November 26, 1986

Richard Kacich
Operating Nuclear Plant Licensing
Northeast Utilities Service Company
Post Office Box 270
Hartford, Connecticut 06141-0270

Dear Mr. Kacich:

SUBJECT: SAI DRAFT REVIEW OF HADDAM NECK
PROBABILISTIC SAFETY STUDY

Enclosed for your review and comment is SAI's draft review of the Haddam Neck Probabilistic Safety Study. Our current schedule is to have SAI finalize this report by January 31, 1987. Therefore, we require your comments and corrections by January 14, 1987. If during your review, you determine that you have extensive comments, please let us know as soon as possible. If you have any questions or need to discuss any part of the report with SAI please contact G. Kelly at 301-492-9427.

Sincerely,

Original signed by: C. I. Grimes

Christopher I. Grimes, Director
Integrated Safety Assessment
Project Directorate
Division of PWR Licensing - B

Enclosure:
As Stated
DISTRIBUTION w/o enclosure*
Docket File
NRC PDR
Local PDR
NSIC*
CGrimes*
PAnderson*
AWang
GKelly*
ISAP Reading
MBoyle*
FCongel
VBenaroya
WRegan
FAkstulewicz*

ISAP:DPL-B	ISAP:DPL-B	ISAP:DPL-B
AW AWang:lt	PAnderson	CGrimes
11/26/86	11/ /86	11/26/86

8612050331 861126
PDR ADOCK 05000213
P PDR

A REVIEW OF THE CONNECTICUT YANKEE (HADDAM NECK) NUCLEAR POWER PLANT PROBABILISTIC SAFETY STUDY



Science Applications International Corporation

SAIC-86/3088

A REVIEW OF THE CONNECTICUT YANKEE (HADDAM NECK) NUCLEAR POWER PLANT PROBABILISTIC SAFETY STUDY

Draft Report

Science Applications International Corporation

Bahman Atefi
Daniel W. Gallagher
Phuoc T. Le
Mary T. Drouin
and
Paul J. Amico*

November 15, 1986

Prepared for

U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Contract No. NRC-03-82-096

8611190217

*Applied Risk Technology Corporation

Post Office Box 1303, 1710 Goodridge Drive, McLean, Virginia 22102, (703) 821-4300

SAIC-86/3088

A REVIEW OF THE CONNECTICUT YANKEE (HADDAM NECK) NUCLEAR POWER PLANT PROBABILISTIC SAFETY STUDY

Draft Report

Bahman Atefi
Daniel W. Gallagher
Phuoc T. Le
Mary T. Drouin
and
Paul J. Amico*

November 15, 1986

Prepared for

U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Contract No. NRC-03-82-096

*Applied Risk Technology Corporation

ACKNOWLEDGEMENTS

This work was supported under Task Order 24 of Contract NRC-03-82-096, "Technical Assistance in Support of Reactor Licensing Actions: Program III." The NRC Project Officer is Mr. S. Singh Bajwa. The work was performed for the Integrated Safety Assessment (ISAP) Directorate, Office of Nuclear Reactor Regulation. Mr. Glenn Kelly of the ISAP Directorate was the technical monitor for the project and participated throughout in many very helpful technical discussions with the review team. Mr. Christopher Grimes, Director, ISAP Directorate, also contributed to the objectives and direction of the review process. The authors would like to thank these individuals for their constructive comments.

Many individuals within SAIC contributed to this report. Mr. Gary DeMoss and Mr. Ernest Lofgren contributed to the development of the methodology for review of the component data base presented in Section 6. Section 8.0 on Operating Experience Analysis was performed by Mr. Stephen Hurrell, Ms. Patti Austin, and Mr. Joseph Minarick. The entire report benefitted from an internal review by Dr. Robert Liner, Dr. David Aldrich, and Mr. Roger Blond. The authors wish to thank these individuals for their insights and contribution to this report.

Finally, the report was patiently prepared by Ms. Margaret Jordan, Mrs. Patricia Hough, and Mrs. Marianne Burns. The authors would like to express their appreciation for the excellent job done by these individuals in typing and editing the report and preparing all the figures.

TABLE OF CONTENTS

Section		Page
ACKNOWLEDGEMENTS		i
LIST OF TABLES		xi
LIST OF FIGURES		xiv
ACRONYMS		xvi
EXECUTIVE SUMMARY		xix
1.0	INTRODUCTION	1-1
1.1	Background	1-1
1.2	Objective, Scope and Review Procedure.	1-2
1.3	Organization of the Report	1-4
2.0	OVERVIEW OF THE HADDAM NECK PLANT DESIGN	2-1
2.1	Safety Functions and Front Line Systems Designed for Mitigation of LOCA Initiators.	2-1
2.2	Safety Functions and Front Line Systems Designed for Mitigation of Transient Initiators	2-10
3.0	INITIATING EVENTS	3-1
3.1	Generic LOCA Initiators.	3-1
3.2	Special LOCA Initiators.	3-5
3.2.1	Unisolated Reactor Coolant Pump Seal Failure	3-5
3.2.2	Steam Generator Tube Rupture	3-6
3.2.3	LOCA Outside Containment	3-7
3.2.4	Catastrophic Pressure Vessel Rupture	3-9

TABLE OF CONTENTS (cont'd)

