualitative Insight

No unusual system dependencies or characteristics were identified for this system.

6.12 Code Safety Valves (SRVs)

CC-1 is equipped with two Code safety valves on the pressurizer. These valves are entirely mechanical devices. Their set points are 2500 and 2565 psia. At least one valve must be operable when the plant is at power. Testing or maintenance can only be accomplished when the plant is at a cold shutdown.

A fault tree model was not constructed for these valves. Generic operating experience for code safety valves was used for quantification of failure probabilities. A probability of 2E-5 per demand was applied to the event "failure of one of two code safety valves to open" and 2.4E-3 per demand for "failure of both valves to reclose." See Appendix C for more discussion of the quantification of these valves.

6.13 Emergency Electrical Power System

6.13.1 Description

The Emergency Electrical Power System consists of both the emergency AC system and the 125 VDC system. The emergency AC system is designed to provide electrical power to components in vital systems which are needed to mitigate the consequences of LOCAs and transients. The DC system provides continuous power for control, instrumentation, reactor protection, and engineered safety features actuation systems.

The emergency AC system is composed of two trains (A-train and B-train), each consisting of a diesel generator, 4160 V switchgear, 480 V load centers and motor control centers, two 120 V instrumentation panels, and associated transformer and circuit breakers. The DC system is composed of four separate trains (two A-trains and two B-trains), each comprising a 125 VDC battery, bus, battery charger, and control panels.

Figure 6-22 shows a simplified diagram of the emergency AC and DC systems.

Most of the emergency AC and DC systems are in continuous operation and, as such, are not initiated in response to an abnormal situation. The exception to this is the operation of the diesel generators, which are in the standby mode awaiting a start signal. Automatic actuation of the diesel generators can result from SIAS initiation or undervoltage on the 4160 V buses or manually.

The emergency AC and DC system (mainly the diesel generators) depends upon a number of interfacing systems to successfully fulfill their design function. These systems provide support functions to the diesel generators, such as cooling, ventilation, and actuation. The systems which provide these functions are the Room Cooling and Ventilation System, Service Water System, and Engineered Safety Features Actuation System.

Figure 6-23 shows the support systems required for operation of the emergency AC and DC system.

6.13.2 Fault Tree Top Events

There are six top events for the Emergency Electrical Power System fault tree. These top events define the loss of power events on four 120 VAC buses and two 480 VAC motor control centers. These events were developed to include the faults in the emergency AC and DC systems up to the 4160 V buses and the diesel generators. A list of the six top events for the Emergency Electrical Power System fault tree is provided below:

1. "Loss of power at 120V Bus ELC0011A"

2. "Loss of power at 120V Bus ELC0012B"

3. "Loss of power at 120V Bus ELC0013B"

4. "Loss of power at 120V Bus ELC0014A"

5. "Loss of power at 480V Bus ELC104RB"

6. "Loss of Power at 480V Bus ELC114RA"

6.13.3 Assumptions

The major assumptions which were made during the fault tree analysis of the emergency AC and DC system are listed below:

1. While the AC and DC buses can be manually cross-tied, no credit was given for this in the fault tree since the cross-ties are normally locked open and require operator action to align.

2. Room cooling and ventilation is assumed to be needed only by the diesel generators, and not by the switchgears, load centers, motor control centers, and the batteries. Since the loads following an accident will be lower, adequate ventilation can be obtained by opening doors and the time required to heatup is significantly longer.

3. The diesel generator dependency on control power was developed to include only the battery faults, thus avoiding circular logic problems in the fault tree.

4. The diesel generators are actuated by both the SIAS and the undervoltage signal but are loaded only on an undervoltage signal. Diesel generator #12 is a swing diesel and was assumed to require operator alignment to the unit requiring power on a simultaneous undervoltage to both units.

5. Maintenance contribution has not been considered for the buses, batteries, battery chargers, and inverters since a review of plant logs showed it to be negligible.

6. Manual recovery actions are not allowed in the DC system analysis.

6.13.4 Qualitative Insights

The qualitative insights presented below were gained at the system level. Quantitative evaluation showed that they were significant to risk (see Chapter 8).

1. The failure of either of two 125 VDC buses were found to result in a reactor trip and to simultaneously degrade safety systems. These events were treated as a special initiating event and are discussed in Chapter 4.

2. Diesel generator #12 was found either to line up randomly or not to line up at all on a simultaneous loss of offsite power to both units. Subsequent failure of the operator to align the diesel to Unit 1 was a significant contributor to a number of dominant sequences.

6.14 Engineered Safety Features Actuation System (ESFAS)

6.14.1 Description

The Engineered Safety Features Actuation System (ESFAS) continuously monitors critical plant parameters, processes the received information and automatically actuates equipment required to control and mitigate the consequences of incidents which could lead to radiation exposure to plant personnel and to the general public.

The ESFAS comprises four independent monitoring channels (sensor subsystems ZD, ZE, ZF, ZG) and two independent actuation systems (actuation channels ZA, ZB) which provide actuation of the required equipment to satisfy the following functional requirements during mitigation of an incident. These are:

1. Secondary Heat Removal - AFAS

   The Auxiliary Feedwater Actuation System:

   a. Starts the AFW pumps.

   b. Blocks AFW flow to a ruptured steam generator.

   AFAS is initiated by low steam generator level.

AFAS blocking to a steam generator is initiated by a differential pressure between steam generators coincident with identification of steam generator low level.

2. Core Cooling - SIAS

   The major effects of the Safety Injection Actuation System actuation are to:

   a. Start HPSI/R pumps.

   b. Start LPSI/R pumps.

   c. Initiate operation of all valves which require repositioning to allow injection of water from the RWT into the reactor core.

   d. Initiate RCS boration.

   e. Isolate letdown flow.

   f. Actuate all support system equipment required to provide energy removal from the primary system (containment) to the ultimate heat sink (Chesapeake Bay). These systems are CCWS, SRWS, and SWS.

   g. Initiate starting of the emergency diesel generators.

   h. Initiate sequential loading of the emergency diesel generators following a coincidental LOSP.

   i. Open containment spray mode isolation valves.

   SIAS actuation occurs upon detection of low pressurizer pressure or high containment pressure.

3. Containment Depressurization - CSAS

   The major effects of the Containment Spray Actuation System are to:

   a. Start the containment spray pumps.

   b. Shift containment coolers to low speed and increase SRW cooling flow through the containment coolers.

   CSAS is initiated by detection of high containment pressure.

4. Long Term Containment Energy Removal - RAS

The major effects of the Recirculation Actuation System are:

a. Align HPSI/R pump and containment spray pump suction headers to draw water from the containment emergency sump instead of the RWT.

b. Turn off the LPSI/R pumps.

RAS is initiated by low level in the RWT.

5. Loss of AC Power - Undervoltage (UV) Detection

The major effects of UV detection are to:

a. Isolate the 4KV buses from their normal AC feed sources.

b. Shed the loads from the 4KV buses.

c. Start the diesel generators and close the 4KV bus feed breakers from the emergency diesel generators.

d. Provide the signal which initiates the sequential loading of the 4KV bus following its connection to the diesel.

UV detection is initiated by undervoltage detected on the 4KV bus.

6. Loading of Emergency Diesel Generators - Shutdown Sequencer (SDS) and LOCA Sequencer (LOCAS)

The major effects of SDS are to:

a. Block and then sequence the critical loads in programmable time increments to the diesel generator when there is a LOSP. These loads involve the systems which maintain the energy removal path from containment to the ultimate heat sink, the instrument air compressors and the switchgear room HVAC units.

The major effects of LOCAS are to:

a. Block and then sequence the critical loads to the diesel generator in programmable time increments during a LOSP coincident with a LOCA.

The critical loads in this case include the components which maintain the energy removal path from containment to the ultimate heat sink and the components required to provide core cooling, containment heat removal, containment depressurization, secondary heat removal (AFW) and primary system boration.

SDS is initiated by undervoltage at the 4KV bus (UV)

The LOCA sequencer is initiated by undervoltage at the 4KV bus coincident with receipt of an SIAS (UV, SIAS).

Equipment

The ESFAS consists of two sections:

1. Sensor Subsystem

2. Actuation Subsystem

Each initiating function is monitored by four isolated, redundant sensors for each actuation system. Upon receipt of a signal which is outside the prescribed limits for that function, a bistable provides a digital input to the actuation logic (exception: RWT level actuation is from a level switch which provides a digital input directly).

The actuation logic system processes the digital inputs from the sensor subsystem and provides an actuation signal when two out of four sensor loops (ZD,ZE,ZF,ZG) have changed state. The actuation signal actuates two independent actuation channels (ZA and ZB), which in turn actuate multiple actuation relays which control the individual components.

Figure 6-24 is a simplified schematic of the ESFAS. Figure 6-25 shows the support systems required for operation of the ESFAS.

6.14.2 Fault Tree Top Events

About 100 components modeled in the CC-1 IREP study require ESFAS action. Therefore, the ESFAS fault tree has about 100 top events which are referenced by the "component actuation system fault module" contained in the front line and support system fault trees. The top events are "ESFAS fails to actuate component."

6.14.3 Assumptions

A list of the major assumptions which were made during the construction of the ESFAS fault tree is provided below:

1. Wire faults (open or shorts) were neglected unless they could disable multiple trains of redundant equipment since their failure rate was small compared to those of other components in a train.

2. Spurious blocking signals to the sequencer are neglected. These signals would also start the diesel generators and result in the diesel generator breakers closing. The fault developed is that the sequencer does not receive the subsequent signal to remove the block.

3. Failure of the A2 and/or B2 subchannels of under UV load shed Signal Group to load shed plant components is assumed to fail the diesel by overloading it when the diesel generator breaker closes.

4. When voltage is restored to the 4KV Bus, the under-voltage signal must clear to allow a component to start either manually or via an ESFAS signal. This fault is considered negligible since it requires at least 2 simultaneous relay failures to fail one train of ESF equipment and four simultaneous failures to fail the system.

6.14.4 Qualitative Insights

No unusual system dependencies or characteristics were identified for this system.

6.15 <u>Service Water System (SRWS)</u>

6.15.1 Description

The Service Water System (SRWS) is designed to remove heat from various plant components and to transfer this heat to the SWS for ultimate disposal in Chesapeake Bay.

The SRWS consists of two subsystems, each of which contains an electric motor-driven pump and a shell and tube heat exchanger. A third motor-driven pump can be used to supply either of the two subsystems in the event that the normal pump is lost.

Two 2350-gallon head tanks located in the auxiliary building furnish the required net positive suction head for the SRWS pumps.

Figure 6-26 shows a simplified flow diagram for the CC-1 SRWS. Although the SRWS supplies cooling water to a number of plant systems and components, only the containment air coolers and the emergency AC power diesel generators were considered in this study.

During normal power operation, two service water (SRW) pumps (#11 and #12) will be running, with the third pump (#13) in standby. This third pump (#13) can be lined up to take suction from and discharge to either subsystem 11 or 12, using either head tank. Normally, pump #13 is lined up mechanically to subsystem 12. Electrically, pump #13 is normally aligned to receive power from 4160 VAC bus #11, which also supplies power to pump #11. Pump #12 receives power from 4160 VAC bus #14. This configuration insures that the diesel generator supplying emergency AC power will have a source of cooling water available.

Pump #13 can be manually aligned, using key-operated disconnect links, to receive power from either 4160 V bus #11 or #14. In addition, the two subsystems may be cross-connected manually and one heat exchanger used to remove the full heat load within the time restraint specified in the plant Technical Specifications. Although two SRW pumps supply the required cooling during normal operation, only one pump is required to handle the SRWS cooling load following a LOCA. An SIAS or an SDS signal will automatically start pumps #11 and #12 if their control switches are in the "normal" position and their respective supply buses are energized. Pump 13 will start on an SIAS or an SDS signal only if the other SRW pump (either #11 or #12), aligned electrically to the same bus as pump #13, does not start within one second after the start signal is applied to its control circuit.

The SRWS depends upon a number of other support systems for successful performance of its design function. These systems are identified in the dependency diagram shown in Figure 6-27.

In this study, out of the various systems which receive cooling water from the SRWS, only the CARCS and the emergency AC power system, (more specifically, the diesel generators), were analyzed. (Diesel generator 12 can be supplied with cooling water from the SRWS of either unit CC-1 or CC-2; however, credit was not given for this on the DG #12 fault tree. It was treated as a recovery operation.) For this reason, fault trees were drawn only for the failure of the SRW supply for these two systems.

6.15.2 Fault Tree Top Event

The top event for each of the fault trees was defined as follows: Loss of Service Water Cooling for Component (either containment cooler or diesel generator). Failure of the SRWS to fulfill its design function was defined as failure to provide sufficient heat removal using either of the two SRWS trains.

6.15.3 Assumptions

The major assumptions which were made during the fault tree analysis of the SRWS are listed as follows:

1. Component outages due to maintenance were considered for maintenance of active components and the heat exchangers only.

2. Although the two independent SRWS subsystems are connected by a number of crossties, these crossties were not considered in this analysis because each contains at least one normally closed, manual valve.

3. Although the capability exists, via manual realignment, to supply the SRWS at Unit 1 with SRWS from Unit 2, this capability was not considered.

4. SRW pump #13 was assumed to be aligned electrically with 4160 VAC bus 11 and mechanically with SRW Subsystem #12. Because pump #13 is not an automatic backup to either subsystem individually, it was not modeled on the fault tree but was treated as a recovery action.

5. As discussed in Appendix B regarding the containment air coolers, only one containment air cooler is necessary to successfully fulfill the system function following a LOCA or a transient. Consequently, failure of the SRW supply isolation valves to isolate the turbine area components and/or the spent fuel pool coolers was not considered as an SRWS failure.

6. Secondary piping which was less than 1/2 the diameter of the main SRWS piping was not considered as a possible division source in this analysis since all lines require failure of two normally closed manual valves.

7. Gross failure of the unpressurized SRW head tanks was not considered because of its relative improbability when compared to other SRWS failures.

8. Those branches of the SRWS which provide service water cooing to components other than the containment air coolers and the emergency diesel generators were not considered in this analysis.

9. All four of the coolers of the containment fans were assumed to be operating at the time the transient initiator occurs.

6.15.4 Qualitative Insights

The failure of the inlet and outlet valves on SRW heat exchanger #12 were found to result in a reactor trip and simultaneously degraded safety systems. These events were treated as a special initiating event dand are discussed in Chapter 4.

6.16 Component Cooling Water System (CCWS)

6.16.1 Description

The Component Cooling Water System (CCWS) is designed to remove heat from various plant components in order to maintain their required operating temperature. The heat absorbed during this cooling process is transmitted to the Salt Water System (SWS) for ultimate disposal in Chesapeake Bay.

The CCWS is a closed system with cross-connected trains. It consists of three motor-driven pumps, two component cooling heat exchangers, a head tank, a chemical additive tank and associated valves, piping, instrumentation, control, and auxiliary systems. Of the several components depending on CCWS for their cooling requirements, only the following items are considered for this study:

1. LPSI/R Pump Seal's Coolers and Bearing Jacket

2) HPSI/R Pump Seal's Coolers and Bearing Jacket

3) Shutdown Cooling Heat Exchangers

Figure 6-28 shows a simplified diagram of the CCWS.

During normal operation, two of the three component cooling pumps (#11 and #12) are running and one component cooling heat exchangers (#11) is inservice. However, one pump and one heat exchanger is sufficient for providing the component cooling requirements during normal operation. The third component cooling pump (#13) remains in standby, and can be lined up to replace any of the inservice pumps when necessary. In this study, it was considered that pump #13 is lined up to operate as a backup for pump #11.

Upon initiation of SIAS signal, two component cooling pumps will receive a start signal and the outlet valves on the shutdown cooling heat exchangers will open automatically.

If a loss of power to the ESF buses should occur, the component cooling pumps will be load shed, and can be restarted manually after the diesel generator picks up the bus. If an SIAS signal is present, the component cooling pumps will automatically be sequenced back on the diesel generators.

The CCWS interfaces with the SWS via the component cooling heat exchangers. The CCWS operation depends on other support systems in the plant, including AC power, DC power, and the ESFAS. Figure 6-29 shows the dependency diagram for the CCWS.

6.16.2 Fault Tree Top Events

There are five top events representing the loss of component cooling to the following components:

1. The three HPSI/R pumps in the recirculation phase.

2. The two shutdown cooling heat exchangers (CSS/SDHX heat exchangers).

Success of the CCWS is defined as one component cooling pump and one component cooling heat exchanger circulating water and removing heat from the above components of the front line systems.

6.16.3 Assumptions

Major assumptions which were made during the fault tree analysis of the CCWS are listed as follows:

1. Two component cooling pumps and one component cooling heat exchanger are in service; however, successful operation required only one pump and one heat exchanger.

2. Only the shutdown cooling heat exchangers (SDHX) and HPSR pump coolers were considered as items cooled by CCWS since the LPSI/R pumps require cooling only in the recirculation mode which was not modeled but instead treated as a recovery action.

3. Maintenance on manual valves was neglected since a review of plant logs showed that it was negligible.

6.16.4 Qualitative Insights

The qualitative insight presented below is gained at the system level. Quantitative evaluation showed that this insight is insignificant to risk (see Chapter 8).

Failure of a single, normally open, manual valve (CCW-258) in the pump seal cooling portion of the component cooling water system will fail the following:

a. Low pressure system injection pumps in the recirculation mode.

b. High pressure system injection pumps in the recirculation mode.

This particular valve is a horizontally-mounted gate valve with low pressures placed on it by demineralized water flow. Because of the mounting arrangement, a stem break might not plug the valve and the assessed failure probability is judged to be conservative.

6.17 Salt Water System (SWS)

6.17.1 Description

The SWS provides cooling water from the ultimate heat sink (Chesapeake Bay) to the CCWS and and SRWS heat exchangers, to the ECCS pump room coolers, and several other plant systems. The SWS consists of two subsystems, each of which supply one heat exchanger or air cooler of the above systems. Normally, Subsystem 11 is fed by pump 11 which is aligned electrically to 4 KV Bus 11 (Load Group A). Subsystem 12 is fed by Pump 12 which is powered by 4 KV Bus 14 (Load Group B), or by the standby Pump 13. Pump 13 can be mechanically aligned to either subsystem (normally to Subsystem 12) and electrically aligned to either Load Group (normally to Load Group A). Figure 6-30 is a simplified diagram of the SWS and Figure 6-31 shows the support systems required for successful operation of the SWS.

Normally, both subsystems are operating. For the LOCA case, the SWS has two modes of operation. During the injection phase, throttling valves to the component cooling heat exchangers are shut by a SIAS signal, since this system has no significant heat loads in this mode. SIAS also signals the service water heat exchanger valves to go fully open. Since SRW cools the CARCS, this permits maximum heat transfer from the containment to the ultimate heat sink.

At the start of the recirculation phase, the RAS causes the CCWS heat exchanger valves to resume their normal throttling mode of operation. The SRW heat loads have been reduced at this point and now component cooling is required to cool the hot containment sump water being recirculated through the shutdown cooling heat exchangers. During both phases, SWS flow is provided to the ECCS pump room coolers.

The post-LOCA plant cooldown can be accomplished by one SWS subsystem.

6.17.2 Fault Tree Top Events

The SWS provides cooling to six separate heat exchangers required to mitigate the LOCA. The fault tree has the following top events:

1. Failure to provide SWS cooling water to ECCS pump room cooler 11.

2. Failure to provide SWS cooling water to ECCS pump room cooler 12.

3. Failure to provide SWS cooling water to SRW HX 11.

4. Failure to provide SWS cooling water to SRW HX 12.

5. Failure to provide cooling water to component cooling HX 11 during the recirculation phase.

6. Failure to provide cooling water to component cooling HX 12 during the recirculation phase.

6.17.3 Assumptions

A list of major assumptions is provided below:

1. SWS pump 13 is electrically aligned to 4KV bus 11 (same as pump 11 in loop 11) and is mechanically aligned to loop 12 (pump 12); therefore, it will start automatically on loss of pump 11 but it will discharge to loop 12. Since pump 13 is not an automatic backup to either subsystem individually, it was not modeled on the fault tree but instead was treated as a possible recovery action.

2. Valves which are throttled during normal operations (e.g., CV5210 and CV5212), and which are required to go full-open upon SIAS, are treated as normally closed, fails closed, valves.

3. The SWS pumps have no external lubrication system, nor do they have any external cooling (either lube oil cooers or room coolers). Therefore, these faults have been grouped with the local pump faults.

4. Both loops of the SWS are used during normal operation and any failure would be noticed within a short time (i.e., a few minutes). Therefore, restoration faults after maintenance on SWS components have been neglected.

5. During injection, failure of the CCW heat exchanger to isolate is assumed to fail the cooling of the SRW heat exchanger.

6. During the recirculation phase, failure of the SRW heat exchanger outlet valves CV5210 and CV5212 to throttle, is considered to cause the failure of cooling CCW heat exchangers 11 and 12, respectively.

6.17.4 Qualitative Insights

Some qualitative insights gained at the system level are presented below. Quantitative evaluation show that these insights are insignificant to risk (see Appendix C).

1. A single normally open manual valve (SWS-197) failure in the SWS (at the discharge of the two SRWS heat exchangers) leads to failure of the SRWS and consequent failure of of:

    a. both diesel generators (during loss of ofsite power);

    b. containment fan coolers.

2. A single normally open manual valve (SWS-196) failure in the SWS (at the discharge of the two CCWS heat exchangers) leads to failure of the CCWS and ECCS pump room coolers 11 and 12, and consequent failure of:

    a. Containment Spray Recirculation System

    b. High Pressure Recirculation System

    c. Low Pressure Recirculation System

6.18 <u>Heating and Ventilation</u>

6.18.1 Description (Diesel Generator Room Ventilation System)

The Diesel Generator Room Ventilation System is required to limit the diesel generator room to a temperature of less than 120°F, at which point the reliability of the diesel is considered suspect. Annunciation of a high temperature condition is provided in the control room, when diesel generator room temperature rises to 110°F.

The cooling system consists of a vane axial fan drawing air from either inside or outside of the room, or a combination of both, to regulate the temperature in the room. The room is maintained at a positive pressure and excess air is forced from the room through an exhaust damper which opens when the fan starts. A functional diagram of the system is shown in Figure 6-32. Figure 6-33 is a dependency diagram showing the support systems required for successful operation of the system.

The inlet and exhaust dampers fail open on loss of instrument air or loss of electric power. The inlet and recirculation dampers have dual pneumatic operators and are coupled together.

6.18.1.1 Fault Tree Top Event and Assumptions

The fault tree top event, the loss of adequate diesel generator room cooling, was developed using the following assumptions.

1. Only local faults leading to loss of power to the fans were included since otherwise circular logic would be introduced into the diesel generator fault tree.

2. Loss of actuation was not considered since the generation of the start signal within the diesel start logic was not modeled in the diesel generator tree (i.e., the same signal that starts the DG results in an actuation signal to the room ventilation.

6.18.2 Description (ECCS Pump Room Cooling)

Each ECCS pump room (east and west) contains a cooling system consisting of a forced air/salt water cooled heat exchange. This cooling system is only required during periods of operation when the ECCS pumps are in operation. Air is forced across the heat exchanger by a bank of three (west room)

or four (east room) fans. Recent calculations done by BG&E* for the NRC show that room cooling is only needed during the long-term heat removal or recirculation phase

The system is designed to maintain the room temperature below 110°F. Reliability of the components in the pump room is unaffected until the temperature reaches 120°F. The limiting component is the containment spray pump air cooled shaft seal, which is designed to operate with an air temperature of 120°F. A functional diagram of the cooling system is shown in Figure 6-32. Figure 6-33 shows the support systems required to operate the system.

The controlling process parameter is room temperature, measured by TE 5404 (5405). The normal range of operation is 95°F to 104°F. With room temperature increasing at 104°F, the output of the temperature controller matches the set point of pressure switch PS 5404 (PS 5403) which, then actuates and:

1. Turns on the fans.

2. Opens the saltwater inlet valves by deenergizing SV 5170 (5173) and saltwater valve SV 5171 (5174). With room temperature decreasing at 95°F, the output of the temperature controller TC 5404 (5405) allows reset of PS 5404 (5403) which reenergizes SV 5170 (5173) to close the saltwater inlet valve and also turns off the fans.

The automatic system can be overridden by the hand switches to the following extent.

HS 5404 (5404A) OFF - FANS OFF

HS 5404 (5404A) ON - FANS ON

HS 5404 (5404A) AUTO - FANS CONTROLLED BY PS 5404 (5403)

#11 ECCS Pump Room - Inlet & Outlet Valves Open/Auto/Close (HS 5172)

#12 ECCS Pump Room - Inlet Valve Open/Auto/Clos. (HS 5173)

---

*Ref: Discussions with Niall Hunt of BG&E.

Loss of instrument air or electric power opens the saltwater valves, however, short term loss of air is precluded by the installation of accumulators on the air supply.

6.18.2.1 Fault Tree Top Event and Assumptions

Top logic for each tree (Room 11 and Room 12) consisted of loss of forced air cooling or loss of saltwater to the coolers leading to system failure. The loss of saltwater portion of the fault tree interfaced with the saltwater fault tree.

The fault tree top event is defined as "Room 11 (12) cooling or ventilation system faults."

The following assumptions were made during the fault tree analysis:

1. To simplify the fault trees, the fans were considered as a single unit, as were their controls and electric feed breakers.

2. Loss of heat removal to fan coolers was considered to fail the room cooling system.

6.18.3 Qualitative Insights

A qualitative insight gained at the system level is presented below. Quantitative evaluation showed that this insight is significant to risk (see Chapter 8).

The ECCS pump room cooling is tested on the average only once a year; therefore, the fault duration time for time-dependent component failure modes are about six times that for similar components tested monthly.

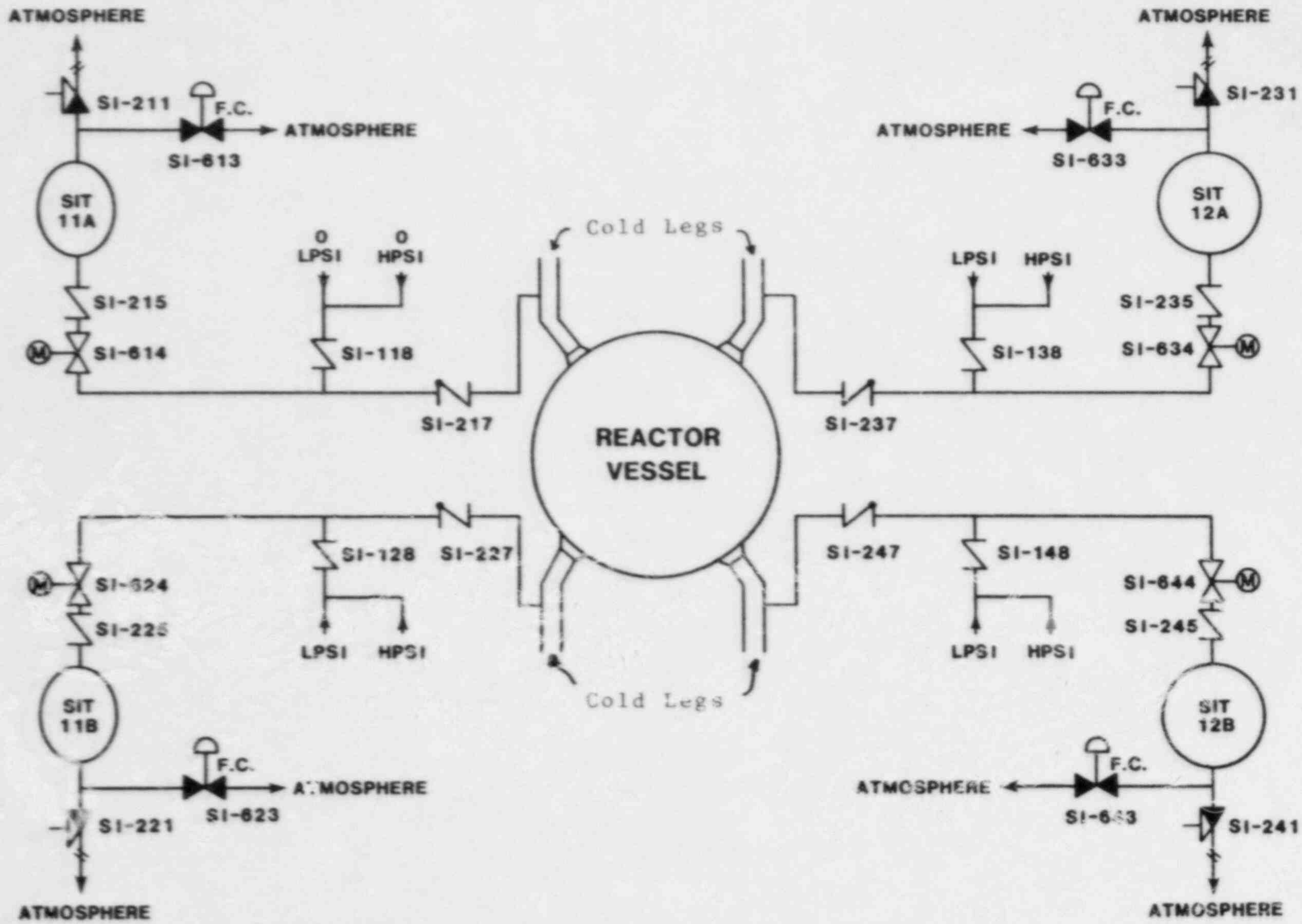


Figure 6-1 Simplified Diagram of SITs

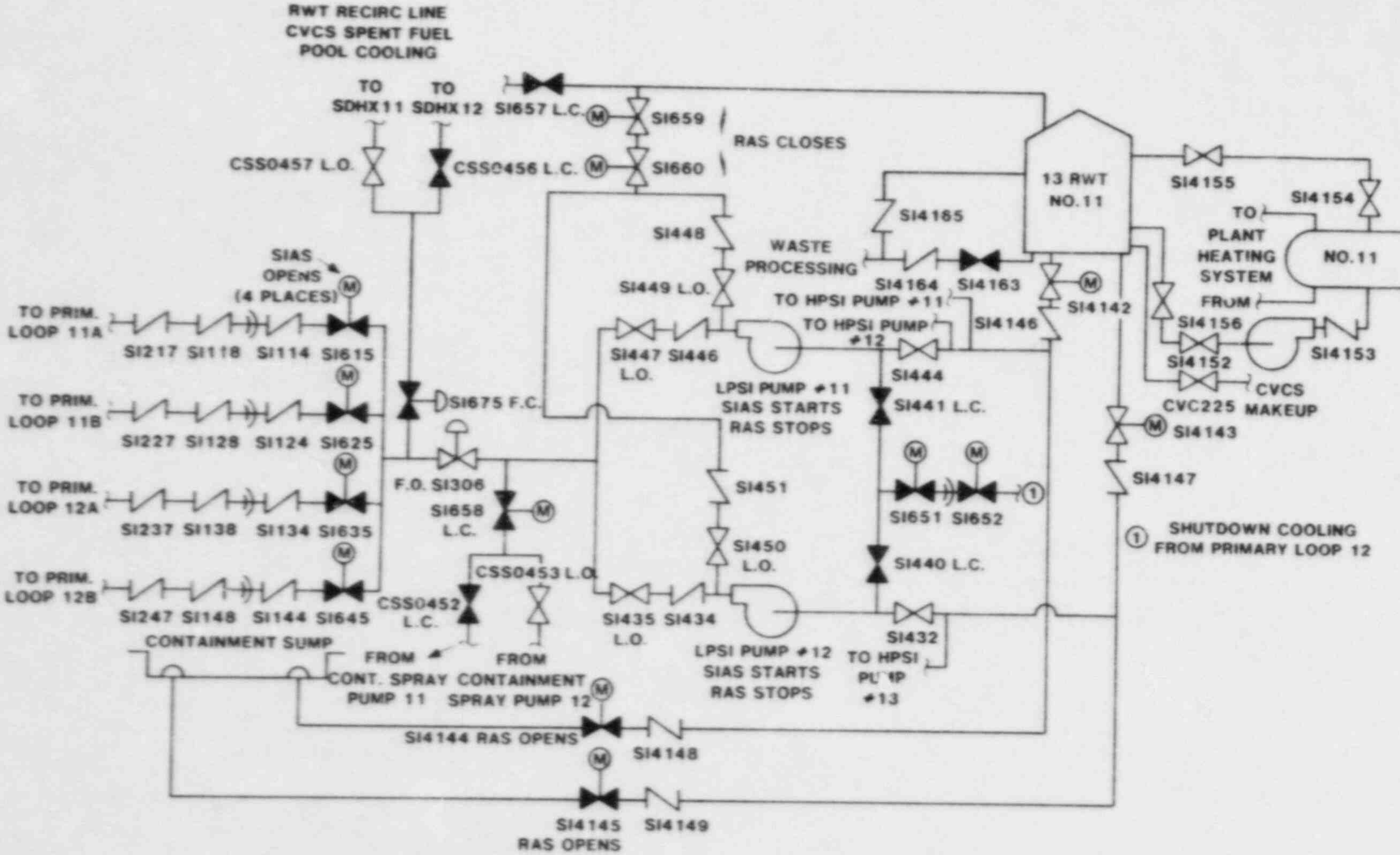


Figure 6-2 Simplified Diagram of LPSI/R

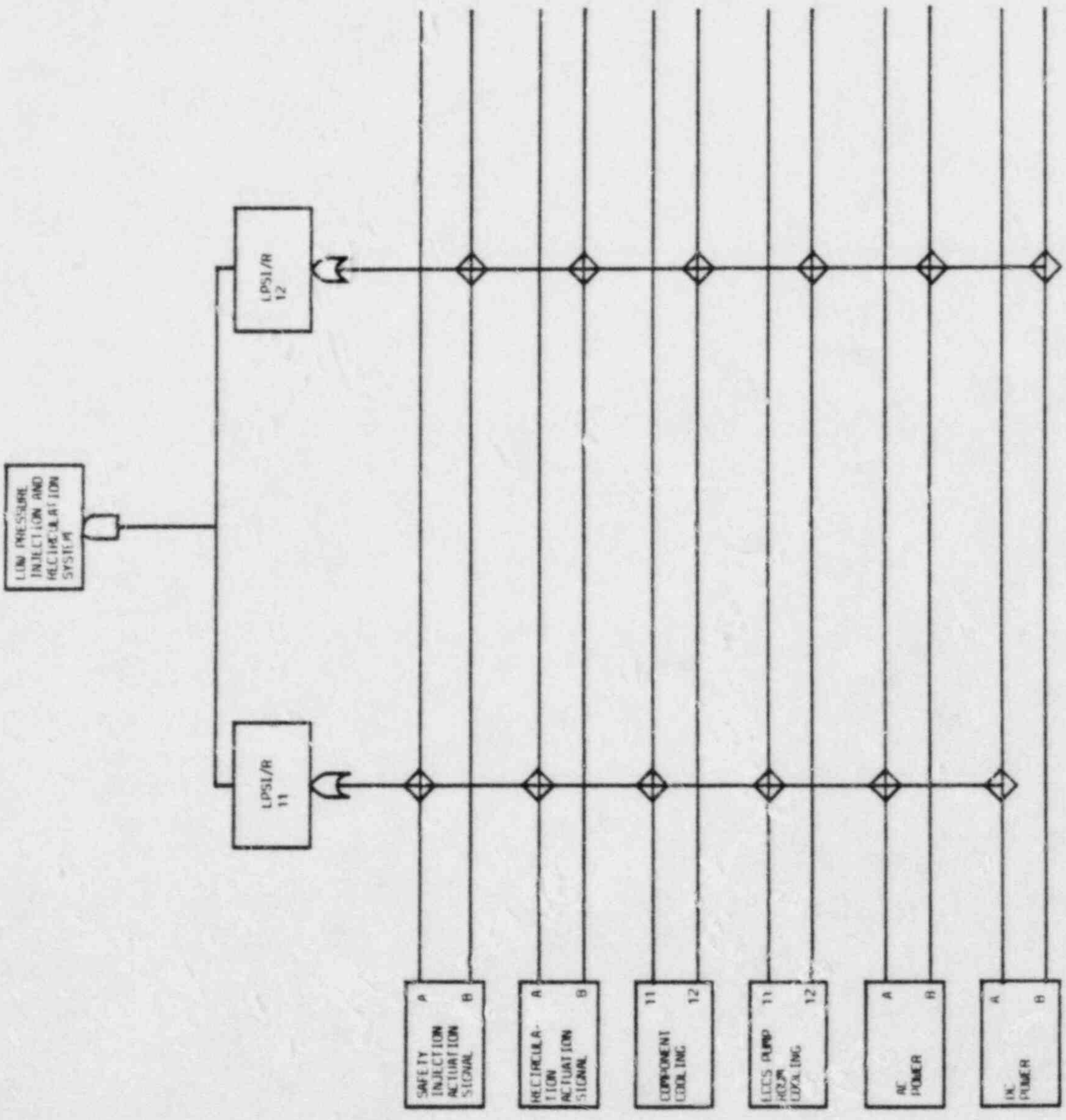


Figure 6-3 LPSI/R Support System Dependency Diagram

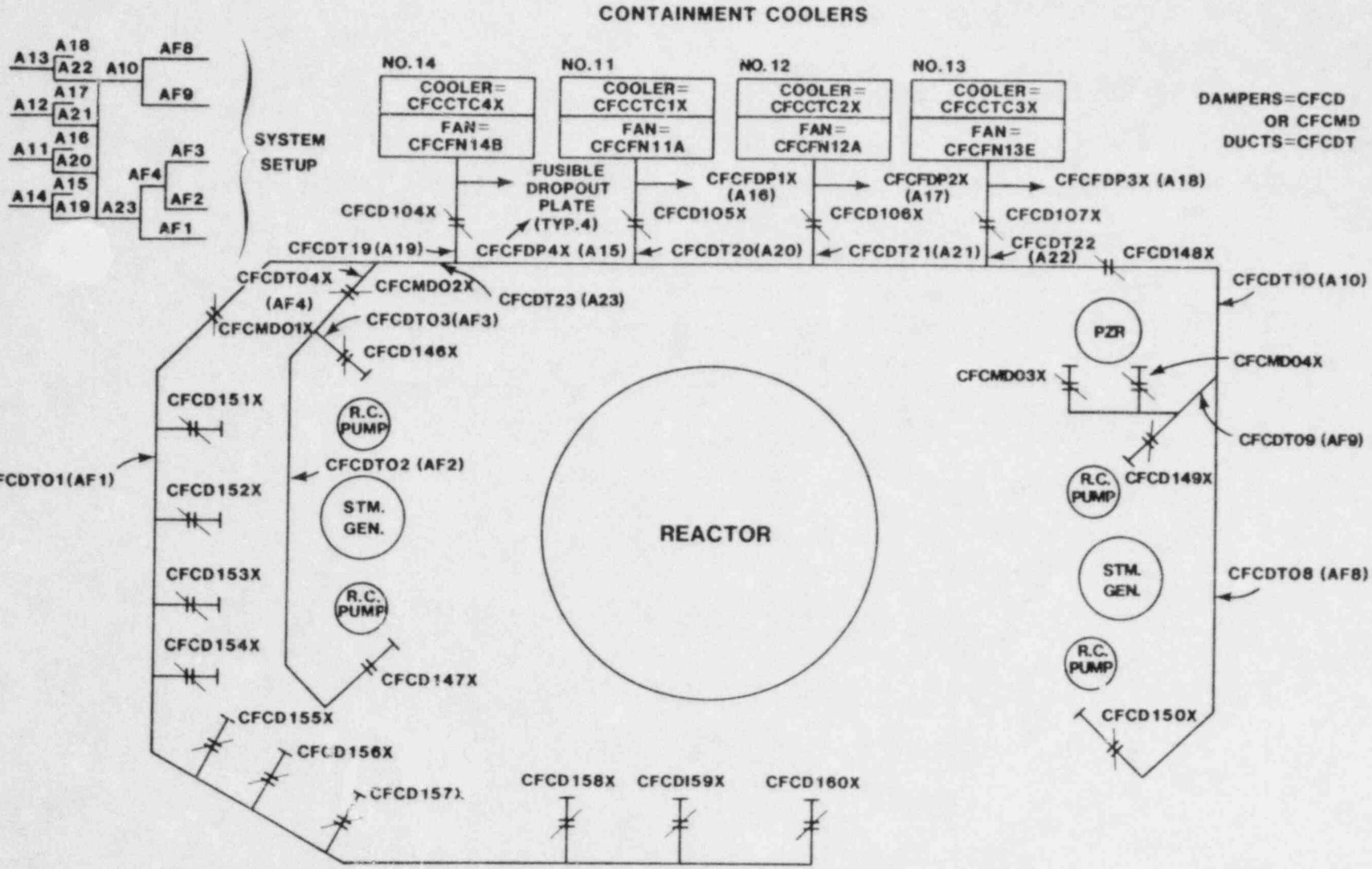
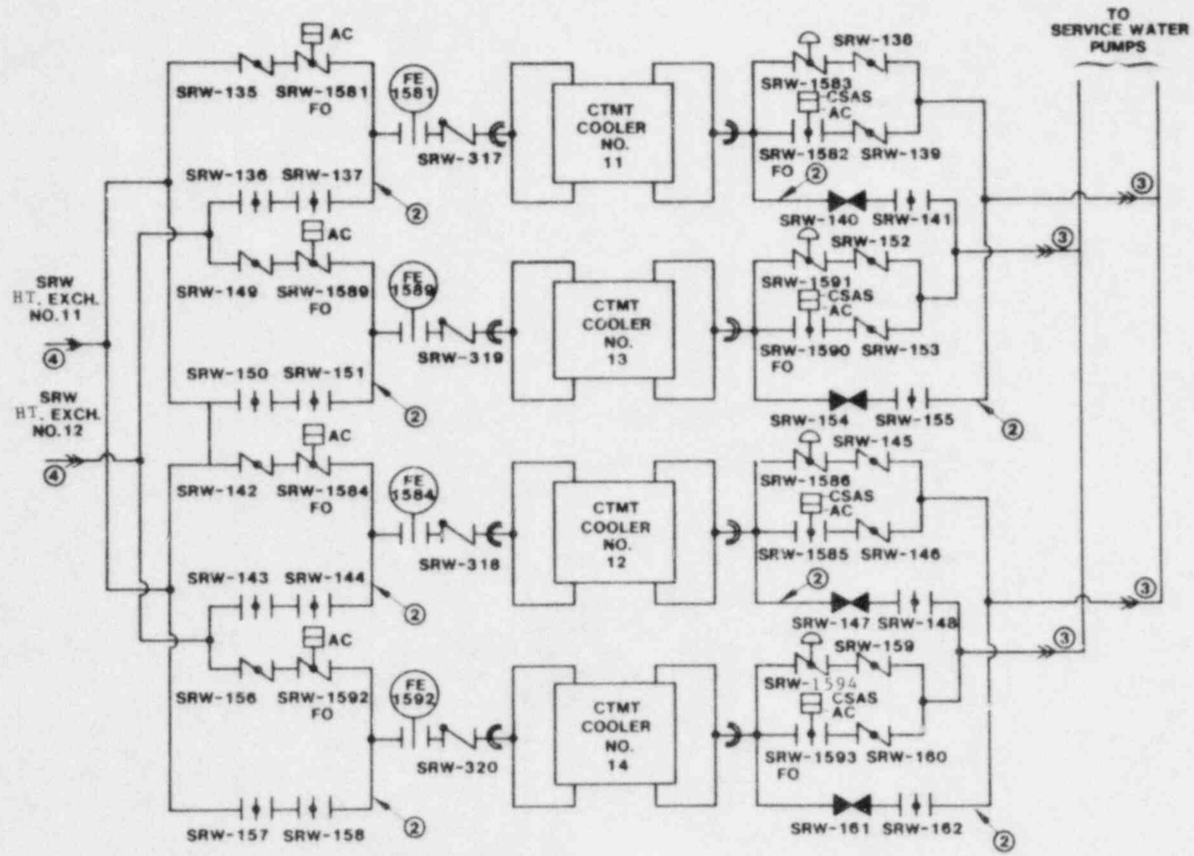


Figure 6-4 Simplified Diagram of CARCS



NOTES:

1. SRW-1581-1586 AND SRW-1589-1594 ARE ACTUATED BY SOLENOID VALVES.
2. THE VALVES IN THESE PIPE SEGMENTS ARE NORMALLY LOCKED CLOSED. NO CREDIT IS TAKEN FOR THESE SEGMENTS AS ALTERNATE INLET/OUTLET PATHS IN THE FAULT TREE.
3. DISCHARGE END OF CARCS MODEL.
4. COOLANT SOURCE OF CARCS MODEL.