Section		Page
3.3	Transient Initiating Events	3-9
3.3.1	General Plant Transient	3-11
3.3.2	Total Loss of Main Feedwater	3-11
3.3.3	Main Feedline Break	3-14
3.3.4	Steamline Break Upstream of the Non-Return Valve	3-14
3.3.5	Steamline Break Downstream of the Non-Return Valve	3-15
3.3.6	Loss of Offsite Power	3-17
3.4	Plant-Specific Transient Initiators	3-17
3.4.1	Insufficient Flow of Service Water System	3-19
3.4.2	Loss of Central Air System.	3-20
3.4.3	Loss of Motor Control Center 5 (MCC-5)	3-23
3.4.4	Loss of DC Bus 1.	3-24
3.4.5	Loss of DC Bus 2.	3-24
3.4.6	Total Loss of DC System	3-24
3.4.7	Total Loss of Semi-Vital AC System.	3-24
3.5	Summary	3-24
4.0	REVIEW OF THE EVENT TREE ANALYSIS	4-1
4.1	General Event Tree Findings	4-3
4.1.1	Analysis of Random and Consequential Small LOCAs	4-4
4.1.2	Treatment of Consequential RCP Seal LOCA	4-6
4.1.3	Need for Containment Heat Removal with Bleed-and-Feed	4-9
4.1.4	Treatment of Consequential Loss of Semi-Vital AC (SVA)	4-10
4.1.5	Local Manual Control of Auxiliary Feedwater.	4-11

TABLE OF CONTENTS (cont'd)

Section		Page
4.2	Specific Event Tree Findings	4-11
4.2.1	Large LOCA Event Tree	4-11
4.2.2	Medium LOCA Event Tree	4-13
4.2.3	Small LOCA Event Tree	4-13
4.2.4	Steam Generator Tube Rupture (SGTR) Event Tree	4-17
4.2.5	Steamline Break Upstream of Nonreturn Valves (NRVs) Event Tree	4-20
4.2.6	Steamline Break Downstream of Nonreturn Valves (NRVs) Event Tree	4-20
4.2.7	Main Feedline Break Event Tree	4-24
4.2.8	Unisolated RCP Seal Leakage Event Tree	4-24
4.2.9	General Plant Transient Event Tree	4-26
4.2.10	Total Loss of Main Feedwater Event Tree	4-26
4.2.11	Loss of DC Bus 2 Event Tree	4-26
4.2.12	Loss of Offsite Power (LOSP) Event Tree	4-26
4.2.13	Loss of Offsite Power and MCC-5 Event Tree	4-32
4.2.14	Loss of Offsite Power and One Emergency Bus Event Tree	4-34
4.2.15	Station AC Blackout Event Tree	4-34
4.2.16	Insufficient Flow of Service Water Event Tree	4-36
4.2.17	Loss of Control Air Event Tree	4-38
4.2.18	Loss of MCC-5 Event Tree	4-38
4.2.19	Total Loss of DC Event Tree	4-41
4.2.20	Loss of DC Bus 1 Event Tree	4-44
4.2.21	Loss of Semi-Vital AC Event Tree	4-44
4.2.22	Anticipated Transients Without Scram Event Tree	4-44
4.2.23	Consequential Small LOCA Event Tree	4-44
4.2.24	Consequential Steam Generator Tube Rupture (SGTR) Event Tree	4-49

TABLE OF CONTENTS (cont'd)

Section		Page
5.0	SYSTEM RELIABILITY ANALYSIS REVIEW	5-1
5.1	AC Power System	5-5
	5.1.1 Comments	5-8
	5.1.2 Other Observations	5-8
	5.1.3 Requantification	5-9
5.2	MCC-5 and Semi-Vital AC Power	5-9
	5.2.1 Comments	5-12
	5.2.2 Other Observations	5-12
	5.2.3 Requantification	5-12
5.3	DC Power System	5-14
	5.3.1 Comments	5-14
	5.3.2 Other Observations	5-16
	5.3.3 Requantification	5-17
5.4	Steamline/Feedline Isolation	5-17
	5.4.1 Comments	5-19
	5.4.2 Other Observations	5-19
	5.4.3 Requantification	5-19
5.5	High Pressure Safety Injection (HPSI) System	5-21
	5.5.1 Comments	5-21
	5.5.2 Other Observations	5-24
	5.5.3 Requantification	5-25

TABLE OF CONTENTS (cont'd)

Section		Page
5.6	Low Pressure Safety Injection (LPSI) System	5-25
	5.6.1 Comments	5-25
	5.6.2 Other Observations	5-28
	5.6.3 Requantification	5-28
5.7	Residual Heat Removal (RHR) System	5-28
	5.7.1 Comments	5-29
	5.7.2 Other Observations	5-29
	5.7.3 Requantification	5-32
5.8	Charging System	5-32
	5.8.1 Comments	5-35
	5.8.2 Other Observations	5-35
	5.8.3 Requantification	5-37
5.9	Component Cooling Water System.	5-37
	5.9.1 Comments	5-39
	5.9.2 Other Observations	5-39
	5.9.3 Requantification	5-43
5.10	Service Water System.	5-43
	5.10.1 Comments	5-46
	5.10.2 Other Observations	5-46
	5.10.3 Requantification	5-46

TABLE OF CONTENTS (cont'd)

Section		Page
5.11	Instrument Air System	5-48
	5.11.1 Comments	5-49
	5.11.2 Other Observations	5-49
	5.11.3 Requantification	5-52
5.12	Main and Auxiliary Feedwater System	5-52
	5.12.1 Comments	5-55
	5.12.2 Other Observations	5-55
	5.12.3 Requantification	5-55
5.13	Safety Injection Actuation System	5-57
	5.13.1 Comments	5-60
	5.13.2 Other Observations	5-60
	5.13.3 Requantification	5-60
5.14	Containment Spray System.	5-62
	5.14.1 Comments	5-64
	5.14.2 Other Observations	5-64
	5.14.3 Requantification	5-64
5.15	Containment Air Recirculation Fan System.	5-66
	5.15.1 Comments	5-67
	5.15.2 Requantification	5-67
5.16	Integrated Safety Injection for SGTR.	5-67
	5.16.1 Comments	5-68
	5.16.2 Requantification	5-71

TABLE OF CONTENTS (cont'd)