Figure 6-5 CARCS Service Water Supply

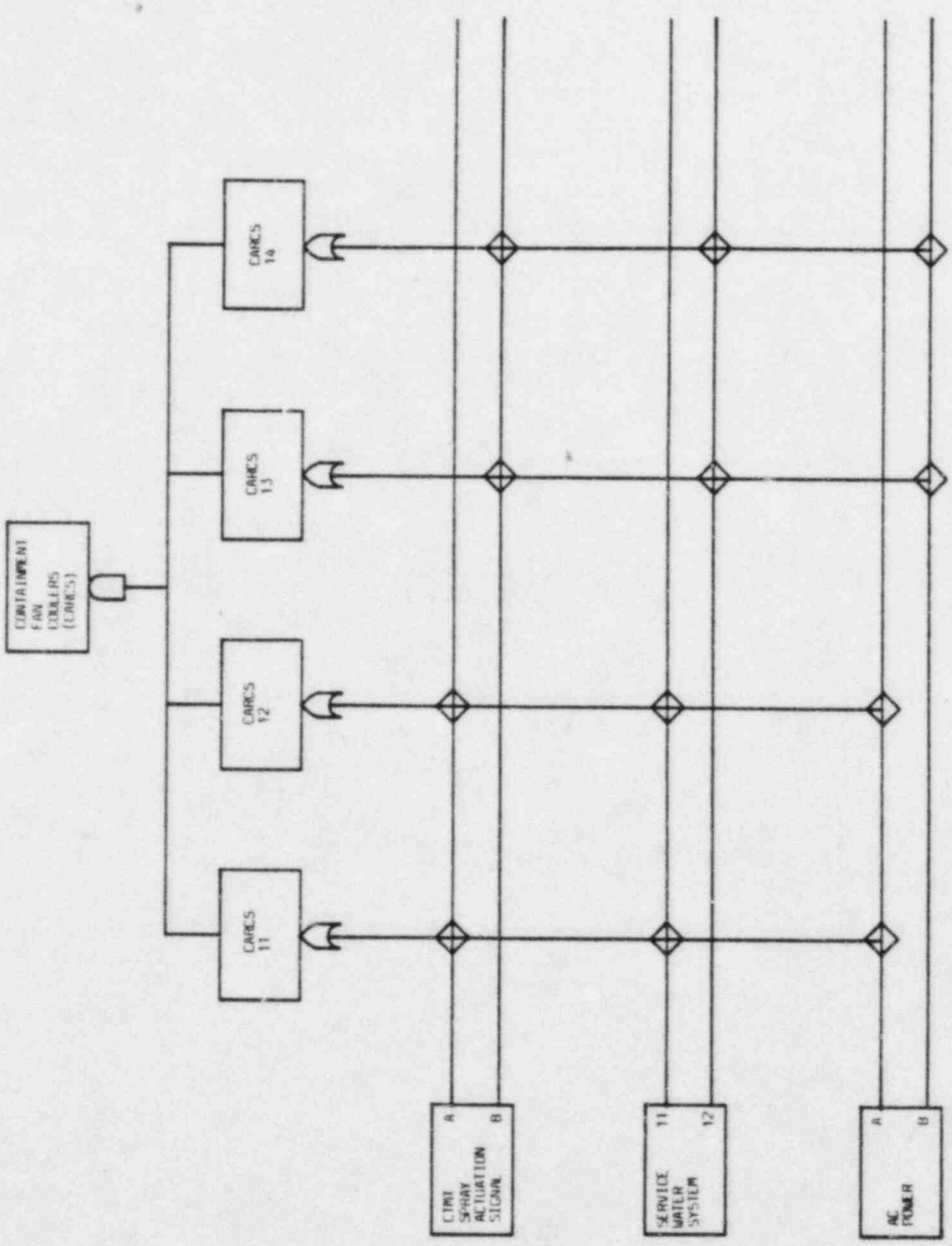


Figure 6-6 CARCS Support Dependency Diagram

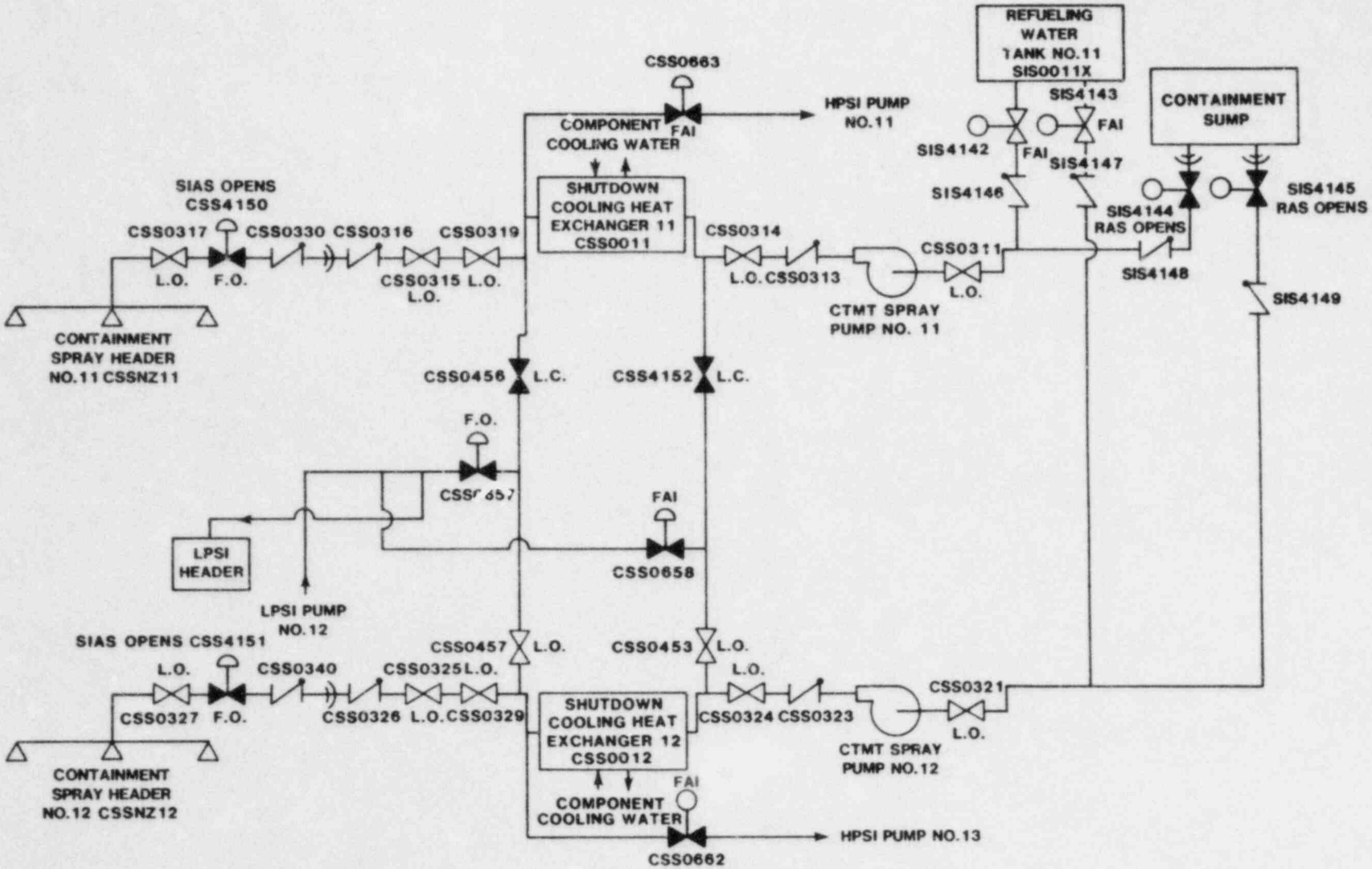


Figure 6-7 Simplified Diagram of CSSI/R/SDHX

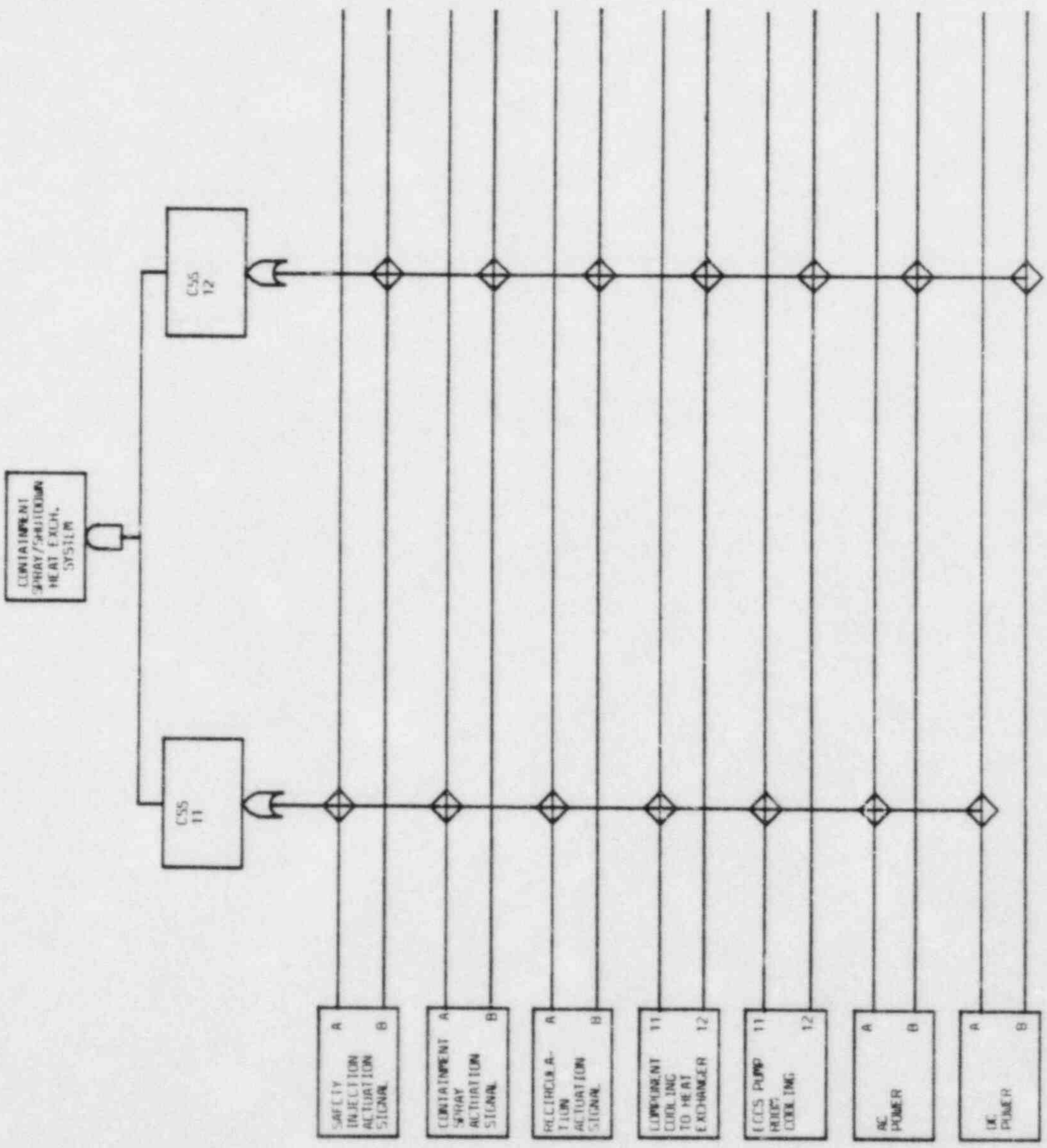


Figure 6-8 CSS/SDHX Support System Dependency Diagram

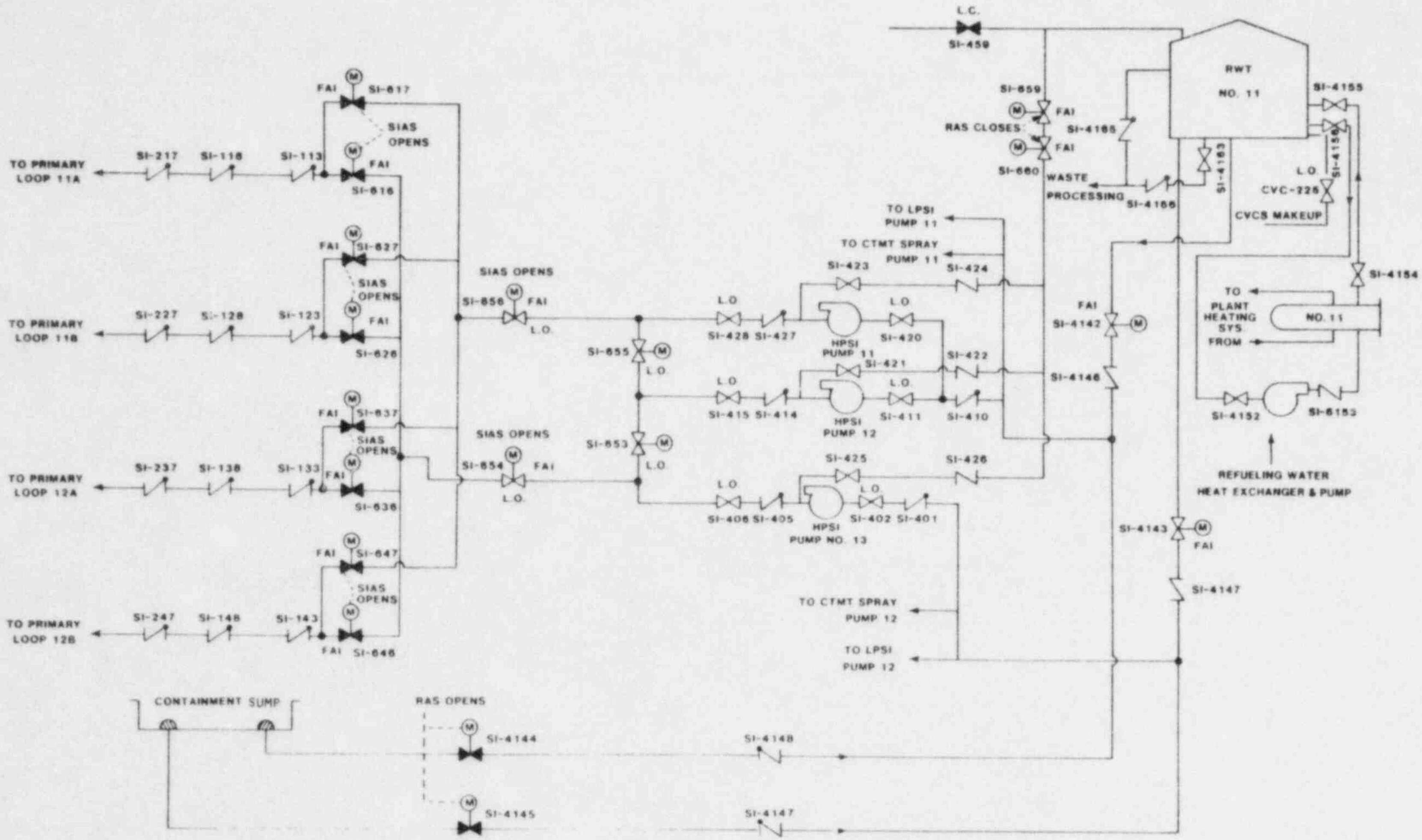


Figure 6-9 Simplified Diagram of HPSI/R

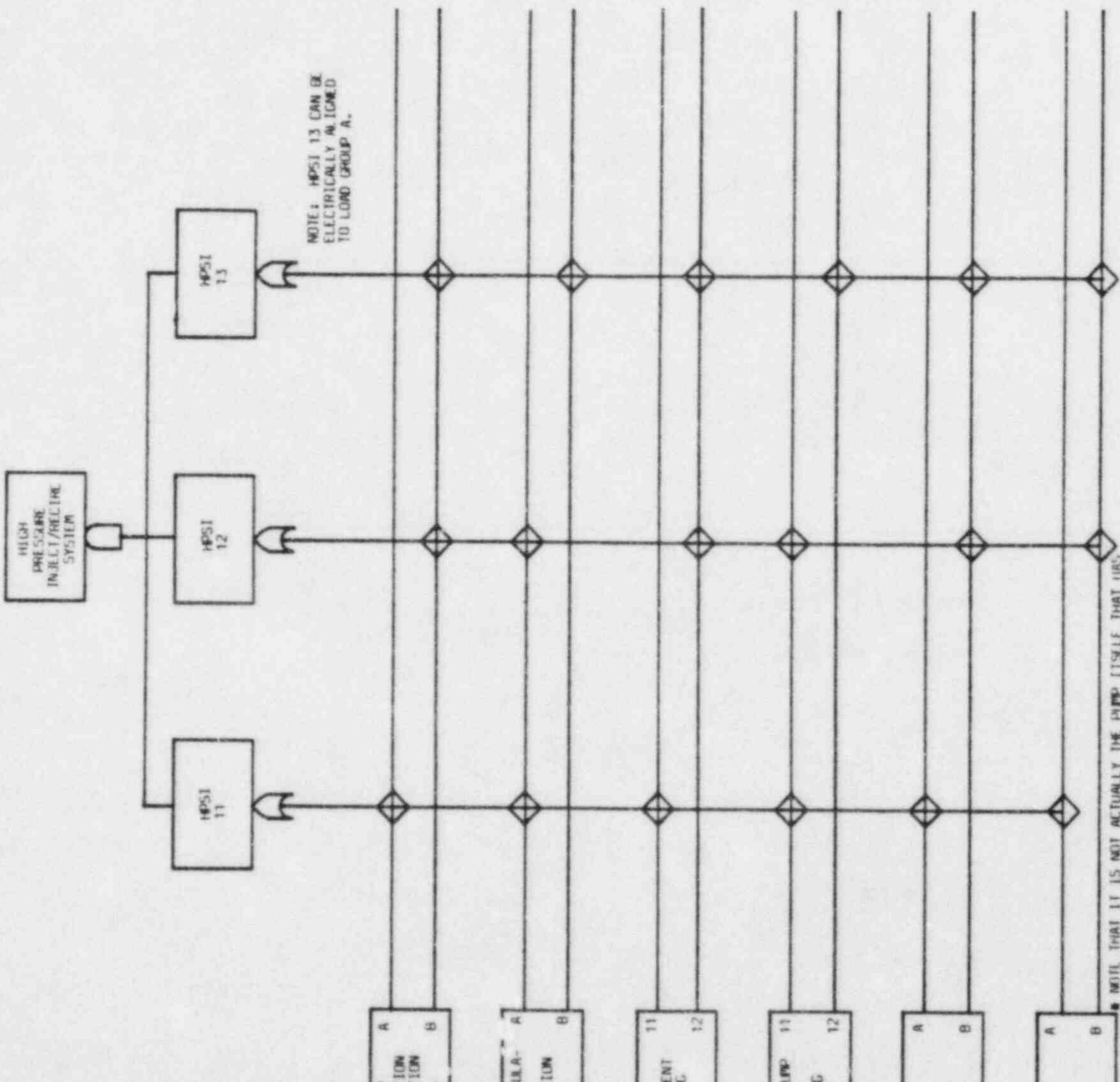


Figure 6-10 HPSI/R Support System Dependency Diagram

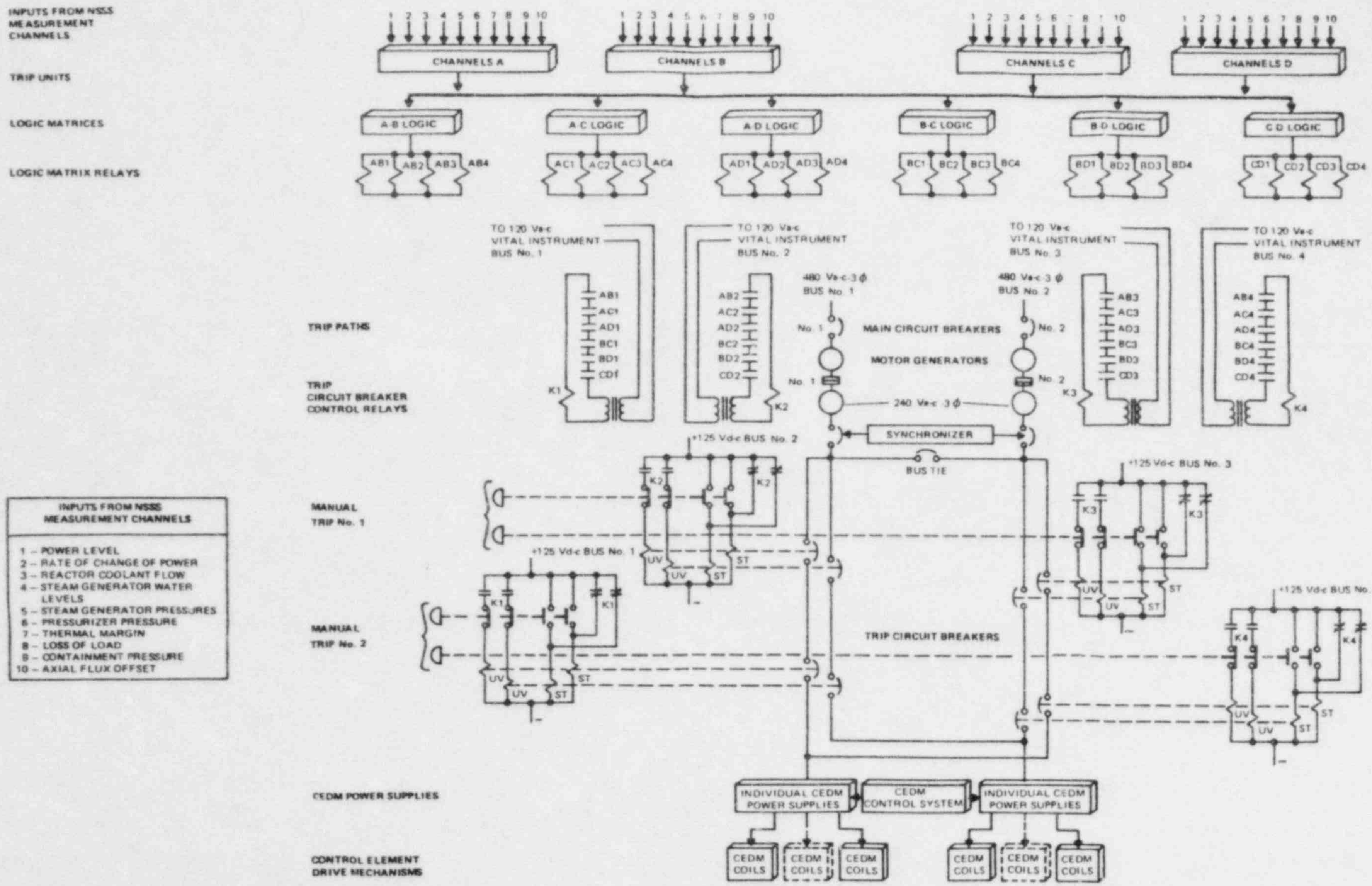


Figure 6-11 Simplified Functional Diagram of the Reactor Protection System

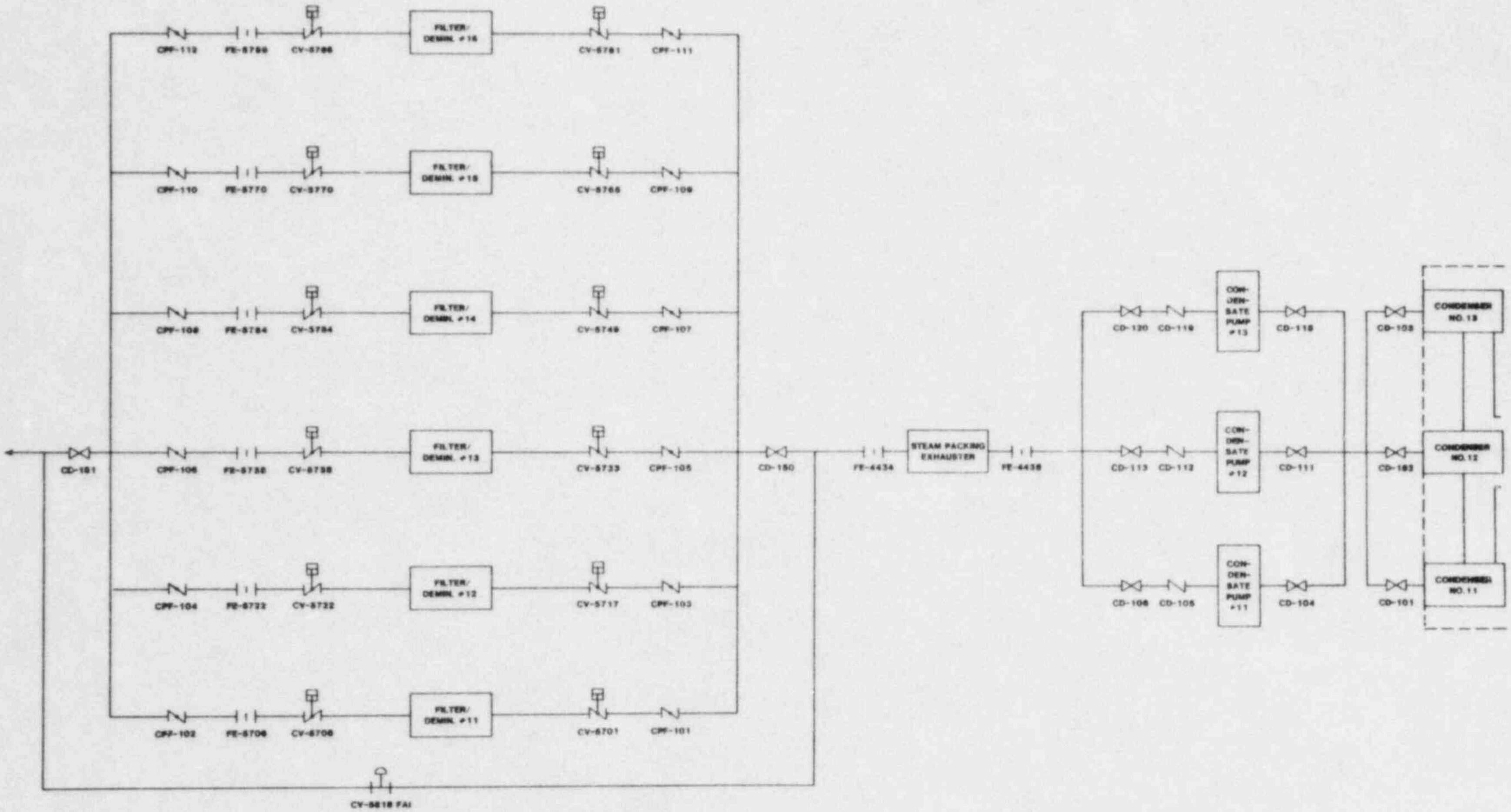


Figure 6-12 (Sheet 1) Simplified Diagram of MFWCS

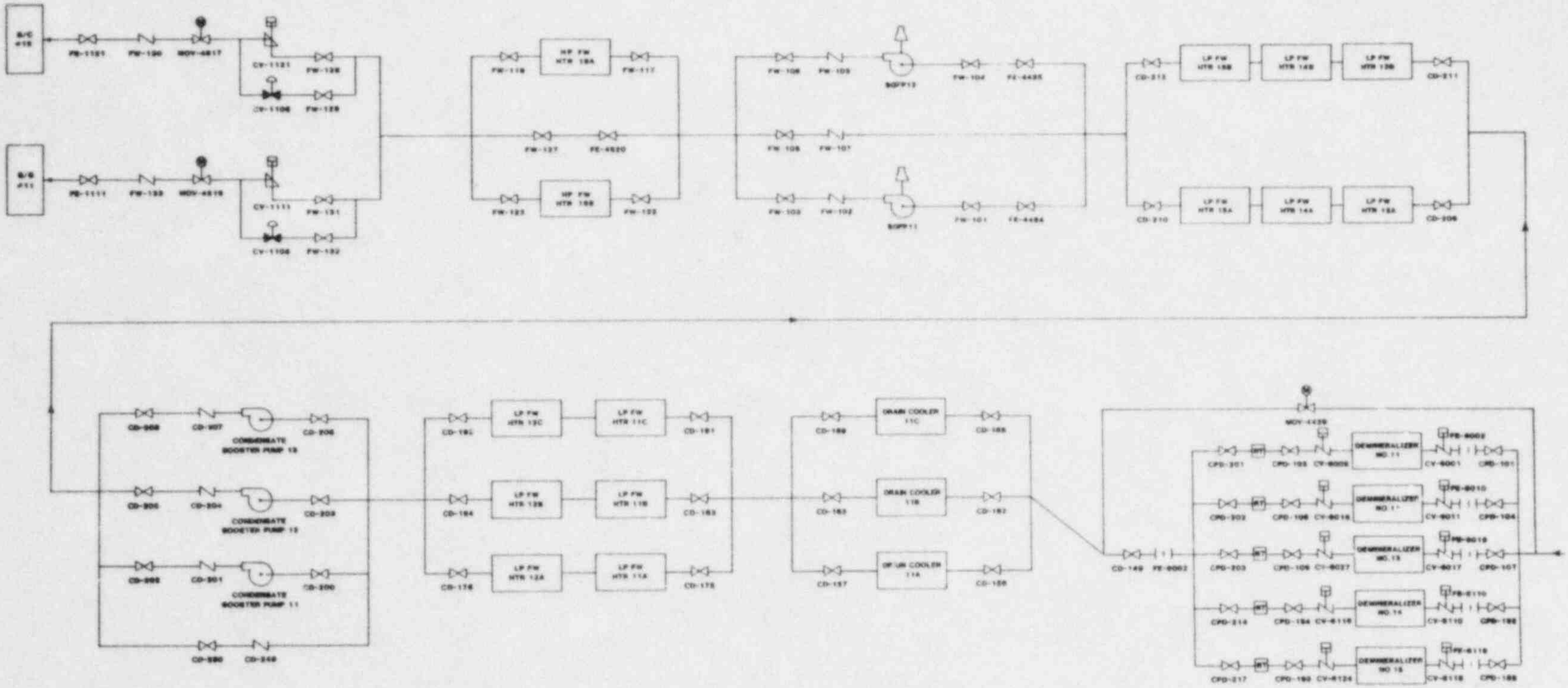


Figure 6-12 (Sheet 2) Simplified Diagram of MFWCS

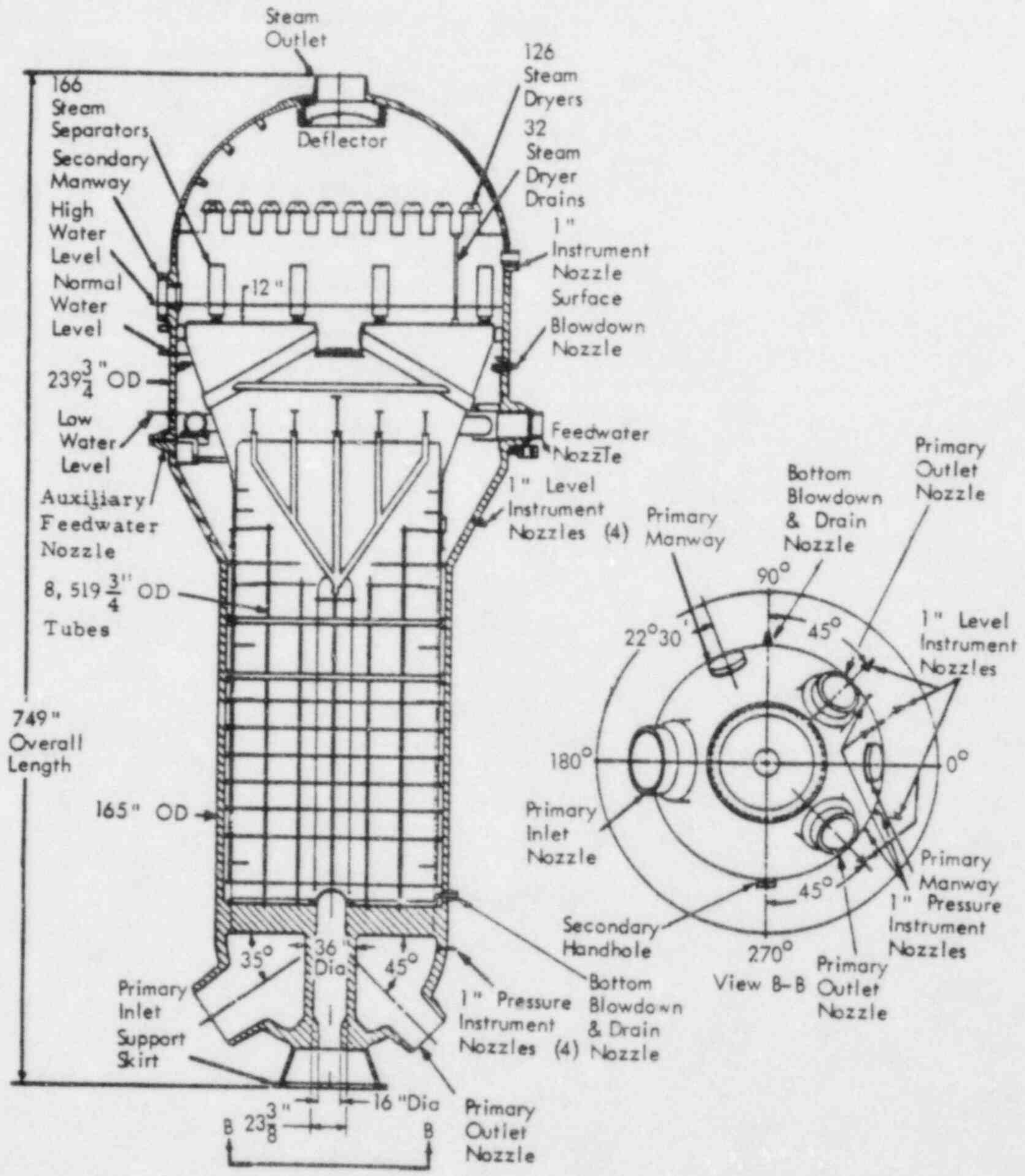


Figure 6-13 Simplified Diagram of the Steam Generators

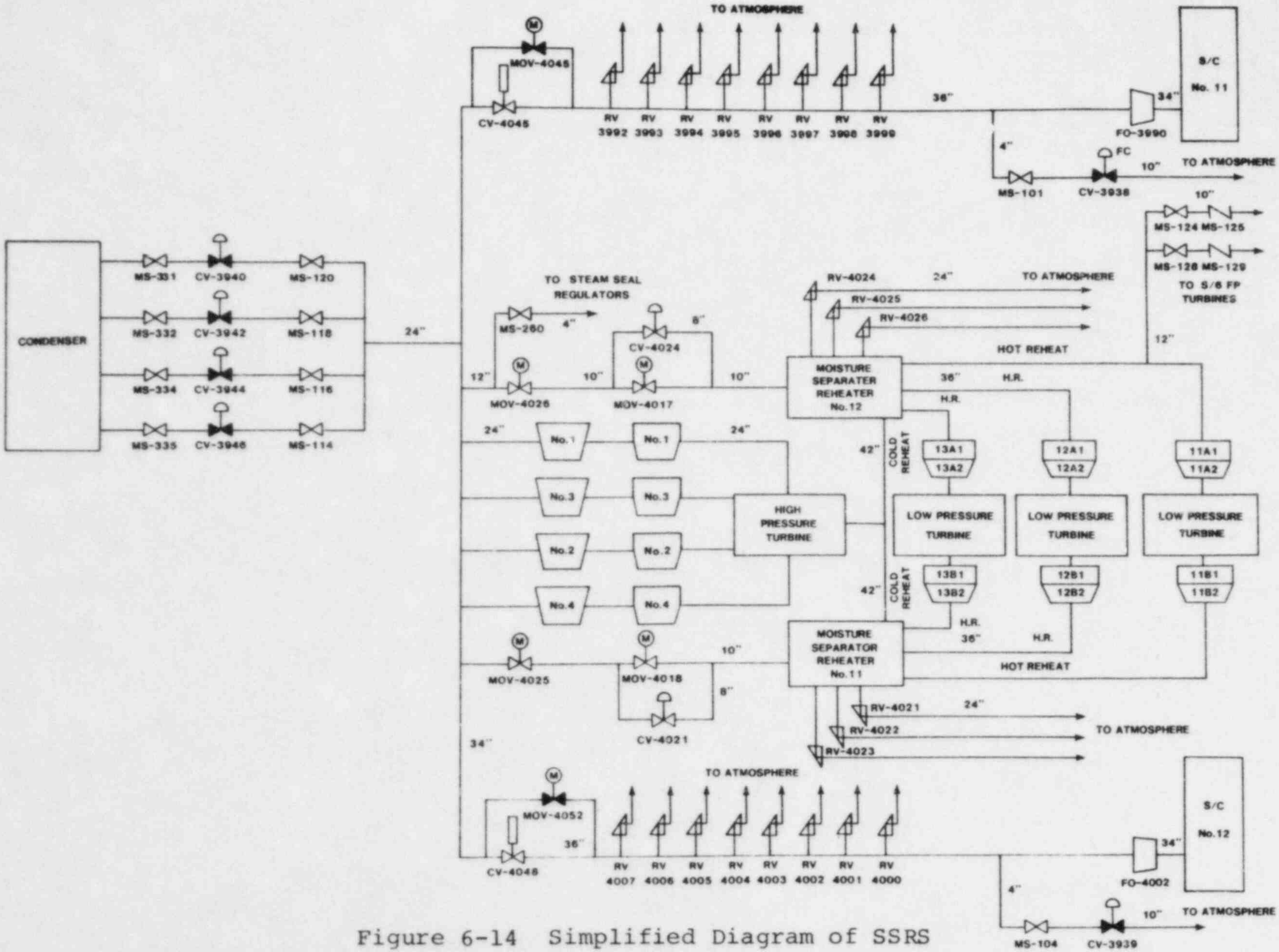


Figure 6-14 Simplified Diagram of SSRS

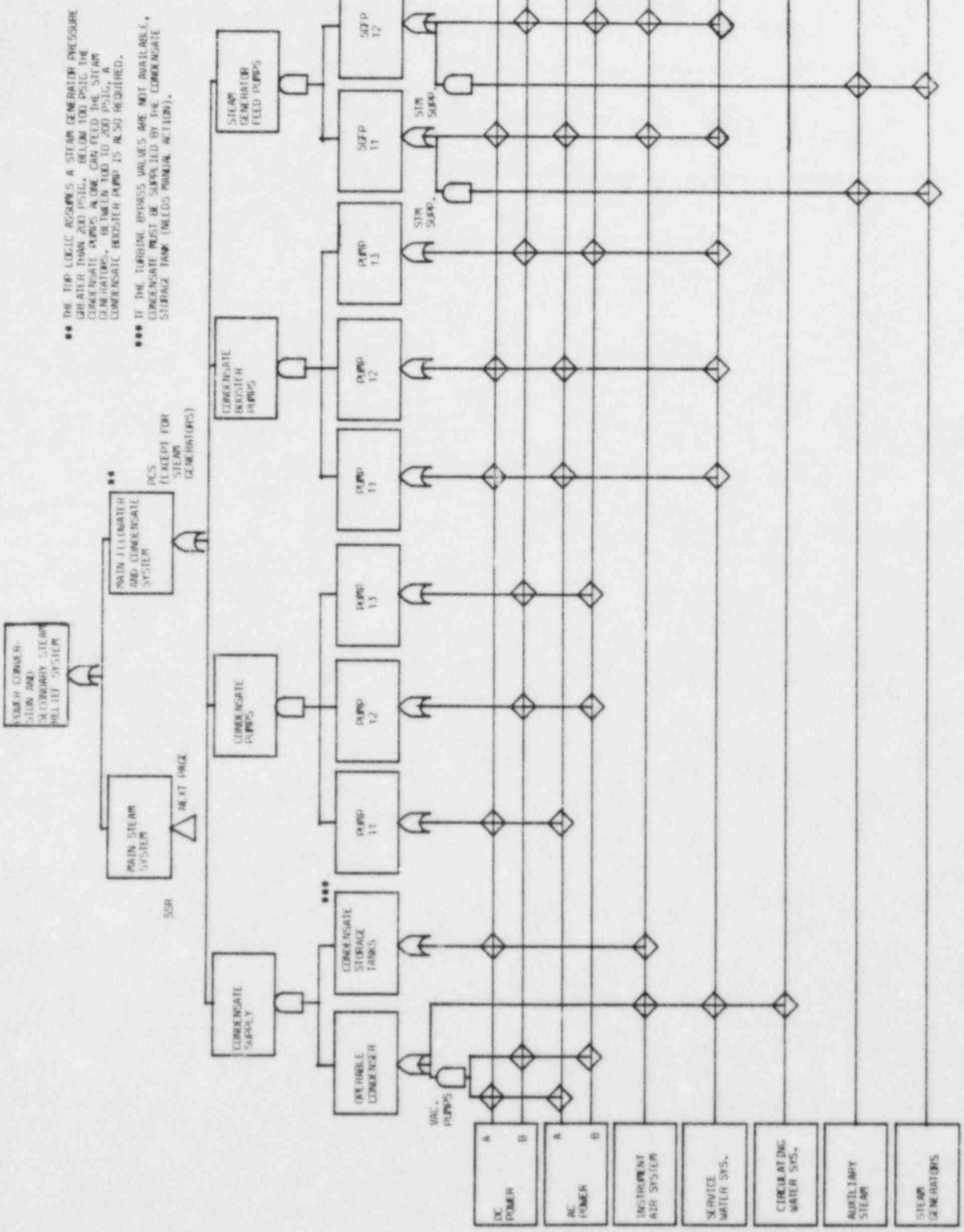


Figure 6-15 PCS Support System Dependency Diagram

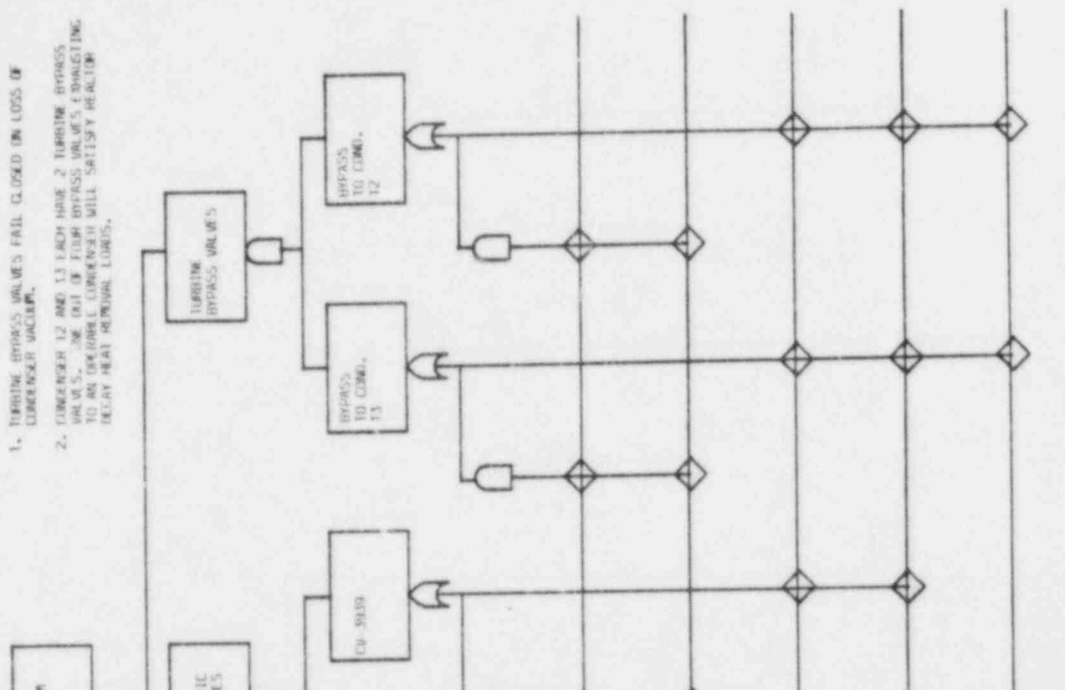


Figure 6-16 SSR Support System Dependency Diagram

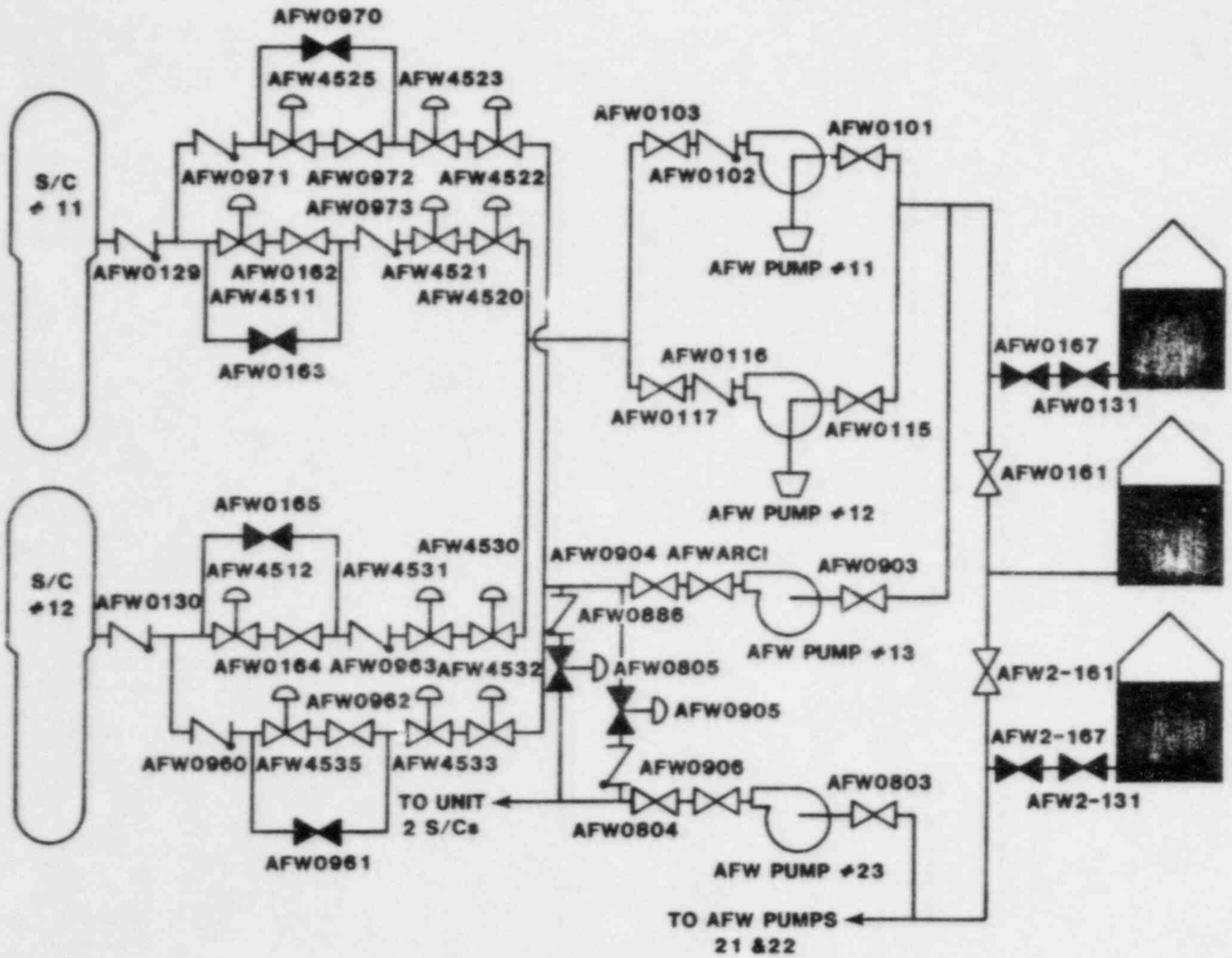


Figure 6-17 (Sheet 1) Simplified Diagram of AFWS

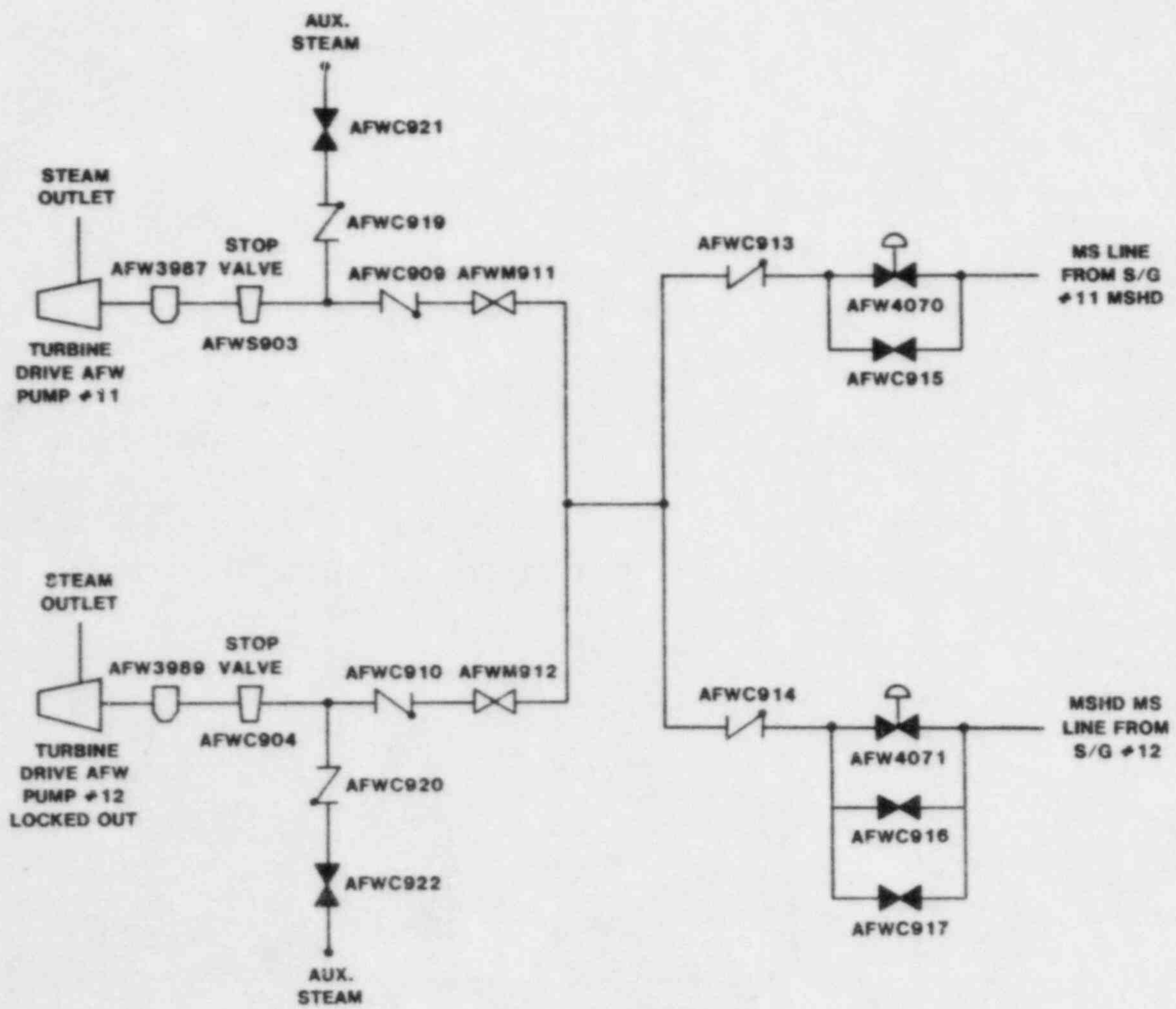


Figure 6-17 (Sheet 2) Simplified Diagram of AFWS

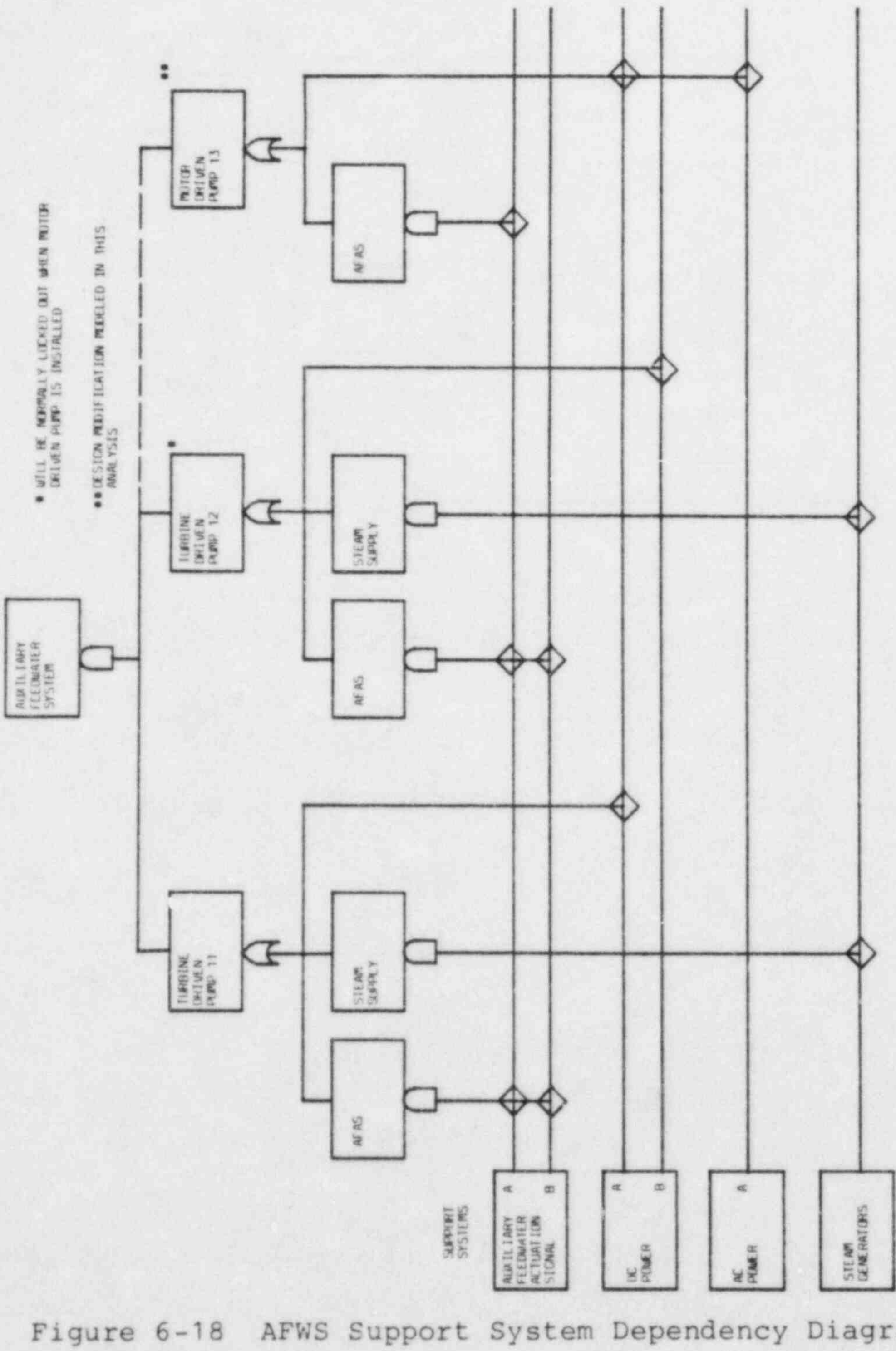


Figure 6-18 AFWS Support System Dependency Diagram

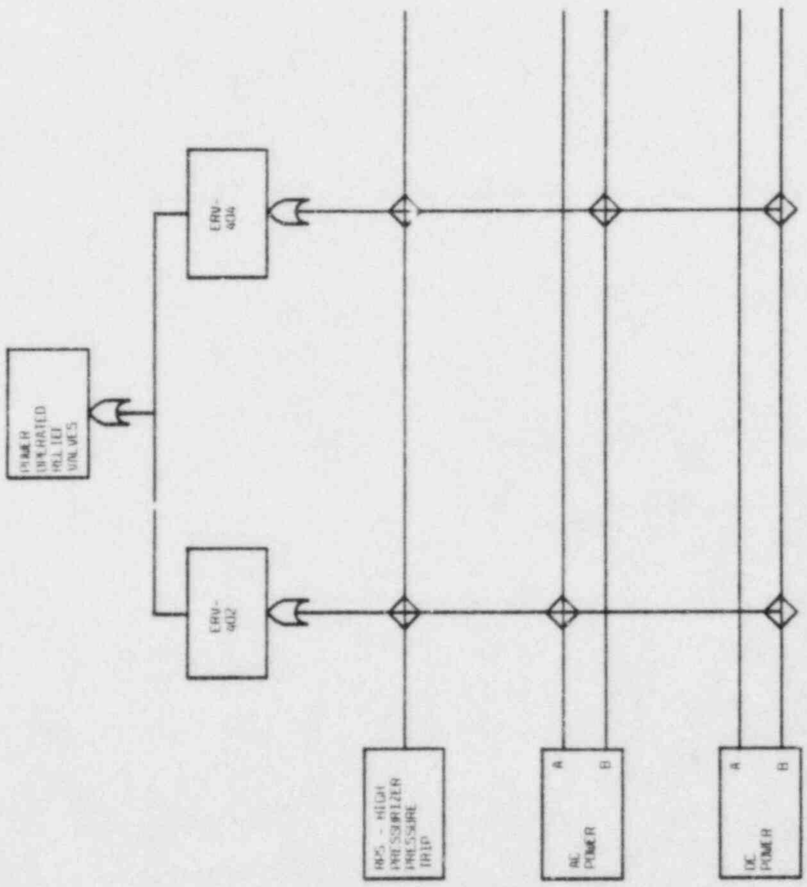


Figure 6-19 PORVs Support System Dependency Diagram

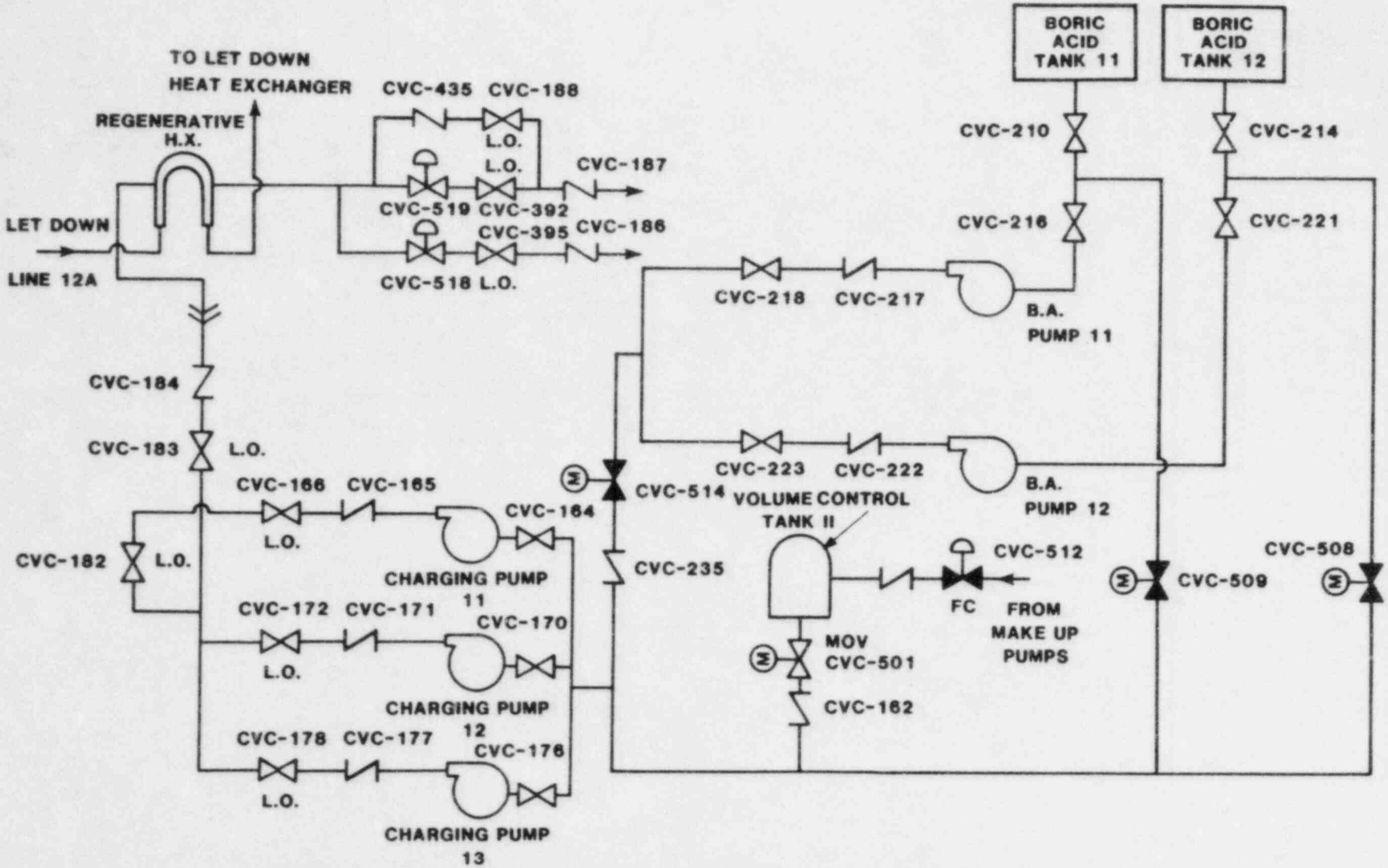


Figure 6-20 Simplified Diagram of CVCS

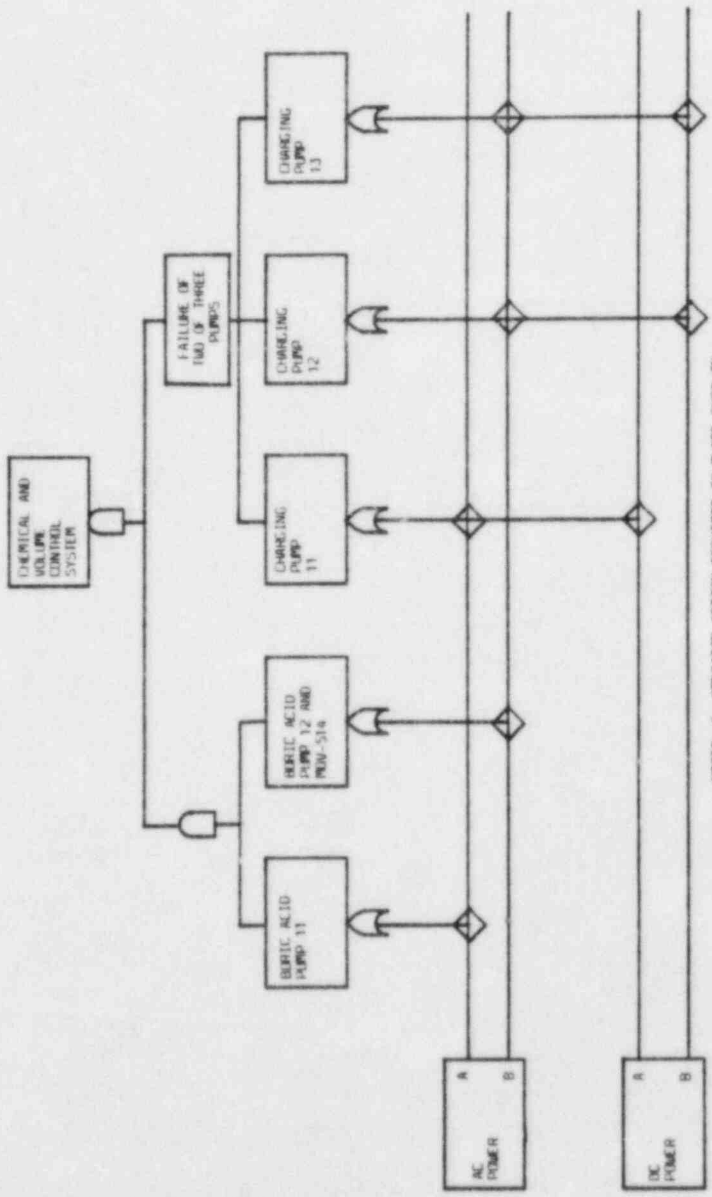


Figure 6-21 CVCS Support System Dependency Diagram

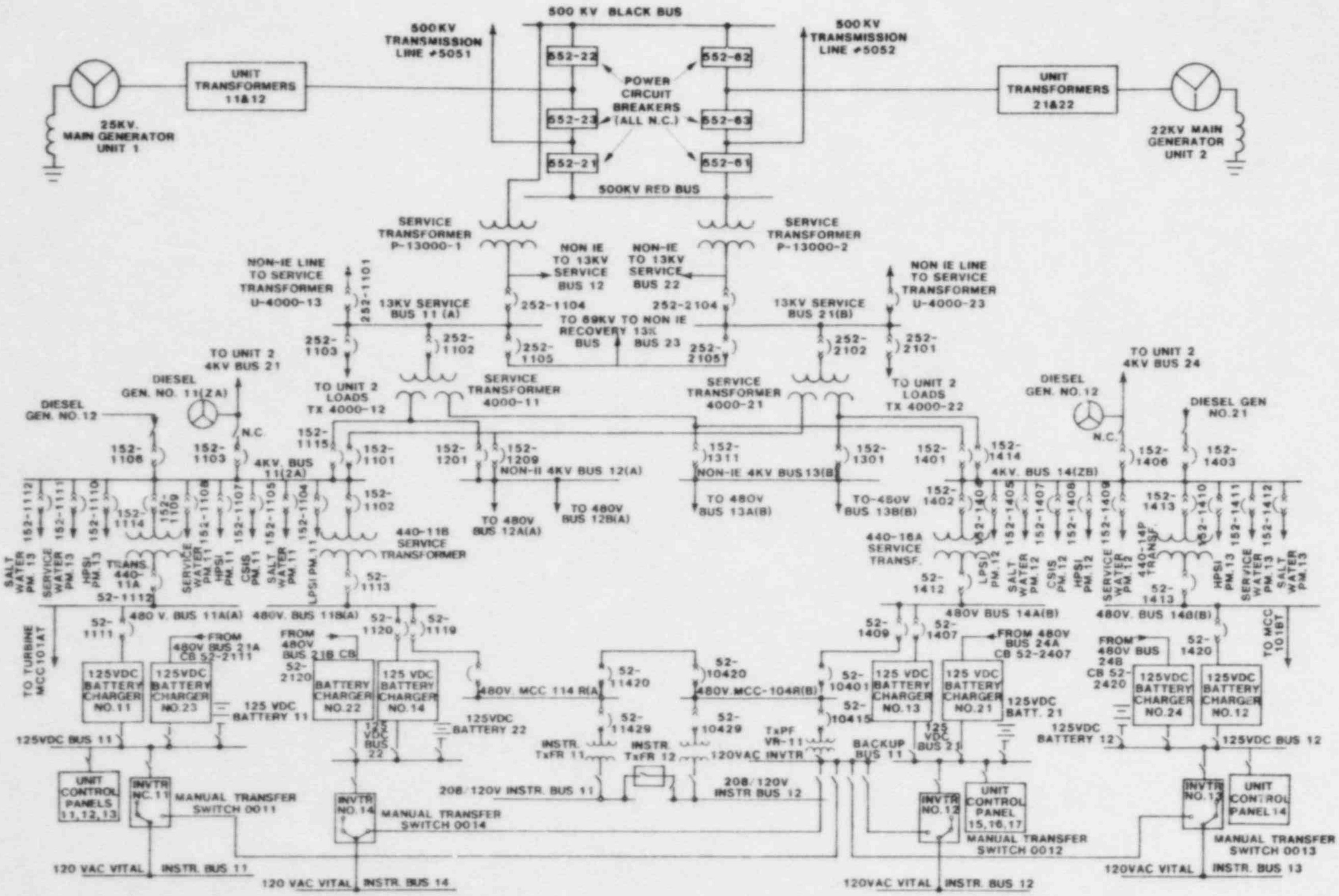


Figure 6-22 Simplified Diagram of Emergency AC and DC System

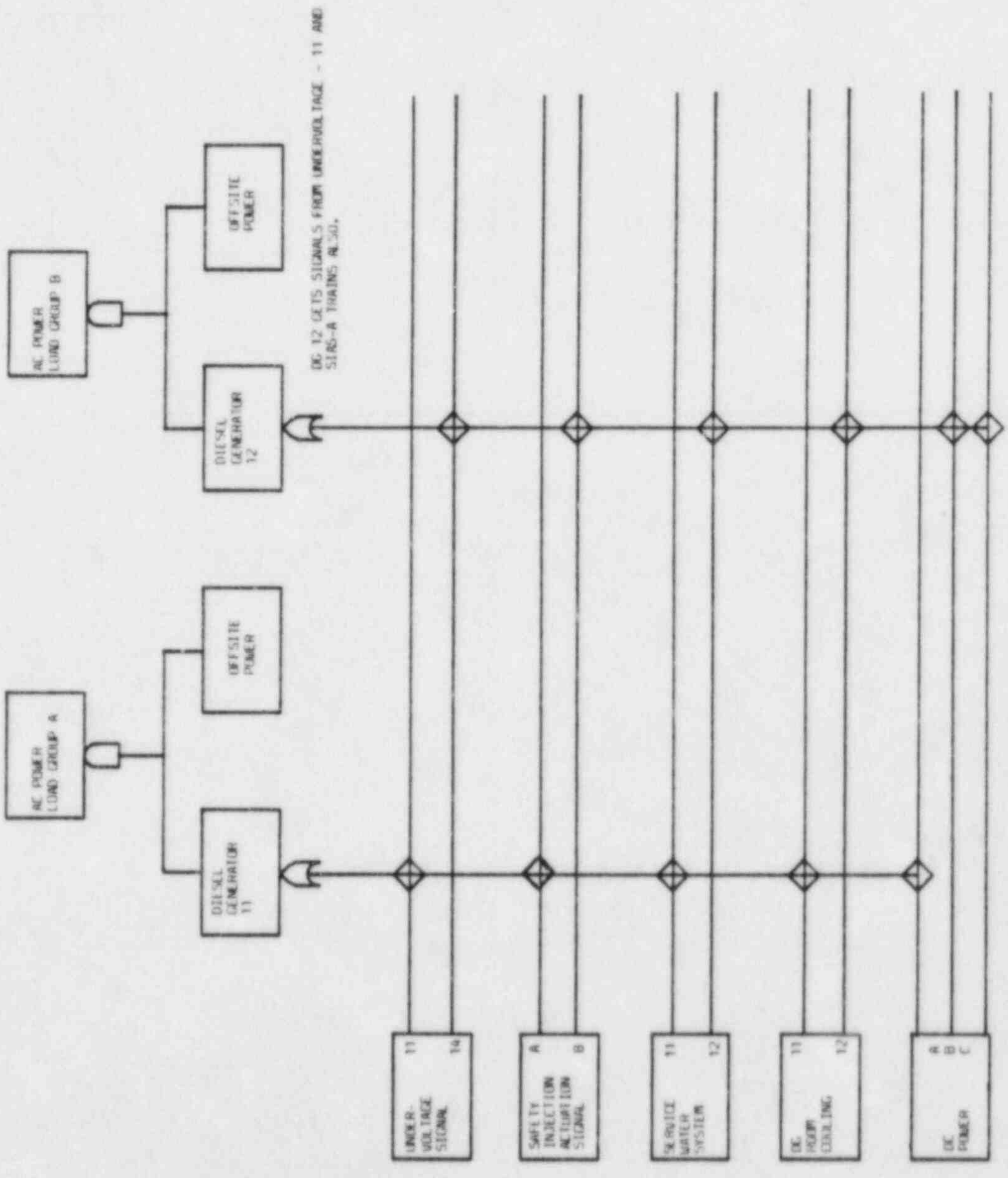


Figure 6-23 Emergency AC Support System Dependency Diagram (Sheet 1)

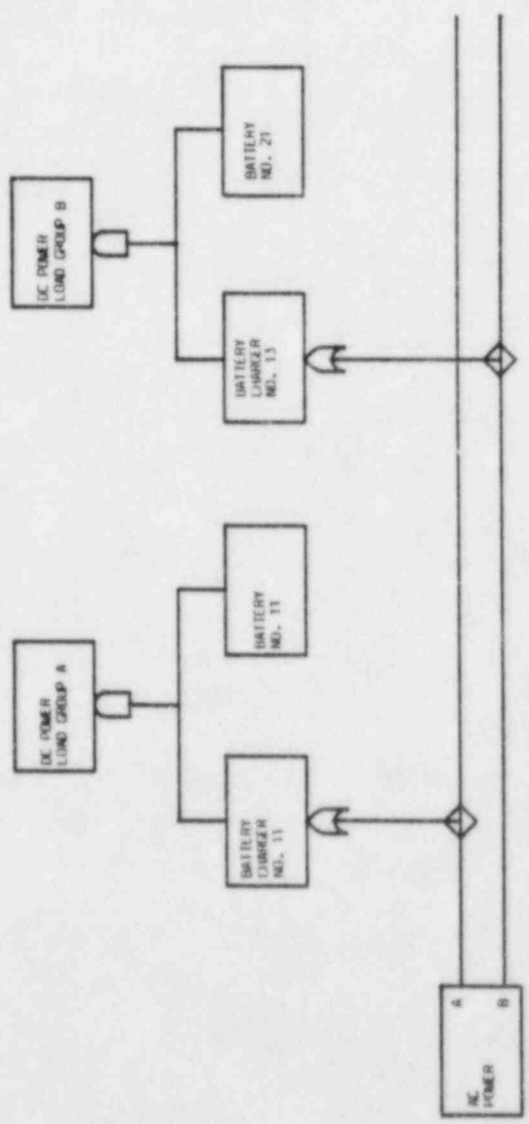


Figure 6-23 Emergency DC Support System Dependency Diagram (Sheet 2)

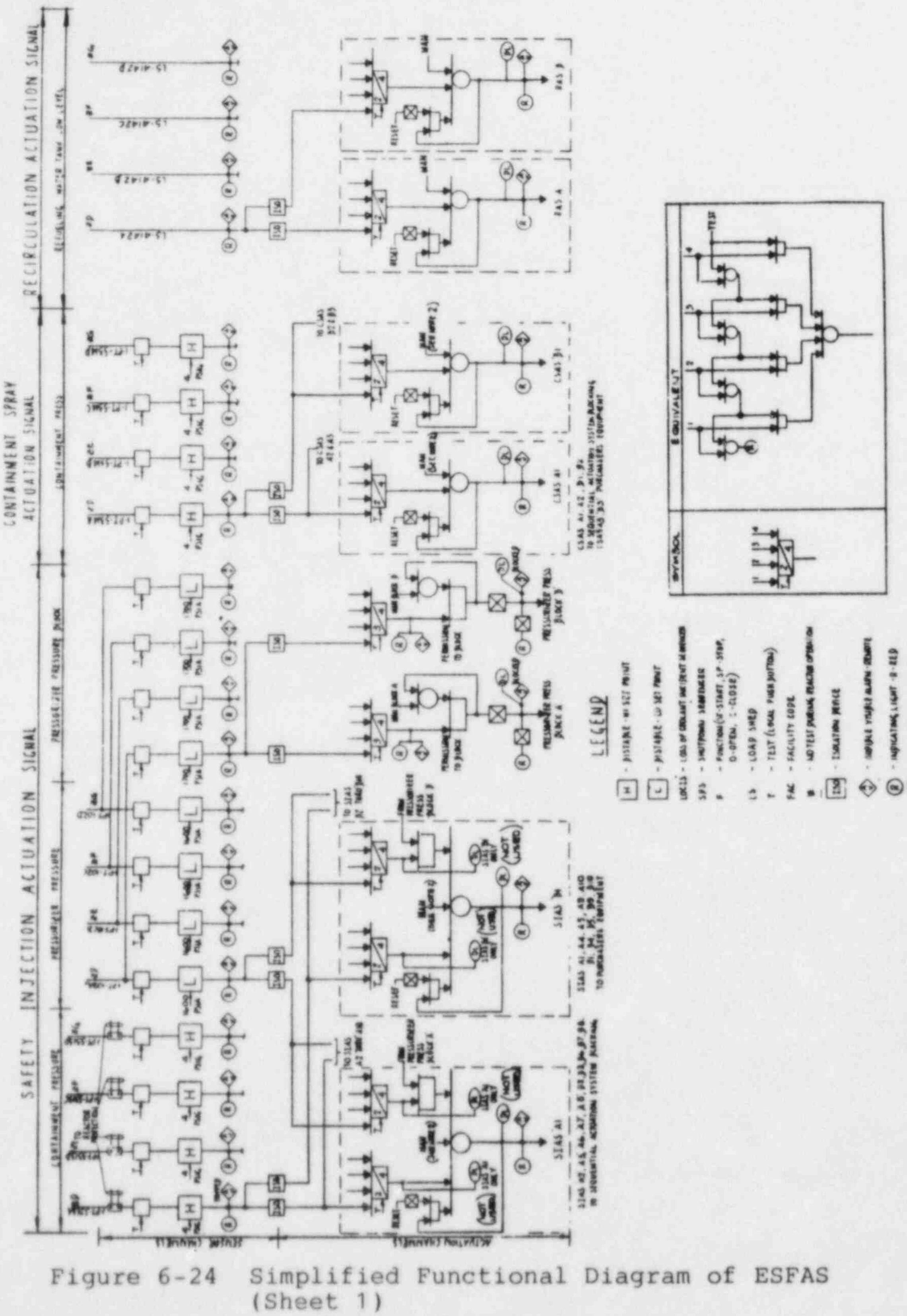


Figure 6-24 Simplified Functional Diagram of ESFAS (Sheet 1)

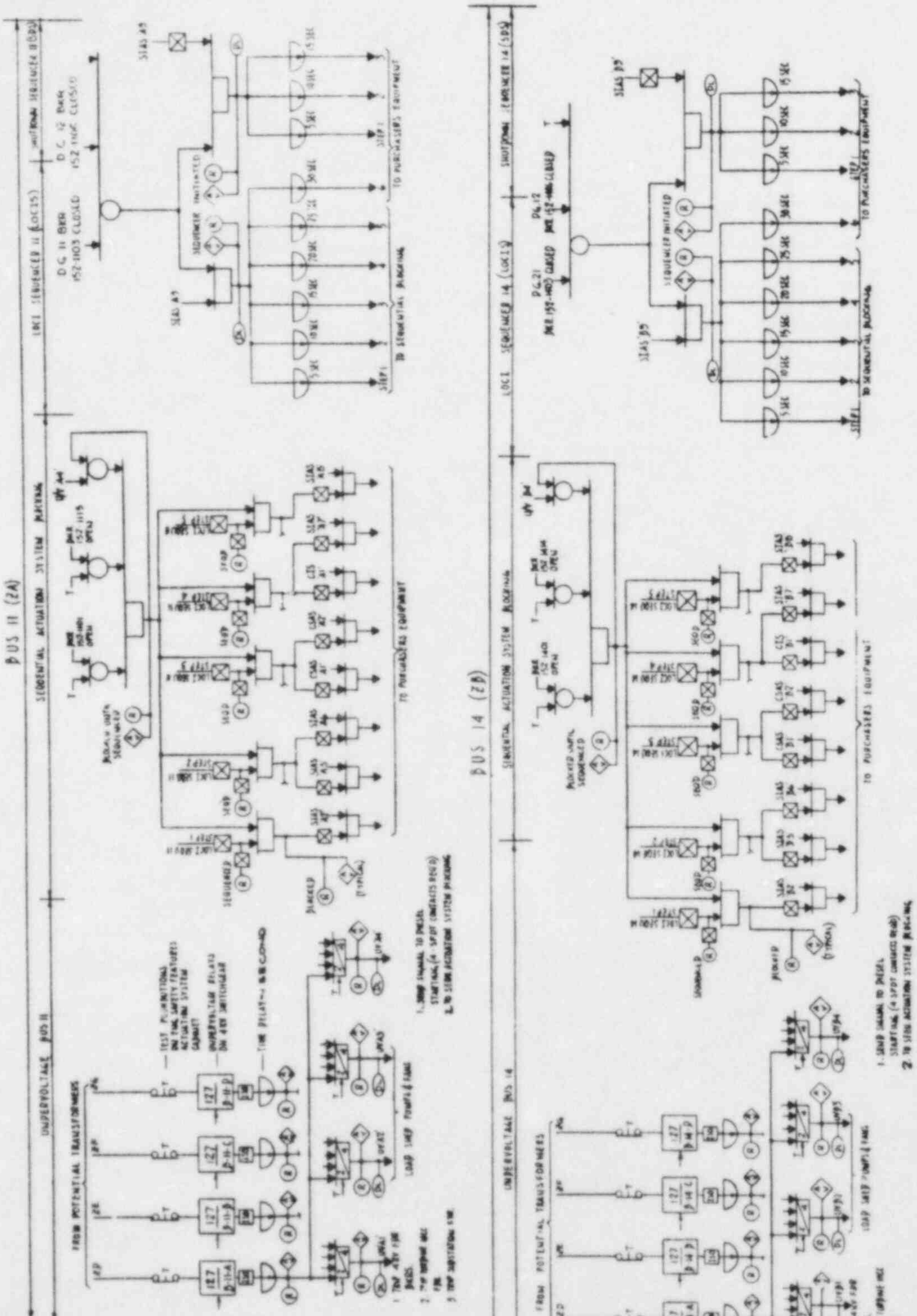


Figure 6-24 Simplified Functional Diagram of ESFAS (Sheet 2)

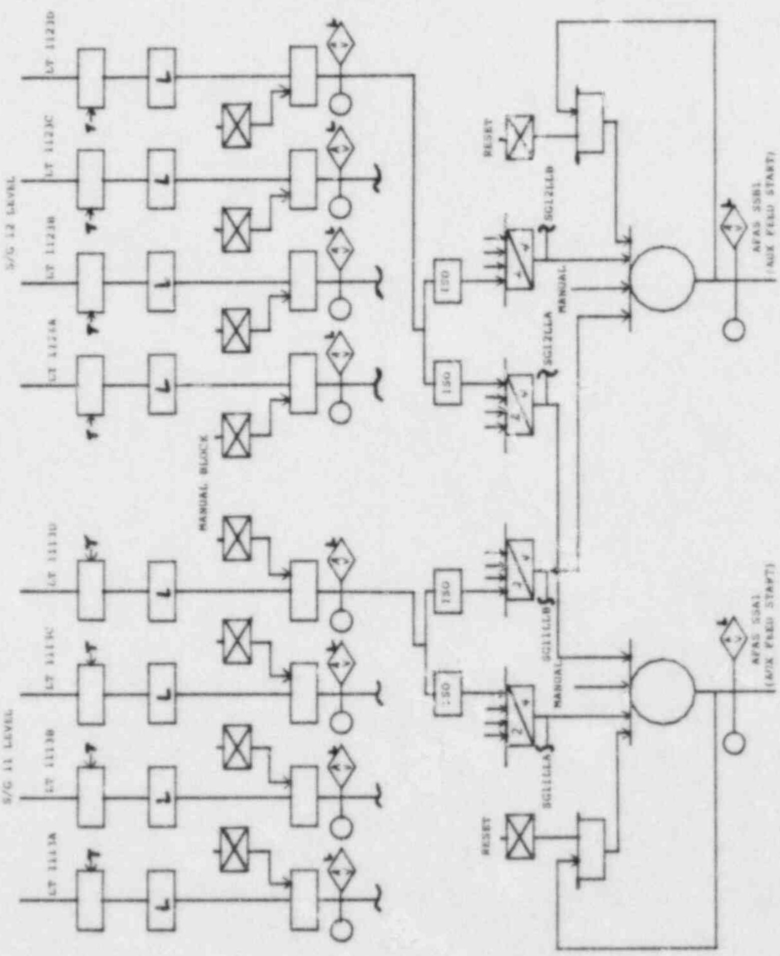


Figure 6-24 Simplified Functional Diagram of ESFAS (Sheet 3)