Section		Page
5.17	Additional Event Quantification	5-71
5.17.1	Comments	5-71
5.17.2	Requantification	5-73
6.0	COMPONENT RELIABILITY ANALYSIS	6-1
6.1	Review of the Component Data Base	6-1
6.2	Review of the Common-Cause Failure Analysis	6-19
7.0	REVIEW OF THE HUMAN RELIABILITY ANALYSIS	7-1
7.1	General Comment on the HRA.	7-1
7.1.1	The Overall HRA Process and Documentation.	7-2
7.1.2	Treatment of the Effect of Loss of Instrumentation	7-2
7.1.3	Consideration of Operator Misdiagnosis	7-7
7.2	Review of the Cognitive Human Errors Analysis	7-9
7.2.1	Cognitive Human Actions Important to the PSS Results	7-16
7.2.2	Cognitive Human Actions Not Important to the PSS Results.	7-19
7.2.3	Additional Cognitive Human Actions Required in the HRA.	7-19
7.2.4	Summary of the Results of the Review of Cognitive Human Errors	7-21
7.3	Review of the Analysis of Manipulative Human Errors	7-21
7.3.1	Manipulative Human Actions Important to the PSS Results.	7-28

TABLE OF CONTENTS (cont'd)

Section		Page
7.3.2	Manipulative Human Actions Not Important to the PSS Results.	7-34
7.3.3	Summary of the Results of the Review of Manipulative Human Actions.	7-35
8.0	OPERATING EXPERIENCE ANALYSIS.	8-1
8.1	Approach.	8-1
8.2	Sources of Information	8-2
8.3	Event Selection	8-2
8.4	Potentially Serious Events.	8-4
8.4.1	Chemical and Volume Control System	8-4
8.4.2	Pressurizer and Associated Equipment	8-7
8.4.3	Emergency AC Power	8-10
8.4.4	Auxiliary Feedwater System	8-14
8.4.5	Containment Air Recirculation (AR) System.	8-17
8.4.6	Reactor Protection System (RPS).	8-19
8.4.7	Main Steam Line Valves and Instrumentation	8-21
8.5	Transient Frequency at Haddam Neck.	8-23
8.6	Potential Impact of Events Observed at Other Plants on Haddam Neck	8-27
8.7	Summary	8-33
9.0	REVIEW OF THE HADDAM NECK PSS EVENT TREE QUANTIFICATION	9-1
9.1	Haddam Neck PSS Quantification Procedure	9-1
9.2	Review of the Haddam Neck PSS Quantification Procedure . .	9-3
9.3	Results of the PSS Quantification Procedure Review	9-6

TABLE OF CONTENTS (cont'd)

Section		Page
9.3.1	Assumptions	9-6
9.3.2	Quantification Errors	9-9
9.3.3	Summary	9-12
10.0	MODEL REQUANTIFICATION, RESULTS AND INSIGHTS	10-1
10.1	Requantification Process	10-1
10.2	Results of the Requantification	10-3
10.3	Insights	10-16
11.0	REFERENCES	11-1

LIST OF TABLES

Table		Page
2.1	LOCA-Mitigating Functions and Front Line Systems	2-3
2.2	Success Criteria for Front Line Systems Used to Mitigate the Consequences of LOCA Initiators	2-5
2.3	Transient-Mitigating Functions and Front Line Systems	2-12
2.4	Success Criteria for Front Line Systems Used to Mitigate the Consequences of Transient Initiators	2-13
3.1	Review of the Haddam Neck LOCA Initiators	3-3
3.2	Review of Special LOCA Initiators Considered in the Haddam Neck PSS	3-10
3.3	Transient Initiators Included in the General Plant Transient Category in the Haddam Neck PSS	3-12
3.4	Review of the Generic Transient Initiators Considered in the Haddam Neck PSS	3-18
3.5	List of All Initiating Events Used in the Haddam Neck PSS	3-26
4.1	Definition of Various Plant Damage States for Core Melt Sequences	4-2
5.1	Support States Modeled in the PSS.	5-4
5.2	MCC-5 Modified System Unavailabilities	5-13
5.3	Steamline/Feedline Isolation System: Modified System Unavailabilities	5-20
5.4	RHR System Modified System Unavailabilities	5-33
5.5	Charging System Modified System Unavailabilities	5-38
5.6	Component Cooling Water System Modified System Unavailabilities	5-44
5.7	Main and Auxiliary Feedwater Systems Modified System Unavailabilities	5-58
5.8	Additional Quantification Methodologies.	5-72
5.9	Additional Events Requantification Results	5-74

LIST OF TABLES (continued)

Table		Page
6.1	Review of the Haddam Neck Plant-Specific Components Failure on Demand	6-3
6.2	Review of the Haddam Neck Plant-Specific Hourly Components Failure Rate	6-5
6.3	Review of the Generic Failure Data Used in the Haddam Neck PSS	6-12
6.4	Results of the Test on Compatibility of the Plant-Specific Data with the Generic Data	6-16
6.5	Review of the Component Failure Data Used in the Haddam Neck PSS	6-20
6.6	Generic Beta Factors for a Select Group of Components	6-25
6.7	Review of the Haddam Neck PSS Common Cause Analysis Results	6-26
7.1	Description of SHARP Steps	7-3
7.2	Adjustment to HEPs for Support State	7-6
7.3	Cognitive Operator Actions Evaluated in the PSS	7-10
7.4	Description of HCR Model Parameters	7-13
7.5	Results of Review of Cognitive Human Errors	7-22
7.6	Manipulative Operator Actions Evaluated in the PSS	7-24
7.7	Results of Review of Manipulative Human Errors	7-36
8.1	Chemical and Volume Control System	8-5
8.2	Pressurizer and Associated Equipment	8-8
8.3	Emergency AC Power	8-11
8.4	Auxiliary Feedwater System	8-15
8.5	Containment Air Recirculation System	8-18
8.6	Reactor Protection System	8-20
8.7	Main Steam Line Valves and Instrumentation	8-22
8.8	Haddam Neck Transient Experience Versus Industry Average	8-24
8.9	Accident Sequence Precursors With Potential Applicability to Haddam Neck	8-28
8.10	Potentially Serious Events Identified	8-34