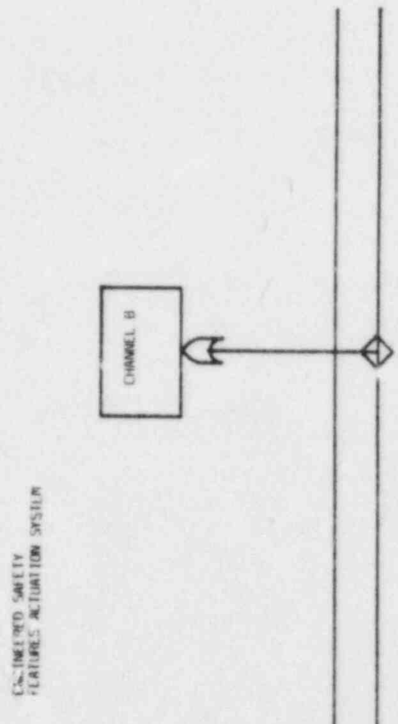


Figure 6-25 ESFAS Support System Dependency Diagram

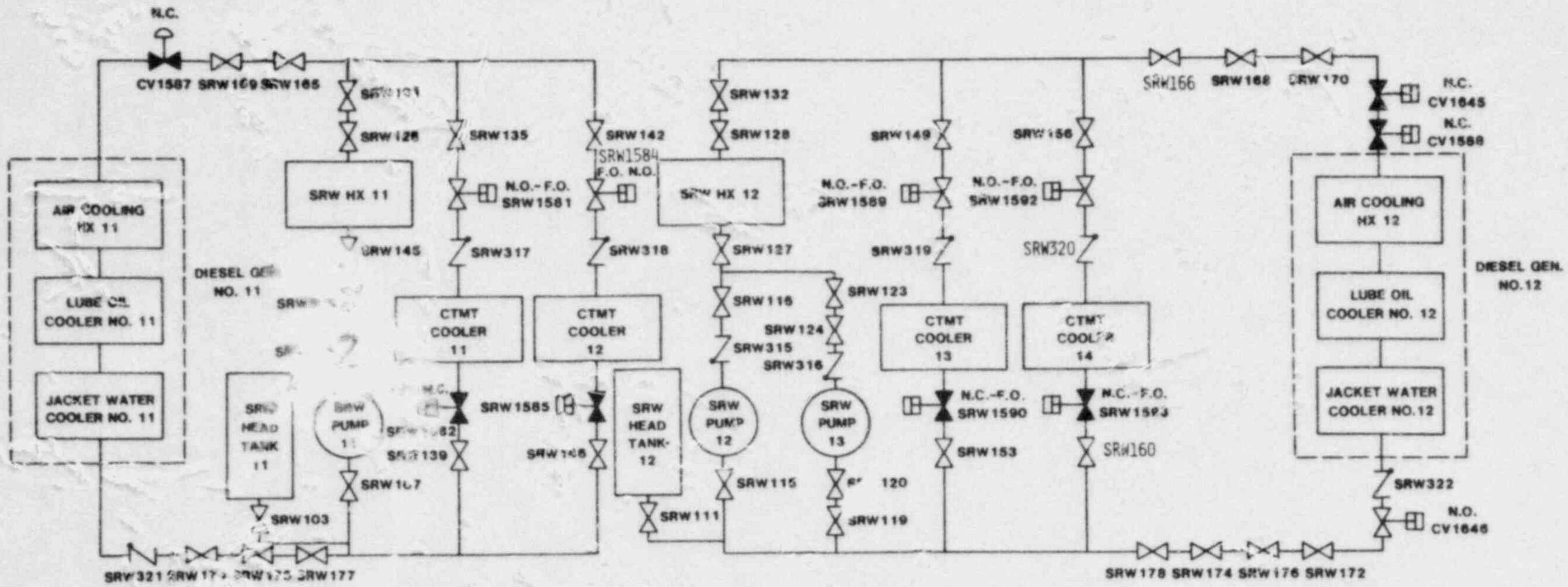


Figure 6-26 Simplified Diagram of Service Water System

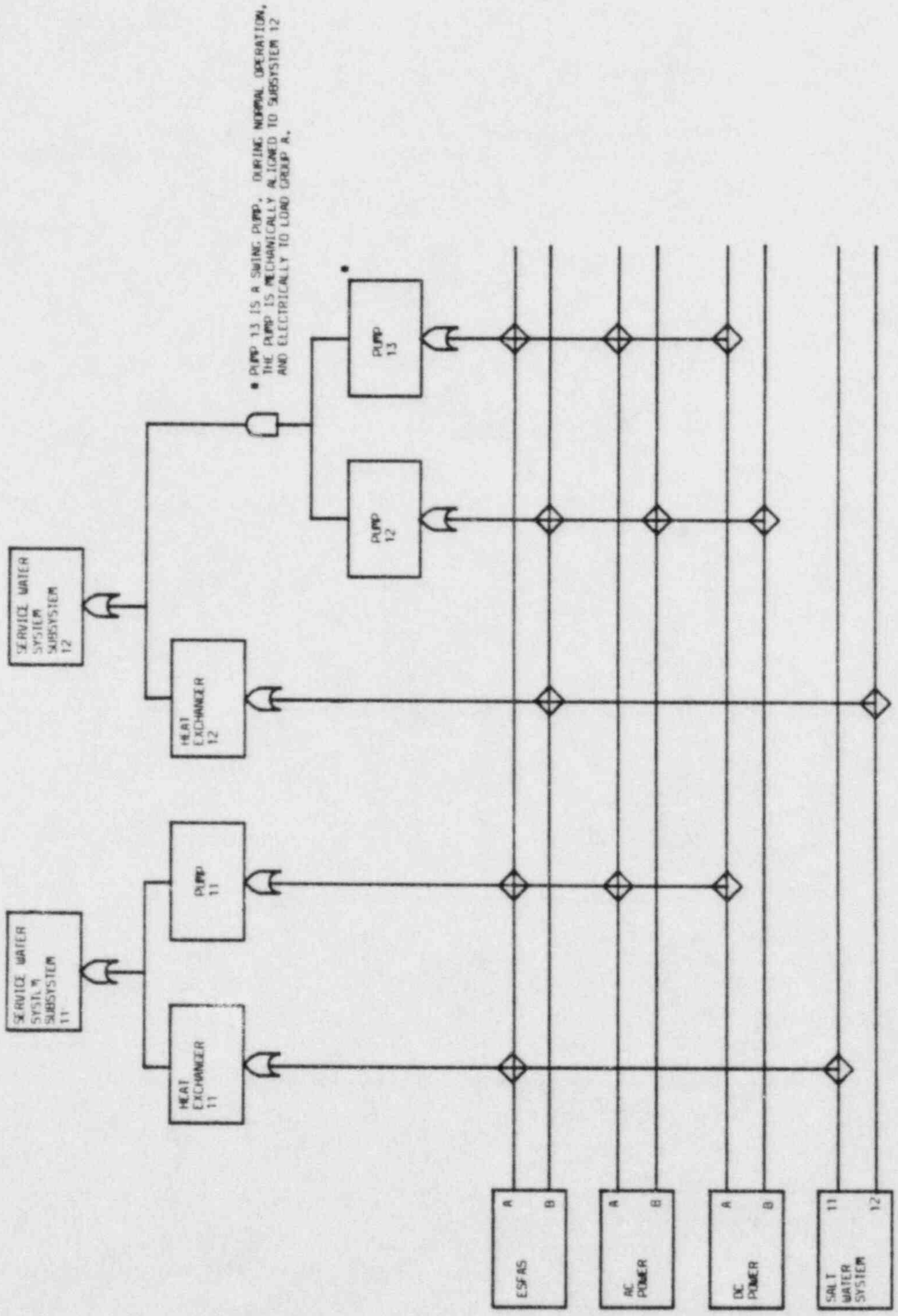


Figure 6-27 SRWS Support System Dependency Diagram

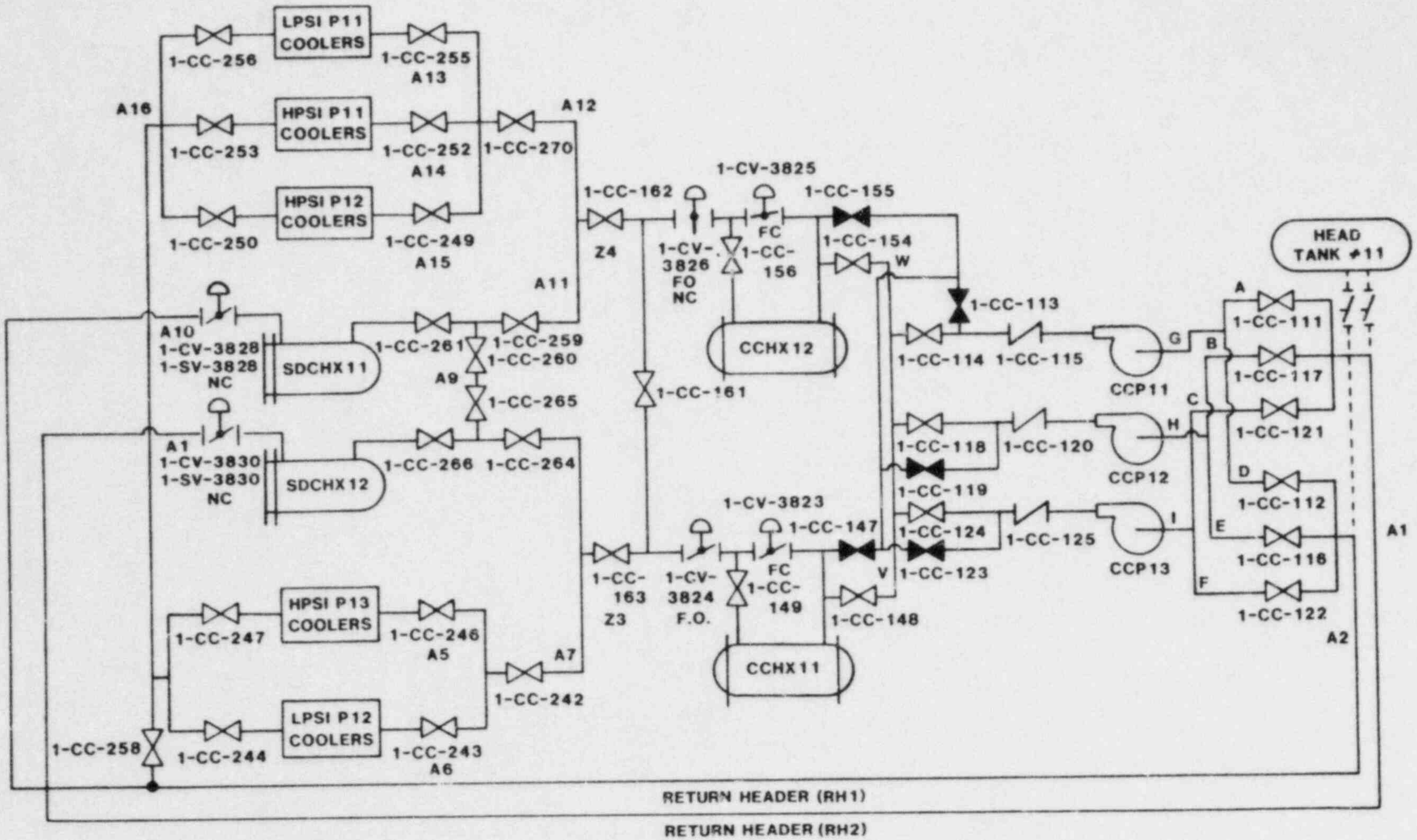


Figure 6-28 Simplified Diagram of CCWS

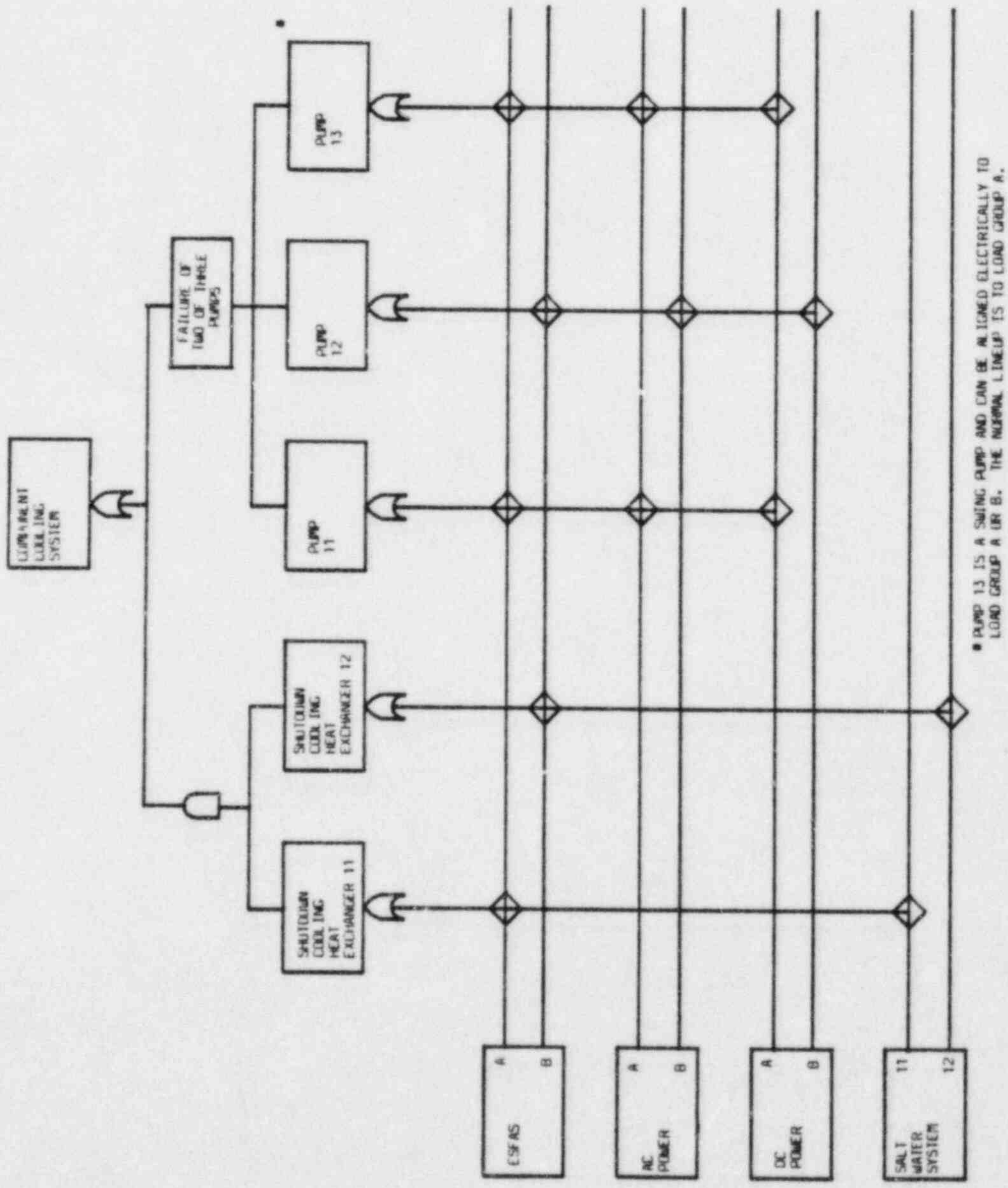


Figure 6-29 CCWS Support System Dependency Diagram

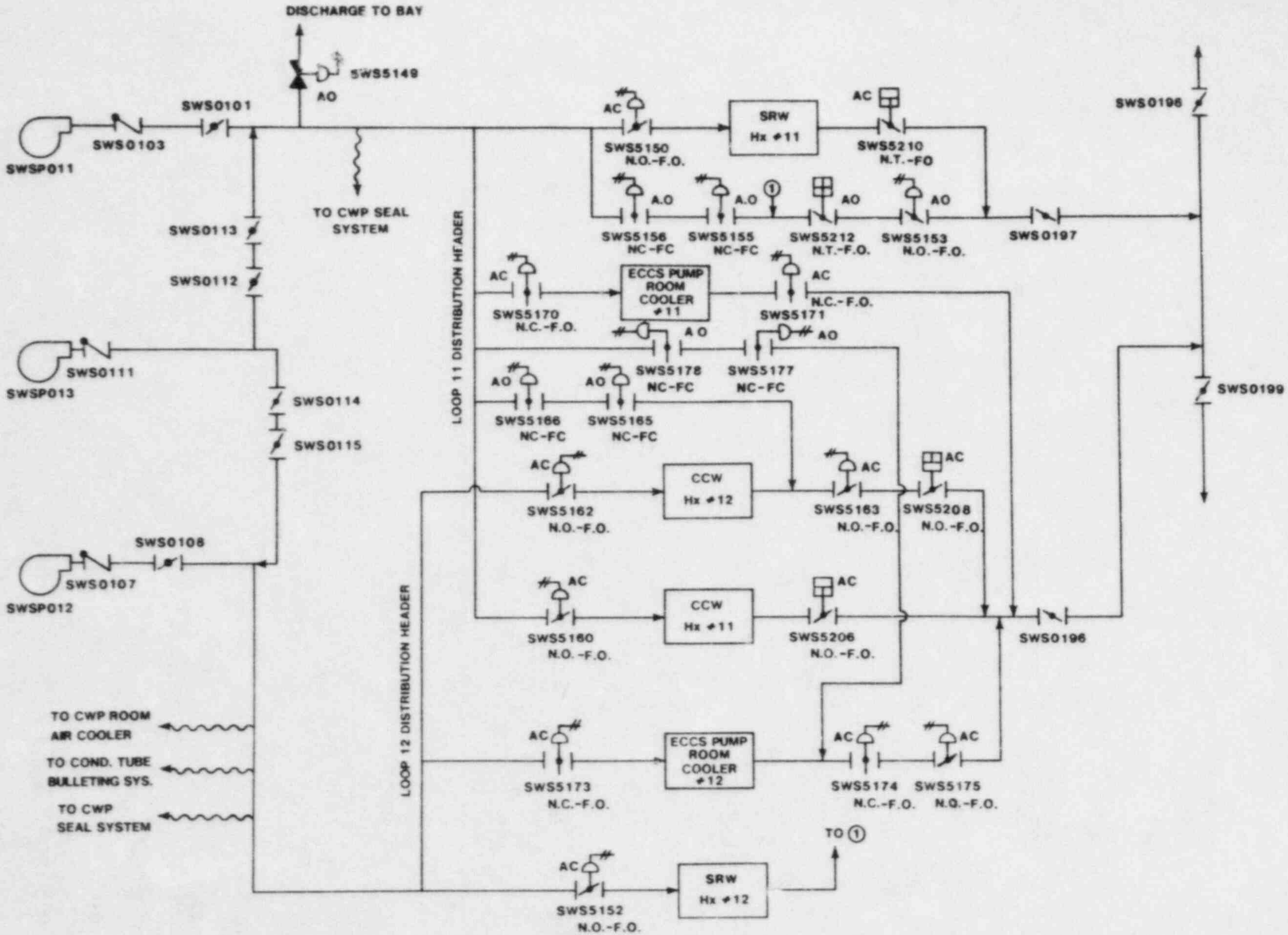


Figure 6-30 Simplified Diagram of SWS

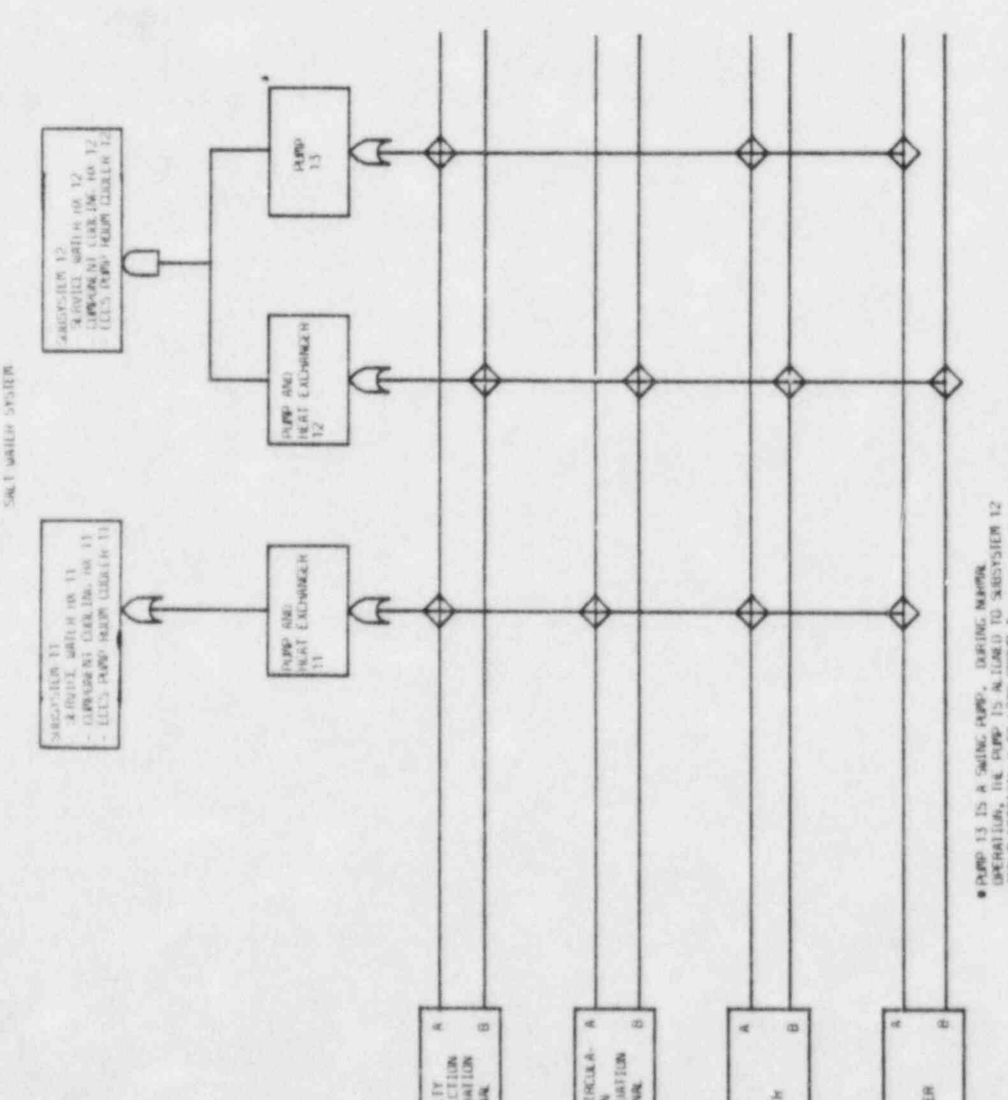
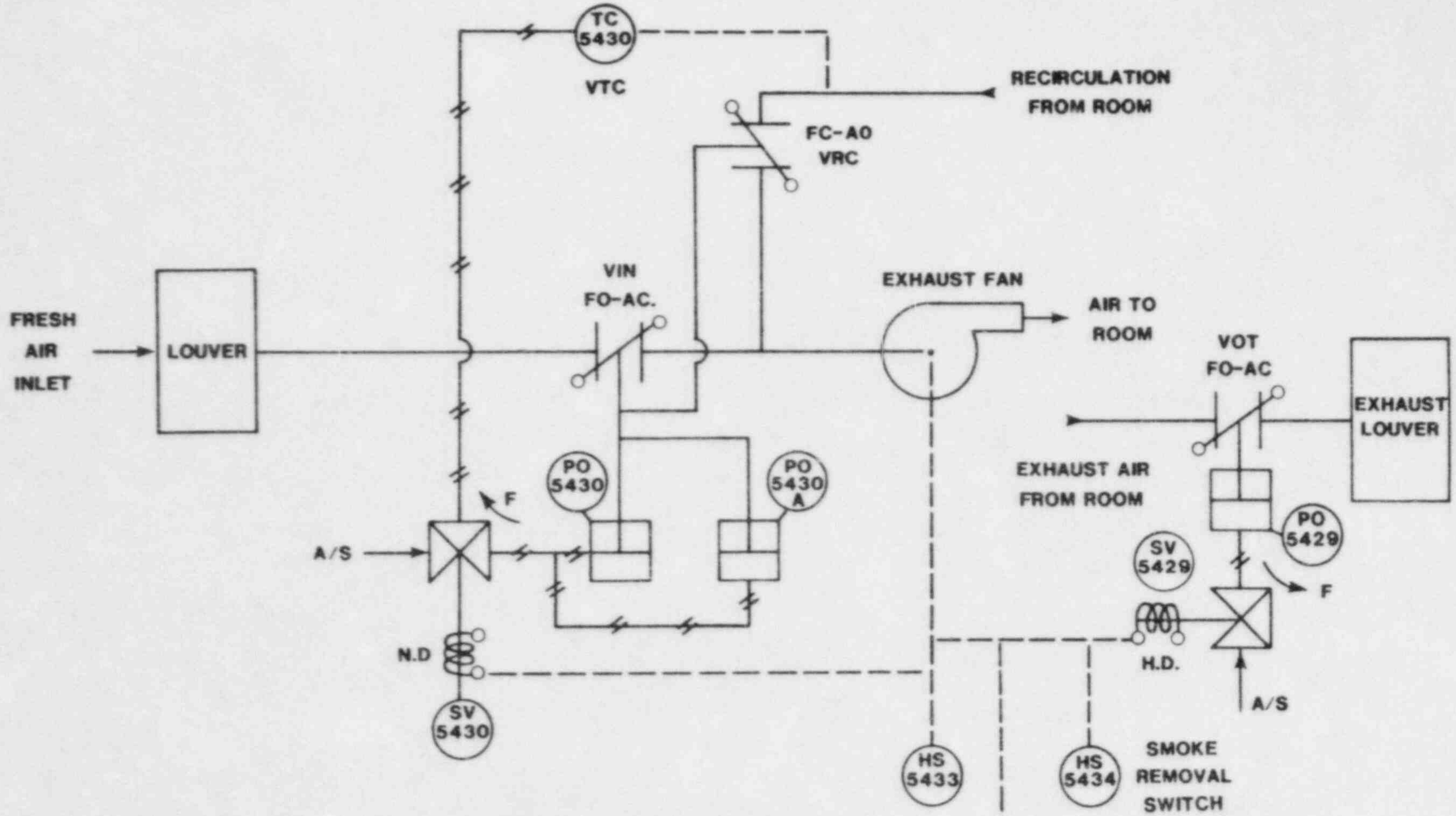


Figure 6-31 SWS Support System Dependency Diagram



1. FAN START INITIATED BY SIGNAL FROM DIESEL START LOGIC
2. HS5433-3 POSITION SWITCH-LOCAL FAN CONTROL
   STOP/AUTO/START-SPRING LOADED TO "AUTO"
3. FAN START FUNCTION-DE-ENERGISES SV5430 TO ALLOW POSITIONING
   AIR SIGNAL TO FAN INLET DAMPERS DE-ENERGISES
   SV5429 TO OPEN EXHAUST DAMPER
4. SMOKE REMOVAL SW. HS5434-OPENS EXHAUST DAMPER-SWITCH IS OUTSIDE D/G ROOM

Figure 6-32 (Sheet 1) Simplified Diagram of Heating and Ventilation System
(Diesel Generator #11 Room Cooling) (DG # 12 similar)

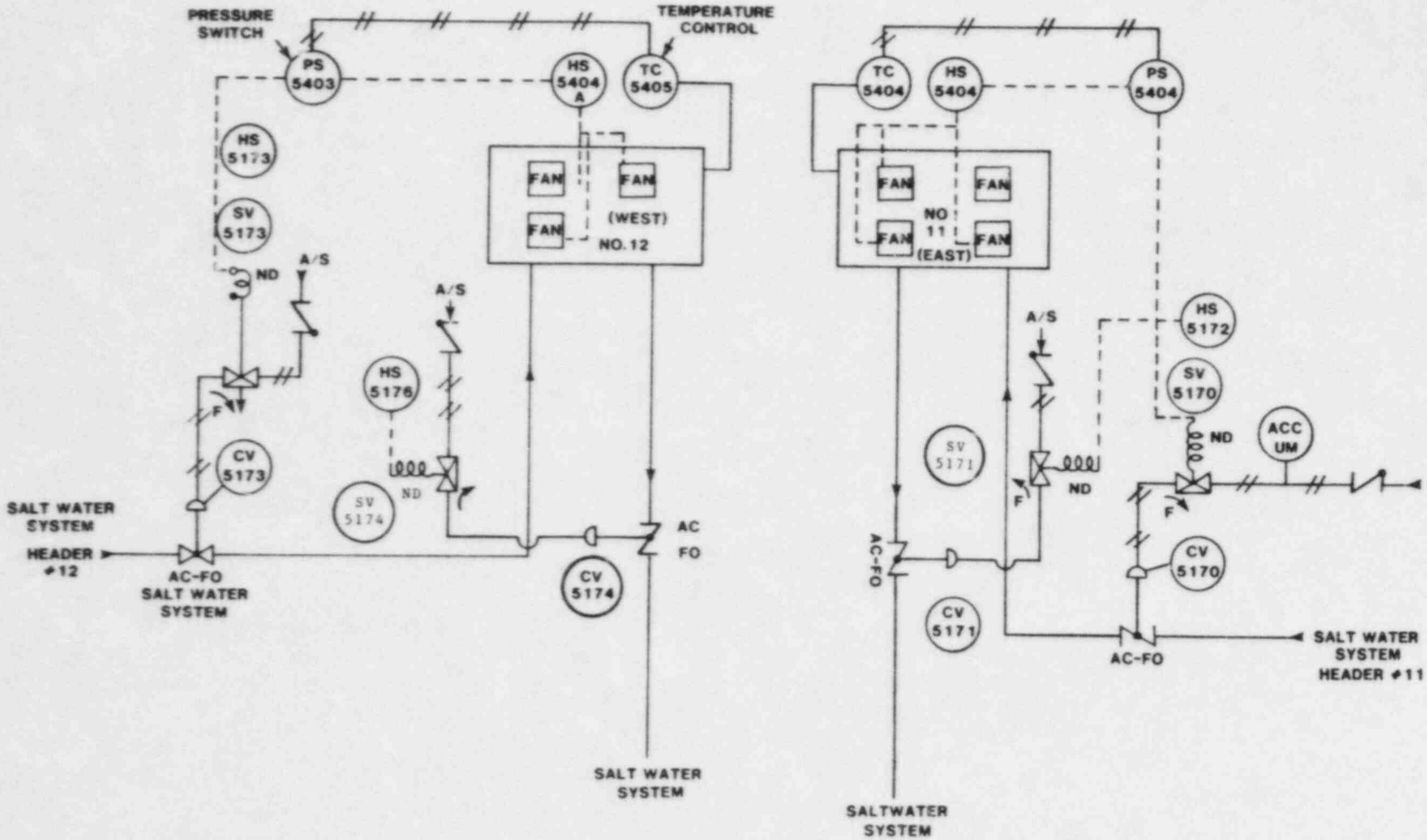


Figure 6-32 (Sheet 2) Simplified Diagram of Heating and Ventilation System (ECCS Pump Room Air Coolers)

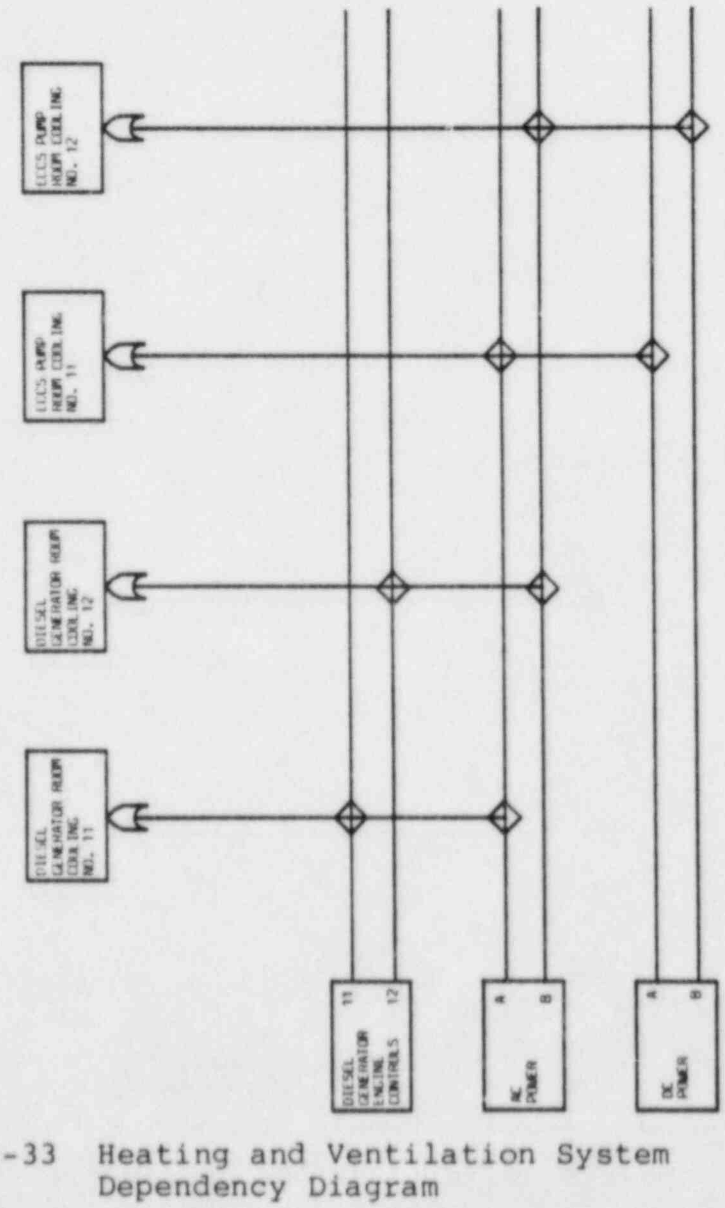


Figure 6-33 Heating and Ventilation System Dependency Diagram

CHAPTER 7

ACCIDENT SEQUENCE QUANTIFICATION

7.1 Introduction

The CC-1 quantification procedure was performed in two separate steps in order to simplify the procedure and reduce the total amount of work necessary to account for post-accident recovery actions. The first step was a screening quantification where sequences were quantified based on generic and plant-specific data without considering any recovery action. In the second step, the sequences which were identified in the screening quantification as "dominant sequences" (i.e., sequences with a frequency of 1E-6/yr and higher) were requantified to incorporate the effect of recovery actions if recovery considerations were applicable. The end result was the final dominant sequence with their frequencies and cut sets. The reader is referred to Appendix C for a more detailed discussion of the quantification process.

For the first step of quantification (i.e., screening quantification), a number of tasks were performed to obtain the dominant cut sets of the event tree sequences. These tasks are as follows:

1. Collection and calculation of hardware failure data, human error data, and plant specific data.

2. Merging front-line system fault trees with support system fault trees.

3. Truncation of Boolean equations representing the merged front-line system fault trees.

4. Determination of the dominant cut sets of all the dominant sequences (i.e. cutsets with a probability greater than 1E-8)

5. Evaluation of the effect of the success events in the sequences on the cut sets of the failure events and calculation of the frequencies of the sequences.

For the second step of the quantification (i.e., final quantification), the following tasks were performed.

6. Identification of the cut sets of the sequences where the possibility of recovery exists.

7. Revision of data to include better human error and recovery action data and final calculation of the dominant sequence frequencies.

For Boolean calculations such as merging fault trees and truncating Boolean equations, the code SETS [4] was used. This code, developed by Sandia National Laboratories, is a general program for the manipulation of Boolean equations which can be applied to fault trees to find minimal cut sets.

A brief discussion of each quantification step is presented in Sections 7.2 and 7.3 and an example in Section 7.4. A more detailed description of the quantification process is presented in Appendix C.

7.2 Screening Quantification

Tasks (1) through (5) are screening quantifications tasks that are described below:

1. Collection and Calculation of Hardware Failure Data, Human Error Data, and Plant-Specific Data.

The hardware failure probabilities used in the calculations are based on the generic data base given in the IREP Procedures Guide [3]. This data source is shown in Table 7.1. This was supplemented by the revised WASH-1400 data base [8] shown in Table 7.2 which was the original data base supplied by the NRC for use in the IREP program.

The required human failure data were obtained by constructing THERP models and quantifying them using data suggested in the Human Reliability Handbook (NUREG/CR-1278) [5]. A THERP diagram is used to predict human error probabilities, and to evaluate the degradation of a man-machine system likely to be caused by human error alone, operational procedures and practices, or other system and human characteristics that influence human systems behavior. Discussions of plant administrative controls were held with the plant staff and a review of the plant operating, test, and maintenance procedures was conducted by the analysts. In addition, a detailed set of photographs of the plant control panels in the control room was used to identify possible conditions which may influence the Performance Shaping Factors and potential sources of error associated with the task of interest. Finally, the human error probabilities were calculated by using data obtained from the Handbook. These values are then used in the fault trees for final quantification of the sequence probabilities.

A plant-specific data base was generated by reviewing the CC-1 maintenance reports, but its use was limited to those items for which no failure rate data was provided in the IREP data base or if the plant data was significantly different from generic data. For example, no data was provided for Engineered Safety Features Actuation System (ESFAS) logic module failures, so plant-specific data was used. Also, while generic data was used for the initiating event frequencies, they were compared

to the plant specific data and no significant differences were found.

Component unavailability due to maintenance was evaluated using plant specific maintenance procedures and data. As a matter of policy, periodic preventive maintenance is not done on most safety components at CC-1. The average maintenance frequency (in hours) was calculated by counting the number of maintenance actions recorded for each type of component and dividing by the operating hours of the plant. The average duration of maintenance acts was also estimated based on plant experience. The product of these two figures (average maintenance frequency and average maintenance duration) was used to calculate the probability of unavailability due to maintenance.

Data for the loss and restoration of normal AC power was obtained from EPRI NP-2301 "Loss of Offsite Power in Nuclear Power Plants: Data and Analysis" [16] and NUREG/CR-3226 "Station Blackout Accident Analysis" [17].

2. Merging Front-Line System Fault Trees with Support System Fault Trees

The front-line fault trees were merged (combined) with their support system fault trees, as well as support system to support system fault trees, to form a complete merged fault tree for each system on the systemic event trees. This task is automatically performed by SETS. The merged front-line system was then manually checked to assure accuracy and consistency.

A major problem encountered during the merging process was the existence of circular logic in a number of the system models. This problem can occur when two support systems need support from each other. For example, the emergency electrical power system needs the SRWS (to cool the diesel generators) and the emergency electrical power system provides power to the SRWS. It was necessary to eliminate the circular logic in order to manipulate and evaluate the Boolean equations for the system fault trees and, subsequently, the accident sequences. This was accomplished by cutting the system level circular logic loops at logical points. The circular logic loops at CC-1 all involved AC power and were cut at the 4KV AC buses. The AC power tree support systems were merged individually with the AC power system only up to the 4KV AC buses so as to put all local AC faults of these buses into the support system fault trees. Then these support system trees were merged with the whole emergency electrical power fault tree to form a merged AC power tree with its support systems and no circular logic. This AC fault tree with all its support systems could then be merged with all other systems in the usual way.

3. Truncation of Front-Line System Merged Trees

Fault trees obtained through the merging process are often very large and contain up to five thousand events. The number of cut sets for these trees was also very large and generating them, if possible, requires a prohibitive amount of computer time. Therefore, it was necessary to eliminate all cut sets with small probabilities so as to save computer time and reduce the size of the Boolean equations. These truncated equations were later used in the event tree sequence evaluation procedures.

All of the merged front-line systems were truncated at an unavailability cutoff value of 1E-8. That is, all the cut sets with an unavailability of less than 1E-8 were eliminated from the Boolean equations. The truncation process was performed by using a bottom-up procedure. In this procedure, selected stop points (i.e., intermediate events which are solved to obtain their truncated Boolean equations) were used in the tree, and stop points near the bottom of the tree were truncated first. These stop point truncations are used in the higher level stop point truncations. The process is repeated until, eventually, the last stop point (i.e., the top event) was reached and truncated. An average of 15 to 30 stop points were used in each tree. Stop points were often "AND" gates where probabilities were reduced due to multiplication of input probabilities. However, in certain cases "OR" gates were also used as stop points. As a result of this truncation, some error is introduced into the process. It is not possible at this present time to make a mathematical estimate of the amount neglected; however, the amount neglected is judged to be small since the dominant cut sets retained are usually several orders of magnitude larger than the cut off.

4. Determination of Dominant Cut Sets of the Sequences

In this step, all the event tree sequences that lead to a core melt were quantified. The truncated Boolean equations representing failure of each front-line system were combined to form one equation to represent the failure of the front-line systems in the sequence. The effect and treatment of successes of front-line systems in a sequence will be discussed in the next section. Consider a core melt sequence containing failure of the HPSI and CARCS systems. In order to calculate the probability of core melt due to this sequence, the Boolean equations for these two systems must be "ANDED" together. The result was then Boolean reduced and truncated at 1E-8 and cut sets were obtained. By using this method, the Boolean equationobtained for the product becomes fairly small because the front-line systems that are multiplied together are often highly independent producing very small probabilities when system equations are "ANDED." Some of the event tree sequences

contained failures of systems that were not developed into fault trees but instead represented as a single event quantified from industry data (such as RPS, and SRVs fail to reclose). In the sequences where failure of these systems occurs, failure of each was "ANDED" to the set of events in each dominant cut set. In addition, to obtain a complete set of cut sets, the appropriate initiating event must also be incorporated into the dominant cut sets.

5. Evaluation of the Effect of Success Events on Event Tree Sequences

As was discussed in section (4), the dominant cut sets obtained in that step include only the failure contribution of the front-line systems. In order to account for the success events of the sequences, one can find the complement of the truncated equations for front-line systems, and where applicable, "AND" this with the equation obtained in section (4) for individual sequences. The difficulty with this method is that finding the complement equation in a reduced form is a nontrival task; therefore, it was decided to account for the success event contributions by using a comparative method.

In the comparative method, the cut sets of a sequence obtained in step (4) are compared to the cut sets of those front-line systems that succeed in that sequence. If cut sets of the succeeded system were a subset of any of the sequence cut sets, then that cut set was eliminated from the list of sequence cut sets. For example, if ABC was a sequence cut set, and BC was a cut set of a front-line system that had succeeded in this sequence, then ABC was removed from the list of the sequence cut sets. This procedure is implemented in the SETS code.

Incorporation of the effects of the success states into in the sequences is important because it eliminates failure modes that are inconsistent with the success states. For example, assume in a sequence the High Pressure Safety Injection (HPSI) system has succeeded, but the High Pressure Safety Recirculation (HPSR) system has failed; and further assume that a dominant cut set of both HPSI and HPSR is failure of two diesel generators. For this sequence, the failure of two diesel generators is not a possible cut set. Because the success of HPSI requires the functioning of at least one of the two diesel generators, and the failure of HPSR requires both diesel generators to fail. This example demonstrates the importance of considering success events in the quantification of event tree sequences. In most cases, system successes have a significant impact on the probabilities of the sequences.

7.3 Final Quantification

Tasks (6) and (7) are final quantification tasks and are described below.

6. Identification of the Cut Sets of the Sequences Where the Possibility of Recovery Action Exists

The cut sets of the sequences obtained through the screening quantification were examined to identify possible recovery actions that would significantly reduce the failure probability associated with the sequences. There were 23 different recovery actions identified. These recovery actions and their application to the individual cut sets in the sequences are discussed in more detail in Appendix C. Those which contributed to the final dominant sequences are discussed in Chapter 8 in the discussion of each individual dominant sequence.

The dominant cut sets of the sequences were also examined to identify human errors that were significantly contributing to the frequency of the sequences. The purpose of this process was to reevaluate human error failure probabilities for these effects. Two actions were identified which contributed significantly to the frequencies of some sequences. First, operator initiation of emergency boration in failure to scram sequences. This was originally quantified using a value of 0.5. Upon performing a THERP analysis, this value was reduced to 0.1. Second, operator initiation of the second CCW heat exchanger in the recirculation phase of Small-small LOCAs initially was quantified using a value of 0.05, but consideration of the long time available before the operator must perform this action and the indications available to the operator reduced this value to 0.01.

7. Revision of Data to Include Recovery Action and Final Calculation of the Dominant Sequence Frequencies

In this task, the effects of recovery actions and probability of non-recovery on the sequence frequencies were accounted for by "ANDING" a non-recovery action to each of the cut sets of each sequence and recalculating the sequence frequencies. This non-recovery factor was dependent on the type of action required for recovery and the critical recovery time, the maximum time the system could be failed before recovery. The results obtained through this process are the final results as presented in Chapter 8. The explicit recovery model used and how the values for the individual recovery actions were chosen is described in Appendix C.

7.4 Example Calculation

The sequence quantification process used in this CC-1 analysis will be illustrated using sequence S_2-59. This sequence is initiated by a Small-small LOCA (S_2) and is depicted on the Small-small LOCA systemic event tree in Chapter 5. Sequence S_2-59 involves, in addition to event S_2: failure of the High Pressure Safety Injection (HPSI) System (event D"). This sequence also includes the successful operation of these systems: the Reactor Protection System (RPS) (event $\overline{K}$); the Auxiliary Feedwater System (AFW)(event $\overline{L}$); the Containment Air Recirculation and Cooling System (CARCS) (event $\overline{C}$); the Containment Spray System, Injection (CSSI) (event $\overline{C'}$); and the Containment Spray System, Recirculation (CSSR) (event $\overline{F}$). The Boolean representation of the sequence S_2D'' is $S_2\overline{K}\overline{L}D''\overline{C}\overline{C'}\overline{F}$.

Of the six systems, only the reactor protection system (event K) can be considered independent. The availability of this system and the initiating event frequency are:

$F(S_2)$ = 2.1E-2/yr
$P(\underline{K})$ = 3E-5
$P(K)$ = 1-3E-5~1

The remaining systems in this sequence are dependent due to shared components, subsystem or support systems and must be analyzed together. The first step in analyzing the $\overline{L}D''\overline{C}\overline{C'}\overline{F}$ part of the sequence was to use SETS to evaluate the probability for the event D". In this part of the analysis, the following sequence dependent events were set to the values they should have for this sequence: (1) the event accounting for a LOCA initiator was set to "1"; (2) the event accounting for a Large LOCA initiator was set to "0"; (3) the event accounting for a loss of offsite power (LOSP) was set to "1E-3," its value when LOSP is considered an independent event, not an initiator; (4) the event accounting for the LOCA occurring in one of the injection lines was set to "1"; (5) the events accounting for the requirement of SIAS actuation were set to "1"; (6) the events accounting for no LOSP were set to ".999"; (7) the special initiating events DC bus 11 and SRW valve 128 were set to their independent failure values; and (8) the operator failures to actuate SIAS or CSAS were set to their Small-small LOCA values. With a minimum cut set truncation value of 1E-8, the event D" had an estimated probability of 2.7E-4.

The Boolean expression for D" was then compared to the Boolean expressions for the succeeded events $\overline{L}$, $\overline{C}$., $\overline{C'}$ and $\overline{F}$. to determine logically inconsistent cut sets between the success and failure states. As a result, approximately half of the cut sets in the failure equation were eliminated and the new estimated probability for $\overline{L}D''\overline{C}\overline{C'}\overline{F}$ was 1.3E-4. Since $\overline{K}$ is independent of all other events and has a probability of $\sim$1,

then multiplying by $\overline{K}$ and the initiator frequency yields a screening value of 2.75E-6/yr for the sequence S_2-59.

For the final quantification, the dominant cut sets for the sequence were examined to determine the effects of possible recovery actions. Human errors that had a significant effect on the sequence probability were also reevaluated. However, there were no human errors contributing to the dominant cut sets of this sequence.

Two recovery actions were judged possible for this sequence: (1) manual actuation of HPSI from the control room given that auto-actuation had failed, and (2) realigning the electric power supply of the swing HPSI pump #13 from the control room given that a loss of offsite power, failure of DG#12 and failure of HPSI pump #11 had occurred. For both of these events, a probability of .01 was assessed for non-recovery given that more than one hour is available to the operator to start primary makeup. These actions affected over 90% of the sequence cut sets; however, they did not affect the dominant two cut sets. After applying these non-recovery factors, the probability value of $\overline{KL}D''\overline{C}\overline{C}'\overline{F}$ was reduced from 1.3E-4 to 7.7E-5.

The final quantification value for the sequence S_2-59, therefore, becomes 1.6E-6/yr: the initiating event value of 2.1E-2/yr times the 7.7E-5 probability of the system failures.

Table 7.1a **Generic Data Base***

Component and Failures Modes	Mean	Median	Error Factor	Remarks
1. Pumps				
1.1 Motor-driven				Pump and motor; excludes control circuits.
1.1.1 Failure to start	3E-3/d	1E-3/d	10	
1.1.2 Failure to run, given start				
1.1.2.1 Normal Environment	3E-5/h	1E-5/h	10	
1.1.2.2 Extreme Environment	3E-3/d	1E-3/h	10	Considered as interface with heavy chemical environment such as concentrated boric acid.
1.2 Turbine-driven				Pump, turbine, steam and throttle valves, and governor.
1.2.1 Failure to start (includes under and over speed)	3E-2/d	1E-2/d	10	
1.2.2 Failure to run, given start	1E-5/h	1E-5/h	3	
1.3 Diesel-driven				Pump, diesel, lube oil system, fuel oil, suction and exhaust air, and starting system.
1.3.1 Failure to start	1E-3/d	1E-3/d	3	
1.3.2 Failure to run, given start	8E-4/h	1E-4/h	30	
2. Valves				Catastrophic leakage or "rupture" valves assigned by engineering judgment; catastrophic leakage assumes the valve to be in a closed state, then the valve fails.
2.1 Motor-operated				
2.1.1 Failure to open	3E-3/d	1E-3/d	10	
2.1.2 Failure to remain open	1E-7/h	1E-7/h	3	
2.1.3 Failure to close	3E-3/d	1E-3/d	10	
2.1.4 Internal leakage (catastrophic)	5E-7/h	1E-8/h	100	
2.2 Solenoid-operated				
2.2.1 Failure to operate	1E-3/d	1E-3/d	3	
2.3 Air/Fluid-operted				
2.3.1 Failure to operate	3E-3/d	1E-3/d	10	
2.4 Check valves				
2.4.1 Failure to open	1E-4/d	1E-4/d	3	
	3E-7/h	1E-7/h	10	Hourly rate is based on one actuation per month.
2.4.2 Failure to close	1E-3/d	1E-3/d	3	
	3E-6/h	1E-6/h	10	Hourly rate is based on one actuation per month.
2.4.3 Internal Leakage				
2.4.3.1 Minor	3E-5/h	1E-6/h	10	
2.4.3.2 Catastrophic	5E-7/h	1E-8/h	100	Valve initially closed, then failed.
2.5 Vacuum breakers				Applies only to BWRs.
2.5.1 Failure to open	1E-5/d	1E-5/d	3	
2.5.2 Failure to close	1E-5/d	1E-5/d	3	
2.6 Manual valves				Failure to operate is dominated by human error; hourly rate
2.6.1 Failure to operate	1E-4/d	1E-4/d	3	
	3E-7/h	1E-7/h	10	is based on one actuation per month.