LIST OF TABLES (continued)

Table		Page
10.1	List of Event Trees That Were Modified in this Review . . .	10-2
10.2	Changes in Accident Initiator Frequencies Used in the Requantification Process	10-4
10.3	Human Error Probabilities Changed or Added in the Review	10-5
10.4	Results of the Review of the Haddam Neck PSS System Unavailabilities	10-6
10.5	Results of the Core Melt Frequency By Initiators	10-11
10.6	List of Dominant Core Melt Sequences Generated as a Result of the Review	10-17

LIST OF FIGURES

Figure		Page
4.1	Large-Break LOCA Event Tree	4-12
4.2	Medium-Break LOCA Event Tree	4-14
4.3	Small LOCA Event Tree	4-15
4.4	Small-Small LOCA Event Tree	4-16
4.5	Steam Generator Tube Rupture Event Tree	4-21
4.6	Steamline Break Upstream of the Nonreturn Valves (NRVs) Event Tree	4-22
4.7	Steamline Break Downstream of the Nonreturn Valve Event Tree	4-23
4.8	Main Feedline Break Event Tree	4-25
4.9	Unisolated RCP Seal Leakage Event Tree	4-27
4.10	General Plant Transient Event Tree	4-28
4.11	Total Loss of Main Feedwater Event Tree	4-29
4.12	Loss of DC Bus 2 Event Tree	4-30
4.13	Loss of Offsite Power Event Tree	4-31
4.14	Loss of Offsite Power and MCC-5 Event Tree	4-33
4.15	Loss of Offsite Power and One Emergency Bus Event Tree	4-35
4.16	Station AC Blackout Event Tree	4-37
4.17	Insufficient Flow of Service Water Event Tree	4-39
4.18	Loss of Control Air Event tree	4-40
4.19	Loss of MCC-5 Event Tree	4-42
4.20	Total Loss of DC Event Tree	4-43
4.21	Loss of DC Bus 1 Event Tree	4-45
4.22	Loss of Semi-Vital AC Event Tree	4-46
4.23	Anticipated Transient Without Scram Event Tree	4-47
4.24	Consequential Small LOCA Event Tree	4-48
4.25	Consequential Steam Generator Tube Rupture Event Tree	4-50
5.1	Simplified Schematic of the CY Electrical Distribution System	5-6
5.2	AC Power Dependency Diagram	5-7
5.3	MCC-5 and Semi-Vital AC System Diagram	5-10
5.4	Semi-Vital AC and MCC-5 Dependency Diagram	5-11
5.5	DC Power System Dependency Diagram	5-15

LIST OF FIGURES (Continued)

Figure		Page
5.6	Steamline/Feedline Isolation System Dependencies Diagram	5-18
5.7	Simplified Flow Diagram for HPSI System	5-22
5.8	High Pressure Safety Injection System Dependency Diagram	5-23
5.9	Simplified Flow Diagram for LPSI System	5-26
5.10	Low Pressure Safety Injection System Dependency Diagram	5-27
5.11	Simplified Flow Diagram for RHR System.	5-30
5.12	RHR System Dependency Diagram	5-31
5.13	Simplified Flow Diagram for Charging System.	5-34
5.14	Charging System Dependency Diagram	5-36
5.15	Simplified Flow Diagram for CCW System	5-40
5.16	CCW System Dependency Diagram.	5-42
5.17	Simplified Flow Diagram for SW System.	5-45
5.18	SW System Dependency Diagram	5-47
5.19	Simplified Flow Diagram for Control Air System	5-50
5.20	Control Air System Dependency Diagram.	5-51
5.21	Simplified Flow Diagram for PCS/AFW System	5-54
5.22	AFW System Dependency Diagram	5-56
5.23	SIAS Logic Diagram	5-59
5.24	SIAS Dependency Diagram.	5-61
5.25	Containment Spray System	5-63
5.26	Containment Spray System Dependency Diagram.	5-65
5.27	Simplified Flow Diagram for Integrated SI System	5-69
5.28	Integrated SI System Dependency Diagram.	5-70
7.1	Human Error Fault Tree for Node LTC.	7-31
7.2	Data Worksheet Associated With Human Error Fault Tree for Node LTC	7-32
10.1	Results of the Core Melt Frequency By Initiators	10-12

ACRONYMS

AEC	Atomic Energy Commission
AFWS	Auxiliary Feedwater System
AOV	Air Operated Valve
APS	Accident Precursor Study
ATWS	Anticipated Transient Without Scram
BAF	Bleed and Feed
CARFANS	Containment Air Recirculation Fans
CCWS	Component Cooling Water System
CHR	Containment Heat Removal
CLCW	Closed Cooling Water (System)
CMF	Core Melt Frequency
CRDM	Control Rod Drive Mechanism
CST	Condensate Storage Tank
CSs	Containment Sprays
CVCS	Chemical and Volume Control System
DG	Diesel Generator
ECCS	Emergency Core Cooling System
ER	Emergency Boration
ETA	Event Tree Analysis (Computer Code)
FANs	Containment Recirculation Fan Coolers
FCV	Flow Control Valve
FW	Feedwater
HCR	Human Cognitive Reliability (Model)
HEP	Human Error Probability
HPR	High Pressure Recirculation
HPSI	High Pressure Safety Injection
HRA	Human Reliability Analysis
IA	Instrument Air (system)
IREP	Interim Reliability Evaluation Program
ISAP	Integrated Safety Assessment Program
LER	Licensee Event Report
LOCA	Loss of Coolant Accident
LOSP	Loss of Offsite Power
LPSI	Low Pressure Safety Injection
LTOP	Low Temperature Overpressure (lines)
MCC	Motor Control Center
MFWS	Main Feedwater System
MSIV	Main Steam Isolation Valve

MSTV	Main Steam Trip Valve
MWe	Megawatt Electric
MWth	Megawatt Thermal
NRC	Nuclear Regulatory Commission
NRR	Nuclear Reactor Regulation (NRC Office)
NRV	Nonreturn valve (steamline)
NUSCO	Northeast Utilities Services Company
OA	Operator Action
OAT	Operation Action Tree
PAB	Primary Auxiliary Building
PCS	Power Conversion System
PD	Primary Depressurization
PIT	Primary Integrity
PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSS	Probabilistic Safety Study
PWR	Pressurized Water Reactor
RCP	Reactor Coolant Pump
RHR	Residual Heat Removal System
RMQS	Risk Management Query System (Computer Code)
RPS	Reactor Protection System
RWST	Refueling Water Storage Tank
SAIC	Science Applications International Corporation
SBD	Secondary Blowdown
SEP	Systematic Evaluation Program
SG	Steam Generator
SGC	Steam Generator Cooling
SGTR	Steam Generator Tube Rupture
SHARP	Systematic Human Action Reliability Procedure
SIAS	Safety Injection Actuation System
SOV	Solenoid Operated Valve
SRO	Senior Reactor Operator
SRV	Safety Relief Valve
SS	Shift Supervisor
SSR	Secondary Steam Relief
SVA	Semi-vital AC (system)
SWS	Service Water System

ACRONYMS (continued)

THERP	Technique for Human Error Rate Prediction
TMI	Three Mile Island
TPR	Two Path Recirculation
TRC	Time Reliability Correlation
VCT	Volume Control Tank

EXECUTIVE SUMMARY

Science Applications International Corporation (SAIC), under contract to the U.S. Nuclear Regulatory Commission (NRC), has conducted a review of the Connecticut Yankee (Haddam Neck) Plant Probabilistic Safety Study (PSS). The Haddam Neck PSS is a "Level 1" study that examines accidents arising from internally initiated events. This study was performed by the Northeast Utilities Services Company (NUSCO) as a part of the NRC's Integrated Safety Assessment Program (ISAP) for this plant. This program was initiated by the NRC to assess, prioritize, and resolve all outstanding regulatory or safety-related issues for each nuclear power plant. One of the requirements of this program is performance by the licensee of a plant-specific Probabilistic Safety Assessment (PSA) for the plant under consideration. There are two reasons for conducting a plant-specific PSA. The first is to identify any areas of plant vulnerability due to weaknesses in the plant design, hardware, or procedures. The second is to provide a probabilistic basis for resolving those NRC-required or utility-sponsored safety or regulatory issues that are amenable to probabilistic analysis. The program was initiated in 1985 on the basis of voluntary participation by licensees. The first plants volunteered by their licensee to participate in this program were Northeast Utilities' Millstone Nuclear Power Station Unit 1 and Haddam Neck Nuclear Power Plant.

The objectives of this review were to validate the results of the Haddam Neck PSS, identify and resolve technical disagreements with the licensee's analysis, and document any unresolved differences. The review has met the objective of validating the PSS in the sense that the PSS results were reproduced within a very small margin of error using the licensee's models and assumptions. The Haddam Neck core melt model was next revised based on changes to event trees, initiating event frequencies, system models, component data, and human error probabilities produced in this review. As a result of the requantification, the total core melt frequency increased by 50%. This change in itself is not significant. However, the recommended changes are significant to the extent they provide a more qualitatively accurate model of the plant's response to accident initiators.

The scope of this review includes initiating events, event tree analysis, system modeling, component failure data, human reliability analysis, plant operating history, quantification, and dominant core melt sequences. In reviewing each of these topics, the emphasis was placed on verifying the accuracy, completeness, and correct representation of the dominant contributors to the core melt frequency for the Haddam Neck plant. Throughout this review, an attempt was made to use realistic assumptions and to replace any overly conservative assumptions in the PSS with more realistic assumptions. This is quite important for two reasons. First, the objective of the Haddam Neck PSS is to provide a realistic picture of the core melt portion of the risk associated with the operation of this plant. Overly conservative assumptions can distort this picture. Second, the results of the PSS are used to resolve some of the Haddam Neck ISAP topics. Conservative assumptions in some areas of the PSS can distort the true risk or safety significance of some topics, which could result in diversion of the utility's resources and implementation schedule away from the most risk or safety-significant topics.

The review process began with a meeting between the review team, the utility analysts, and the NRC staff. In this meeting, the utility analysts presented the results of the Haddam Neck PSS. The principal source of information throughout the review was the Haddam Neck PSS. Following an initial review period, preliminary results of the review of the initiating events, event tree analysis, and a portion of the fault tree analyses were submitted to the NRC as an interim report. A second meeting between the review team, the utility analysts, and the NRC staff was held to discuss the questions and comments in the interim report and to review the more detailed documents that were not included in the Haddam Neck PSS report. In addition to these meetings, conference calls between the review team, the utility analysts, and the NRC staff were used throughout the review process for quick resolution of technical questions or comments. This iterative review process was extremely important in ensuring correct interpretation of the PSS evaluation process and results by the review team and contributed to the effectiveness of the review.

More complete and thorough documentation of the PSS would have facilitated the review process and reduced the number of questions. Documentation of several areas in the PSS, namely, component

unavailabilities due to test and maintenance outages, fault tree analysis, human reliability analysis, and especially the quantification process, was not as complete as it could have been. The review team thus had to spend several days at the utility headquarters to review the details not included in the PSS report and had to make several conference calls to corroborate quantification assumptions.

To verify the results of the Haddam Neck PSS and the review team's understanding of the quantification process, the PSS model was quantified using the licensee's data, model, and assumptions. All the Haddam Neck PSS dominant accident sequences were generated using an SAIC proprietary computer code. Only a few minor errors and conservative assumptions were found in the PSS quantification process. Numerically, the effect of these errors on the total core melt frequency was on the order of 2%. More importantly, these minor errors had almost no effect on the selection of the dominant accident sequences in this model.