*Adapted from EGG-EA-5887. [18]

Table 7.1a **(continued)**

Component and Failures Modes	Mean	Median	Error Factor	Remarks
2.7 Code safety valves				Applies only to PWRs; premature opening treated as an initiating event.
2.7.1 Failure to open	1E-5/d	1E-5/d	3	
2.7.2 Failure to close, given open	1E-2/d	1E-2/d	3	
2.8 Primary safety valves				Applies only to BWRs.
2.8.1 Failure to open	1E-5/d	1E-5/d	3	
2.8.2 Failure to close, given open	3E-2/d	1E-2/d	10	
2.9 Relief valves				
2.9.1 Failure to open	3E-4/d	1E-4/d	10	
2.9.2 Failure to close,given open	2E-2/d	2E-2/d	3	
2.10 Stop check valves				
2.10.1 Failure to open	1E-4/d	1E-4/d	3	
3. Switches				Where torque/limit switches are used as part of pumps/valves, switch failure rate is included in pump/valve failure rate.
3.1 Torque				
3.1.1 Failure to Operate	1E-4/d	1E-4/d	3	
3.2 Limit				
3.2.1 Failure to operate	1E-4/d	1E-4/d	3	
3.3 Pressure				
3.3.1 Failure to operate	1E-4/d	1E-4/d	3	
3.4 Manual				
3.4.1 Failure to transfer	3E-5/d	1E-5/d	10	
4. Other				
4.1 Circuit breaker				For sizes 4 kV and smaller.
4.1.1 Failure to transfer	3E-3/d	1E-3/d	10	
4.1.2 Spurious trip	3E-5/d	1E-5/d	10	
4.2 Fuses				
4.2.1 Premature open	3E-6/d	1E-6/h	10	
4.3 Buses				
4.3.1 All modes	1E-8/h	1E-8/h	3	
4.4 Orifices				WASH-1400 data; no alternate data available.
4.4.1 Failure to remain open (plug)	3E-4/d	3E-4/d	3	
4.4.2 Rupture	3E-8/h	1E-8/h	10	
4 5 Transformers				
4.5.1 All modes	1E-6/h	1E-6/h	3	

*Adapted from EGG-EA-5887. [18]

Table 7.1a **(continued)**

Component and Failures Modes	Mean	Median	Error Factor	Remarks
4.6 Emergency diesel (complete plant)				Engine frame and associated moving parts, generator coupling, governor, output breaker, static exciter, lube oil system, fuel oil, intake and exhaust air, starting system; excludes starting air compressor and accumulator, fueling storage and transfer, load sequencers, and synchronizers. Failure to start is failure to start, accept load, and run for 1/2 hour; failure to run is failure to run for more than 1/2 hour, given start.
4.6.1 Failure to start	3E-2/d	3E-2/d	3	
4.6.2 Failure to run, given start (emergency conditions)	3E-3/h	1E-3/h	10	
4.7 Relays				
4.7.1 Contacts fail to transfer (open or close)	3E-4/d	1E-4/d	10	
4.7.2 Coil failure (open or short)	3E-6/h	1E-6/h	10	
4.8 Time Delay Relays				
4.8.1 Premature transfer	3E-4/d	1E-4/d	10	
4.8.2 Fails to transfer				
4.8.2.1 Bimetallic	5E-6/h	5E-6/h	3	Non-consensus source. Data source is MIL-HDBK-217B [19]. Fail-to-transfer rates are not currently available for non-bimetallic time delay relays.
4.9 Battery power system (wet cell)				Assumes out-of-spec cell replacement.
4.9.1 Fails to provide proper output	1E-6/h	1E-6/h	3	
4.10 Battery charger				
4.10.1 Failure to operate	1E-6/h	1E-6/h	3	
4.11 DC motor-generators				
4.11.1 Failure to operate	3E-6/h	1E-6/h	10	
4.12 Inverters				
4.12.1 Failure to operate	1E-4/h	1E-4/h	3	
4.13 Wires (per circuit)				Consistent with IEEE-500 data for 1000 circuit feet
4.13.1 Open circuit	3E-6/h	1E-6/h	10	
4.13.2 Short to ground	3E-7/h	1E-7/h	10	
4.13.3 Short to powered	3E-8/h	1E-8/h	10	
4.14 Solid state devices				For more detailed information, see MIL-HDBK-217C [20].
4.14.1 High power applications	3E-6/h	1E-6/h	10	
4.14.2 Low power applications	3E-6/h	1E-6/h	10	
4.14.3 Bistables	3E-7/d	1E-7/d	10	

*Adapted from EGG-EA-5887. [18]

Table 7.1a (concluded)

Component and Failures Modes	Mean	Median	Error Factor	Remarks
4.15 Terminal Boards				Values given are per terminal.
4.15.1 Open circuit	3E-7/h	1E-7/h	10	
4.15.2 Short to adjacent circuit	3E-7/h	1E-7/h	10	
4.16 Dampers				
4.16.1 Failure to operate	3E-3/d	1E-3/d	10	
4.17 Air coolers				
4.17.1 Failure to operate	1E-5/h	1E-5/h	3	Not consensus data. Plant-specific from ANO-1 IREP study.
4.18 Heat exchangers				
4.18.1 Tube leak (per tube)	3E-9/h	1E-9/h	10	
4.18.2 Shell leak	3E-6/h	1E-6/h	10	
4.19 Strainer/filter				For clear fluids; contaminated fluids
4.19.1 Plugged	3E-5/h	1E-5/h	10	or fluids with a heavy chemical burden should be considered on a plant-specific basis.
4.20 Scram systems				
4.20.1 Failure to scram	3E-5/d	3E-5/d	3	
4.21 Instrumentation (general)				
4.21.1 Failure to operate	3E-6/h	1E-6/h	10	

*Adapted from EGG-EA-5887. [18]

Table 7.1b Multipliers to Compute Mean From Median

Error Factor	Multiplier
3	1.25
10	2.66
30	8.48
100	50.33

Table 7.2a Mechanical Component Failure Rate Data
(from WASH-1400, Table III 4-1)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE		MEDIAN	EF	
Pumps (includes driver):						
Motor & turbine driven (generic class):						
Failure to start on demand:	D (A)	3E-4	3E-3	1E-3	3	
Failure to run, given start (normal environments):	O	3E-6	3E-4	3E-5	10	
Failure to run, given start (extreme, post accident environments inside containment):	O	1E-4	1E-2	1E-3	10	
Failure to run, given start (post accident, after environmental recovery):	O	3E-5	3E-3	3E-4	10	
Turbine driven pumps:						
Failure to start on demand:	D	1E-3	1E-2	3E-3	3	A
Failure to run, given start (normal environment):	O	1E-5	1E-4	3E-5	3	A
Valves:						
Motor operated:						
Failure to operate (includes driver):	D (B)	3E-4	3E-3	1E-3	3	
Failure to remain open (plug):	D (C)	3E-5	3E-4	1E-4	3	
Failure to remain open (plug):	s	1E-7	1E-6	3E-7	3	
Rupture:	s	1E-9	1E-7	1E-8	10	
Solenoid operated:						
Failure to operate:	D (D)	3E-4	3E-3	1E-3	3	
Failure to remain open (plug):	D	3E-5	3E-4	1E-4	3	
Rupture:	s	1E-9	1E-7	1E-8	10	
Air-fluid operated:						
Failure to operate:	D (B)	1E-4	1E-3	3E-4	3	
Failure to remain open (plug):	D	3E-5	3E-4	1E-4	3	
Failure to remain open (plug):	s	1E-7	1E-6	3E-7	3	
Rupture:	s	1E-9	1E-7	1E-8	10	
Check valves:						
Failure to open:	D	3E-5	3E-4	1E-4	3	
Internal leak (severe):	D	1E-7	1E-6	3E-7	3	
Rupture:	s	1E-9	1E-7	1E-8	10	
Vacuum Valve:						
Failure to operate:	D	1E-5	1E-4	3E-5	3	
Manual Valve:						
Failure to operate:	D	3E-5	3E-4	1E-4	3	A
Failure to remain open (plug):	D	3E-5	3E-4	1E-4	3	
Rupture:	s	1E-9	1E-7	1E-8	10	
Primary Safety Valves (PWRs):						
Failure to open:	D	1E-3	1E-2	3E-3	3	R
Premature open:	s	1E-6	1E-5	3E-6	3	R
Failure to reclose (given valve open):	D (E)	3E-3	3E-2	1E-2	3	R

Table 7.2a (Concluded)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE		MEDIAN	EF
Primary safety valves (BWRs):					
Failure to open:	D	3E-3	3E-2	1E-2	3 R
Premature open:	s	1E-6	1E-5	3E-6	3 R
Failure to reclose (given valve open):	D	1E-3	1E-2	3E-3	3 R
Test Valves, Flow Meters, Orifices:					
Failure to remain open (plug):	D	1E-4	1E-3	3E-4	3
Rupture:	s	1E-9	1E-7	1E-8	10
Pipes					
Pipe ≤ 3-inch diameter (per section):					
Rupture/plug:	s + 0	3E-11	3E-8	1E-9	30
Pipe > 3-inch diameter (per section):					
Rupture/plug:	s + 0	3E-12	3E-9	1E-10	30
Clutch, Mechanical:					
Failure to operate:	D (D)	1E-4	1E-3	3E-4	3
Scram Rods (Single):					
Failure to insert:	D	3E-5	3E-4	1E-4	3

Table 7.2b Electrical Component Failure Rate Data
(from WASH-1400, Table III 4-2)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE		MEDIAN	EF
Clutch, Electrical:					
Failure to operate:	D (B)	1E-4	1E-3	3E-4	3
Premature disengagement:	0	1E-7	1E-5	1E-6	10
Motors, Electric:					
Failure to start:	D (B)	1E-4	1E-3	3E-4	3
Failure to run, given start (normal environment):	0	3E-6	3E-5	1E-5	3
Failure to run, given start (extreme environment):	0	1E-4	1E-2	1E-3	10
Relays:					
Failure to energize:	D (B)	3E-5	3E-4	1E-4	3
Failure of NO contacts to close, given energized:	0	1E-7	1E-6	3E-7	3
Failure of NO contacts by opening, given not energized:	0	3E-8	3E-7	1E-7	3
Short across NO/NO contact:	0	1E-9	1E-7	1E-8	10
Coil open:	0	1E-8	1E-6	1E-7	10
Coil short to power:	0	1E-9	1E-7	1E-8	10
Circuit Breakers:					
Failure to transfer:	D (B)	3E-4	3E-3	1E-3	3
Premature transfer:	0	3E-7	3E-6	1E-6	3
Switches:					
Limit:					
Failure to operate:	D	1E-4	1E-3	3E-4	3
Torque:					
Failure to operate:	D	3E-5	3E-4	1E-4	3
Pressure:					
Failure to operate:	D	3E-5	3E-4	1E-4	3
Manual:					
Failure to transfer:	D	3E-6	3E-5	1E-5	3
Switch Contacts:					
Failure of NO contacts to close, given switch operation:	0	1E-8	1E-6	1E-7	10
Failure of NC by opening, given no switch operation:	0	3E-9	3E-7	3E-8	10
Short across NO/NC contact:	0	1E-9	1E-7	1E-8	10
Battery Power System (Wet Cell):					
Failure to provide proper output:	s	1E-6	1E-5	3E-6	3
Transformers:					
Open circuit primary or secondary:	0	3E-7	3E-6	1E-6	3
Short primary to secondary:	0	3E-7	3E-6	1E-6	3
Solid State Devices, Hipower Applications (Diodes, Transistors, etc.):					
Fails to function:	0	3E-7	3E-5	3E-6	10
Fails shorted:	0	1E-7	1E-5	1E-6	10

Table 7.2b (Concluded)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE		MEDIAN	EF
Solid State Devices, Low Power Applications:					
Fails to function:	O	1E-7	1E-5	1E-6	10
Fails shorted:	O	1E-8	1E-6	1E-7	10
Diesels (Complete Plant):					
Failure to start:	D	1E-2	1E-1	3E-2	3
Failure to run, emergency conditions, given start:	O	3E-4	3E-2	3E-3	10
Diesels (Engine Only):					
Failure to run, emergency conditions, given start:	O	3E-5	3E-3	3E-4	10
Instrumentation--General (Includes transmitter, amplifier and output device):					
Failure to operate:	O	1E-7	1E-5	1E-6	10
Shift in calibration:	O	3E-6	3E-4	3E-5	10
Fuses:					
Failure to open:	D	3E-6	3E-5	1E-5	3
Premature open:	O	3E-7	3E-6	1E-6	3
Wires (typical circuits, several joints):					
Open circuit:	O	1E-6	1E-5	3E-6	3
Short to ground:	O	3E-8	3E-6	3E-7	10
Short to power:	O	1E-9	1E-7	1E-8	10
Terminal Boards:					
Open connection:	O	1E-8	1E-6	1E-7	10
Short to adjacent circuit:	O	1E-9	1E-7	1E-8	10

Table 7.2 (Notes)

NOTES: (A) Demand probabilities are based on the presence of proper input control signals. For turbine pumps, the effect of failures of valves, sensors, and other auxiliary hardware may result in significantly higher overall failure rates for turbine driven pump systems.

(B) Demand probabilities are based on presence of proper input control signals.

(C) Plug probabilities are given in demand probability, and per hour rates, since phenomena are generally time-dependent, but plugged condition may only be detected upon a demand of the system.

(D) Demand probabilities are based on presence of proper input control signals.

(E) These rates are based on LERs for B&W pressurizer PORV failure to reseat given the valve has opened.

ABBREVIATIONS:

(1) For failure rate type abbreviations:
D = demand failure rate--failures per demand
O = operating failure rate--failures per hour of operation
S = standby failure rate--failures per hour of standby
S+D = standby or operating failure rate--failures per hour

(2) Remarks (last column) abbreviations:
R = failure rate shown is a revision of WASH-1400 value
A = failure rate shown is in addition to WASH-1400 failure rates.

CHAPTER 8

RESULTS

8.1 Dominant Accident Sequences

The culmination of the analysis was the determination of those sequences contributing most to the risk from core melt at the plant. The process that was followed to arrive at this point is described in Chapter 7 and is explained in detail in Appendix C. This chapter presents the results of that process.

The total core melt frequency for Calvert Cliffs Unit 1 was determined to be 1.3E-4/yr and consisted almost entirely of sequences with frequencies greater than 1.0E-6/yr. The list of these sequences is shown in Table 8.2 and a legend for all the terms can be found in Table 8.1. Most of these sequences were evaluated according to the process described in Chapter 7.

Two of the sequences were not identified by the event tree accident sequence definition process. The first was the ATWS(PSF) sequence. This sequence is a composite sequence to estimate the likelihood of any transient initiator followed by failure to scram resulting in primary system failure. The results of CE analyses [21] and NRC analysis in support of the ATWS rule [22] were used to estimate the frequency of this event. The second is the Blackout sequence. This sequence involves a loss of offsite power (LOSP) followed by the loss of all three diesel generators. Auxiliary Feedwater works initially, but fails after four hours due to battery depletion; AC power is not recovered. This sequence was not identified at the time the fault trees were originally constructed, but as a result of the NRC sponsored Station Blackout Program [17]. The sequence actually modeled that is similar to this Blackout sequence is T_1-85. Sequence T_1-85 involves failure of two diesel generators and failure of auxiliary feedwater immediately after the LOSP due to hardware failures. This sequence (T_1-85) was also identified in the Station Blackout Program, but was found to be less important (this is confirmed by our results).

An estimate was made of the contribution to core melt of all the sequences with frequencies less than 1.0E-6/yr. These sequences can be divided into two groups: (1) The twenty-six of the original candidate dominant sequences which dropped below 1.0E-6/yr when recovery was applied to them, and (2) two hundred and sixty-eight sequences out of the total of 308 sequences defined for Calvert Cliffs which were below the 1.0E-6/yr cutoff in the screening quantification stage. For group (1), their frequencies after recovery was applied were summed and came to 5.1E-6/yr. For group (2), their frequencies were either calculated explicitly by evaluating the whole sequence (done for about 50% of the sequences) or an upper

bound on the point estimate was calculated from knowledge of the initiating events, undeveloped events and evaluating some of the developed events (see the discussion in Appendix C on the screening calculation for more details). Summing the frequencies of these sequences resulted in a contribution of 2.7E-5/yr before recovery was applied. Only a few of the sequences were near the 1.0E-6/yr cutoff and contributed significantly to this number. These few were found to be similar to existing candidate dominant sequences and to have similar recovery potential. Since the dominant sequences were reduced by a factor of 10 by application of recovery, this factor was applied to the group (2) contribution to give a final frequency estimate of 2.7E-6/yr Upon summing the group (1) and (2) estimates, we get 7.8E-6/yr or 6% of the total core melt frequency. This estimate was added into the total core melt frequency estimate.

From the list of dominant sequences in Table 8.2, the following general classes of accident sequences were found to contribute most to the CC-1 core melt frequency:

1. Anticipated Transients Without Scram (ATWS) contributed 33% of the core melt frequency.

2. Small-small LCCAs (S_2) contributed 20% of the core melt frequency.

3. The special transient initiator T_{DC} (loss of DC bus 11) contributed 16% of the core melt frequency.

4 Loss of Offsite Power (T_1) transients contributed 12% of the core melt frequency.

5. Loss of PCS (T_2) transients contributed 6% of the core melt frequency (not including the ATWS sequence).

6. All other transients (T_4) contributed 5% of the core melt frequency (not including the ATWS sequences).

7. Transients requiring pressure relief (T_3) contributed 1% of the core melt frequency (not including the ATWS sequences).

In order to get an estimate of the consequences which may be expected from core melt accidents, all the sequences with frequencies greater than 1.0E-6/yr were analyzed by Battelle Columbus Laboratories (BCL) to determine which containment failure modes and release categories would be expected from the occurrence of each sequence. The sequence frequency was then multiplied by the containment failure mode probability, and the resulting frequency was assigned to the proper release category. The results of this analysis are shown in Tables 8.3 and 8.4, and discussed in Section 8.2.

Sensitivity analyses were performed on the dominant accident sequences and are discussed in detail in Section 8.3. Various phenomenological and modeling uncertainties were examined.

The remainder of this section describes in detail the accident sequences with frequencies greater than, or equal to, 1.0E-6/yr. The descriptions include the dominant cut sets of the sequences and details of the insights gained, major assumptions made, and a discussion of the recovery factors applied to each sequence.

8.1.1 ATWS(PSF)

8.1.1.1 Description

This sequence is an anticipated transient without scram (ATWS) followed by primary system failure (PSF) due to overpressure and is assessed to result in a LOCA and subsequent core melt. The CARCS and/or CSSI systems succeed and cool the containment.

As a result of some transient, the PCS is either tripped, fails, or runs back and AFW and/or the PCS is removing heat from the primary at a reduced rate (i.e., at least ~5% of full power). The resulting imbalence between the energy removal rate (~5%) and the energy production rate (~100%) leads to the heatup of the primary system and an increase in system pressure. The magnitude of the pressure increase is determined by several variables: the initial power level, final heat removal rate, and the net reactivity in the core. Assuming the initial power and final heat removal rate are ~100% and ~5%, respectively, then the major determining factor is the moderator temperature coefficient (MTC) of reactivity. The MTC determines the negative feedback between the rise in temperature and the resulting decrease in power due to the negative reactivity added by the decreasing density or voiding of the primary coolant. The less negative (i.e., closer to zero) the MTC, the smaller the feedback and the higher the peak pressure.

Given that the peak pressure exceeds the service level C(3200 psia) limit, various types of system damage have been postulated: (1) If the pressure should exceed 3500 psia then the reactor vessel head will lift [21] and will likely fail to reseat completely, (2) the response of the steam generator tubes (particularly older tubes) is uncertain at these differential pressures and a large number could potentially rupture [22], and (3) because there is insufficient analysis of the operability of check valves in the primary system for pressures exceeding service level C, there is an assessment that the CVCS and HPSI systems would be unavailable some significant fraction of the time due to the check valves being

forced shut and deformed to the point of inoperability. [22] Thus, continued reactor cooling and long-term recovery after the system has been overpressured is questionable. For the purpose of this analysis, it was assumed that pressures in excess of 3200 psia are equated to core melt.

The sequence frequency is estimated at 2.8E-5/yr and contributes 20% of the total core melt frequency.

8.1.1.2 Quantification

In order to estimate the frequency of an ATWS event followed by an unfavorable MTC, one must multiply the transient frequency by both the failure to scram probability and the probability of having an unfavorable MTC (i.e., the probability of having an MTC value that results in the peak pressure exceeding the service level C limit) for that initiator.* Upon summing the results for the various initiators, the estimate of the frequency of this sequence is calculated to be:

$$\begin{aligned} f(\mathrm{ATWS(PSF)}) &= T_2 \bullet k \bullet P_2(\mathrm{MTC}) + T_3 \bullet k \bullet P_3(\mathrm{MTC}) + 0.5 \bullet T_4 \bullet k \bullet P_4(\mathrm{MTC}) \\ &= 0.8 \bullet 3E\text{-}5 \bullet 0.5 + 1.85 \bullet 3E\text{-}5 \bullet 0.1 + 0.5 \bullet 6.8 \bullet 3E\text{-}5 \bullet 0.1 \\ &= 1.2E\text{-}5 + 5.6E\text{-}5 + 1.0E\text{-}5 \\ &= 2.8E\text{-}5/yr \end{aligned}$$

The sources of the various numbers are discussed in the next section.

8.1.1.3 Major Assumptions and Recovery actions

Because of the short time (~2 minutes) before pressure exceeds service level C, no credit has been given for any recovery actions. The IREP recovery model does not give credit for any action required to be performed in less than 5 minutes.

T_1(Loss of Offsite Power) transients were not quantified since the initiator directly results in a de-energization of the motor-generator sets and the use of a 3E-5 probability for failure to scram was assessed as being too high for this initiator. The failure to scram would need to result from some mechanical common mode failure of all or most of the control rod drive mechanisms and was assessed as being negligible.

For T_2 (Loss of Feedwater) transients a probability of 0.5 was chosen for an unfavorable MTC. The peak pressure predicted for this type of transient was 4200 psia for a new

---

*The MTC becomes more negative as a core approaches end-of-life. Thus, new cores will result in higher peak pressures than old cores. The probability of an unfavorable MTC is equivalent to the fraction of core life in which the peak pressure is expected to exceed 3200 psia for each specific transient type.

core [21] and allows for the reactor vessel head lifting at ~3500 psia to relieve some of the pressure. This predicted peak pressure greatly exceeds the service level C (3200 psia) limit and a LOCA, due to failure of the vessel head to reseat or steam generator tube rupture or some other break in the primary, combined with failure of CVCS and HPSI to supply makeup due to stuck check values results in core melt. The value of 0.5 for the probability of a pressure transient exceeding service level C and resulting in core melt comes from NUREG-0460 [23] and is the same as that used in the NRC analysis in support of the ATWS rule [22].

For T_3 (Turbine Trip) transients, the system response has a peak predicted pressure of ~3400 psia for a new core. This is different from the response of larger CE plants for which the peak pressures from turbine trips and loss of feedwater are roughly the same (i.e., both ~4,000 psia). The NRC analysis in support of the ATWS rule [22] groups CE and B&W plants and uses a probability of 0.5 for exceeding service level C for turbine trip transients. However; this value, while appropriate for larger CE plants, was judged to be too large for smaller plants like Calvert Cliffs. A value of 0.1 was chosen based on the following considerations: (1) the 3400 psia peak pressure is based on a nominal full power initiator, but the analysis models initiators occurring from 25-110% power, and (2) the probability of having an unfavorable MTC should be significantly less than for the loss of feedwater case since the transient is less severe and the value of the MTC needed to exceed 3200 psia should be much higher than in the loss of feedwater case (e.g., a factor of ~4 increase in the MTC would be needed to produce pressure comparable to the loss of feedwater initiator). The actual value was estimated by shifting the MTC probability table in NUREG-0460, Vol. 4 [23] to reflect the less severe characteristics of the sequence.

For T_4 (all other) transients, it was assessed that approximately 50% of the initiators would not result in runback of the PCS and that no heat imbalance or pressure transient would result. The remaining 50% were assessed as resulting in a turbine trip and runback of the PCS or conditions roughly similar to a turbine trip. The pressure transient for these initiators would be similar to the T_3 transient described previously. A value of 0.1 for the probability of an unfavorable MTC was therefore used in this case, also.

The value of 3E-5 used for the failure to scram probability is a generic value taken from NUREG-0460 [23]. This is the same as the value used in the NRC analysis in support of the ATWS rule [22]. Since the dominant contributors to failure to scram are likely to be common modes that result in failure of all rods to insert (e.g., Salem failure to scram on February 22 and 25, 1983), this number was used to represent failure of all rods to insert, and no credit was taken for the possibility of

some rod insertion that would significantly reduce the peak pressure.

8.1.1.4 Engineering Insights

As discussed in the previous section with the IREP recovery model and without ATWS procedures and training, no credit was given for operator actions mitigating this event. Calvert Cliffs has recently implemented a new ATWS procedure which directs the operator to: (1) trip the reactor manually, (2) de-energize the motor-generator sets, and (3) to initiate emergency boration. The de-energization of the motor-generator sets should bypass any actuation or control circuit failures (e.g., the Salem incident) and result in successful scram. If done quickly enough, this could result in a reduction in any pressure transient. With appropriate operator training, it may be possible to mitigate this sequence.

The only other ways of reducing this sequence's frequency or mitigating the results appear to involve changes to the plant such as: (1) reduce the number of transients, (2) improve the RPS reliability, (3) qualify the primary system and valve operability at higher pressures (~3500 psia), (4) do improved analysis to show peak pressures are not as high as currently predicted, or (5) change the fuel loading so that a more negative MTC is obtained.

8.1.2 Sequence T_{DC}-82 ($T_{DC}L$)

8.1.2.1 Description

In this sequence, a failure of DC bus 11 (T_{DC}) results in a trip of Units 1 and 2 and failure of the PCS with degradation of the safety systems. The plant scrams successfully, but AFW (L) subsequently fails. CARCS and CSSI succeed and cool the containment. As a result of the lack of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to the low head of the HPSI pumps and the uncertainty as to whether or not the pressure could be reduced enough for the HPSI pumps to be able to inject water, [24, 25]. Recent calculations done by EG&G for the Station Blackout Program [26] indicate that approximately 86 minutes is available to start an AFW pump in order to prevent core uncovery.

The sequence frequency is estimated as 2.1E-5/yr and contributes 16% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.2.2 Dominant Cut Sets - $T_{DC}L$

Cut Set	Frequency (/yr)	% of Sequence
T_{DC}*RA-3*AFWP11-PTD-LF	6.8E-6	32
T_{DC}*RA-3*AFWP11-PTD-PRMN	5.3E-6	25
T_{DC}*RA-3*AFWS903A-NOC-LF	1.4E-6	7
T_{DC}*RA-3*AFW3987A-NOC-LF	1.4E-6	7
T_{DC}*RA-16*AFW4530-N-PRMN	7.2E-7	3
T_{DC}*RA-16*AFW4520-N-PRMN	7.2E-7	3
T_{DC}*RA-4*AFWP11-PTD-PRTS	5.0E-7	2
T_{DC}*AFW4511-CV-OE*AFW4531-NOC-LF	3.6E-7	2
T_{DC}*AFW4511-CV-OE*AFW4530-NOC-LF	3.6E-7	2
T_{DC}*AFW4511-CV-OE*AFW4512-NOC-LF	3.6E-7	2
T_{DC}*RA-3*AFW0103-X-FRFT	2.9E-7	1
T_{DC}*RA-3*AFWM911X-X-PRMN	2.3E-7	1
T_{DC}*RA-3*AFWC909X-CCC-LF	1.4E-7	1
T_{DC}*RA-3*AFW0102-CCC-LF	1.4E-7	1
	1.9E-5	90%

Term Descriptions

T_{DC} = Failure of DC bus 11; this results in failure of PCS, the failure of AFW motor-driven pump #13 and the opening of steam admission valve 4071 and feedwater valves 4512 and 4535 to steam generator #12; f = 3.6E-2/yr.

RA-3 = Operator fails to start locked-out AFW turbine-driven pump #12; p = 4E-2.

AFWP11-PTD-LF = Local fault of AFW turbine-driven pump #11; p = 4.7E-3.

AFWP11-PTD-PRMN = Maintenance of AFW turbine-driven pump #11; p = 1.4E-3.

AFWS903A-NOC-LF = Local fault of valve in steam admission line to AFW turbine-driven pump #11; p = 1E-3.

AFW3987A-NOC-LF = Local fault of valve in steam admission line to AFW turbine-driven pump #11; p = 1E-3.

RA-16 = Operator fails to crossfeed from unit 2's AFW; p = 1E-1.

AFW4530-N-PRMN = Feedwater valve whose maintenance fails delivery from both AFW turbine-driven pumps; p = 2E-4.

Term Descriptions (Cont.)

AFW4520-N-PRMN	=	Feedwater valve whose maintenance fails delivery from both AFW turbine-driven pumps; p = 2E-4.
RA-4	=	Operator fails to restore AFW turbine-driven pump #11 from test; p = 1E-2.
AFWP11-PTD-PRTS	=	AFW turbine-driven pump #11 in test; p = 1.4E-3.
AFW4511-CV-OE	=	Operator fails to increase flow to steam generator #11 given plugging of valve to steam generator #12; p = 1E-2.
AFW4531-NOC-LF	=	Local fault of feedwater valve to steam generator #12, fails turbine pump flow to that steam generator; p = 1E-3.
AFW4530-NOC-LF	=	Local fault of feedwater valve to steam generator #12, fails turbine pump flow to that steam generator; p = 1E-3.
AFW4512-NOC-LF	=	Local fault of feedwater valve to steam generator #12, fails turbine pump flow to that steam generator; p = 1E-3.
AFW0103-X-FRFT	=	Failure to restore from test an AFW turbine-driven pump #11 discharge valve; p = 2E-4.
AFWM911X-X-PRMN	=	Maintenance of valve in AFW turbine-driven pump #11 steam admission line; p = 1.6E-4.
AFWC909X-CCC-LF	=	Local fault of check valve in AFW turbine-driven pump #11 steam admission line; p = 1E-4.
AFW0102-CCC-LF	=	Local fault of check valve in AFW turbine-driven pump #11 discharge line; p = 1E-4.

8.1.2.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 4.9E-4yr. The recovery actions involve: (1) starting the locked-out AFW turbine pump #12 (RA-3, p = .04), (2) actuating the AFW turbine pump #11 manually from the control room (RA-2, p = .02), (3) feeding AFW from unit 2's AFW system (RA-16, p = .1), or (4) realigning AFW turbine pump #11 from test (RA-4, p = .01).

It is assumed due to discussions with plant personnel that the operator would be reluctant to manually close the motor pump circuit breaker due to the lack of pump protection resulting from the DC bus loss; therefore, other recovery actions were preferentially considered. Also, while all the cut sets could be recovered by cross-feeding from unit 2's AFW system once the AFW modification is completed (see Section 6.9 of main report or Appendix B.9), credit for this was only given when no other reasonable recovery action was possible. Because the procedures for dealing with these events have not been written, we judged that there would be some reluctance on the part of unit 2's operators to divert flow to unit 1 and decrease the reliability of their own AFW supply and a 0.1 non-recovery probability was used for this event.

It may also be possible for the operator to restart one train of the PCS system; however, no credit was given for this action since the operator would preferentially be directed to the AFW system and, by the time he decided to try to restart the PCS, it is assumed that it would be too late. The application of the recovery actions reduced the sequence frequency to 2.1E-5/yr.

8.1.2.4 Engineering Insights

For this sequence, the loss of DC bus 11 results in a trip of both unit 1 and 2, fails auto AFAS actuation and DC breaker control power to the motor-driven AFW pump #13, AFW steam admission valve 4071 fails open and AFW train A feedwater valves fail open resulting in auto start of AFW turbine-driven pump #11. However, various single faults of AFW pump #11 result in a loss of all AFW. For most faults (75% of the sequence frequency), it is possible for the operator to manually start the locked-out turbine pump #13; however, for the case where feedwater valves 4530 or 4520 have been isolated for maintenance requiring disassembly (6% of the sequence frequency), the two turbine pumps are both unavailable. The only recovery is to then cross-feed from unit 2's AFW system.

8.1.3 Sequence S_2-50 (S_2H)

8.1.3.1 Description

In this sequence, a Small-small LOCA (S_2) occurs followed by successful scram and operation of AFW and HPSI providing both secondary heat removal and primary system makeup. When the RWT depletes and switchover to recirculation occurs (anywhere from 4 to 12 hours into the transient depending on the size of the leak), HPSR (H) fails. Due to the lack of primary makeup, the core then uncovers and core melt ensues. CARCS and CSSR succeed and cool the containment.

The sequence frequency is estimated as 1.4E-5/yr and contributes 11% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.3.2 Dominant Cut Sets

Because of the large number of cut sets of relatively equal value which comprise this sequence even after the application of recovery, only cut sets whose frequency is greater than 2.1E-8/yr are listed here. These cut sets comprise 74% of the sequence frequency. A more detailed list of cut sets for all dominant sequences can be found in Appendix C.

Cut Sets	Freq. (/yr)	% of Sequence
S_2*CCW0258X-XOC-LF	7.6E-7	5
S_2*CCW3826N-NCC-OE*SWS5206A-NCC-LF	6.3E-7	5
S_2*CCW3826N-NCC-OE*SWS5160A-NCC-LF	6.3E-7	5
S_2*CCW3826N-NCC-OE*CCW3823N-NTO-LF	6.3E-7	5
S_2*HPIOC13B-CBL-LF*ECCFANWE-CBL-LF	4.6E-7	3
S_2*HPI0013B-BOO-LF*ECCFANWE-CBL-LF	4.2E-7	3
S_2*HPI0013B-PMD-LF*ECCFANWE-CBL-LF	4.2E-7	3
S_2*HPIOC13B-CBL-LF*SWS5171A-NCC-LF	2.1E-7	2
S_2*HPIOC13B-CBL-LF*SWS5170A-NCC-LF	2.1E-7	2
S_2*HPIOC13B-CBL-LF*SIS4144A-VCC-LF	2.1E-7	2
S_2*HPI0013B-BOO-LF*SWS5171A-NCC-LF	1.9E-7	1
S_2*HPI0013B-BOO-LF*SWS5170A-NCC-LF	1.9E-7	1
S_2*HPI0013B-BOO-LF*SWS4144A-VCC-LF	1.9E-7	1
S_2*HPI0013B-PMD-LF*SWS5171A-NCC-LF	1.9E-7	1
S_2*HPI0013B-PMD-LF*SWS5170A-NCC-LF	1.9E-7	1
S_2*HPI0013B-PMD-LF*SWS4144A-VCC-LF	1.9E-7	1
S_2*SWS5206A-NCC-LF*SWS5208B-NCC-LF	1.9E-7	1
S_2*SWS5206A-NCC-LF*SWS5163B-NCC-LF	1.9E-7	1
S_2*SWS5206A-NCC-LF*SWS5162B-NCC-LF	1.9E-7	1
S_2*SWS5206A-NCC-LF*CCW3826N-NCC-LF	1.9E-7	1
S_2*SWS5206A-NCC-LF*CCW3825N-NTO-LF	1.9E-7	1
S_2*SWS5160A-NCC-LF*SWS5208B-NCC-LF	1.9E-7	1
S_2*SWS5160A-NCC-LF*SWS5163B-NCC-LF	1.9E-7	1
S_2*SWS5160A-NCC-LF*SWS5162B-NCC-LF	1.9E-7	1
S_2*SWS5160A-NCC-LF*CCW3826N-NCC-LF	1.9E-7	1
S_2*SWS5160A-NCC-LF*CCW3825N-NTO-LF	1.9E-7	1
S_2*CCW3823N-NTO-LF*SWS5208B-NCC-LF	1.9E-7	1
S_2*CCW3823N-NTO-LF*SWS5163B-NCC-LF	1.9E-7	1
S_2*CCW3823N-NTO-LF*SWS5162B-NCC-LF	1.9E-7	1
S_2*CCW3823N-NTO-LF*CCW3826N-NCC-LF	1.9E-7	1
S_2*CCW3823N-NTO-LF*CCW3825N-NTO-LF	1.9E-7	1
S_2*HPIOC13B-CBL-LF*ECCR1448-BCO-LF	1.5E-7	1
S_2*HPIOC13B-CBL-LF*ECCFCB48-BCO-LF	1.5E-7	1
S_2*HPI0013B-CBL-LF*ECCFANWE-CBL-LF	1.5E-7	1
S_2*HPI0013B-PMD-LF*ECCR1448-BCO-LF	1.4E-7	1
S_2*HPI0013B-PMD-LF*ECCFCB48-BCO-LF	1.4E-7	1
S_2*HPI0013B-BOO-LF*ECCR1448-BCO-LF	1.4E-7	1

Cut Sets	Freq. (/yr)	% of Sequence
S_2*HPI0013B-BOO-LF*ECCFCB48-BCO-LF	1.4E-7	1
S_2*HPI0013B-P-PRMN*ECCFANWE-CBL-LF	1.1E-7	.8
S_2*HPR0013B-PMD-LF*ECCFANWE-CBL-LF	1.0E-7	.8
S_2*HPI0013B-CBL-LF*SWS5171A-NCC-LF	6.9E-8	.5
S_2*HPI0013B-CBL-LF*SWS5170A-NCC-LF	6.9E-8	.5
S_2*HPI0013B-CBL-LF*SIS4144A-VCC-LF	6.9E-8	.5
S_2*HPI0406X-XOC-LF*ECCFANWE-CBL-LF	5.9E-8	.4
S_2*HPI0405X-CCC-LF*ECCFANWE-CBL-LF	5.5E-8	.4
S_2*RA-18*CCW3826N-NCC-OE*SWS5206A-NCC-CC	5.3E-8	.4
S_2*RA-18*CCW3826N-NCC-OE*SWS5160A-NCC-CC	5.3E-8	.4
S_2*HPI0013B-CBL-LF*ECCR1448-BCO-LF	5.0E-8	.4
S_2*HPI0013B-CBL-LF*ECCFCB48-BCO-LF	5.0E-8	.4
S_2*HPI0013B-P-PRMN*SWS5171A-NCC-LF	5.0E-8	.4
S_2*HPI0013B-P-PRMN*SWS5170A-NCC-LF	5.0E-8	.4
S_2*HPI0013B-P-PRMN*SIS4144A-VCC-LF	5.0E-8	.4
S_2*HPR0013B-PMD-LF*SWS5171A-NCC-LF	4.6E-8	.3
S_2*HPR0013B-PMD-LF*SWS5170A-NCC-LF	4.6E-8	.3
S_2*HPR0013B-PMD-LF*SIS4144A-VCC-LF	4.6E-8	.3
S_2*RA-20*SIS4144A-BOO-CC*HPI0C13B-CBL-LF	4.4E-8	.3
S_2*RA-20*SIS4144A-BOO-CC*HPI0013B-BOO-LF	4.0E-8	.3
S_2*RA-20*SIS4144A-BOO-CC*HPI0013B-PMD-LF	4.0E-8	.3
S_2*HPI0C13B-CBL-LF*ECCFANEA-FAN-LF	3.8E-8	.3
S_2*HPI0013B-P-PRMN*ECCR1448-BCO-LF	3.6E-8	.3
S_2*HPI0013B-P-PRMN*ECCFCB48-BCO-LF	3.6E-8	.3
S_2*HPI0013B-BOO-LF*ECCFANEA-FAN-LF	3.4E-8	.2
S_2*HPI0013B-PMD-LF*ECCFANEA-FAN-LF	3.4E-8	.2
S_2*HPI0C13B-CBL-LF*ECCFANEA-FANPRMN	3.4E-8	.2
S_2*HPR0013B-PMD-LF*ECCR1448-BCO-LF	3.4E-8	.2
S_2*HPR0013B-PMD-LF*ECCFCB48-BCO-LF	3.4E-8	.2
S_2*ECCFANEA-FANPRMN*HPI0013B-PMD-LF	3.2E-8	.2
S_2*ECCFANEA-FANPRMN*HPI0013B-BOO-LF	3.2E-8	.2
S_2*SIS4148X-CCC-LF*HPI0C13B-CBL-LF	2.7E-8	.2
S_2*HPI0406X-XOC-LF*SWS5171A-NCC-LF	2.7E-8	.2
S_2*HPI0406X-XOC-LF*SWS5170A-NCC-LF	2.7E-8	.2
S_2*HPI0406X-XOC-LF*SIS4144A-VCC-LF	2.7E-8	.2
S_2*SIS4148X-CCC-LF*HPI0013B-BOO-LF	2.5E-8	.2
S_2*SIS4148X-CCC-LF*HPI0013B-PMD-LF	2.5E-8	.2
S_2*HPI0405X-CCC-LF*SWS5171A-NCC-LF	2.5E-8	.2
S_2*HPI0405X-CCC-LF*SWS5170A-NCC-LF	2.5E-8	.2
S_2*HPI0405X-CCC-LF*SIS4144A-VCC-LF	2.5E-8	.2
S_2*SWSTD13-LF*CCW3826N-NCC-OE	2.3E-8	.2
S_2*CCWHP13C-H-PRMN*ECCFANWE-CBL-LF	2.1E-8	.2
	1.2E-5	86

Term Descriptions

S_2 = Small-small LOCA; f = 2.1E-2/yr.

CCW0258X-XOC-LF = Local fault of CCW valve resulting in common mode failure of all LPSR and HPSR pump seal cooling and pump failure in the recirculation phase; p = 3.6E-5.

Term Descriptions (Cont.)

CCW3826N-NCC-OE = Failure of the operator to open CCW HTX#12 outlet valve resulting in failure of CCW HTX #12, this fails 1/2 of CCW; p = 1E-2.

SWS5206A-NCC-LF = Local fault of salt water valve fails CCW HTX #11 cooling resulting in failure of 1/2 of CCW; p = 3E-3.

SWS5160A-NCC-LF = Local fault of salt water valve fails CCW HTX #11 cooling resulting in failure of 1/2 of CCW; p = 3E-3.

CCW3823N-NTO-LF = Local fault of bypass valve on CCW HTX #11 results in failure of heat removal, fails 1/2 of CCW; p = 3E-3.

SWS5206A-NCC-CC = Control fault of salt water valve fails CCW HTX #11 cooling resulting in failure of 1/2 of CCW; p = 2.5E-3.

SWS5160A-NCC-CC = Control fault of salt water valve fails CCW HTX #11 cooling resulting in failure of 1/2 of CCW; p = 2.5E-3.

HPIOC13B-CBL-LF = Failure of control cable to HPSI pump #13, p = 3.3E-3.

HPI0013B-BOO-LF = Failure of HPSI pump #13 power breaker to close; p = 3E-3.

HPI0013B-PMD-LF = Local fault of HPSI pump #13; p = 3E-3.

ECCFANWE-CBL-LF = Failure of power cable to ESF room 11 room coolers, fails HPSR pumps #11 and #12 and CSSR pump #11; p = 6.6E-3.

SWS5171A-NCC-LF = Failure of salt water valve results in failure of ESF pump room cooling and fails HPSR pump #11 and #12 and CSSR pump #11; p = 3E-3.

SWS5170A-NCC-LF = Failure of salt water valve results in failure of ESF pump room cooling and fails HPSR pump #11 and #12 and CSSR pump #11; p = 3E-3.

SIS4144A-VCC-LF = Local fault of sump valve fails suction to HPSR pumps #11 and #12 and CSSR pump #11, p = 3E-3.

Term Descriptions (Cont.)

SWS5208B-NCC-LF = Failure of salt water valve fails cooling to CCW HTX #12 failing 1/2 of CCW; p = 3E-3.

SWS5163B-NCC-LF = Failure of salt water valve fails cooling to CCW HTX #12 failing 1/2 of CCW; p = 3E-3.

SWS5162B-NCC-LF = Failure of salt water valve fails cooling to CCW HTX #12 failing 1/2 of CCW; p = 3E-3.

CCW3826N-NCC-LF = Local fault of outlet valve on CCW HTX #12 fails 1/2 of CCW; p = 3E-3.

CCW3825N-NTO-LF = Local fault of CCW HTX #12 bypass valve results in failure to remove heat, fails 1/2 of CCW; p = 3E-3.

ECCR1448-BCO-LF = Local fault of power breaker for ESF room #11 cooling, fails HPSR pumps #11 and #12 and CSSR pump #11 in recirculation; p = 2.2E-3.

ECCFCB48-BCO-LF = Local fault of power breaker for ESF room #11 cooling, fails HPSR pumps #11 and #12 and CSSR pump #11 in recirculation; p = 2.2E-3.