Following duplication and verification of the PSS results, the Haddam Neck core melt model was revised based on a series of changes to a number of the event trees. This revised model was requantified using changes in initiating event frequencies, system models, component data, and human error probabilities produced in this review. The change in core melt frequency for each initiator category is shown in Table 1. The total core melt frequency as a result of the requantification increased from 5.4E-4 per year to 8.1E-4 per year, i.e., by about 50%. This change in core melt frequency in itself is not very significant. What is significant are the changes in the contribution of different initiators to the core melt frequency, the creation of new dominant accident sequences, and the rearrangement of the PSS dominant core melt sequences as a result of the review and requantification.

Five major factors contributed to changes in the relative importance of the dominant contributors to the PSS core melt frequency. The first is related to the rate of Reactor Coolant Pump (RCP) seal leakage given total loss of cooling to all four RCP seals. In the PSS, it was assumed that the maximum flow rate per RCP given seal failure is 50 gpm, which led to the conclusion that even if all four RCP seals fail, the normal plant makeup system can provide the lost coolant. In this review, this

Table 1. Results of the Core Melt Frequency By Initiators

Accident Initiator	Core Melt Frequency (Percent Contribution) PSS	Review Results
1. Small-Break LOCA	1.3E-4 (24%)	1.2E-4 (15%)
2. New Small-Small Break LOCA	-	5.4E-6 (0.6%)
3. Loss of Offsite Power	1.2E-4 (22%)	2.0E-4 (25%)
4. Medium-Break LOCA	8.1E-5 (15%)	1.4E-4 (17%)
5. General Plant Transient	5.3E-5 (10%)	1.1E-4 (14%)
6. Loss of MCC-5	3.3E-5 (6%)	6.8E-5 (8%)
7. Loss of DC Bus 1	2.9E-5 (5%)	1.1E-5 (1%)
8. Total Loss of Main Feedwater	1.3E-5 (2%)	2.2E-5 (2.7%)
9. Large-Break LOCA	1.2E-5 (2%)	1.1E-5 (1%)
10. Steamline Break Downstream of NRV	1.1E-5 (2%)	4.9E-6 (0.6%)
11. Steam Generator Tube Rupture	1.0E-5 (2%)	4.8E-5 (6%)
12. Unisolated RCP Seal Leakage	8.4E-6 (2%)	8.2E-6 (1%)
13. Main Feedline Break	7.4E-6 (1%)	8.7E-6 (1%)
14. Steamline Break Upstream of NRV	7.0E-6 (1%)	7.6E-6 (1%)
15. Insufficient Flow of Service Water	5.9E-6 (1%)	3.2E-6 (0.4%)
16. LOCA Outside Containment	5.4E-6 (1%)	1.0E-5 (1%)
17. Total Loss of DC Power	4.4E-6 (0.8%)	4.4E-6 (0.5%)
18. Loss of Control Air	3.4E-6 (0.1%)	1.4E-5 (2%)
19. Loss of DC Bus 2	2.6E-6 (0.4%)	8.4E-7 (0.1%)
20. Loss of Semi-Vital AC	1.3E-6 (0.2%)	1.6E-5 (2%)
Total	5.4E-4	8.1E-4

assumption was not accepted and an average flow rate of 100 gpm per pump was suggested. This change resulted in classification of this event as a small-small break LOCA, requiring both high pressure injection and recirculation.

The second factor, which again is due to the RCP seal leakage rate, is related to the station blackout sequences where because of a higher assumed RCP seal leakage rate, the offsite power recovery times before core uncovery for different scenarios were essentially cut in half.

The third factor that had a large impact on the results was the addition of a cognitive operator error in manually controlling the Auxiliary Feedwater System (AFWS) in all event trees in which actuation and control of this system is lost from the control room.

The fourth major factor was the division of the PSS small-break LOCA range into two break size ranges. The reason for this division was that the systems required to mitigate the consequences of a small LOCA in the lower range of this break size are different from the upper range of this break size. Specifically, in the lower range (which in this review is called new small-small break LOCA), coolant flow out of the break is not sufficient to remove decay heat, so decay heat removal using steam generator cooling is required. Steam generator cooling for decay heat removal is not necessary for the upper end of this break range (new small-break LOCA). Since there are more alternative methods for keeping the core covered and cooled in the small-small break range than in the small-break range, and the RCP seal failure falls in the small-small break range, the adverse effects of the first factor, namely, large RCP seal leakage, were somewhat limited by this division.

The fifth major factor which affected the core melt profile of this plant is a more realistic treatment of the initiating event frequencies and recovery potential for the "Loss of Motor Control Center 5 (MCC-5)" and "Loss of Control Air" initiating events. These assumptions prevented the contribution from these initiators from becoming very dominant due to effects of the first and third changes discussed above.

As a result of the review process, a series of insights into areas of plant vulnerability were gained. In the revised model, approximately 68%

of the total core melt frequency can be attributed to sequences that include failure of the high pressure recirculation (HPR) function. The high failure probability of this function is due to two basic reasons. The first is that the charging system in this plant can only inject into Loop 2. Thus, if the LOCA is due to a break in Loop 2, the recirculation function is lost. The second reason is that the switchover from high pressure injection to recirculation is a manual operation. This introduces two additional potential causes of failure for this function compared to automatic switchover systems, namely the cognitive and manipulative operator errors. In one of the ISAP topics (Topic 1.27), the licensee has suggested addition of an alternative HPR path through the use of the high pressure safety injection (HPSI) pump as a backup to the charging pumps. This change would reduce the contribution to the core melt frequency from sequences including failure of HPR from 68% to about 30%.

The second area of plant vulnerability is the loss of Motor Control Center 5 (MCC-5). In the revised model, failure of MCC-5 contributes approximately 12% to the total core melt frequency. The reason for this large contribution to the core melt frequency is that MCC-5 provides the only non-redundant power source to a number of key safety system valves and instruments. The licensee is considering several alternatives for correcting this situation.

The third area of plant vulnerability is the dependence of the auxiliary feedwater system (AFWS) on control air. If air is not available to several AFWS air-operated valves, operator action must be taken to control AFW locally in the pump room. In the revised model, sequences including this dependency contribute 12% of the total core melt frequency. One potential fix for this problem would be the installation of backup compressed air bottles for the auxiliary feedwater system, which would eliminate the total dependency of the system on control air.

In addition to the above areas of plant vulnerability, a series of insights about methodology and assumptions used in the probabilistic analyses in general and in the Haddam Neck PSS specifically, were gained from the review process. They are presented in Section 10.0 of this report.

In summary, except for the changes discussed above, the review indicates that the model developed in the Haddam Neck PSS adequately represents the core melt profile associated with the operation of this plant.

1.0 INTRODUCTION

Science Applications International Corporation (SAIC), under contract to the Nuclear Regulatory Commission (NRC), has reviewed a plant-specific Probabilistic Safety Study (PSS) and an analysis of a series of safety-related issues performed by the Northeast Utilities Services Company (NUSCO) for the Connecticut Yankee (Haddam Neck) Plant. Both the licensee's study and SAIC's review are part of the NRC's Integrated Safety Assessment Program (ISAP) for this plant. This report presents the results of the Haddam Neck PSS review.

1.1 Background

The Integrated Safety Assessment Program (ISAP) was initiated by the NRC to examine the outstanding regulatory and safety-related requirements or issues pertinent to each nuclear power plant. The primary objective of this program is to assess the importance of each requirement or issue with respect to its impact on the risk associated with the operation of the plant and to prioritize the issues and develop an appropriate schedule for implementation of changes necessary for resolution of these issues. The ISAP pilot program was initiated in 1985 on the basis of voluntary participation by licensees. The first plants volunteered by their licensee to participate in the pilot program were Northeast Utilities' Millstone Nuclear Power Station Unit 1 and the Haddam Neck Nuclear Power Plant.

The issues, or "ISAP topics," that are considered for each plant include:

1. Issues identified in Phase II of the Systematic Evaluation Program (SEP), pending licensing requirements including TMI Action Plan items for the particular facility, pending Unresolved and Generic Safety Issues, and licensee-initiated improvement projects.

2. Significant events that have occurred during the operation of the plant.

3. Dominant contributors to plant risk based on a plant-specific Probabilistic Safety Analysis (PSA).*

The first plant evaluated under this program was Northeast Utilities' Millstone Unit 1. The second plant being evaluated under this program is Northeast Utilities' Connecticut Yankee (Haddam Neck) Plant, a 590 MWe pressurized water reactor. The utility recently performed a "level 1" Probabilistic Safety Study (PSS) that examines internally initiated events at the plant (1). This study is the subject of our review. In addition, the licensee is currently in the process of evaluating some of the ISAP topics using probabilistic techniques. These topics will also be examined on the basis of the PSS and this review and the results will be presented in a separate report.

1.2 Objective, Scope and Review Procedure

The objective of this study is a detailed review of the Haddam Neck PSS. The purpose of this detailed review is to validate the results of the PSS, identify and resolve technical disagreements with the licensee's analysis, and document any unresolved differences. The outcome of the review should provide the basis for the NRC to accept and use the Haddam Neck PSS in regulatory decision-making in general, and to resolve the ISAP topics in particular.

The scope of this study includes review of the initiating events, event tree analysis, system modeling, component failure data, human reliability analysis, operating experience, quantification, and the dominant core melt sequences. In reviewing each of these topics, the emphasis was placed on ensuring the accuracy, completeness, and correct representation of the core melt contribution to risk associated with the operation of the plant.

The principal source of information throughout the review process was the Haddam Neck PSS (1). Shortly after the initiation of the project, a three-day meeting was held between the SAIC review team, NRC staff, and the

---

* The terms "Probabilistic Safety Assessment" (PSA) and "Probabilistic Risk Assessment" (PRA) are synonymous.

utility analysts. In this meeting the utility analysts presented the results of the Haddam Neck PSS and the insights they had gained from the study.

The initial results of the review were documented in an interim report which contained the preliminary results of the review of the initiating events, event tree analysis, and a portion of the fault tree analyses (2). Several questions about the assumptions used in the development of various areas of the Haddam Neck PSS were included in this interim report.

A second meeting with the utility analysts and the NRC staff was held to discuss the questions and comments included in the interim report and to review some of the more detailed documents that were not included in the Haddam Neck PSS report. The areas where more detailed information was necessary included the system fault trees, calculational files for the human reliability analysis, and quantification assumptions.

To verify the results of the Haddam Neck PSS and the review team's understanding of the quantification process, the PSS model was quantified using the licensee's data, models, and assumptions. All the Haddam Neck PSS dominant accident sequences were generated using SAIC's proprietary computer code Risk Management Query System (RMQS) (3). This was followed by requantification of the model based on changes to initiating event frequencies, event tree models, system unavailabilities, and human error calculations produced as a result of this review. The differences in the results and the dominant accident frequencies are discussed in detail in Section 10.0.

Throughout this review, an attempt was made to replace overly conservative assumptions in the Haddam Neck PSS with realistic assumptions. This was done for two reasons. First, the objective of the PSS is to provide a realistic picture of the plant's operational risk and overly conservative assumptions can distort this picture. Second, the results of the Haddam Neck PSS are used for the resolution of some of the Haddam Neck ISAP topics. Conservative assumptions in some areas of the PSS could distort the true risk or safety importance of the topics. This could result in diversion of the utility's resources and implementation schedule toward those topics that are not the most risk or safety significant.