HPI0013B-CBL-LF = Failure of HPSI pump #13 power cable; p = 1.1E-3.

HPI0013B-P-PRMN = Maintenance of HPSI pump #13; p = 7.9E-4.

HPI0406X-XOC-LF = Failure of HPSI pump #13 discharge valve; p = 4.3E-4.

HPI0405X-CCC-LF = Failure of HPSI pump #13 discharge valve; p = 4.3E-4.

RA-18 = Failure of operator to manually open SWS pneumatic valves; p = .1.

RA-20 = Failure of operator to manually open containment sump valve, fails 1/2 of HPSR and CSSR pump suction; p = 0.25.

SIS4144A-BOO-CC = Control circuit fault of sump valve fails suction to HPSR pumps #11 and #12 and CSSR pump #11; p = 2.5E-3.

ECCFANEA-FAN-LF = Local fault of room cooling fans in ESF room #11, fails HPSR pumps #11 and #12 and CSSR pump #11; p = 5.4E-4.

Term Descriptions (Cont.)

ECCFANEA-FANPRMN = Maintenance of room cooling fans in ESF room #11 fails HPSR pumps #11 and #12 and CSSR pump #11 p = 4.9E-4.

SIS4148X-CCC-LF = Failure of valve in sump fails suction to HPSR pumps #11 and #12 and CSSR #11; p = 4E-4.

SWSTD13-LF = Short in one-second time delay in salt water pump #13 results in failure of salt water pump #11 failing heat removal to CCW HTX #11, fails 1/2 of CCW; p = 1.1E-4.

CCWHP13C-H-PRMN = Maintenance of HPSR pump #13 heat exchanger; p = 1.6E-4.

8.1.3.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 3.3E-5/yr. All of the most significant cut sets involve failure of pump seal or pump room cooling. For pump seal cooling, since only CCW heat exchanger #11 is normally in service, the most important recovery action is for the operator to manually open the discharge valve on CCW heat exchanger #12 in order to place it in operation (CCS3826N-NCC-OE, p = .01). For pump room cooling, the operator can manually start the pump room coolers for control faults (local) (RA-17, p =.01). If the sump valves fail due to control faults, the operator can manually open the valves (local) (RA-20, p = .25). The application of recovery actions reduces the sequence frequency to 1.4E-5/yr.

It is assumed in this sequence that the operator must go to recirculation from the sump in order to continue cooling the plant. It is possible for shutdown cooling to be used if the plant is cooled down fast enough so that recirculation from the sump is never needed. However, it is unclear whether or not the operators would be directed to do this in an accident situation, and recovery credit was not given for this action. Also, since the LPSR and CSS pumps require the same room and seal cooling support as the HPSR pumps, the support system failures which dominate this sequence would fail this mode of operation as well.

Possibly significant conservatisms exists for this sequence:

1. CCW seal cooling failure is assumed to fail the pumps. Recent calculations show possibly two hours would be necessary to fail the seals and, even then, this might not fail the pumps. If the pumps did not fail due to seal cooling failure, the sequence frequency would be reduced to 1.0E-5/yr.

2. Room cooling needs are based on all pumps running. For this size LOCA, all but one pump would be shut down. This would significantly reduce the heat up rate. If the pumps did not fail due to room cooling failure, the sequence frequency would be reduced to 1.2E-5/yr.

3. If both of the above conservatisms are combined, the final sequence frequency would reduce to approximately 1.5E-6/yr.

8.1.3.4 Engineering Insights

About 25% of the sequence frequency is due to failures of HPSI pump #13 combined with failure of pump room cooling to ESF room #11. The reason that pump room cooling is so significant is that the system is not tested often (on the average of twice a year). This means that the average time a fault could be expected to exist is about three months (i.e., one half the test interval) and that any time-dependent failures are going to have an unavailability about six times that for a similar component tested monthly.

About 40% of the sequence frequency is due to cut sets involving component cooling water faults. The largest contributors being: (1) the failure of a single valve in the CCW return line for all HPSR and LPSR pump coolers which would result in failure of all HPSR and HPSR pumps, and (2) the failure of the operator to open the outlet valve on CCW heat exchanger #12 from the control room combined with some other single failure of CCW heat exchanger #11.

8.1.4 Sequence S_2-52 (S_2FH)

8.1.4.1 Description

In this sequence, a Small-small LOCA (S_2) occurs and is followed by successful scram and operation of AFW and HPSI providing both secondary heat removal and makeup. When the RWT depletes and switchover to recirculation occurs (anywhere from 4 to 12 hours into the accident), HPSR (H) and CSSR (F) fail. Due to the lack of primary makeup, the core then uncovers and melt ensues. CARCS succeeds and cools the containment.

The sequence frequency is estimated as 1.1E-5/yr and contributes 9% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.4.2 Dominant Cut Sets

Because of the large number of cut sets of relatively equal value which comprise this sequence event after the application of recovery, only the cut sets whose frequency is greater than 2.9E-8/yr are listed here. These cut sets comprise 79% of the

sequence frequency. A more detailed list of cut sets for all the dominant sequences can be found in Appendix C.

Cut Sets	Freq. (/yr)	% of Sequence
S_2*ECCFANWE-CBL-LF*ECCFANWW-CBL-LF	9.2E-7	8
S_2*SWS5173B-NCC-LF*ECCFANWE-CBL-LF	4.2E-7	4
S_2*SIS4145B-VCC-LF*ECCFANWE-CBL-LF	4.2E-7	4
S_2*SWS5171A-NCC-LF*ECCFANWW-CBL-LF	4.2E-7	4
S_2*SWS5170A-NCC-LF*ECCFANWW-CBL-LF	4.2E-7	4
S_2*SIS4144A-VCC-LF*ECCFANWW-CBL-LF	4.2E-7	4
S_2*ECCFANWE-CBL-LF*ECCR0448-BCO-LF	3.0E-7	3
S_2*ECCFANWE-CBL-LF*ECCCB048-BCO-LF	3.0E-7	3
S_2*ECCR1448-BCO-LF*ECCFANWW-CBL-LF	3.0E-7	3
S_2*ECCFCB48-BCO-LF*ECCFANWW-CBL-LF	3.0E-7	3
S_2*RAS-RSPLX-CM*OP-FL-MN-RAS	2.9E-7	3
S_2*SIS4145B-VCC-LF*SWS5171A-NCC-LF	1.9E-7	2
S_2*SIS4145B-VCC-LF*SWS5170A-NCC-LF	1.9E-7	2
S_2*SWS5173B-NCC-LF*SWS5171A-NCC-LF	1.9E-7	2
S_2*SWS5173B-NCC-LF*SWS5170A-NCC-LF	1.9E-7	2
S_2*SIS4144A-VCC-LF*SIS4145B-VCC-LF	1.9E-7	2
S_2*SIS4144A-VCC-LF*SWS5173B-NCC-LF	1.9E-7	2
S_2*SIS5171A-NCC-LF*ECCR0448-BCO-LF	1.4E-7	1
S_2*SIS5171A-NCC-LF*ECCCB048-BCO-LF	1.4E-7	1
S_2*SWS5170A-NCC-LF*ECCR0448-BCO-LF	1.4E-7	1
S_2*SWS5170A-NCC-LF*ECCCB048-BCO-LF	1.4E-7	1
S_2*SIS4144A-VCC-LF*ECCR0448-BCO-LF	1.4E-7	1
S_2*SIS4144A-VCC-LF*ECCCB048-BCO-LF	1.4E-7	1
S_2*ECCR1448-BCO-LF*SWS5173B-NCC-LF	1.4E-7	1
S_2*ECCR1448-BCO-LF*SIS4145B-VCC-LF	1.4E-7	1
S_2*ECCFCB48-BCO-LF*SWS5173B-NCC-LF	1.4E-7	1
S_2*ECCFCB48-BCO-LF*SIS4145B-VCC-LF	1.4E-7	1
S_2*ECCR1448-BCO-LF*ECCR0448-BCO-LF	1.0E-7	.9
S_2*ECCR1448-BCO-LF*ECCCB043-BCO-LF	1.0E-7	.9
S_2*ECCFCB48-BCO-LF*ECCR0448-BCO-LF	1.0E-7	.9
S_2*ECCFCB48-BCO-LF*ECCCB048-BCO-LF	1.0E-7	.9
S_2*RA-20*SIS4145B-BOO-CC*ECCFANWE-CBL-LF	8.7E-8	.9
S_2*RA-20*SIS4144A-BOO-CC*ECCFANWW-CBL-LF	8.7E-8	.8
S_2*ECCFANWE-CBL-LF*ECCFANWB-FAN-LF	7.5E-8	.7
S_2*ECCFANWW-CBL-LF*ECCFANEA-FAN-LF	7.5E-8	.7
S_2*ECCFANWE-CBL-LF*ECCFANWB-FANPRMN	6.8E-8	.6
S_2*ECCFANWW-CBL-LF*ECCFANEA-PANPRMN	6.8E-8	.6
S_2*ECCFANWE-CBL-LF*SIS4149X-CCC-LF	5.5E-8	.5
S_2*ECCFANWW-CBL-LF*SIS4148X-CCC-LF	5.5E-8	.5
S_2*SWS0196X-XOC-LF	5.0E-8	.5
S_2*RA-20*SIS4145B-CBL-LF*ECCFANWE-CBL-LF	4.2E-8	.4
S_2*RA-20*SIS4144A-CBL-LF*ECCFANWW-CBL-LF	4.2E-8	.4
S_2*RA-20*SIS4145B-BOO-CC*SWS5171A-NCC-LF	3.9E-8	.4
S_2*RA-20*SIS4145B-BOO-CC*SWS5170A-NCC-LF	3.9E-8	.4
S_2*RA-20*SIS4145B-BOO-CC*SWS4144A-VCC-LF	3.9E-8	.4
S_2*RA-20*SIS4144A-BOO-CC*SWS5173B-NCC-LF	3.9E-8	.4
S_2*RA-20*SIS4144A-BOO-CC*SIS4145B-VCC-LF	3.9E-8	.4

Cut Sets	Freq. (/yr)	% of Sequence
S_2*RA-18*SWS5175B-NOC-CC*ECCFANWE-CBL-LF	3.5E-8	.4
S_2*RA-18*SWS5174B-NOC-CC*ECCFANWE-CBL-LF	3.5E-8	.4
S_2*RA-18*SWS5173B-NCC-CC*ECCFANWE-CBL-LF	3.5E-8	.4
S_2*RA-18*SWS5171A-NCC-CC*ECCFANWW-CBL-LF	3.5E-8	.4
S_2*RA-18*SWS5170A-NCC-CC*ECCFANWW-CBL-LF	3.5E-8	.4
S_2*ECCFANWB-FAN-LF*SIS4144A-VCC-LF	3.4E-8	.3
S_2*ECCFANWB-FAN-LF*SIS5171A-NCC-LF	3.4E-8	.3
S_2*ECCFANWB-FAN-LF*SWS5170A-NCC-LF	3.4E-8	.3
S_2*ECCFANEA-FAN-LF*SWS5173B-NCC-LF	3.4E-8	.3
S_2*ECCFANEA-FAN-LF*SIS4145B-VCC-LF	3.4E-8	.3
S_2*RA-20*SIS4144A-BOO-CC*SIS4145B-BOO-CC	3.3E-8	.3
S_2*ECCFANWB-FANPRMN*SIS4144A-VCC-LF	3.1E-8	.3
S_2*ECCFANWB-FANPRMN*SIS5170A-NCC-LF	3.1E-8	.3
S_2*ECCFANWB-FANPRMN*SIS5171A-NCC-LF	3.1E-8	.3
S_2*ECCFANEA-FANPRMN*SIS5173B-NCC-LF	3.1E-8	.3
S_2*ECCFANEA-FANPRMN*SIS4145B-VCC-LF	3.1E-8	.3
S_2*RA-20*SIS4145B-BOO-CC*ECCR1448-BCO-LF	2.9E-8	.3
S_2*RA-20*SIS4145B-BOO-CC*ECCFCB48-BCO-LF	2.9E-8	.3
S_2*RA-20*SIS4144A-BOO-CC*ECCR0448-BCO-LF	2.9E-8	.3
S_2*RA-20*SIS4144A-BOO-CC*ECCCB048-BCO-LF	2.9E-8	.3
	8.8E-6	79

Term Descriptions

S_2 = Small-small LOCA; f = 2.1E-2/yr.

ECCFANWE-CBL-LF = Local fault of power cable to ESF pump room #11 fan cooling, fails HPSR pumps #11 and #12 and CSSR pump #11; p = 6.6E-3.

ECCFANWW-CBL-LF = Local fault of power cable to ESF pump room #12 fan cooling, fails HPSR pump #13 and CSSR pump #12; p = 6.6E-3.

SWS5173B-NCC-LF = Local fault of SWS valve, fails ESF pump room cooler #12 failing HPSR pump #13 and CSSR pump #12; p = 3E-3.

SIS4145B-VCC-LF = Local fault of sump valve, fails suction to HPSR pump #13 and CSSR pump #12; p = 3E-3.

SWS5171A-NCC-LF = Local fault of SWS valve, fails ESF pump room cooler #11 failing HPSR pumps #11 and #12 and CSSR pump #11, p = 3E-3.

SWS5170A-NCC-LF = Local fault of SWS valve, fails ESF pump room cooler #11 failing HPSR pumps #11 and #12 and CSSR pump #11, p = 3E-3.

Term Descriptions (Cont.)

SIS4144A-VCC-LF = Local fault of sump valve, fails suction to HPSR pumps #11 and #12 and CSSR pump #11; p = 3E-3.

ECCR0448-BCO-LF = Local fault of breaker, fails power to ESF pump room #12 coolers failing HPSR pump 13 and CSSR pump #12; p = 2.2E-3.

ECCCB048-BCO-LF = Local fault of breaker, fails power to ESF pump room #12 coolers failing HPSR pump 13 and CSSR pump #12; p = 2.2E-3.

ECCR1448-BCO-LF = Local fault of breaker, fails power to ESF pump room #11 coolers failing HPSR pumps 11 and 12 and CSSR pump #11; p = 2.2E-3.

ECCFCB48-BCO-LF = Local fault of breaker, fails power to ESF pump room #11 coolers failing HPSR pumps 11 and 12 and CSSR pump #11; p = 2.2E-3.

RAS-RSPLX-CM = Common mode sensor failure, fails auto recirculation realignment from RWT to sump, fails all ESF pumps; p = 1.4E-3.

OP-FL-MN-RAS = Operator fails to realign ESF pump from RWT to sump, fails all ESF pumps in recirculation; p = 1E-2.

RA-20 = Operator fails to manually open a sump MOV resulting in failure of pump suction to either HPSR pumps #11 and #12 and CSSR pump #11 or HPSR pump #13 and CSSR pump #12; p = .25.

SIS4145B-BOO-CC = Control circuit fault of sump valve, fails suction to HPSR pump #13 and CSSR pump #12; p = 2.5E-3.

SIS4144B-BOO-CC = Control circuit fault of sump valve, fails suction to HPSR pumps #11 and #12 and CSSR pump #11; p = 2.5E-3.

ECCFANWB-FAN-LF = Local fault of ESF pump room #12 cooling fans, fails HPSR pump #13 and CSSR pump #12; p = 5.4E-4.

ECCFANEA-FAN-LF = Local fault of ESF pump room #11 cooling fans, fails HPSR pumps #11 and #12 and CSSR pump #11; p = 5.4E-4.

Term Description (Cont.)

ECCFANWB-FANPRMN = Maintenance of ESF pump room #12 cooling fans, fans HPSR pump #13 and CSSR pump #12; p = 4.9E-4.

ECCFANEA-FANPRMN = Maintenance of ESF pump room #11 cooling fans, fails HPSR pumps #11 and #12 and CSSR pump #11; p = 4.9E-4.

SIS4149X-CCC-LF = Local fault of sump valve, fails suction to HPSR pump #13 and CSSR pump #12; p = 4E-4.

SIS4148X-CCC-LF = Local fault of sump valve, fails suction to HPSR pumps #11 and #12 and CSSR pump #11; p = 4E-4.

SWS0196X-XOC-LF = Local fault of SWS ESF and CCW HTX outlet valve failing heat removal from all ESF pump room coolers and both CCW HTXs. This fails all HPSR, LPSR, and CSSR pumps and both shutdown heat exchangers; p = 2.4E-6.

SIS4145B-CBL-LF = Failure of sump MOV power cable, fails suction to HPSR pump #13 and CSSR pump #12; p = 1.1E-3.

SIS4144A-CBL-LF = Failure of sump MOV power cable, fails suction to HPSR pump #11 and #11 and CSSR pump #11; p = 1.1E-3.

RA-18 = Operator fails to manually open SWS pneumatic valves to an ESF room cooler, fails one room cooler; p = .1.

SWS5175B-NOC-CC = Control fault of ESF pump room cooler #12 outlet valve, fails HPSR pump #13 and CSSR pump #12, p = 2.5E-3.

SWS5174B-NOC-CC = Control fault of ESF pump room cooler #12 outlet valve, fails HPSR pump #13 and CSSR pump #12, p = 2.5E-3.

SWS5173B-NCC-CC = Control fault of ESF pump room cooler #12 inlet valve, fails HPSR pump #13 and CSSR pump #12; p = 2.5E-3.

SWS5171A-NCC-CC = Control fault of ESF pump room cooler #11 outlet valve, fails HPSR pumps #11 and #12 and CSSR pump #11; p = 2.5E-3.

SWS5170A-NCC-CC = Control fault of ESF pump room cooler #11 inlet valve, fails HPSR pumps #11 and #12 and CSSR pump #11; p = 2.5E-3.

8.1.4.3 Major Assumptions and Recovery Actions

The initial screening value for the sequence was 5.7E-5/yr. The recovery actions involve either: (1) manually starting the ECCS room cooling fans given auto-actuation has failed (RA-17, p = .01), (2) manually opening the sump MOVs given valve control circuit faults (RA-20, p = .25) or (3) manually opening SWS valves to the ESF pump room coolers given valve control circuit faults (RA-18, p = .1). The application of recovery actions reduces the sequence frequency to 1.1E-5/yr.

Again, as with S_2-50, if only one pump is running, then failure of room cooling might not be a failure of the pumps and the sequence frequency would be about 1.1E-6/yr. Also, the operators are assumed to go to recirculation, not shutdown cooling.

8.1.4.4 Engineering Insights

Over 85% of frequency of this sequence involves cut sets with ESF pump room cooling failures. As discussed for the previous sequence, the long test interval for the room cooling system results in the unavailabilities of components with time-dependent failure modes being six times that of a similar component with a monthly test interval, thus increasing their contribution to this sequence.

8.1.5 Sequence T_2-82 (T_2L)

8.1.5.1 Description

In this sequence, a loss of PCS (T_2) occurs and is followed by a loss of AFW (L). The reactor has scrammed and CARCS and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for use of feed and bleed due to information presented in References 24 and 25. Recent calculations done by EG&G for the Station Blackout program [26] indicate that 86 minutes is available to start an AFW pump in order to prevent core uncovery.

The frequency of this sequence is estimated to be 7.1E-6/yr and it contributes 6% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.5.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
T_2*RA-1*AFW0161-XOC-LF	2.8E-6	39
T_2*RA-3*AFWP11-PTD-LF*AFWP13-PMD-LF	5.6E-7	8

Cut Set	Frequency (/yr)	% of Sequence
T_2*RA-3*AFWP11-PTD-LF*CBP13-BOO-LF	4.5E-7	6
T_2*RA-3*AFWP11-PTD-PRMN*AFWP13-PMD-LF	4.4E-7	6
T_2*RA-3*AFWP11-PTD-PRMN*CBP13-BOO-LF	3.6E-7	5
T_2*RA-2*ELC0011A-INV-LF*AFWP11-PTD-LF	1.8E-7	3
T_2*RA-2*ELC0011A-INV-LF*AFW4070B-NCC-LF	1.5E-7	2
T_2*RA-2*ELC0011A-INV-LF*AFWP11-PTD-PRMN	1.4E-7	2
T_2*RA-3*AFWP11-PTD-LF*AFWP13-PMD-PRMN	1.2E-7	2
T_2*RA-3*AFWP13-PMD-LF*AFWS903A-NOC-LF	1.2E-7	2
T_2*RA-3*AFWP13-PMD-LF*AFW3987A-NOC-LF	1.2E-7	2
T_2*RA-3*ESFSQNCA-LOG-LF*AFWP11-PTD-LF	9.6E-8	1
T_2*RA-3*CBP13-BOO-LF*AFWS903A-NOC-LF	9.6E-8	1
T_2*RA-3*CBP13-BOO-LF*AFW3987A-NOC-LF	9.6E-8	1
	5.8E-6	82

Term Descriptions

T_2	=	Loss of PCS transient; f = .8/yr.
RA-1	=	Operator fails to realign AFW to CST #11 and start locked-out turbine-driven AFW pump #12; p = .1.
RA-2	=	Operator fails to manually actuate AFW motor-driven pump #13 given failure of auto start; p = .02.
RA-3	=	Operator fails to manually start locked-out AFW turbine-driven pump #12; p = .04.
AFW0161-XOC-LF	=	Local fault of CST #12 AFW suction valve, fails all operating AFW pumps; p = 3.6E-5.
AFWP11-PTD-LF	=	AFW turbine-driven pump #11, local fault; p = 4.7E-3.
AFWP11-PTD-PRMN	=	AFW turbine-driven pump #11, maintenance; p = 3.7E-3.
AFWS903A-NOC-LF	=	Local fault of steam admission valve to AFW turbine-driven pump #11; p = 1E-3.
AFW3987A-NOC-LF	=	Local fault of steam admission valve to AFW turbine-driven pump #11; p = 1E-3.
AFWP13-PMD-LF	=	AFW motor-driven pump #13, local fault; p = 3.7E-3.

Term Descriptions (Cont.)

AFWP13-PMD-PRMN	=	AFW motor-driven pump #13, maintenance; p = 3.7E-4.
CBP13-BOO-LF	=	AFW motor-driven pump #13, circuit breaker; p = 3E-3.
ELC0011A-INV-LF	=	11A vital AC bus, fails AFW turbine-driven steam admission valve 4071 due to no actuation signal and fails actuation of motor-driven AFW pump; p = 2.4E-3.
AFW4070B-NCC-LF	=	Local fault of Train B AFW turbine steam admission valve fails 1/2 of AFW steam supply; p = 4E-3.
ESFSQNCA-LOG-LF	=	Faults in ESFAS sequencer fail AFAS auto-actuation of AFW motor-driven pump #13; p = 6.4E-4.

8.1.5.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 1.8E-4/yr. The recovery actions for all cut sets involve recovering one train of AFW. These recovery actions are (1) manually starting the motor AFW pump from the control room (RA-2, p = .02), or (2) locally starting the locked out turbine pump #12 (RA-3, p = .04) and possibly realigning AFW suction to CST #11 (RA-1, p = .1). The application of these recovery actions reduces the sequence frequency to 7.1E-6/yr.

8.1.5.4 Engineering Insights

The major contributor to this sequence is the plugging failure of the single valve in the suction train of the AFW system. In addition to realigning the AFW suction to an alternate CST and starting the locked out turbine pump, it is also possible to recover by aligning unit 2's AFW system to unit 1; however, procedures have not yet been developed for this and, because of the chance that cold water might be injected into unit 2's steam generators through its open feedwater regulation valves, no credit was given for this unless it was the only action possible.

8.1.6 Sequence T_4-173 (T_4KU)

8.1.6.1 Description

This sequence is a T_4 (all other) transient followed by a failure to scram (K) and failure of emergency boration (U). The reactor vessel has survived the initial pressure transient due to an assessed PCS runback. The CE analyses [21] and NRC

analysis in support of the ATWS rule [22] state that greater than 10 minutes are available for the operator to initiate emergency boration. In this study, we have assessed that if the operator fails to start shutting the reactor down within 20-30 minutes, then core melt will result. The CARCS and/or CSSI systems succeed and cool the containment.

This sequence frequency is estimated as 6.7E-5/yr and contributes 5% of the total core melt frequency. The dominant contributors to this sequences are outlined below.

8.1.6.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
T_4*K*CVCSTART-HSF-OE	5.1E-6	76
T_4*K*CVCOC12B-P-PRMN *CVCOC13X-P-PRMN	7.0E-7	10
T_4*K*CVC0514B-VCC-LF	3.1E-7	5
T_4*K*CVCR514B-BOO-CC	2.6E-7	4
T_4*K*CVC0514B-CBL-LF	1.1E-7	2
	6.5E-6	96

Term Descriptions

T_4 = All other transients requiring reactor trip, for failure to scram only 50% result in situations which demand immediate shutdown and result in severe pressure transients; f = 3.4/yr.

K = Failure to scram; p = 3E-5.

CVCSTART-HSF-OE = Failure of the operator to initiate emergency boration within 20-30 minutes; p = 0.05.

CVCOC12B-P-PRMN = Maintenance of charging pump #12; p = 8.2E-2.

CVCOC13X-P-PRMN = Maintenance of charging pump #13; p = 8.2E-2.

CVC0514B-VCC-LF = Local Fault of CVCS MOV 514 (common mode failure of CVCS); p = 3E-3.

CVCR514B-BOO-CC = Control circuit fault of CVCS MOV 514 (common mode failure of CVCS); p = 2.5E-3.

CVC0514B-CBL-LF = Power cable to CVCS MOV 514 fails open (common mode failure of CVCS): p = 1.1E-3.

8.1.6.3 Major Assumptions and Recovery Actions

The T_4 transient group is a collection of all transient initiators which do not affect safety system reliability or cause a loss of PCS. For sequences where reactor scram is successful, all the initiators require the same safety system response; however, for sequences involving failure to scram, the response of the PCS system may vary depending upon the specific initiator. For some initiators such as closure of an MSIV, increase in feedwater flow, partial loss of feedwater, total loss of RCS flow, condenser leakage, leakage in secondary system, S/G relief values opening, and trips from unknown causes, we expect an independent turbine trip and runback of the PCS system. While for initiators such as spurious scram signals, rod drop, high or low pressurizer pressure, boron dilution, loss of RCS flow in one loop, or pressurizer spray failure, we expect the PCS to stay at full flow. The original grouping of the transients was done assuming successful scram and, therefore, did not take this variability into account. In the quantification of the failure to scram sequences, the assessment was made that only 50% of the T_4 transients resulted in a turbine trip and subsequent PCS runback or had characteristics roughly similar to a turbine trip. If the PCS were to remain at full flow, then reactor heat removal would be successful and the plant would be in a temporarily safe condition. However, some subsequent actions would have to be taken to terminate the incident.

Under the general rules for recovery adopted in this study, only one operator recovery action is allowed unless: (1) sufficient time and indication is available for the operators to perform multiple actions; or (2) multiple actions are necessary to recover the sequence to a non-core melt. In this sequence the recovery action is the operator initiation of emergency boration and due to the high stress and short time, no other recovery actions were allowed.

Given the high stress in the failure to scram scenario, the operator failure to perform an appropriate action is typically assumed to be 0.1 in past PRAs (our generic recovery model assumes 0.1 at 10 minutes). However, the thermal-hydraulic analyses [21] show that the operator should have longer than 10 minutes. After examining the thermal-hydraulic characteristics of the sequence and the various uncertainties in system response and phenomenology, it was judged that some operator action would be necessary within 20-30 minutes. A THERP analyses of the emergency boration procedure is presented

in Appendix B.19 which leads to a value of 0.05 and this value corresponds to the 0.05 probability of operator failure in 20-30 minutes from our generic recovery model.

8.1.6.4 Engineering Insights

There are substantial uncertainties associated with the accident progression for this sequence. The CE analyses [21] show that after a moderately severe pressure transient (i.e., less than ~3400 psia) with the loss of ~1/3 of the amount of water necessary to uncover the core, a quasi-equilibrium state is reached by about 10 minutes with pressure at/or about 1800 psia and increasing slowly. Given no further coolant loss, possibly several hours, would be available for subsequent operator action. However, no long-term analyses have been done on ATWS sequences and the long-term response can only be estimated based on the above runs. Also, there is a question as to whether the reactor coolant pumps (RCPs) will trip.

The fact that saturation conditions will be reached in some parts of the core does not necessarily lead to the cavitation of the RCP's. If the pumps do not trip, then the amount of voiding in the core will be reduced and the pressure may actually increase back to the PORV setpoint due to the power remaining slightly higher than the secondary heat removal rate, though this remains uncertain. Given that coolant loss through the PORVs occurs, it is estimated that core uncovery (which is equivalent to core melt in our analysis) will occur at greater than 40 minutes. In order to give time for the boron to begin reducing pressure about 5-10 minutes would be needed. Therefore, for this analysis, operator initiation of emergency boration would need to occur at greater than 20-30 minutes. Long-term analysis for various initiators, times of boration initiation and boron mixing assumption, RCP response, and secondary heat removal rates would be necessary to resolve the timing questions. Follow-on analysis by the SASA program is planned in order to determine the long-term characteristics of this sequence.

The plant has implemented a new emergency procedure explicitly for ATWS which directs the operator to (1) trip the reactor manually, (2) de-energize the motor-generator sets, and (3) to initiate emergency boration. However, the common mode failure of the operators in a high stress situation to identify the failure to scram and take action dominates this sequence. The value of 0.05 for operator failure in the high stress situation remains unchanged, based on our generic recovery model, and the sequence frequency is not significantly affected by the new procedure. Although it appears, that with this new procedure and improved operator training, some mitigation of this sequence could be obtained.

8.1.7 Sequence T_4-147 (T_4ML)

8.1.7.1 Description

In this sequence, a T_4 (all other) transient occurs and is followed by a loss of PCS (M) and AFW (L). The reactor has scrammed and CARCS and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to information presented in References 24 and 25. Recent calculations done by EG&G for the Station Blackout program [26] indicate that 86 minutes are available to start an AFW pump in order to prevent core uncovery.

The sequence frequency is estimated as 6.3E-6/yr and contributes 5% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.7.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
T_4*RA-2*ELC0011A-INV-LF*AFWP11-PTD-LF	1.5E-6	24
T_4*RA-2*ELC0011A-INV-LF*AFW4070B-NCC-LF	1.3E-6	21
T_4*RA-2*ELC0011A-INV-LF*AFWP11-PTD-PRMN	1.2E-6	19
T_4*RA-2*ELC0011A-INV-LF*AFWP11-PTD-PRTS	4.6E-7	7
T_4*RA-2*ELC0011A-INV-LF*AFWS903A-NOC-LF	3.3E-7	5
T_4*RA-2*ELC0011A-INV-LF*AFW3987A-NOC-LF	3.3E-7	5
T_4*RA-1*PCS-LF*AFW0161-XOC-LF	1.2E-7	2
T_4*RA-2*ELC0011A-INV-LF*AFW0103-X-FRFT	6.5E-8	1
T_4*RA-2*ELC0012B-INV-LF*AFALOGCA-LOG-LF	6.5E-8	1
T_4*RA-2*ELC0011A-INV-LF*AFALOGCB-LOG-LF	6.5E-8	1
T_4*RA-2*ELC0011A-INV-LF*AFW4530-N-PRMN	6.5E-8	1
T_4*RA-2*ELC0011A-INV-LF*AFW4520-N-PRMN	6.5E-8	1
T_4*RA-1*ELC0011A-INV-LF*AFW0161-XOC-LF	5.8E-8	1
T_4*RA-1*ELC0012B-INV-LF*AFW0161-XOC-LF	5.8E-8	1
T_4*RA-2*ELC0011A-INV-LF*AFWM911X-X-PRMN	5.2E-8	1
T_4*RA-2*ELC0011A-CBL-LF*AFWP11-PTD-LF	5.2E-8	1
	5.8E-6	92

Term Descriptions

T_4 = All other transients requiring reactor trip; f = 6.8/yr.

RA-2 = Operator fails to manually start AFW motor-driven pump from control room given that auto-actuation failed; p = .02.

Term Descriptions (Cont.)

ELC0011A-INV-LF = Local fault of vital AC inverter #11 causes failure of AFAS actuation of motor-driven AFW pump and AFW turbine-driven pump steam admission valve 4071, one feedwater regulating valve fails closed, one feedwater bypass valve fails full open, one main feedwater pump minimum flow recirculation valve fails full open, and one turbine bypass valve fails closed. If operating at power, a low suction trip of main feedwater pumps will occur. If operating at 5% in runback mode, may still get a pump trip depending on dynamics of suction pressure and steam pressure; p = 2.4E-3.

AFWP11-PTD-LF = Local fault of AFW turbine-driven pump #11; p = 4.7E-3.

AFW4070B-NCC-LF = Local fault of AFW steam admission valve, fails 1/2 of steam supply; p = 4E-3.

AFWP11-PTD-PRMN = Maintenance of AFW turbine-driven pump #11; p = 3.7E-3.

AFWP11-PTD-PRTS = AFW turbine-driven pump #11 unavailable due to test; p = 1.4E-3.

AFWS903A-NOC-LF = Local fault of valve in steam admission line to AFW turbine-driven pump #11; p = 1E-3.

AFW3987A-NOC-LF = Local fault of valve in steam admission line to AFW turbine-driven pump #11; p = 1E-3.

RA-1 = Operator fails to realign AFW suction to CST #11 and start locked-out AFW turbine-driven pump #12, all actions must be done locally; p = 0.1.

PCS-LF = Local fault causes failure of PCS; p = 4.8E-3.

AFW0161-XOC-LF = Local fault of AFW suction valve results in cavitation failure of all operating AFW pumps; p = 3.6E-5.

Term Descriptions (Cont.)

AFW0103-X-FRFT	=	Failure to restore AFW turbine-driven pump #11 discharge valve from test; p = 2E-4.
ELC0012B-INV-LF	=	Local fault of vital AC inverter #12, results in similar effects to inverter #11 above except that the AFW motor-driven pump does not fail and AFW steam admission valve 4070 fails closed failing 1/2 AFW turbine pump steam supply; p = 2.4E-3.
AFALOGCA-LOG-LF	=	Local fault of AFAS logic unit fails actuation of motor-driven AFW pump and AFW steam admission valve 4071 failing 1/2 AFW turbine pump steam supply; p = 2E-4.
AFALOGCB-LOG-LF	=	Local fault of AFAS logic unit fails actuation of AFW steam admission valve 4070 failing 1/2 steam supply to AFW turbine pumps; p = 2E-4.
AFW4530-N-PRMN	=	Maintenance of feedwater valve fails delivery by both turbine-driven AFW pumps; p = 2E-4.
AFW4520-N-PRMN	=	Maintenance of feedwater valve fails delivery by both turbine-driven AFW pumps; p = 2E-4.
AFWM911X-X-PRMN	=	Maintenance of valve in AFW turbine-driven pump #11 steam admission line; p = 1.6E-4.
ELC0011A-CBL-LF	=	Local fault of cable from vital AC inverter #11, same effect as inverter fault above; p = 7.5E-5.

8.1.7.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 3.1E-4/yr. The important recovery action involved starting the AFW motor-driven pump from the control room given that auto actuation has failed (RA-2, p = .02). The application of this recovery action reduces the sequence frequency to 6.3E-6/yr.

8.1.7.4 Engineering Insights

The failure of the vital bus 11A inverter is postulated as causing PCS failure due to instabilities induced in the

feedwater flow; however, while this is true at ~80% flow, after a transient where PCS has run back, this is not necessarily true. If the failure occurred while the PCS was running back, it probably would cause the PCS to trip. If the inverter fault will not cause the PCS to trip, the sequence frequency becomes negligible.

8.1.8 Sequence T_1-81-65 (T_1Q-D"CC')

8.1.8.1 Description

This sequence is a loss of offsite power (T_1) followed by a transient-induced LOCA(Q). AFW works but HPSI (D"), CSSI(C') and CARCS(C) fail. Due to the lack of primary system makeup, the core uncovers in about 1 hour (see the EG&G Station Blackout Analysis [26]).

The frequency of this sequence is estimated to be 5.3E-6/yr and contributes 4% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.8.2 Dominant Cut Sets

Because of the large number of cut sets of relatively equal value which comprise this sequence even after the application of recovery, only cut sets where frequency is greater than 2.4E-8/yr are listed here. These cut sets comprise 71% of the sequence frequency. A more detailed list of cut sets for all the dominant sequences can be found in Appendix C.

Cut Sets	Freq. (/yr.)	% of Sequence
T_1*RA-LOSP1*ELC0021B-GEN-OPF *ELC0011A-GEN-LF	1.1E-6	21
T_1*RA-LOSP1*ELC0012B-GEN-LF *ELC0011A-GEN-LF	5.9E-7	9
T_1*RA-LOSP1*ELC0021B-GEN-OPF *ELC0011A-G-PRMN	1.4E-7	3
T_1*RA-LOSP1*ELC0021B-GEN-OPF *ELC0011A-G-FRFT	1.1E-7	2
T_1*RA-LOSP1*OP-FAIL-TO-ALIGN *ELC0011A-GEN-LF	9.5E-8	2
T_1*RA-LOSP1*SDSSQNCA-LOG-LF *ELC0021B-GEN-OPF	8.1E-8	2
T_1*RA-LOSP1*SRW1587A-NCC-LF *ELC0021B-GEN-OPF	6.4E-8	1
T_1*RA-LOSP1*ELC1103A-BOO-LF *ELC0021B-GEN-OPF	6.4E-8	1
T_1*RA-LOSP1*DGVCT11A-BOO-LF *ELC0021B-GEN-OPF	6.4E-8	1
T_1*RA-LOSP1*DGVOT11A-DCC-LF *ELC0021B-GEN-OPF	6.4E-8	1

Cut Sets	Freq. (/yr.)	% of Sequence
T_1*RA-LOSP1*DGVRC11A-DCO-LF *ELC0021B-GEN-OPF	6.4E-8	1
T_1*RA-LOSP1*DGVIN11A-DCC-LF *ELC0021B-GEN-OPF	6.4E-8	1
T_1*RA-LOSP1*SWS1105A-BOO-LF *ELC0021B-GEN-OPF	6.4E-8	1
T_1*RA-LOSP1*SRWA011A-BOO-LF *ELC0021B-GEN-OPF	6.4E-8	1
T_1*RA-LOSP1*ELC0012B-GEN-LF *ELC0011A-G-PRMN	6.2E-8	1
T_1*RA-LOSP1*ELC0011A-GEN-LF *ELC0012B-G-PRMN	6.2E-8	1
T_1*RA-LOSP1*ELC0021B-GEN-OPF *ELC1103A-BOO-CC	5.3E-8	1
T_1*RA-LOSP1*ELC0021B-GEN-OPF *SWS5210A-NTC-CC	5.3E-8	1
T_1*RA-LOSP1*ELC0021B-GEN-OPF *SWS5210A-NOC-CC	5.3E-8	.9
T_1*RA-LOSP1*ELC0012B-GEN-LF *ELC0011A-G-FRFT	4.8E-8	.9
T_1*RA-LOSP1*ELC0011A-GEN-LF *ELC0012B-G-FRFT	4.8E-8	.9
T_1*RA-LOSP1*SDSSQNCA-LOG-LF *ELC0012B-GEN-LF	3.6E-8	.7
T_1*RA-LOSP1*SDSSQNCB-LOG-LF *ELC0011A-GEN-LF	3.6E-8	.7
T_1*RA-LOSP1*ELC0021B-GEN-OPF *ELC0011A-G-PRTS	3.2E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *SRW1587A-NCC-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *ELC1103A-BOO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *DGVCT11A-BOO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *DGVOT11B-DCC-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *DGVRC11A-DCO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *DGVIN11A-DCC-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *SWS1105A-BOO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *SRWA011A-BOO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0011A-GEN-LF *SRW1588B-NCC-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0011A-GEN-LF *ELC1406B-BOO-LF	2.8E-8	.6
T_1*RA-LOSP1*ELC0011A-GEN-LF *DGVCT12C-BOO-LF	2.9E-8	.6

Cut Sets	Freq. (/yr.)	% of Sequence
T_1*RA-LOSP1*ELC0011A-GEN-LF *DGVOT12C-DCC-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0011A-GEN-LF *DGVRC12C-DCO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0011A-GEN-LF *DGVIN12C-DCC-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0011A-GEN-LF *SWS1405B-BOO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0011A-GEN-LF *SRWA012B-BOO-LF	2.9E-8	.6
T_1*RA-LOSP1*ELC0012B-GEN-LF *ELC1103A-BOO-CC	2.4E-8	.5
T_1*RA-LOSP1*ELC0012B-GEN-LF *SWS5210A-NTC-CC	2.4E-8	.5
T_1*RA-LOSP1*ELC0012B-GEN-LF *SWS5150A-NOC-CC	2.4E-8	.5
T_1*RA-LOSP1*ELC0011A-GEN-LF *ELC1406B-BOO-CC	2.4E-8	.5
T_1*RA-LOSP1*ELC0011A-GEN-LF *SWS5153B-NOC-CC	2.4E-8	.5
T_1*RA-LOSP1*ELC0011A-GEN-LF *SWS5212B-NTC-CC	2.4E-8	.5
	3.7E-6	71

Term Descriptions

T_1	=	Loss of Offsite Power; f = .14/yr.
RA-LOSP1	=	Non-recovery of offsite power within one hour; p = .45.
ELC0021B-GEN-OPF	=	Undeveloped event representing all diesel generator 21 faults, diverts DG #12 to Unit 2 and fails train B of AC power; p = .12.
ELC0011A-GEN-LF	=	Local fault of DG #11, fails train A of AC power; p = 5.4E-2.
ELC0012B-GEN-LF	=	Local fault of DG #12, fails train B of AC power; p = 5.4E-2.
ELC0011A-G-PRMN	=	Maintenance of DG #11, fails train A of AC power; p = 6.6E-3.
ELC0011A-G-FRFT	=	Failure to restore DG #11 following test, fails train A of AC power; p = 5E-3.
OP-FAIL-TO-ALIGN	=	Operator fails to align DG #12 to Unit 1, fails train B of AC power; p = 1E-2.

Term Descriptions (Cont.)

SDSSQNCA-LOG-LF	=	Local fault of shutdown sequencer logic unit fails to sequence loads to DG #11, fails all train A components; p = 3.8E-3.
SRW1587A-111CC-LF	=	Local fault of outlet valve from DG #11 coolers, fails DG #11 and train A of AC power; p = 3E-3.
ELC1103A-BOO-LF	=	Local fault of DG #11 circuit breaker, fails DG #11 power output and train A of AC power; p = 3E-3.
DGVCT11A-BOO-LF	=	Local fault of power breaker to diesel generator #11 room cooling, fails DG #11 and train A of AC power; p = 3E-3.
DGVOT11A-DCC-LF	=	Damper fails to operate; fails DG #11 room cooling, fails DG #11 and train A of AC power; p = 3E-3.
DGVRC11A-DCO-LF	=	Damper fails open; fails DG #11 room cooling, fails DG #11 and train A of AC power; p = 3E-3.
DGVIN11A-DCC-LF	=	Damper fails to operate; fails DG #11 room cooling, fails DG #11 and train A of AC power; p = 3E-3.
SWS1105A-BOO-LF	=	Local fault of power breaker on SWS pump #11, fails DG #11 cooling and train A of AG power; p = 3E-3.
SRWA011A-BOO-LF	=	Local fault of power breaker on SRW pump #11, fails DG #11 cooling and train A of AC power; p = 3E-3.
ELC0012B-G-PRMN	=	Maintenance of DG #12, fails train B of AC power; p = 6.6E-3.
ELC1103A-BOO-CC	=	Control circuit faults of DG #11 breaker, fails DG #11 power output and train A of AC power; p = 2.5E-3.
SWS5210A-NTC-CC	=	Control circuit fault of service water heat exchanger #11 outlet valve, fails DG #11 and train A of AC power; p = 2.5E-3.
SWS5150A-NOC-CC	=	Control circuit fault of service water heat exchanger #11 inlet valve, fails DG #11 and train A of AC power; p = 2.5E-3.

Term Descriptions (Cont.)

ELC0012B-G-FRFT	=	Failure to restore DG #12 following test, fails train B of AC power; p = 5E-3.
SDSSQNCB-LOG-LF	=	Local fault of shutdown sequencer fails loading of all AC train B components; p = 3.8E-3.
ELC0011A-G-PRTS	=	DG #11 unavailable during period of alignment after test, fails train A of AC power; p = 1.5E-3.
SRW1588B-NCC-LF	=	Local fault of inlet valve to DG #12 coolers, fails DG #12 and train B of AC power; p = 3E-3.
ELC1406B-BOO-LF	=	Local fault of DG #12 breaker, fails DG #12 power output and train B of AC power; p = 3E-3.
DGVCT12C-BOO-LF	=	Local fault of power breaker to DG #12 room cooling, fails DG #12 and train B of AC power, p = 3E-3.
DGVOT12C-DCC-LF	=	Damper fails to operate; fails DG #12 room cooling, DG #12 and train B of AC power; p = 3E-3.
DGVOT12C-DCO-LF	=	Damper fails open; fails DG #12 room cooling, DG #12 and train B of AC power; p = 3E-3.
DGVIN12C-DCC-LF	=	Damper fails to operate; fails DG #12 room cooling, DG #12 and train B of AC power; p = 3E-3.
SWS1405B-BOO-LF	=	Local fault of SWS pump #12 power breaker, fails DG #12 cooling and train B of AC power; p = 3E-3.
SRWA012B-BOO-LF	=	Local fault of SRW pump #12 power breaker, fails DG #12 cooling and train B of AC power; p = 3E-3.
ELC1406B-BOO-CC	=	Control circuit fault of DG #12 breaker, fails DG #12 power output and train B of AC power; p = 2.5E-3.
SWS5153B-NOC-CC	=	Control circuit fault of service water heat exchanger outlet valve, fails DG #12 cooling and train B of AC power; p = 2.5E-3.

Term Descriptions (Cont.)

SWS5212B-NTC-CC = Control circuit fault of service water heat exchanger outlet valve, fails DG #12 cooling and train B of AC power; p = 2.5E-3.

Note: 1. Failure of train A of AC power fails 1/2 of all ESF systems and the motor-driven AFW pump.

2. Failure of train B of AC power fails 1/2 of all ESF systems, but does not affect the AFW system.

8.1.8.3 Major Assumptions and Recovery Actions

The initial screening valve for this sequence was 1.3E-5/yr. The recovery action is to restore offsite AC power within one hour, close the PORV block valve and start HPSI to restore vessel inventory (RA-LOSP1, p = .45). Other recovery actions are possible for some cut sets but are not likely in the limited time available. The application of this recovery action reduces the sequence frequency to 5.3E-6/yr.

8.1.8.4 Engineering Insights

The dominant failures for this sequence are double failures of both diesel generators either from local faults or diesel support systems (room or DG cooling). Many of these faults are not of the type which would cause immediate failure of the diesels. Therefore, AC power may or may not be available to the PORVs in the early stages of the accident when the pressure transient occurs. For purposes of simplifying the quantification, both PORVs were conservatively assumed to have AC power available and to open if the pressure reached the PORV set point in the early stages of the accident (p = .07 for T_1 initiators). If both open, both need to reclose and a failure to reclose of 2E-2/demand for each valve was used for a total of 4E-2 for 1 of 2 valves failing to reclose. Given that a PORV stuck open, then failure of the diesel generators was assumed to occur before the operator could close the block valve (i.e., the diesels fail within about 3-5 minutes due to loss of cooling, and our recovery model does not allow recovery within the first five minutes).

8.1.9 Sequence T_1-82 (T_1L)

8.1.9.1 Description

This sequence is initiated by a loss of offsite power (T_1) followed by failure of AFW (L). The plant scrams successfully and CARCS and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the

core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to the low head of the HPSI pumps and the uncertainty as to whether or not the pressure could be reduced enough to initiate HPSI [24, 25]. Recent calculations done by EG&G for the Station Blackout program [26] indicate that approximately 86 minutes is available to start an AFW pump in order to prevent core uncovery.

The sequence frequency is estimated as 4.9E-6/yr and contributes 4% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.9.2 Dominant Cut Sets

Because of the large number of cut sets of relatively equal value which comprise this sequence even after the application of recovery, only the cut sets whose frequency is greater than 1.7E-8/yr. are listed here. These cut sets comprise 86% of the sequence frequency. A more detailed list of cut sets for all the dominant sequences can be found in Appendix C.

Cut Sets	Freq. (/yr)	% of Sequence
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0011A-GEN-LF	6.4E-7	13
T_1*RA-1*AFW0161-XOC-LF	5.0E-7	10
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0011A-GEN-LF	5.0E-7	10
T_1*RA-LOSP1*RA-3*AFWS903A-NOC-LF *ELC0011A-GEN-LF	1.4E-7	3
T_1*RA-LOSP1*RA-3*AFW3987A-NOC-LF *ELC0011A-GEN-LF	1.4E-7	3
T_1**RA-3*AFWP11-PTD-LF *AFWP13-PMD-LF	9.7E-8	2
T_1*RA-3*AFWP11-PTD-LF *CBP13-BOO-LF	7.9E-8	2
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0011A-G-PRMN	7.8E-8	2
T_1*RA-3*AFWP11-PTD-PRMN *AFWP13-PMD-LF	7.7E-8	2
T_1*RA-LOSP1*RA-16*AFW4530-N-PRMN *ELC0011A-GEN-LF	6.8E-8	1
T_1*RA-LOSP1*RA-16*AFW4520-N-PRMN *ELC0011A-GEN-LF	6.8E-8	1
T_1*RA-3*AFWP11-PTD-PRMN *CBP13-BOO-LF	6.2E-8	1
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0011A-G-PRMN	6.2E-8	1
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0011A-G-FRFT	5.9E-8	1
T_1*RA-LOSP1*RA-4*AFWP11-PTD-PRTS *ELC0011A-GEN-LF	4.8E-8	1

Cut Sets	Freq. (/yr)	% of Sequence
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0011A-G-FRFT	4.7E-8	1
T_1*RA-LOSP1*RA-3*SDSSQNCA-LOG-LF *AFWP11-PTD-LF	4.5E-8	1
T_1*AFWN-PIP-LFB	4.3E-8	.8
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *SRW1587A-NCC-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC1103A-BOO-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *DGVCT11A-BOO-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *DGVOT11A-DCC-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *DGVRC11A-DCO-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *DGVIN11A-DCC-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *SWS1105A-BOO-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *SRWA011A-BOO-LF	3.6E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *SDSSQNCA-LOG-LF	3.5E-8	.7
T_1*RA-LOSP1*AFW4511-CV-OE *AFW4530-NOC-LF*ELC0011A-GEN-LF	3.4E-8	.7
T_1*RA-LOSP1*AFW4511-CV-OE *AFW4531-NOC-LF*ELC0011A-GEN-LF	3.4E-8	.7
T_1*RA-LOSP1*AFW4511-CV-OE *AFW4512-NOC-LF*ELC0011A-GEN-LF	3.4E-8	.7
T_1*RA-LOSP1*AFW4512-CV-OE *AFW4520-NOC-LF*ELC0011A-GEN-LF	3.4E-8	.7
T_1*RA-LOSP1*AFW4512-CV-OE *AFW4521-NOC-LF*ELC0011A-GEN-LF	3.4E-8	.7
T_1*RA-LOSP1*AFW4512-CV-OE *AFW4511-NOC-LF*ELC0011A-GEN-LF	3.4E-8	.7
T_1*RA-2*AFWP11-PTD-LF *ELC0011A-INV-LF	3.2E-8	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC1103A-BOO-CC	3.0E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *SWS5210A-NTC-CC	3.0E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *SWS5150A-NOC-CC	3.0E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC1103A-BOO-LF	2.8E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *DGVCT11A-BOO-LF	2.8E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *DGVOT11A-DCC-LF	2.8E-8	.6

Cut Sets	Freq. (/yr)	% of Sequence
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *DGVRC11A-DCO-LF	2.8E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *DGVIN11A-DCC-LF	2.8E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *SWS1105A-BOO-LF	2.8E-8	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *SRWA011A-BOO-LF	2.8E-8	.6
T_1*RA-LOSP1*RA-3*AFW0103-X-FRFT *ELC0011A-GEN-LF	2.7E-8	.6
T_1*RA-2*ELC0011A-INV-LF *AFW4070B-NCC-LF	2.7E-8	.6
T_1*RA-2*ELC0011A-INV-LF *AFWP11-PTD-PRMN	2.5E-8	.5
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC1103A-BOO-CC	2.3E-8	.5
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *SWS5210A-NTC-CC	2.3E-8	.5
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *SWS5150A-NCC-CC	2.3E-8	.5
T_1*RA-LOSP1*RA-3*AFWM911X-X-PRMN *ELC0011A-GEN-LF	2.2E-8	.5
T_1*RA-3*AFWP11-PTD-LF *AFWP13-PMD-PRMN	2.1E-8	.4
T_1*RA-3*AFWP13-PMD-LF *AFWS903A-NOC-LF	2.1E-8	.4
T_1*RA-3*AFWP13-PMD-LF *AFW3987A-NOC-LF	2.1E-8	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0011A-G-PRTS	1.8E-8	.4
T_1*RA-3*CBP13-BOO-LF *AFW33987A-NOC-LF	1.7E-8	.4
T_1*RA-3*CBP13-BOO-LF AFWS903A-NCC-LF	1.7E-8	.4
T_1*RA-LOSP1*RA-3*AFWS903A-NOC-LF *ELC0011A-G-PRMN	1.7E-8	.4
T_1*RA-LOSP1*RA-3*AFW3987A-NOC-LF *ELC0011A-G-PRMN	1.7E-8	.4
	3.9E-6	80

Term Descriptions

T_1 = Loss of offsite power; f = .14/yr.

RA-LOSP1 = Failure to recover offsite power within one hr.; p = .45.

RA-3 = Operator fails to manually start locked-out AFW turbine-driven pump #12; p = 4E-2.

Test Descriptions (Cont.)

AFWP11-PTD-LF	=	Local fault of AFW turbine-driven pump #11; p = 4.7E-3.
ELC0011A-GEN-LF	=	Local fault of diesel generator #11, fails AFW motor-driven pump #13 and 1/2 of all ESF systems; p = 5.4E-2.
RA-1	=	Operator fails to manually realign AFW suction to CST #11 and start locked-out turbine-driven AFW pump #12; p = .1.
AFW0161-XOC-LF	=	Local fault of AFW suction valve to CST #12, fails all running AFW pumps; p = 3.6E-5.
AFWP11-PTD-PRMN	=	Maintenance of AFW turbine-driven pump #11; p = 3.7E-3.
AFWP11-PTD-PRTS	=	AFWS turbine-driven pump #11 unavailable due to test; p = 1.4E-3.
RA-4	=	Local operator fails to return AFW from test; p = 1E-2.
AFWS903A-NOC-LF	=	Local fault of valve in turbine-driven AFW pump #11 steam admission line; p = 1E-3.
AFW3987A-NOC-LF	=	Local fault of valve in turbine-driven AFW pump #11 steam admission line; p = 1E-3.
ELC0011A-G-PRMN	=	Maintenance of diesel generator #11, fails motor-driven AFW pump #13 and 1/2 of all ESF systems; p = 6.6E-3.
RA-16	=	Operator fails to initiate crossfeeding from Unit 2's motor-driven delivery by AFW pump; p = .1.
AFW4530-N-PRMN	=	Maintenance of valve in AFW turbine pumps feedwater lines, fails delivery by both turbine-driven AFW pumps; p = 2E-4.
AFW4520-N-PRMN	=	Maintenance of valve in AFW turbine pumps feedwater lines, fails delivery by both turbine-driven AFW pumps; p = 2E-4.
ELC0011A-G-FRFT	=	Diesel generator #11 not returned from test, fails 1/2 of all ESF systems and motor-driven AFW pump; p = 5E-3.

Test Descriptions (Cont.)

SDSSQNCA-LOG-LF = Shutdown sequencer logic unit fails to sequence loads to DG #11, fails 1/2 of all ESF systems and motor-driven AFW pump; p = 3.8E-3.

AFWP13-PMD-LF = Local fault of motor-driven AFW pump #13; p = 3.7E-3.

CBP13-BOO-LF = Local fault of motor-driven AFW pump #13 power breaker; p = 3E-3.

SRW1587A-NCC-LF = Local fault of diesel generator #11 cooling outlet valve, fails diesel generator cooling and fails AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

ELC1103A-BOO-LF = Local fault of diesel generator #11 breaker, fails 1/2 of all ESF systems and AFW motor-driven pump; p = 3E-3.

DGVCT11A-BOO-LF = Local fault of power breaker to diesel generator #11 room coolers, fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor driven AFW pump; p = 3E-3.

DGVOT11A-DCC-LF = Damper fails to operate, fails diesel generator #11 room cooling; fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor driven AFW pump; p = 3E-3.

DGVRC11A-DCO-LF = Damper fails open, fails diesel generator #11 room cooling; fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor driven AFW pump; p = 3E-3.

DGVIN11A-DCC-LF = Damper fails to operate, fails diesel generator #11 room cooling; fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor driven AFW pump; p = 3E-3.

SWS1105A-BOO-LF = Local fault of SWS pump #11 power breaker, fails diesel generator #11 cooling and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

Term Descriptions (Cont.)

SRWA011A-BOO-LF = Local fault of SRW pump #11 power breaker, fails diesel generator #11 cooling and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

ELC1103A-BOO-CC = Control circuit fault of diesel generator #11 output breaker, fails 1/2 of all ESF systems and motor-driven AFW pump; p = 2.5E-3.

SWS5210A-NTC-CC = Control circuit fault of outlet valve on SRW HTX #11, fails cooling to diesel generator #11 and failure of AC power to 1/2 of all ESF systems and AFW motor-driven pump; p = 2.5E-3.

SWS5150A-NOC-CC = Control circuit fault of inlet valve to SRW HTX #11, fails cooling to diesel generators #11 and results in failure of AC power to 1/2 of all ESF systems and AFW motor-driven pump; p = 2.5E-3.

AFW4511-CV-OE = Operator fails to increase flow to steam generator #11 when flow to other steam generator is blocked; p = 1E-2.

AFW4530-NOC-LF = Local faults of feedwater valve fails AFW turbine-driven pump flow to steam generator #12; p = 1E-3.

AFW4531-NOC-LF = Local faults of feedwater valve fails AFW turbine-driven pump flow to steam generator #12; p = 1E-3.

AFW4512-NOC-LF = Local faults of feedwater valve fails AFW turbine-driven pump flow to steam generator #12; p = 1E-3.

AFW4512-CV-OE = Operator fails to increase flow to steam generator #12 when flow to other steam generator is blocked; p = 1E-2.

AFW4520-NOC-LF = Local fault of feedwater valve fails AFW turbine-driven pump flow to steam generator #11; p = 1E-3.

AFW4521-NOC-LF = Local fault of feedwater valve fails AFW turbine-driven pump flow to steam generator #11; p = 1E-3.

Term Descriptions (Cont.)

AFW4511-NOC-LF = Local fault of feedwater valve fails AFW turbine-driven pump flow to steam generator #11; p = 1E-3.

AFW0103-X-FRFT = AFW turbine-driven pump #11 discharge valve, fail to return from test; p = 2E-4.

AFWM911X-X-PRMN = Maintenance of valve in AFW turbine-driven pump #11 steam admission line; p = 1.6E-4.

ELC0011A-G-PRTS = Diesel generator #11 unavailable due to test, fails 1/2 of all ESF systems and motor-driven AFW pump; p = 1.5E-3.

ELC0011A-INV-LF = Local faults of vital AC inverter #11, fails auto-actuation of train A SIAS and motor-driven AFW pump; p = 2.4E-3.

8.1.9.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 2.4E-4/yr. The recovery actions involve recovery of AFW by either (1) starting the locked out AFW turbine pump #12 (RA-3, p = .04), (2) realigning AFW pump 11 from test (RA-4, p = .01), (3) crossfeeding from unit 2 (RA-16, p = .1) or (4) recovering offsite power and either crossfeeding from unit 2 or restarting the PCS (RA-LOSP1, p = .45). The application of these recovery actions reduces the sequence frequency to 4.9E-6/yr.

8.1.9.4 Engineering Insights

The dominant failure modes for this sequence are of two types: (1) loss and non-recovery of offsite AC power combined with failure of DG #11 due to local faults (which fails the motor-driven AFW pump) and failure of turbine-driven AFW pump #11 (41% of the sequence frequency), or (2) loss and non-recovery of offsite AC power and failure of AFW suction valve 161 (10% of the sequence frequency). The factor prime contributor of the dominant cut sets of this sequence is the diesel generator unavailability.

8.1.10 Sequence Station Blackout

8.1.10.1 Description

As mentioned at the beginning of this section, this sequence was not modeled explicitly on the event trees. This is a new sequence identified by the Station Blackout program [17]. In this sequence, a loss of offsite power occurs

followed by the loss of all onsite AC power. The AFW system succeeds until battery depletion occurs some four hours into the accident (offsite and onsite AC power not being recovered). Due to a lack of secondary heat removal, the primary heats up and boils off. Within another two hours, core uncovery followed by core melt occurs. All containment heat removal systems are failed due to the lack of AC power.

The sequence frequency is estimated as 4.4E-6/yr and contributes 3% of the total core melt frequency.

8.1.10.2 Quantification

An estimate of the frequency of this sequence can be made using the following formula:

f(Blackout) = (frequency of LOSP)*(probability of non-recovery of offsite AC within six hours)*(probability of failure of all onsite AC)*(probability of non-recovery of onsite AC).

= .14/yr*0.18*1.7E-3*0.1

= 4.4E-6/yr

A discussion of the derivation of the various numbers appears in the next section.

8.1.10.3 Major Assumptions and Recovery Actions

The number used for the frequency of loss of offsite power was the generic number taken from EPRI-2230 [7]. This corresponds closely to the number calculated in EPRI-2301 [16] for the Calvert Cliffs grid and to the plant specific number calculated from Calvert Cliffs data. There was no statistical difference and so the generic number was used.

The probability of non-recovery of AC within six hours comes from the Station Blackout program [17] and is the generic value used for all plants. This value is not significantly different from the value determined for the Calvert Cliffs grid in EPRI-2301 [16].

At Calvert Cliffs failure of two diesel generators (DGs #11 and #12) will fail all AC power to unit 1, but will not result in the depletion of all DC power. The third DG, #21, while supplying AC power to unit 2 buses, will also charge two of the four shared DC buses. These DC buses power instrumentation on unit 1 which would allow a continued operation of the AFW system. In order to have a long-term loss of DC power, all three DGs must fail. The fault trees representing the DG and DG support systems were solved in order to estimate the DG unavailabilities upon loss of offsite power. The total DG

unavailability (including support system faults) was found to be p = 0.12. About 50% of the unavailability is due to support system faults, the rest is a combination of local DG faults and test and maintenance outages. Since no significant common modes were found to exist between the DGs, the onsite reliability is estimated is estimated as 0.12*0.12*0.12 ≈ 1.7E-3 for failure of all three diesels.

There are two plausible recovery actions for onsite AC: (1) restoring a diesel generator or, (2) restore onsite power by connecting an existing 69KV line to a neighboring grid. Data from the Station Blackout program indicated that restoring a diesel generator is not very likely (~0.5 probability); therefore, no credit was given for this action. Instead, the second recovery action of connecting the 69KV line was used. A non-recovery factor of 0.1 was estimated for this action based on the fact that this is a relatively complicated and unusual action (no procedure), but that a long time (~6 hours) is available to perform it. Since most causes of a loss of offsite power have been identified as plant or local grid related [17], the use of this line is plausible recovery action.

8.1.10.4 Engineering Insights

In light of the importance of loss of offsite power sequences, in general, and station blackout in particular, the utility is reviewing its procedure for connecting the 69KV line. Also, as a result of Task Action Plan A-44 Station Blackout, it is likely that all plants will be required to have improved loss of offsite power procedures. These improved procedures and other changes should result in significant mitigation of loss of offsite power sequences in the future.

8.1.11 Sequence T_4-152 (T_4KQ)

8.1.11.1 Description

In this sequence, a T_4 (all others) transient occurs and is followed by failure to scram and an induced LOCA due to a stuck open relief valve (Q). The primary system has survived the initial pressure transient, due to an assessed PCS runback, and the operator has successfully initiated emergency boration. Due to the high initial pressure, high rate of coolant loss, and low rate of pressure reduction coupled with the low head of the HPSI pumps, core uncovery and melt occurs before injection can be successfully implemented.

This sequence frequency is estimated as 4.3E-6/yr and contributes 3% of the total core melt frequency. The dominant contributors are outlined below.

8.1.11.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
T_4*K*Q	4.3E-6	100

Term Descriptions

T_4 = All other transients requiring reactor trip, for failure to scram only 50% results in pressure transients severe enough to demand the PORVs; f = 3.4/yr.

K = Failure to scram; p = 3E-5.

Q = Failure of 1 of 4 reliei valves to reclose; p = 4.2E-2.

8.1.11.3 Major Assumptions and Recovery Actions

As with the TKU sequences, there are similar phenomenological uncertainties associated with the TKQ sequences. No explicit analyses have been done for sequences with a stuck-open PORV. The short-term response must be deduced from the TK analyses and then the long-term response must be extrapolated. From the CE analysis [21] for plants in Calvert Cliffs class, we find that for TK sequences, the pressure remains above the HPSI pump shutoff head until some time (~5 minutes) after boration is initiated.

However, these analyses assume perfect mixing of the boron and that the reactor coolant pumps (RCPs) have tripped. Non-uniform mixing would increase the time before pressure would begin to drop. If the RCPs failed to trip (and it is not clear at present if they would trip), then reactor power might decrease slower due to the sweeping of voids from the core by the forced flow. This may affect the rate of pressure reduction or even increase pressure.

Complicating this scenario is the stuck-open PORV itself. Core uncovery can be expected to occur in about 40 minutes due to the loss of coolant, but the mass loss should result in a decrease in pressure. It is problematical if the pressure decrease due to the mass loss can result in pressure reaching the HPSI shutoff head before core uncovery can occur. The RCPs not tripping, the increased heat removal rate through the PORV, and the longer the operator delays boration initiation all tend to make power equilibrate at a higher level and to keep the pressure up.

Current expert opinion is that, for a plant with system characteristics such as Calvert Cliffs, that the race between core uncovery (assumed to be equivalent to core melt in our analysis) and the initiation of successful makeup is too close to call without explicit long-term thermal-hydraulic analyses. In this study, therefore, this sequence has been modeled as resulting in core melt. Follow-on analyses by the SASA program are planned in order to clarify the long-term characteristics of this sequence.

A possible recovery action is to close the PORV block valve. However, in this sequence, one operator action has already occurred, i.e., the initiation of emergency boration. Given that the operator can initiate emergency boration any time from 0 to 30 minutes, that leaves 10 to 40 minutes for the operator to recognize that the PORV is stuck open and to decide to isolate the PORV under an ATWS condition. It was decided that, due to the lack of ATWS procedures, lack of ATWS operator training, the high stress, and the short time (~10 minutes) that no credit should be given for this action.

8.1.11.4 Engineering Insights

Since these calculations were made, Calvert Cliffs has implemented a new emergency procedure for ATWS events which directs the operators to (1) trip the reactor manually, (2) de-energize the motor generator sets, and (3) to initiate emergency boration. The second step, de-energizing the motor generator sets should effectively bypass the most frequent of the electrical or mechanical common mode failures and result in a reactor scram in a majority of cases. The uncertainties in the accident phenomenology and the uncertainty in the time at which the operator performs the emergency boration or de-energizes the motor-generator sets make it difficult to determine the affect on the sequence without explicit thermal-hydraulic calculations Although it appears that, with this new procedure and improved operator training, some mitigation could be obtained.

8.1.12 Sequence T_3-139 (T_3KU)

8.1.12.1 Description

This sequence is a T_3 (requires primary pressure relief) transient followed by a failure to scram (K) and failure of emergency boration(U). The primary system has survived the initial pressure transient (with PCS runback). CE analyses [21] and NRC analysis in support of the ATWS rule [22] state that greater than 10 minutes are available for the operator to initiate emergency boration. In this study, we have assessed that if the operator fails to start shutting the reactor down within the 20-30 minute time frame, then core melt will result.

This sequence frequency is estimated as 3.7E-6/yr and contributes 3% of the total core melt frequency. The dominant contributors are outlined below.

8.1.12.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
T_3*K*CVCSTART-HSF-OE	2.8E-6	76
T_3*K*CVCOC12B-P-PRMN *CVCOC13X-P-PRMN	3.8E-7	10
T_3*K*CVCO514B-VCC-LF	1.7E-7	5
T_3*K*CVCR514B-BOO-CC	1.4E-7	4
T_3*K*CVCO514B-CBL-LF	6.0E-8	2
	3.6E-6	96

Term Descriptions

T_3 = Transients requiring primary system pressure relief; f = 1.85/yr.

K = Failure to scram; p = 3E-5.

CVCSTART-HSF-OE = Failure of the operator to initiate emergency boration; p = 0.05.

CVCOC12B-P-PRMN = Maintenance of charging pump #12; p = 8.2E-2.

CVCOC13X-P-PRMN = Maintenance cf charging pump #13; p = 8.2E-2.

CVCO514B-VCC-LF = Local Fault of CVCS MOV 514 (common mode failure of CVCS); p = 3E-3.

CVCR514B-BOO-CC = Control circuit fault of CVCS MOV 514 (common mode failure of CVCS); p = 2.5E-3.

CVCO514B-CBL-LF = Power cable to CVCS MOV 514 fails open (common mode failure of CVCS); p = 1.1E-3.

8.1.12.3 Major Assumptions and Recovery Actions

Given the high stress in the failure to scram scenario, the operator failure to perform an appropriate action is typically assumed to be 0.1 in past PRAs (our generic recovery model assumes 0.1 at 10 minutes). However, the thermal-hydraulic analyses [21] show that the operator should have longer than 10 minutes. After examining the thermal-hydraulic characteristics of the sequence and the various uncertainties in system response

and phenomenology, it was judged that some operator action would be necessary within 20-30 minutes. A THERP analyses of the emergency boration procedure is presented in Appendix B.19 which leads to a value of 0.05 and this value corresponds to the 0.05 probability of operator failure in 20-30 minutes from our generic recovery model.

8.1.12.4 Engineering Insights

The response of this sequence is the same as the T_4KU sequence and the reader is referred to Section 8.1.6.4 for discussion of the thermal-hydraulic characteristics.

8.1.13 Sequence T_3-118 (T_3KQ)

8.1.13.1 Description

In this sequence, a T_3 (requires primary pressure relief) transient occurs and is followed by failure to scram and an induced LOCA due to a stuck open relief valve (Q). The primary system has survived the initial pressure transient, due to the PCS runback, and the operator has successfully initiated emergency boration. Due to the high initial pressure, high rate of coolant loss, and low rate of pressure reduction coupled with the low head of the HPSI pumps, core uncovery and melt occurs before injection can be implemented.

This sequence frequency is estimated to be 2.3E-6/yr and contributes 2% of the total core melt frequency. The dominant contributors are outlined below.

8.1.13.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
T_3*K*Q	2.3E-6	100

Term Descriptions

T_3 = Transients requiring primary system pressure relief; f = 1.85/yr.

K = Failure to scram; p = 3E-5/yr.

Q = Failure of 1 of 4 relief valves to reclose; p = 4.2E-2.

8.1.13.3 Major Assumptions and Recovery Actions

The assumptions and recovery actions are the same as for the T_4KQ sequence (see Section 8.1.11.3).

8.1.13.4 Engineering Insights

See Section 8.1.11.4 of sequence T_4KQ for insights applicable to this sequence

8.1.14 Sequence T_3-113 (T_3ML)

8.1.14.1 Description

In this sequence, a T_3 (requires primary pressure relief) transient followed by a loss of PCS (M) and AFW (L). The reactor has scrammed and CARCS and CSSI succeed and cool the containment. As a result of the loss of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to information presented in References 24 and 25. Recent calculations done by EG&G for the Station Blackout program [26] indicate that 86 minutes are available to start an AFW pump in order to prevent core uncovery.

The sequence frequency is estimated as 1.7E-6/yr and contributes 1% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.14.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
T_3*RA-2*ELC0011A-INV-LF*AFWP11-PTD-LF	4.1E-7	24
T_3*RA-2*ELC0011A-INV-LF*AFW4070B-NCC-LF	3.5E-7	21
T_3*RA-2*ELC0011A-INV-LF*AFWP11-PTD-PRMN	3.3E-7	19
T_3*RA-2*ELC0011A-INV-LF*AFWP11-PTD-PRTS	1.3E-7	7
T_3*RA-2*ELC0011A-INV-LF*AFWS903A-NOC-LF	9.0E-8	5
T_3*RA-2*ELC0011A-INV-LF*AFW3987A-NOC-LF	9.0E-8	5
T_3*RA-1*PCS-LF*AFW0161-XOC-LF	3.3E-8	2
T_3*RA-2*ELC0011A-INV-LF*AFW0103-X-FRFT	1.8E-8	1
T_3*RA-2*ELC0012B-INV-LF*AFALOGCA-LOG-LF	1.8E-8	1
T_3*RA-2*ELC0011A-INV-LF*AFALOGCB-LOG-LF	1.8E-8	1
T_3*RA-2*ELC0011A-INV-LF*AFW4530-N-PRMN	1.8E-8	1
T_3*RA-2*ELC0011A-INV-LF*AFW4520-N-PRMN	1.8E-8	1
T_3*RA-1*ELC0011A-INV-LF*AFW0161-XOC-LF	1.6E-8	1
T_3*RA-1*ELC0012B-INV-LF*AFW0161-XOC-LF	1.6E-8	1
T_3*RA-2*ELC0011A-INV-LF*AFWM911X-X-PRMN	1.4E-8	1
T_3*RA-2*ELC0011A-CBL-LF*AFWP11-PTD-LF	1.4E-8	1
	1.6E-6	92

Term Descriptions

T_3 = Transients requiring primary system pressure relief; f = 1.85/yr.

Term Descriptions (Cont.)

RA-2	=	Operator fails to manually start AFW motor-driven pump from control room given that auto-actuation failed; p = .02.
ELC0011A-INV-LF	=	Local fault of vital AC inverter #11 causes failure of AFAS actuation of motor-driven AFW pump and AFW turbine-driven pump steam admission valve 4071, one feedwater regulating valve fails closed, one feedwater bypass valve fails full open, one main feedwater pump minimum flow recirculation valve fails full open, and one turbine bypass valve fails closed. If operating at power, low suction trip of main feedwater pumps. If operating at 5% in runback mode, may still get a pump trip depending on dynamics of suction pressure and steam pressure; p = 2.4E-3.
AFWP11-PTD-LF	=	Local fault of AFW turbine-driven pump #11; p = 4.7E-3.
AFW4070B-NCC-LF	=	Local fault of AFW steam admission valve, fails 1/2 of steam supply; p = 4E-3.
AFWP11-PTD-PRMN	=	Maintenance of AFW turbine-driven pump #11; p = 3.7E-3.
AFWP11-PTD-PRTS	=	AFW turbine-driven pump #11 unavailable due to test; p = 1.4E-3.
AFWS903A-NOC-LF	=	Local fault of valve in steam admission line to AFW turbine-driven pump #11; p = 1E-3.
AFW3987A-NOC-LF	=	Local fault of valve in steam admission line to AFW turbine-driven pump #11; p = 1E-3.
RA-1	=	Operator fails to realign AFW suction to CST #11 and start locked-out AFW turbine-driven pump #12, all actions must be done locally; p = 0.1.
PCS-LF	=	Local fault causes failure of PCS; p = 4.8E-3.
AFW0161-XOC-LF	=	Local fault of AFW suction valve results in cavitation failure of all operating AFW pumps; p = 3.6E-5.

Term Descriptions (Cont.)

AFW0103-X-FRFT = Failure to restore AFW turbine-driven pump #11 discharge valve from test; p = 2E-4.

ELC0012B-INV-LF = Local fault of vital AC inverter #12, results in similar effects to inverter #11 above except that the AFW motor-driven pump does not fail and AFW steam admission valve 4070 fails closed failing 1/2 AFW turbine pump steam supply; p = 2.4E-3.

AFALOGCA-LOG-LF = Local fault of AFAS logic unit fails actuation of motor-driven AFW pump and AFW steam admission valve 4071 failing 1/2 AFW turbine pump steam supply; p = 2E-4.

AFALOGCB-LOG-LF = Local fault of AFAS logic unit fails actuation of AFW steam admission valve 4070 failing 1/2 steam supply to AFW turbine pumps; p = 2E-4.

AFW4530-N-PRMN = Maintenance of feedwater valve fails both turbine-driven AFW pumps; p = 2E-4.

AFW4520-N-PRMN = Maintenance of feedwater valve fails both turbine-driven AFW pumps; p = 2E-4.

AFWM911X-X-PRMN = Maintenance of valve in AFW turbine-driven pump #11 steam admission line; p = 1.6E-4.

ELC0011A-CBL-LF = Local fault of cable from vital AC inverter #11, same effect as inverter fault above; p = 7.5E-5.

8.1.14.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 8.5E-5/yr. The important recovery action involved starting the AFW motor-driven pump from the control room given that auto actuation has failed (RA-2, p = .02). The application of this recovery action reduces the sequence frequency to 1.7E-6/R yr.

8.1.14.4 Engineering Insights

The failure of the vital bus 11A inverter is postulated as causing PCS failure due to instabilities induced in the feedwater flow; however, while this is true at ~80% flow, after a transient where PCS has run back, it is not clear what will

happen. This is a dynamic situation with several valves in the PCS system opening or closing, combined with the loss of various instrumentation and may cause a sufficient loss of main feedwater turbine pump NPSH to result in a pump trip. If the failure occurred while the PCS was actually running back, it is judged likely that the PCS would trip. If the inverter fault occurred after the PCS had stabilized itself at the 5% level, then it is not clear what the effect would be.

8.1.15 Sequence S_2-59 (S_2D'')

8.1.15.1 Description

In this sequence, we have a Small-small LOCA (S_2), successful scram and secondary heat removal via the AFW system. However, HPSI (D") fails and we have no makeup in the injection phase. This initiator can be broken up into two parts: (1) reactor coolant pump seal LOCAs (IE=2E-2/yr.) and (2) other Small-small LOCAs (IE=1E-3/yr.). The other Small-small LOCA portion of the sequence is negligible (1E-3/yr. initiating event X 1.3E-4 failure of HPSI = 1.3E-7). Work done by EG&G for the Station Blackout program [26] indicates that for a leak of the maximum expected reactor coolant pump seal LOCA (<500 gpm) with secondary cooling available approximately three hours is available to isolate the leak or start primary makeup. Containment sprays (CSSI) and fans (CARCS) are successful and cool the containment.

The frequency of this sequence is estimated to be 1.6E-6/yr and contributes 1% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.15.2 Dominant Cut Sets

Cut Set	Frequency (/yr)	% of Sequence
S_2*SIS660B-VOC-LF	7.6E-7	48
S_2*SIS659A-VOC-LF	7.6E-7	48
	1.5E-6	94

Term Descriptions

S_2	=	Small-small LOCA; f = 2.1E-2/yr.
SIS660B-VOC-LF	=	Local faults of valve in common HPSI, LPSI, and CSS pump minimum flow recirculation line, fails all HPSI due to pumping against dead head as a result of high primary system pressure (greater than 1275 psia); p = 3.6E-5.
SIS659A-VOC-LF	=	Similar to above valve SIS660B.

8.1.15.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 2.8E-6/yr. The recovery action is to recover HPSI by manually actuating HPSI from the control room (RA-6, p = .01) for auto actuation faults. The application of this recovery action reduces the sequence frequency to 1.6E-6/yr.

8.1.15.4 Engineering Insights

The dominant failures, responsible for 96% of the sequence frequency, are failure of either of the two valves in the common minimum flow recirculation line. These values are common to all HPSI, LPSI, and CSS pumps. For the Small-small LOCA case, if these valves should fail closed, the HPSI pumps were assessed to fail. This is because the slow drop in primary pressure from 1600 to 1275 psi would result in pump heat up and failure due to pumping against dead head for a significant period of time (greater than 10 minutes).

8.1.16 Sequence T_1-85 (T_1LCC')

8.1.16.1 Description

In this sequence, we have a loss of offsite power (T_1) followed by failure of AFW(L), CSSI(C), and CARCS(C'). The plant has scrammed successfully, but due to the lack of secondary heat removal, the core inventory boils off through the cycling open of the PORVs. No credit is given for feed and bleed due to information presented in References 24 and 25. Recent calculations done by EG&G for Station the Blackout program [26] indicate that 86 minutes are available to start an AFW pump in order to prevent core uncovery.

The sequence frequency is estimated as 1.0E-6/yr and contributes 1% of the total core melt frequency. The dominant contributors to this sequence are outlined below.

8.1.16.2 Dominant Cut Sets

Because of the large number of cut sets of relatively equal value which comprise this sequence even after the application of recovery, only cut sets whose frequency is greater than 4.1E-9/yr are listed here. These cut sets comprise 73% of the sequence frequency. A more detailed list of cut sets for all the dominant sequences can be found in Appendix C.

Cut Sets	Freq. (/yr)	% of Sequence
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	8.2E-8	8
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	8.2E-8	8

Cut Sets	Freq. (/yr)	% of Sequence
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	7.7E-8	8
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	6.0E-8	6
T_1*RA-LOSP1*AFW4530-N-PRM *ELC0012B-GEN-LF*ELC0011A-GEN-LF	3.7E-8	4
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0012B-GEN-LF*ELC0011A-GEN-LF	3.7E-8	4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0012B-GEN-LF*ELC0011A-GEN-LF	3.5E-8	3
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0012B-GEN-LF*ELC0011A-GEN-LF	2.7E-8	3
T_1*RA-LOSP1*RA-3*AFWS903A-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	1.6E-8	2
T_1*RA-LOSP1*RA-3*AFW3987A-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	1.6E-8	2
T_1*RA-2*ELC0011A-INV-LF *ELC0012B-INV-LF	1.6E-8	2
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*ELC0011A-G-PRMN	1.0E-8	1
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*ELC0011A-G-PRMN	1.0E-8	1
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*ELC0011A-G-PRMN	9.4E-9	.9
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*ELC0011A-G-FRFT	7.6E-9	.8
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*ELC0011A-G-FRFT	7.6E-9	.8
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0021B-GEN-OPF*ELC0011A-G-PRMN	7.4E-9	.7
T_1*RA-LOSP1*RA-3*AFWS903A-NOC-LF *ELC0012B-GEN-LF*ELC0011A-GEN-LF	7.3E-9	.7
T_1*RA-LOSP1*RA-3*AFW3987A-NOC-LF *ELC0012B-GEN-LF*ELC0011A-GEN-LF	7.3E-9	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*ELC0011A-G-FRFT	7.1E-9	.7
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	6.8E-9	.7
T_1*RA-LOSP1*AFW4520-N-PRMN *OP-FAIL-TO-ALIGN*ELC0011A-GEN-LF	6.8E-9	.7
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *OP-FAIL-TO-ALIGN*ELC0011A-GEN-LF	6.4E-9	.6
T_1*RA-LOSP1*RA-4*AFWP11-PTD-PRTS *OP-FAIL-TO-ALIGN*ELC0011A-GEN-LF	5.7E-9	.6
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0021B-GEN-OPF*ELC0011A-G-FRFT	5.6E-9	.6
T_1*RA-LOSP1*RA-3*SDSSQNCA-LOG-LF *AFWP11-PTD-LF*ELC0021B-GEN-OPF	5.4E-9	.5
T_1*RA-LOSP1*RA-3*AFWP11-PTD-PRMN *ELC0011A-GEN-LF*OP-FAIL-TO-ALIGN	5.0E-9	.5

Cut Sets	Freq. (/yr)	% of Sequence
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*SRW1587A-NCC-LF	4 5E-9	.5
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*ELC1103A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*DGVCT11A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*DGVOT11A-DCC-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*DGVRC11A-DCO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*DGVIN11A-DCC-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*SWS1105A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4530-N-PRMN *ELC0021B-GEN-OPF*SRWA011A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*SRW1587A-NCC-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*ELC1103A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*DGVCT11A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*DGVOT11A-DCC-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*DGVRC11A-DCO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*DGVIN11A-DCC-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*SWS1105A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*AFW4520-N-PRMN *ELC0021B-GEN-OPF*SRWA011A-BOO-LF	4.5E-9	.5
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*SRW1587A-NCC-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*ELC1103A-BOO-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*DGVCT11A-BOO-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*DGVOT11A-DCC-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*DGVRC11A-DCO-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*DGVIN11A-DCC-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*SWS1105A-BOO-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*AFWP11-PTD-LF *ELC0021B-GEN-OPF*SRWA011A-BOO-LF	4.3E-9	.4
T_1*RA-LOSP1*RA-3*SDSSQNCA-LOG-LF *ELC0021B-GEN-OPF*AFWP11-PTD-PRMN	4.3E-9	.4

Cut Sets	Freq. (/yr)	% of Sequence
T_1*RA-LOSP1*AFWP11-PTD-LF *ELC0012B-GEN-LF*ELC0011A-G-PRMN	4.2E-9	.4
T_1*RA-LOSP1*AFWP11-PTD-LF *ELC0011A-GEN-LF*ELC0012B-G-PRMN	4.2E-9	.4
T_1*RA-LOSP1*AFW4511-CV-OE*AFW4530-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	4.1E-9	.4
T_1*RA-LOSP1*AFW4511-CV-OE*AFW4531-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	4.1E-9	.4
T_1*RA-LOSP1*AFW4511-CV-OE*AFW4512-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	4.1E-9	.4
T_1*RA-LOSP1*AFW4512-CV-OE*AFW4520-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	4.1E-9	.4
T_1*RA-LOSP1*AFW4512-CV-OE*AFW4521-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	4.1E-9	.4
T_1*RA-LOSP1*AFW4512-CV-OE*AFW4511-NOC-LF *ELC0021B-GEN-OPF*ELC0011A-GEN-LF	4.1E-9	.4
	7.3E-7	73

Term Descriptions

T_1 = Loss of offsite power; f = .14/yr.

RA-LOSP1 = Non-recovery of offsite power within one hour; p = .45.

AFW4530-N-PRMN = Maintenance of valve in AFW turbine pumps feedwater lines, fails delivery by both turbine-driven AFW pumps; p = 2E-4.

AFW4520-N-PRMN = Maintenance of valve in AFW turbine pumps feedwater lines, fails delivery by both turbine-driven AFW pumps; p = 2E-4.

ELC0021B-GEN-OPF = Undeveloped event representing all diesel generator #21 faults, diverts DG #12 to Unit 2 and fails 1/2 of all ESF systems; p = .12.

ELC0011A-GEN-LF = Local fault of diesel generator #11, fails AFW motor-driven pump #13 and 1/2 of all ESF systems; p = 5.4E-2.

RA-3 = Operator fails to manually start locked-out AFW turbine-driven pump #12; p = 4E-2.

AFWP11-PTD-LF = Local fault of AFW turbine-driven pump #11; p = 4.7E-3.

AFWP11-PTD-PRMN = Maintenance of AFW turbine-driven pump #11; p = 3.7E-3.

Term Descriptions (Cont.)

OP-FAIL-TO-ALIGN = Operator fails to align diesel generator #12 to Unit 1, fails 1/2 of all ESF systems; p = 1E-2.

AFWS903A-NOC-LF = Local fault of valve in turbine-driven AFW pump #11 steam admission line; p = 1E-3.

AFW3987A-NOC-LF = Local fault of valve in turbine-driven AFW pump #11 steam admission line; p = 1E-3.

ELC0011A-G-PRMN = Maintenance of diesel generator #11, fails motor-driven AFW pump #13 and 1/2 of all ESF systems; p = 6.6E-3.

ELC0011A-G-FRFT = Diesel generator #11 not returned from test, fails 1/2 of all ESF systems and motor-driven AFW pump; p = 5E-3.

RA-2 = Operator fails to manually actuate AFW motor-driven pump #13 given failure of auto start; p = .02.

ELC0011A-INV-LF = Local fault of vital AC inverter #11, fails auto-actuation of train A SIAS, and the motor-driven AFW pump; p = 2.4E-3.

ELC0012B-INV-LF = Local fault of vital AC inverter #12, fails auto-actuation of train A SIAS, and the motor-driven AFW pump; p = 2.4E-3.

RA-4 = Local operator fails to return AFW from test; p = 1E-2.

SDSSQNCA-LOG-LF = Shutdown sequencer logic unit fails to sequence loads to DG #11, fails 1/2 of all ESF systems and motor-driven AFW pump; p = 3.8E-3.

SRW1587A-NCC-LF = Local fault of diesel generator #11 cooling outlet valve, fails diesel generator cooling and fails AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

ELC1103A-BOO-LF = Local fault of diesel generator #11 breaker, fails 1/2 of all ECCS systems and AFW motor-driven pump, fails diesel generator cooling and fails AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

Term Descriptions (Cont.)

DGVCT11A-BOO-LF = Local fault of power breaker to diesel generator #11 room coolers, fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

DGVOT11A-DCC-LF = Damper fails to operate, fails diesel generator #11 room cooling; fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

DGVRC11A-DCO-LF = Damper fails open, fails diesel generator #11 room cooling; fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

DGVIN11A-DCC-LF = Damper fails to operate, fails diesel generator #11 room cooling; fails diesel generator #11 and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

SWS1105A-BOO-LF = Local fault of SWS pump #11 power breaker, fails diesel generator #11 cooling and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

SRWA011A-BOO-LF = Local fault of SRW pump #11 power breaker, fails diesel generator #11 cooling and AC power to 1/2 of all ESF systems and motor-driven AFW pump; p = 3E-3.

ELC0012B-G-PRMN = Maintenance of diesel generator #12, fails 1/2 of all ESF systems; p = 6.6E-3.

AFW4511-CV-OE = Operator fails to increase flow to steam generator #11 when flow to other steam generator is blocked; p = 1E-2.

AFW4530-NOC-LF = Local faults of feedwater valve fails AFW turbine-driven pump flow to steam generator #12; p = 1E-3.

AFW4531-NOC-LF = Local faults of feedwater valve fails AFW turbine-driven pump flow to steam generator #12; p = 1E-3.

Test Descriptions (Cont.)

AFW4512-NOC-LF	=	Local faults of feedwater valve fails AFW turbine-driven pump flow to steam generator #12; p = 1E-3.
AFW4512-CV-OE	=	Operator fails to increase flow to steam generator #12 when flow to other steam generator is blocked; p = 1E-2.
AFW4520-NOC-LF	=	Local fault of feedwater valve fails AFW turbine-driven pump flow to steam generator #11; p = 1E-3.
AFW4521-NOC-LF	=	Local fault of feedwater valve fails AFW turbine-driven pump flow to steam generator #11; p = 1E-3.
AFW4511-NOC-LF	=	Local fault of feedwater valve fails AFW turbine-driven pump flow to steam generator #11; p = 1E-3.

8.1.16.3 Major Assumptions and Recovery Actions

The initial screening value for this sequence was 5.9E-5/yr. The recovery actions are to recover offsite power within one hour and start the AFW motor pump (RA-LOSP1, p = .45) or start an AFW train by either (1) starting the locked out turbine pump #12 (RA-3, p = .04), (2) returning turbine pump 11 from test (RA-4, p = .01), (3) starting the motor pump (RA-2, p = .02), or (4) crossfeeding from unit 2 (RA-16, p = .1). The application of these recovery actions reduces the sequence frequency to 1.0E-6 yr.

8.1.16.4 Engineering Insights

Approximately one-third of the sequence frequency is the result of cut sets which contain terms representing maintenance of two AFW feedwater regulation valves. Maintenance of these valves requiring disassembly would require that both AFW turbine-driven pumps be locked out. This event would not have been allowed by technical specifications prior to adding the third motor-driven AFW pump.

8.2 Containment Response and Release Categories

The dominant Calvert Cliffs core melt sequences are listed in Table 8.3, along with the applicable containment failure modes. The accident processes, timing of core melt, containment failure modes, and level of fission product releases to the atmosphere for these sequences are based on previous analysis performed at Battelle Columbus Laboratories on the Calvert Cliffs Unit 2 plant for the RSSMAP program. The containment

failure modes (α, β, γ, δ, ε) and release categories listed in Table 8.4 for the various sequences are the same as those employed for the PWR in the Reactor Safety Study (WASH-1400) [11]. The purpose of the analysis performed at Battelle was to (1) determine the probability of each containment failure mode occurring for each dominant sequence, and (2) determine what release category the full accident sequences belong in. The results of this analysis are shown in Table 8.3

In the quantification of containment failure modes, the probability of containment failure due to in-vessel steam explosions (α) was assumed to be 1E-2 for meltdowns at low pressure and 1E-4 for high primary system pressures. The former corresponds to the steam explosion containment failure probability developed in the Reactor Safety Study; the latter reflects more recent experimental observations indicating reduced potential for energetic interactions at elevated system pressures. All containment failure probabilities are assumed to be the same as in the RSSMAP Calvert Cliffs Study [9].

From Table 8.4, it is seen that all the steam explosion cases for Calvert Cliffs are estimated to fall into Release Category 1, even those in which the sprays are initially operating. In the Reactor Safety Study, the latter were predicted to be in Release Category 3. Examination of the details of the analyses indicates that the higher release fractions currently calculated for steam explosion cases with sprays initially operating are a direct result of larger puff releases associated with the steam explosion itself. The MARCH analyses take into account the vapor generated by the steam explosion and include this in the puff release. For steam explosions at low containment pressures, this results in larger fractional releases than were previously predicted. The results for steam explosion without containment sprays are consistent with previous results.

Based on previous results, sequences involving loss of containment isolation (β) were assigned Category 4 or Category 5 releases, without and with containment sprays, respectively.

Containment failure due to hydrogen burning (γ) was found to lead to Category 2 and 3 releases. The Category 2 releases generally occur in the absence of containment sprays during core meltdown. The Category 3 releases are generally associated with sequences in which containment sprays are operational, but in which hydrogen burning is predicted to fail containment at about the time of vessel bottom head failure.

Containment overpressurization (ε) in the absence of containment heat removal, but with operational emergency core cooling systems, leads to meltdowns in a failed containment and has been found to result in Category 2 releases. Overpressurization due to rapid boiloff of water from the reactor cavity

by quenching of the core debris leads to Category 2 or 3 releases, depending on the availability of the containment sprays up to the time of containment failure. In the complete absence of containment safety features, the difference in time between containment failure due to debris fragmentation and failure due to concrete attack without debris fragmentation is relatively short, and both types of overpressure failure may lead to Category 2 releases. In the intermediate case where the core debris may be only partially quenched, either due to limited fragmentation or other factors, containment failure could possibly be delayed somewhat longer, with resultant Category 3 releases.

Containment meltthrough (ϵ) may be the principal mode of containment failure of the other failure modes are avoided. Meltthrough sequences in which the containment sprays or coolers are operating have been found to result in Category 7 releases. If meltthrough takes place in the absence of containment safety features, Category 6 releases are predicted.

8.3 Sensitivities

Several assumptions were incorporated into the structure of the analytic models utilized in this study. These assumptions were generally founded upon engineering judgment. While we feel that the assumptions are good, we recognize that alternate assumptions could have been made which could significantly impact the model structure. In this section, we investigate the effect that an alternate set of assumptions would have on the quantitative results of this study. This is done by recalculating the affected sequence's frequencies taking into account all deleted or modified cutsets as a result of the modeling change. Table 8.5 summarizes the effect that these sensitivity issues have on the total core melt frequency estimate for the Calvert Cliffs Unit 1.

HPSI Pump Seal Cooling

The fault tree model of HPSI explicitly models the need for HPSI pump seal cooling from the CCW system in the recirculation phase of an accident. However, a recent assessment done by the utility* indicates that up to two hours might be required before the seals would fail in the case of a Large LOCA. For the sequences of interest, Small-small LOCAs, the temperature of the water should be less and possibly even longer times might be required before the failure.

---

*Personal communication with Niall Hunt of BG&E.

If we assume that HPSI pump seal cooling is not required, then sequence S_2H is affected. The frequency of S_2H goes from 1.4E-5/yr to 1.0E-5/yr and the total core melt frequency is not significantly affected.

HPSI Pump Room Cooling

The fault tree models of HPSI and CSSI explicitly model the need for pump room cooling in the recirculation phase of an accident. This need is taken from the FSAR requirement for room cooling following a Large LOCA. A recent assessment done by the utility* indicates that room temperature will indeed reach pump temperature limits rather quickly (~15 minutes) when all pumps are working. However, for the case of a Small-small LOCA where only one pump is running, the heat load is much less. In this case, it is not clear if the room temperature will ever reach the pump temperature limits due to the large heat sink in the room.

A reasonable assumption would be that the HPSI and CSSI pumps would not fail due to a lack of room cooling in the recirculation phase of a Small-small LOCA. Sequences S_2F and S_2FH are affected by this assumption. The frequency of S_2F goes from 1.4E-5/yr to 1.2E-5 and S_2FH goes from 1.1E-5/yr to 1.6E-6/yr. The total core melt frequency is reduced to 1.1E-4/yr.

Crossfeeding AFW From Unit II

As a result of the recent design change in the AFW system, a motor-driven AFW pump has been added to each unit. These motor-driven pumps can each crossfeed the other unit and supply sufficient water to cool down the plant. The actions required can be performed in the control room. New procedures are being written to direct the operator to perform this action.

In the case of loss of offsite power, the likelihood of the operator successfully performing this operation is limited by two considerations: (1) the motor-driven pump is powered by a diesel whose unavailability is ~.12 (including all support system faults), and (2) the AFW needs of his own unit which has also, most likely, tripped. Therefore, for recovery modeling, the most likely recovery action, in this case, was still considered to be the operator starting the locked-out turbine-driven pump.

In the case where offsite power is not lost, starting the other units motor-driven pump would result in cold water being injected into the operating units steam generators, and it was judged that there would be some reluctance on the part of the operator to perform this action. In this report, therefore, it

*Personal communication with Niall Hunt of BG&E.

was decided to use other likely recovery actions, if they were available, and use crossfeeding from the other unit only if no other action was possible. However, given appropriate procedures and operator training, crossfeeding may very well be the preferred action.

If we assume that the operator is likely to perform this action within a one-hour time frame, a probability of non-recovery of p = .01 can be assigned. Applying this recovery action to all non loss of offsite power sequences which involve failure of AFW, the total core melt frequency is reduced from 1.3E-4/yr to 1.0E-4/yr. The sequences affected are $T_{DC}L$, T_2ML, T_4ML, and T_3ML. In order to recalculate the sequence frequencies, the unrecovered frequencies were multiplied by the probability of not crossfeeding (p = .01). This assumes that crossfeeding is the <u>only</u> recovery action. Given the long time available, multiple actions may be possible and even greater reductions realized with appropriately designed procedures.

<u>Primary System "Feed and Bleed" Possible</u>

In this report, no credit was given for the possible use of primary system "feed and bleed." "Feed and Bleed" is an alternate way of cooling down the plant given all secondary heat removal has failed (i.e., PCS and AFW have both failed). It is performed by using HPSI to feed the primary with cold borated water while at the same time bleeding through the PORVs to remove energy from the core.

There are two questions about the feasibility of using this method at Calvert Cliffs. First, the thermal-hydraulic consideration that, due to the low shutoff head of the HPSI pumps (~1275 psia), it may not be possible to reduce the pressure sufficiently by opening the PORVs within the short time available (~ 10 minutes) to initiate "feed and bleed" [24,25]. Second, there are no procedures at Calvert Cliffs for performing this action, and it requires the removal of a trip unit to de-energize a bistable in order to keep the PORVs continuously open.

Given that the thermal-hydraulic question is resolved in favor of "feed and bleed," it is still doubtful if "feed and bleed" could or would be performed at Calvert Cliffs given the current design, operator training, and time available. If appropriate changes were made in operator training and in hardware to make the action easy to perform from the control room, the total core melt frequency could be reduced at most to 1.0E-4/yr with the optimistic assumption that the probability of the operator not performing "feed and bleed" was p = .01. This is the same reduction as for crossfeeding the AFW from the

other unit and affects exactly the same sequences. If a more likely probability of p = 0.1 was used for the operator not performing the "feed and bleed" within ~10 minutes, then no reduction would be realized in the total core melt frequency. Credit would not be given for "feed and bleed", as other more-likely recovery actions would be used instead (i.e., the actions we have given credit for in this analysis).

ATWS

i) Primary System Failure on Exceeding Service Level D

As discussed in Section 8.1.1, any pressure transient following an ATWS event which resulted in pressures greater than the service level C (3200 psia) limit was assessed to result in unacceptable plant conditions and equated to core melt. This position was taken because of the large uncertainty in the system response at pressures greater than this limit. In particular, significant uncertainties exist in the expected response of the reactor vessel head, old steam generator tubes, and HPSI and CVCS check valves at such high pressures. This position is consistent with the NRC analysis in support of the ATWS rule [22], but not with CE analyses [21].

The CE analyses [21] use exceeding the service level D (4200 psia) limit as leading to unacceptable plant conditions. Considerable controversy exists as to which assumption should be used. If the service level D limit is used, as in the CE analysis, then the probability of an unfavorable MTC is 0.04 for all transients (although this was calculated for loss of feedwater transients only and should be less for other transients). The ATWS(PSF) sequence frequency using the service level D limit is reduced from 2.8E-5/yr to 7.3E-6/yr and the T_2KU and T_2KQ sequence frequencies are increased from 8.5E-7/yr to 1.7E-6/yr and 5.0E-7/yr to 1.0E-6/yr, respectively. The total core melt frequency is reduced to 1.1E-4/yr.

ii) TKU Sequences are not Early Core Melts

As discussed in Section 8.1.6, no long-term thermal-hydraulic analyses have been done for this type of sequence. Approximately one third of the amount of water necessary to uncover the core has been lost due to the initial pressure transient. The predicted system response after the pressure transient, assuming the RCP's trip and after PORV closure, shows pressure equilibrating at about 1800 psia and rising slowly. However, there is some doubt that the RCPs will trip as assumed by CE. CE assumed pump cavitation, when the primary system coolant saturated, would degrade pump operation causing a trip. Experimental evidence does not support this contention. Without RCP trip the decreased voiding in the core region may lead primary system pressure to increase, possibly to the PORV setpoint. The time allowed in this analysis for the operator to initiate boration in order to decrease system

pressure enough to prevent subsequent core uncovery is 30 minutes.

Given that the RCP's trip or that the response with the RCP's running is not severe enough to result in continued high pressures and coolant loss, possibly much longer than 30 minutes would be available for the operator to initiate emergency boration (i.e., up to several hours). If we assume that greater than one hour is available, then the probability of operator failure is less than or equal to p = .01 and the frequencies of T_4KU and T_3KU decrease from 6.7E-6/yr to 2.9E-6/yr and 3.7E-6/yr to 1.6E-6/yr, respectively. The total core melt frequency is reduced to 1.2E-4/yr.

iii) TKQ Sequences are not Early Core Melts

As discussed in Section 8.1.11, no thermal-hydraulic analyses have been done for ATWS sequences with stuck-open PORVs. The response has to be extrapolated from the TK sequence analyses. Because of the low shutoff head of Calvert Cliffs HPSI pumps, there is considerable uncertainty as to whether or not pressure can be reduced enough to allow primary makeup in time to prevent core uncovery and melt. The uncertainties in sequence phenomenology and system response make the outcome difficult to predict. Some examples of these uncertainties are: (1) various times of boron initiation, (2) RCP's tripping or not tripping, (3) the effect of the mass loss through the PORV vs. the increased heat removal rate (which results in a higher equilibrium power), and (4) the timing of core uncovery due to the mass lost in the initial pressure transient plus the amount lost through the subsequent sticking open of the PORV. In this analysis, the sequences were modeled as resulting in core uncovery and melt.

If one makes the assumption that the pressure decreases enough so that HPSI injection can successfully be implemented in time to prevent core uncovery, then the sequence frequency can be reduced by allowing multiple recovery actions such as initiating emergency boration and subsequently high pressure injection. Given that the operator may not have initiated emergency boration until 30 minutes into the accident, a time of the order of 10 minutes would be available to perform any additional action.

If we assigned a probability of p = 0.1 to the operator failing to perform any subsequent action then the frequency of T_4KQ decreases from 4.3E-6/yr to 6.1E-7/yr and T_3KQ decreases from 2.3E-6/yr to 3.3E-7 yr. The total core melt frequency decreases to 1.2E-4/yr.

iv) P(MTC) = 0.5 for T_3 and T_4 transients

In this analysis, we have used a value of 0.1 for the probability of having an unfavorable MTC on T_3 and T_4

transients. This value is less than the 0.5 value used for T_2 transients because of the less severe characteristics of the T_3 and T_4 transients (i.e., the lower predicted peak pressures).

The NRC analysis in support of the ATWS rule [22] uses 0.5 for all transients. This value is from NUREG-0460 and was used for all CE and B&W plants because of the similarities in plant responses. While the response of other larger CE plants and B&W plants is similar and this seems to be a reasonable grouping of plants for a generic analysis, the response of Calvert Cliffs is significantly different for T_2 vs. T_3 and T_4 transients.

If, however, we assume that the probability of an unfavorable MTC is 0.5 for all transients, then the ATWS(PSF) frequency increases from 2.8E-5/yr to 9.1E-5/yr and the frequencies of T_4KU, T_3KU, T_4KQ and T_3KQ decrease from a total of 1.7E-5/yr to 8.5E-6/yr (i.e., just multiply by a .5 probability of a favorable MTC). The total core melt frequency increase to 1.9E-4/yr.

v) Failure to Scram Probability

The value used in this study for the probability of failure to scram is 3E-5 and is taken from NUREG-0460 [23]. Although this value was used in the RSSMAP PRA, other IREP studies, the utility group ATWS study [21], and the NRC analysis in support of the ATWS rule [22], considerable controversy still exists about this number.

In order to bound the effects of various sides of this issue, two values have been chosen to perform sensitivity analyses. The first is 1.0E-4. This value is the point estimate based on world-wide LWR RPS experience and is taken from reference 22. It represents three failures in 22,560 demands. The second value is 5.0E-6 and represents the value obtained in the ANO-1 PRA [27] from a fault tree analysis of an RPS system. This value is judged to be typical of an RPS system without any significant common mode failures and to represent a likely lower bound on RPS unavailability.

For the assumption of 1.0E-4/yr, the total core melt frequency is increased from 1.3E-4/yr to 2.4E-4/yr as all ATWS sequences are increased by a factor of 3.3. For the assumption of 5.0E-6/yr, the total core melt frequency decreases from 1.3E-4/yr to 9.1E-5/yr as all ATWS sequences are decreased by a factor of 6.

8.4 Limitations of the IREP Methodology and Analysis and Future Uses of the Models

The quantitative results of this IREP study must be viewed and used with a thorough understanding of the limitations of the methodology used. As previously identified, this is principally a reliability study. While inference regarding risk-dominant accident sequences can be obtained from the analysis, a detailed risk analysis was not performed, nor was it intended. The analysis leading to the grouping of accident sequences into release categories relied heavily on previous studies performed on similar plants and did not do extensive plant-specific analyses. Recognizing the inherent uncertainties in this type of categorization, the information generated was not used as an input to a calculation of consequence distribution. External events such as earthquakes, fires, floods, and other influences from without were not considered. Thus, the quantitative results must be regarded as being incomplete from a risk perspective. However, this analysis does give a good estimate of the frequency of core melt accidents from internal initiators.

In utilizing the results of this study, the following limitations should be recognized:

1. The final generic data base [3] used in the quantification analyses for CC-1 was similar to the WASH-1400 data base but updated as a result of the National Reliability Evaluation Program (NREP). Plant-specific data were utilized when the analyst found it different from the generic base. However, the detailed comprehensive examination of plant logs necessary to fully evaluate in-plant data was not performed.

2. Human performance was modeled using the techniques described in NUREG/CR-1278.[5] However, the systematic bias in human response (either positive or negative) that may result because of morale or management practices was not included. In addition, human acts of commission were, in general, not included in the analysis.

3. An attempt was made to couple the root cause of the initiating event with system faults in analyzing accident sequences. The technique used is believed to be reasonably efficient to identify single failures which may initiate a transient and degrade the performance of one or more safety systems. However, multiple fault scenarios of this type may have been omitted.

4. Coupling of faults associated with design, fabrication, or environmental conditions, was not treated explicitly.

5. Since the dominant accident sequences were identified using upper-bound human error rates and generic data, and then had a second more-sophisticated analysis performed on them, all the residual non-dominant sequence frequencies are evaluated on a more "conservative" basis.

There were also several assumptions made throughout the analysis regarding the depth of analysis which could influence the results. The depth of the analysis in many ways defines the level of interactions or dependencies considered; and, while we believe the assumptions made are valid, the possibility exists that additional dependencies might be identified with further analysis. Examples of the type of assumptions made include (1) including only those single passive failures which can fail an entire system, and (2) ignoring misposition faults for valves which automatically are commanded to the proper position upon engineered safety features actuation and for valves which have position indicated in the control room and are monitored each shift using a checkoff procedure.

The incompleteness and subjectivity associated with the aforementioned topics do not invalidate the analysis performed. The important product of this project is the framework of engineering logic generated in constructing the models, not the precise numbers resulting from the mathematical manipulations of these models.

The patterns, ranges, and relative behaviors which are obtained can be used to develop insights into the design and operation of a plant which can only be gained from an integrated consistent approach such as this IREP analysis. These insights are applicable to utility and regulatory decision making, although they should not be the sole facts for such descriptions. By comparative evaluations, those features of the plant which are predicted to have a more significant influence on risk can be identified, and owner and regulatory efforts can be focussed on them to determine if they are acceptable. Similarly, regulatory efforts addressed should also be evaluated. The rank ordering of risk-dominant accident sequences provides a framework for future value-impact analyses on potential plant modifications.

8.4.1 Application of Results

The generic views regarding the usefulness of the IREP analyses expressed above suggest several concrete applications that can be made. They are presented below in the form of suggestions to plant owners for application of the results. For this program to have value, the models should become a

practical tool for use by licensees as the centerpiece of a risk-management or safety-assurance program. In many cases, the models may have to be perturbed somewhat to achieve the various goals. However, we have attempted to construct them in such a manner as to minimize the difficulty associated with such use. These models should be maintained in a current status and used as tools in operations management. Specific suggestions are listed below.

8.4.1.1 Operator Training and Simulator Design.

The IREP study generated a catalog of severe accident sequences, with rough assessments of the likelihood, severity, and principal root causes of each. Some of these could be included in operator training and simulator design. This information can also be used as a starting point for further studies intended to assess the similarity of the symptom profile among accidents requiring different operator response, and to survey the hazards associated with misdiagnosis or less-than-optimum recovery actions. A natural follow-up is an assessment of the adequacy of instrumentation and status-monitoring equipment.

8.4.1.2 Emergency Planning

The catalog of accident sequences and the likelihood estimates emerging from IREP can be used to train emergency response personnel in what to expect. IREP results can also serve as a basis to improve the set of symptoms to be used as trigger points for the declaration of site or general emergencies, and they can be used in developing guides on the diagnosis and prognosis of accidents as they develop.

8.4.1.3 Adequacy of Procedures

It is common in studies such as IREP to discover a few instances in which emergency procedures or maintenance procedures should be improved and which are of prime importance to the accident susceptibility of the plant. The results herein should be studied to determine if this is the case here. Beyond these lessons, IREP models can be used to measure the importance of individual procedures to safety and to explore the risk associated with errors in following procedures.

8.4.1.4 Adequacy of Limiting Conditions of Operation

An IREP study provides the tools with which to optimize allowable outage times and surveillance intervals. The IREP models can also be used in evaluating requests from utilities to continue power generation when equipment is out of service beyond their specified allowable outage times.

8.4.1.5 Systems Integration Reviews

IREP is designed to model explicit functional dependencies among systems. It is not uncommon to discover that an auxiliary system is a weak link with respect to reliability in such a manner that it governs plant risk. Hard-wired systems interactions, human behavior that can couple the unavailability of several safety systems, and the importance of auxiliary systems to safety have emerged in IREP results. Such findings are not complete or precise; nonetheless, they represent a vast improvement on safety analyses done to date.

8.4.1.6 Significance of Component Reliability

The IREP models can be used to develop quantitative measures of importance to safety for the reliability of components, trains, whole systems, and classes of accident sequences. These methods enable the use of cost-benefit analyses on reliability improvements for components, and the more discriminating use of the more expensive quantification or in-service inspection techniques.

8.4.1.7 System Reliability

Estimates of system reliability can be produced from an IREP study. Quantitative measures of the importance of system components can be calculated from the IREP models, and the more likely failure modes which are believed to dominate the unavailability of these systems are identified. With this information, one can assess the possibility that a failed system could be repaired before its failure reaches a point of no return under accident conditions. Operators can be trained in fault diagnosis and in "quick fixes." The adequacy of diagnostic instrumentation and status monitoring can be assessed. Surveillance practices can be altered to improve the availability of particularly critical systems.

8.4.1.8 Accident Sequences

In addition to identifying accident sequences and estimating their frequency, IREP models can also serve as a test bed with which to explore the effects of changes in design or operations practices. Possible improvements may be obvious in light of the results. In other cases, the effectiveness of hypothetical improvements can be assessed (within the limits of the completeness of the models). A particularly valuable use of these models lies in the evaluation of attendant risks associated with changes, i.e., will a fix for one safety problem make different accident sequences more likely? IREP provides a tool that can be used to address such questions.

8.4.1.9 Evaluation of Operating Occurrences

The IREP models and results can be used in the evaluation of whether or not a fault occurring in plant operation or testing was a precursor of a more serious event, and to evaluate its importance. One can explore each of the classes of severe accident sequences for the role that might have been played by the actual event. In addition, patterns of licensee events or trends can be assessed for risk significance with the IREP models.

8.4.1.10 Validation of IREP Analyses

The occurrence of faults or errors in the operation or testing of the plant can be used to update, validate, or improve the completeness or accuracy of the IREP models and the projected failure frequencies. Doing so has the dual advantage of improving the IREP model for its many other uses, as well as illuminating the safety significance of the operating experience.

8.4.1.11 Design Errors and Generic Safety Issues

There are several cases of safety problems in reactor plants that IREP studies do not analyze. Among these are susceptibility to fires, floods, sabotage, earthquakes, design or installation errors that are not revealed by the explicitly known, hard-wired functional dependencies among systems, and effects assumed to be negligible in the IREP study, such as the role of snubber failures. However, the models generated in IREP can be used to put such concerns into perspective once the concern has been explicitly postulated. For example, one can use IREP to assess which accident sequences might be affected by the postulated safety issue and estimate at what level of severity the deficiency -- if any -- might emerge from the background of minor contributors to risk into one of the dominant concerns. Thus, IREP can be immensely useful even in contexts in which its predictive power is poor.

8.4.2 Conclusions on the Applications of IREP

It should be noted that none of the uses suggested above depend upon the bottom-line predictions of risk. They all depend upon the more trustworthy comparative measures of importance and upon the catalog of accident sequences to which the subject plant is susceptible.

Some of the applications are sensitive to the limitations of the study, particularly in completeness and quantitative accuracy. Nonetheless, the applications can be tailored to the known limitations and the models generated can provide a coherent framework to address the "what if" questions concerning its accuracy in these applications.

The suggested applications of the models in this report do not require a precise analysis of the phenomenology of reactor accidents. Thermal hydraulics, containment challenge analyses, and the like need only be good enough to develop the broad outlines -- the "cliffs and valleys" -- in the accident processes, although there are rare occasions when uncertainties in the modeling of accident processes can make large differences in the course or consequences of reactor accidents.

In general, formal, plant-specific consequence analysis is unnecessary for these applications. It is useful to be able to identify accident sequences with categories of outcome severity, and the applications to emergency planning require some information on offsite consequences. However, the accuracy warranted can be met by interpolating the accident sequences among those in the published risk assessments that have included formal consequence analysis.

It is hoped that studies similar to this IREP analysis will become a common language, shared by the NRC and the licensees, to put safety issues in context. The use of IREP as a tool for safety analysis and in operations management should enable many loopholes in the assurance of reactor safety to be identified and closed, and at the same time, improve the cost-effectiveness and risk-relevance of NRC regulatory initiatives.

Table 8.1

Legend Used in Tables 8.2, 8.3, and 8.4

Initiating Events

S_2 = Small-small LOCA (1.9" in dia.)

T_1 = Loss of Offsite Power

T_2 = Loss of PCS

T_3 = Transients requiring primary relief

T_4 = All other transients

T_{DC} = Loss of 125 VDC bus 11

System Failures

D" = High Pressure Safety Injection

F = Containment Spray System (Recirculation)

H = High Pressure Safety Recirculation System

K = Reactor Protection System

L = Auxiliary Feedwater System

M = Power Conversion System

Q = Relief valves fail to reclose

U = Chemical Volume and Control System

C = Containment Air Recirculation and Cooling System

C' = Containment Spray System (Injection)

Containment Failure Modes

α = Vessel steam explosion

β = Leakage

γ = Hydrogen burning

δ = Overpressure

δ' = Delayed overpressure

ϵ = Basemat meltthrough

Table 8.2

Final Calvert Cliffs Dominant Accident Sequences
(after recovery)

SEQUENCE	DESCRIPTION	IREP FREQUENCY BEFORE RECOVERY (/YR)	IREP FREQUENCY AFTER RECOVERY (/YR)	% TOTAL CM FREQUENCY
ATWS(PSF)	----	2.8E-5	2.8E-5	20
T_{DC}-82	$T_{DC}L$	4.9E-4	2.1E-5	16
S_2-50	S_2H	5.1E-5	1.4E-5	11
S_2-52	S_2FH	5.7E-5	1.1E-5	9
T_2-82	T_2L	1.8E-4	7.1E-6	6
T_4-173	T_4KU	6.7E-6	6.7E-6	5
T_4-147	T_4ML	3.4E-4	6.3E-6	5
T_1-81-65	T_1Q-D"CC'	1.3E-5	5.3E-6	4
T_1-82	T_1L	2.4E-5	4.9E-6	4
Blackout	----	2.4E-4	4.4E-6	3
T_4-152	T_4KQ	4.3E-6	4.3E-6	3
T_3-139	T_3KU	3.7E-6	3.7E-6	3
T_3-118	T_3KQ	2.3E-6	2.3E-6	2
T_3-113	T_3ML	8.5E-5	1.7E-6	1
S_2-59	S_2D"	2.8E-6	1.6E-6	1
T_1-85	T_1LCC'	5.9E-5	1.0E-6	1
Sequences below cutoff	----	----	7.8E-6	6
Total	----	----	1.3E-4	100

Table 8.3

Calvert Cliffs Unit-1 Dominant Accident Sequence
Frequencies by Release Category

	Release Category						
Sequence	1	2	3	4	5	6	7
ATWS(PSF)	α=2.8E-9	--	$\gamma+\delta$=2.0E-5	--	β=2.0E-7	--	ε=8.4E-6
$T_{DC}L$	α=2.1E-9	--	$\gamma+\delta$=1.5E-5	--	β=1.5E-7	--	ε=6.3E-6
S_2H	α=1.4E-7	--	$\gamma+\delta$=9.8E-6	--	β=9.8E-8	--	ε=4.2E-6
S_2FH	α=1.1E-7	$\gamma+\delta$=7.7E-6	--	β=7.7E-8	--	ε=3.3E-6	--
T_2L	α=7.1E-10	--	$\gamma+\delta$=5.0E-6	--	β=5.0E-8	--	ε=2.1E-6
T_4KU	α=6.7E-10	--	$\gamma+\delta$=4.7E-6	--	β=4.7E-8	--	ε=2.0E-6
T_4ML	α=6.3E-10	--	$\gamma+\delta$=4.4E-6	--	β=4.4E-8	--	ε=1.9E-6
T_1Q-D"CC'	α=5.3E-10	δ=4.2E-6	δ'=1.1E-6	β=3.7E-8	--	--	--
T_1L	α=4.9E-10	--	$\gamma+\delta$=3.4E-6	--	β=3.4E-8	--	ε=1.5E-6
Blackout	α=4.4E-10	δ=3.5E-6	δ'=8.8E-7	β=3.1E-8	--	--	--
T_4KQ	α=4.3E-10	--	$\gamma+\delta$=3.0E-6	--	β=3.0E-8	--	ε=1.3E-6
T_3KU	α=3.7E-10	--	$\gamma+\delta$=2.6E-6	--	β=2.6E-8	--	ε=1.1E-6
T_3KQ	α=2.3E-10	--	$\gamma+\delta$=1.6E-6	--	β=1.6E-8	--	ε=6.9E-7
T_3ML	α=1.7E-10	--	$\gamma+\delta$=1.2E-6	--	β=1.2E-8	--	ε=5.1E-7
S_2D"	α=1.6E-10	--	$\gamma+\delta$=1.1E-6	--	β=1.1E-8	--	ε=4.8E-7
T_1LCC'	α=1.0E-10	δ=8.0E-7	δ'=8.0E-7	β=7.0E-9	--	--	--
Category Total	2.6E-7	2.0E-5	7.5E-5	1.5E-7	7.2E-7	3.3E-6	3.1E-5

Table 8.4

Calvert Cliffs Unit-1 Containment Failure
Mode Probabilities

Sequence	Release Category 1	2	3	4	5	6	7
ATWS(PSF)	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
$T_{DC}L$	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
S_2H	α=1E-2	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
S_2FH	α=1E-2	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3	--
T_2L	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
T_4KU	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
T_4ML	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
T_1Q-D"CC'	α=1E-4	δ=.8	δ'=.2	β=7E-3	--	--	--
T_1L	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
Blackout	α=1E-4	δ=.8	δ'=.2	β=7E-3	--	--	--
T_4KQ	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
T_3KU	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
T_3KQ	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
T_3ML	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
S_2D"	α=1E-4	--	$\gamma+\delta$=.7	--	β=7E-3	--	ε=.3
T_1LCC'	α=1E-4	δ=.8	δ'=.2	β=7E-3	--	--	--

Table 8.5

Summary of Sensitivity Issues

Sensitivity Issue		CC-1 Total Core Melt Frequency (/yr)
1.	Base Case	1.3E-4
2.	HPSI Pumps do not Need Seal Cooling	1.3E-4
3.	HPSI Pumps do not Need Room Cooling	1.1E-4
4.	Crossfeeding AFW from Unit 2 (p = .01)	1.0E-4
5.	Primary System "Feed and Bleed" Possible	1.3E-4 to 1.0E-4 (depending on assumptions)
6.	ATWS	
i)	Primary System Failure on Exceeding Service Level D	1.1E-4
ii)	TKU Not Core Melt	1.2E-4
iii)	TKQ Not Core Melt	1.2E-4
iv)	P(MTC) = .5 for T_3 and T_4 Transients	1.9E-4
vii)	Scram Failure Probability = 1E-4	2.4E-4
	= 5E-6	9.1E-5

REFERENCES

1. U. S. Nuclear Regulatory Commission, NRC Action Plan Developed as a Result of the TMI-2 Accident, NUREG-0666, May 1980.

2. Garcia, A. A., et al., Crystal River-3 Safety Study, NUREG/CR-2515, SAND81-7229/1, December 1981.

3. Carlson, D. D., et al., Interim Reliability Evaluation Program Procedures Guide, NUREG/CR-2728, SAND82-1100, Sandia National Laboratories, January 1983.

4. Worrell, R. B. and D. W. Stack, A SETS User's Manual for the Fault Tree Analyst, SAND77-2051, Sandia National Laboratories, November 1978.

5. Swain, A. D. and H. E. Guttmann, Handbook of Human Reliability Analysis with Emphasis on Nuclear Plant Applications, Draft Report, NUREG/CR-12788, SAND80-200, Sandia National Laboratories, September 1980.

6. Calvert Cliffs Nuclear Power Plant Units 1 and 2, Final Safety Analysis Report, Baltimore Gas and Electric Company, January 1971.

7. ATWS: A Reappraisal - Part 3: Frequency of Anticipated Transients, Prepared by Science Applications, Inc., EPRI NP-2230 Project 1233-1, Interim Report, January 1982.

8. Letter from J. A. Murphy, NRC to D. D. Carlson, SNL, Subject, Component Failure Rates to be Used for IREP Quantification, September 26, 1980.

9. Kolb, G. J., et al., Reactor Safety Study Methodology Applications Program: Calvert Cliffs #2 PWR Power Plant, Sandia National Laboratories and Battelle Columbus Laboratories, NUREG/CR-1659/3 of 4, SAND80-1897/3 of 4, May 1982.

10. U. S. Nuclear Regulatory Commission, Generic Evaluation of Feedwater Transients and Small Break Loss-of-Coolant Accidents in Combustion Engineering - Designed Operating Plants, NUREG-0635, January 1980.

11. U. S. Nuclear Regulatory Commission, Reactor Safety Study - An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), October 1975.

12. Memorandum for D. G. Eisenhut, NRC, from T. E. Murley, NRC, Subject, Reactor Coolant Pump Seal Failure, nd.

13. Indian Point Probabilistic Safety Study, PASNY and Consolidated Edison Company, SPRING 1982.

Zion Probabilistic Safety Study, Commonwealth Edison Company, FALL 1981.

14. Memorandum for V. S. Noonan, NRC, from J. E. Jackson, NRC, Subject, Summary of Meeting with Combustion Engineering Owners Group on Reactor Coolant Pump Seal Performance, Generic Issue 23, April 28, 1983.

15. Varnado, G. B., W. H. Horton and P. R. Lobner, Modular Fault Tree Analysis Procedures Guide, NUREG/CR-3268/4 Vols., SAND82-0963/4 Vols., Sandia National Laboratories, August 1983.

16. Loss of Offsite Power at Nuclear Power Plants: Data and Analysis, EPRI NP-2301, Science Applications, Inc., Interim Report, March 1982.

17. Kolaczkowski, A. M. and A. C. Payne, Jr., Station Blackout Accident Analysis (Part of NRC Task Action Plan A-44, NUREG/CR-3226, SAND82-2450, Sandia National Laboratories, May 1983.

18. A. J. Oswald, C. D. Gentillon, S. D. Matthews, and T. R. Meachum, "Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Program (NREP) Guide," EG&G Idaho, INC., EGG-EA-5887, June 1982.

19. "Military Handbook: Reliability Prediction of Electronic Equipment," Rome Air Development Center, Griffith AFB, NY, MIL-HDBK-217C, April 1979.

20. "Military Handbook: Reliability Prediction of Electronic Equipment," Rome Air Development Center, Griffith AFB, NY, MIL-HDBK-217B, April 1979.

21. Power Engineering Services, Technical Support for the Utility Group on ATWS, Task I: Quantitative Evaluation of Industry Proposed Modifications Relative to Existing Plant ATWS Requirements, Appendix D, Science Applications, Inc., SAI-011-82-SJ, December 31, 1981.

ATWS Early Verification: Response to NRC Letter of February 15, 1979, for Combustion Engineering NSSS's, CE Power Systems, CE Inc., CENPD-263-NP, November 1979.

ATWS Analysis: Analysis of Anticipated Transients Without Reactor Scram in Combustion Engineering NSSS's, CE Power Systems, CE Inc., CENPO-158, Rev. 1, May 1976.

22. SECY-83-293, Amendments to 10 CPR, Part 50, Related to Anticipated Transients without Scram (ATWS) Events, NRC, July 19, 1983.

23. U. S. Nuclear Regulatory Commission, Anticipated Transients without Scram for Light Water Reactors, Unresolved Safety Issue Program, Office of Nuclear Reactor Regulation, NUREG/CR-0460, March 1980.

24. U. S. Nuclear Regulatory Commission Memorandum to Karl Kniel, Generic Issues Branch, DST, from Brian W. Sheron, Reactor Systems Branch, DSI, on the Status of Feed and Bleed for Emergency Decay Removal, March 31, 1981.

25. Memorandum from B. W. Sheron, NRC, to T. P. Speis, NRC, Subject, Feed and Bleed Capability in CE Plants Both with and Without PORVs, February 11, 1982.

26. C. D. Fletcher, A Revised Summary of PWR Loss of Offsite Power Calculations, EG&G Idaho, Inc., EGG-CAAD5593, September, 1981.

27. G. J. Kolb, et al., Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One-Unit 1 Nuclear Power Plant; NUREG/CR-2787, SAND82-0978, Sandia National Laboratories, June 1982.

DISTRIBUTION:

US NRC Distribution Contractor (CDSI) (250 copies)
7300 Pearl Street
Bethesda, MD 20014
250 copies for AN, RG

B. Atefi
Science Applications, Inc.
1710 Goodridge Dr.
McLean, VA 22102

R. M. Bernero
Division of Risk Analysis
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission
MS 1130SS
Washington, DC 20555

P. Cybulskis
Battelle Columbus Laboratories
505 King Avenue
Columbus, Ohio 43201

S. M. Davis
Calvert Cliffs Nuclear Power Plant
Lusby, MD 20657

S. M. Davis
Reliability and Risk Assessment Branch
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
Mail Stop 216
Washington, DC 20555

M. L. Ernst
Division of Risk Analysis
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission
MS 1130SS
Washington, DC 20555

W. L. Ferrell
Science Applications, Inc.
505 Marquette NW, Suite 1200
Albuquerque, NM 87102

W. J. Galyean
Science Applications, Inc.
505 Marquette NW, Suite 1200
Albuquerque, NM 87102

DISTRIBUTION (Cont.)

A. A. Garcia
Lawrence Livermore National Laboratories
P. O. Box 808
Livermore, CA 94550

J. Held
Energy Incorporated
1851 So. Central Place
Suite 201
Kent, Washington 98031

R. W. Hunt (8)
Baltimore Gas and Electric
R and AE Unit
Ft. Smallwood Rd. Complex
Baltimore, MD 21203

J. Kelly
Science Applications, Inc.
5 Palo Alto Square, Suite 200
El Camino Real at Page Mill Rd.
Palo Alto, CA 94304

D. M. Kunsman
Science Applications, Inc.
505 Marquette NW, Suite 1200
Albuquerque, NM 87102

D. R. Lasher
Reliability and Risk Assessment Branch
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
Mail Stop 216
Washington, DC 20555

S. Lainoff
Energy Incorporated
1851 So. Central Place
Suite 201
Kent, Washington 98031

Dr. M. Modarres
Department of Chemical and Nuclear Engineering
University of Maryland
College Park, MD 20742

J. A. Murphy
Division of Risk Analysis
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission
Washington, DC 20555

DISTRIBUTION (Cont.)

K. Murphy (25)
Division of Risk Analysis
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission
Washington, DC 20555

National Technical Information Service (25)
US Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

J. J. O'Neill
Florida Power & Light Co.
700 Universe Blvd.
Juno Beach, Florida 33408

P. D. O'Reilly
NUS Corporation
910 Clopper Road
Gaithersburg, MD 20878

M. Raeisinia
c/o B. Atefi
Science Applications, Inc.
1710 Goodridge Dr.
McLean, VA 22102

M. L. Roush
Department of Chemical and Nuclear Engineering
University of Maryland
College Park, MD 20742

Ashok C. Thadani (2)
Reliability and Risk Assessment Branch
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
Mail Stop 216
Washington, DC 20555

J. Young
Energy, Inc.
515 W. Harrison, Suite 220
Kent, Washington 98031

3141 C. M. Ostrander (5)
3151 W. L. Garner
6400 A. W. Snyder
6410 J. W. Hickman
6411 A. S. Benjamin

DISTRIBUTION (Cont.)

6411	J. H. Linebarger
6412	M. P. Bohn
6412	S. W. Hatch
6412	F. T. Harper
6412	G. J. Kolb
6412	S. H. McAhren
6412	A. C. Payne (22)
6412	D. W. Stack
6412	T. A. Wheeler
6412	D. W. Whitehead
6414	D. M. Ericson
6415	D. C. Aldrich
6417	D. W. Carlson
6420	J. V. Walker
6430	N. R. Ortiz
6432	L. D. Chapman
6440	D. A. Dahlgren
6447	D. L. Berry
6450	J. A. Reuscher
8424	M. A. Pound

NRC FORM 335 (11-81)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-3511/1 of 2
SAND83-2086/1 of 2

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant
Volume 1 Main Report

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO.

7. AUTHOR(S)
Arthur C. Payne, Jr.

5. DATE REPORT COMPLETED
MONTH September | YEAR 1983

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Nuclear Fuel Cycle Systems Safety
Division 6412
Albuquerque, New Mexico 87185

DATE REPORT ISSUED
MONTH September | YEAR 1983

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Risk Analysis
Office of Nuclear Regulatory Research
US Nuclear Regulatory Commission
Washington, DC 20555

10. PROJECT/TASK/WORK UNIT NO.

11. FIN NO.
A1241

13. TYPE OF REPORT
Technical (Final Report)

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES
None

14. (Leave blank)

16. ABSTRACT (200 words or less)
This report presents the results of the Probabilistic Risk Assessment (PRA) of Calvert Cliffs Unit 1 Nuclear Power Plant. The analysis was performed as part of the Interim Reliability Evaluation Program (IREP). The analysis used fault tree and event tree models as the primary tools to evaluate the risk due to a core melt at Calvert Cliffs. Core melt sequences initiated by one of three break-size LOCAs or one of six categories of transients were evaluated, and the dominant (i.e., highest frequency) sequences were further analyzed to estimate the magnitude of radionuclide release. The accident sequences were then placed into the release categories defined in the Reactor Safety Study to estimate this magnitude. The most significant sequences contributing to the core melt frequency are (1) Anticipated Transients Without Scram (ATWS)(44% of the total core melt frequency), (2) Small-small LOCAs (i.e., 3" to 1.9" in diameter) with makeup system failure in the recirculation phase (19% of the total core melt frequency), and (3) the loss of a DC bus followed by failure of secondary heat removal (14% of the total core melt frequency). The estimated core melt frequency for Calvert Cliffs Unit 1 (CC-1) is similar to the values predicted by PRAs of other PWRs.

17. KEY WORDS AND DOCUMENT ANALYSIS
IREP
PRA
Calvert Cliffs

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited Unavailability

19. SECURITY CLASS (This report)
Unclassified

21. NO. OF PAGES
245

20. SECURITY CLASS (This page)
Unclassified

22. PRICE
$

1983-0-776-027/611

☆U.S. GOVERNMENT PRINTING OFFICE:1984—776-027 / 4284

Org.	Bldg.	Name	Rec'd by	Org.	Bldg.	Name	Rec'd by

120555078877 1 IANIRG
US NRC
ADM-DIV OF TIDC
POLICY & PUB MGT BR-PDR NUREG
W-501
WASHINGTON DC 20555

Sandia National Laboratories