1.3 Organization of the Report

Section 2.0 contains an overview of the plant design, including success criteria for all the front-line systems used for mitigation of loss-of-coolant and transient-initiated accidents. Section 3.0 deals with the review of all accident initiators identified in the Haddam Neck PSS, including both generic and plant-specific initiators. For each initiator, a unique event tree was developed in the PSS. Section 4.0 includes a detailed review of all the event trees. Section 5.0 contains a review of all the fault trees used for modeling the systems in the plant. The component data and common-cause analyses used for quantifi-cation of the fault trees are reviewed in Section 6.0. The PSS human reliability analysis, encompassing both cognitive and manipulative errors, is reviewed in Section 7.0. Section 8.0 presents the results of the review of the Haddam Neck Plant operating history based on the Licensee Event Reports (LERs). Section 9.0 contains the review of the Haddam Neck accident sequence quantification. The results of the requantification of the Haddam Neck PSS model based on changes to initiating events, event tree models, component data, system reliability analysis and human error probabilities produced as a result of the review are presented in Section 10.0. This section also includes the insights gained from this review process. All references cited in this report are listed in Section 11.0.

2.0 OVERVIEW OF THE HADDAM NECK PLANT DESIGN

The Haddam Neck Plant is a 582 MWe (1,825 MWth) four loop pressurized water reactor (PWR) located on the Connecticut River about twenty-one miles south of Hartford, Connecticut. The nuclear steam supply system and the turbine generator were supplied by Westinghouse Electric Corporation. Stone and Webster was the architect-engineer and the constructor of the plant. The reactor containment is designed for an internal pressure of 40 psig.

The Facility Description and Safety Analysis Report for Haddam Neck Plant was submitted to the Atomic Energy Commission (AEC) on July 19, 1966, and the interim facility license was issued on June 30, 1967. Commercial operation of the plant began January 1, 1968 and the NRC granted a Full Term Operating License on December 27, 1974. Although the plant was designed and constructed in the early years of commercial nuclear power, its basic design is similar to the more recent Westinghouse PWRs.

The critical safety functions that must be performed at this plant to mitigate the progression of an accident are dependent on the nature of the accident initiator. Accident initiators can be grouped into two broad categories: Loss-of-Coolant Accident (LOCA) initiators and transient initiators. The LOCA category in the Haddam Neck PSS includes 7 initiators. The transient category in this study consists of 17 initiators. A unique event tree was developed for each of these initiators in the Haddam Neck PSS. In the next section, the safety functions and associated front-line systems designed for mitigation of each LOCA initiator are discussed. The discussion includes the success criteria for the operation of each of the front line systems. This is followed in Section 2.2 by a discussion of the functions and front line systems designed for mitigation of the transient initiators.

2.1 Safety Functions and Front Line Systems Designed for Mitigation of LOCA Initiators

To mitigate the progression of a LOCA to core meltdown, several functions must be performed. These include reactor shutdown to keep the reactor subcritical, emergency core cooling to make sure the core is covered

and cooled, and containment overpressure protection to avoid containment failure. If the accident progresses to core meltdown, an additional function, namely, containment fission product removal, also must be performed to minimize radioactivity release to the environment. Table 2.1 lists the front line systems used for mitigating LOCAs in this plant along with a description of their basic configuration. The success criteria for these front line systems for each of the LOCA initiators analyzed in the Haddam Neck PSS are shown in Table 2.2.

Following a large LOCA, the reactor automatically becomes subcritical so no system must operate successfully to satisfy the subcriticality function. The emergency core cooling function in all the LOCA cases can be divided into a short term phase, which usually includes injection of coolant into the core for immediate replenishment of the lost coolant, and a long term phase which usually includes recirculation of the coolant for long term cooling of the core. In the case of a large LOCA, the injection function can be provided by the Low Pressure Safety Injection (LPSI) system and the recirculation requirement can be satisfied by the successful operation of Residual Heat Removal (RHR) system pumps taking suction from the sump and delivering coolant to the core through RHR heat exchangers. Heat from the secondary side of the RHR heat exchangers would be removed by the Service Water System (SWS). Containment overpressure protection can be performed by removal of containment heat via Containment Recirculation Fan Coolers (FANs) or Containment Sprays (CSs). The CS is provided by LPSI pumps along with RHR pumps or fire pumps. If the accident progresses to core meltdown, the fission product removal function can be provided by the containment spray subfunction of containment heat removal.

For medium-break LOCAs, again the reactor subcriticality function is provided automatically since the reactor becomes subcritical following the accident. The injection phase of the emergency core cooling function is provided by the High Pressure Safety Injection (HPSI) system and the long term recirculation function is provided by RHR pumps taking suction from the containment sump and delivering the coolant to charging pumps. The containment heat removal function is the same as for the large-break LOCA.

Table 2.1 LOCA-Mitigating Functions and Front line Systems

Function	System (Abbreviation)	Configuration
Reactor Subcriticality	Reactor Protection System (RPS)	
Emergency Core Cooling (Injection)	Charging System	Two 360 gpm centrifugal pumps take suction from RWST, injecting 2300 psig coolant into Loop 2 cold leg only. A third 30 gpm positive displacement pump (metering pump) is used to cool RCP seals during emergency or shutdown conditions.
	High Pressure Safety Injection (HPSI)	Two HPSI pumps take suction from RWST and inject coolant at a pressure below 1500 psig into the cold leg of each reactor coolant loop.
	Low Pressure Safety Injection (LPSI)	Two LPSI pumps capable of injecting at a pressure below 350 psig to the core via four ports in the reactor head.
	Main Feedwater (MFW)	Two 50% capacity motor-driven pumps delivering coolant to four steam generators.
	Auxiliary Feedwater (AFW)	Two 100% capacity turbine-driven pumps delivering coolant to four steam generators. A third motor-driven, non-emergency powered, non-safety grade pump is available for startup.
	HPSI and charging systems along with PORVs in connection with Bleed-and-Feed (BAF)	HPSI and charging configurations are the same as above. The PORVs consist of two motor-operated valves set at 2270 psig. There are also two air-operated block valves in series with PORVs that must open.

Table 2.1 LOCA-Mitigating Functions and Front line Systems (continued)

Function	System (Abbreviation)	Configuration
Emergency Core Cooling (Recirculation)	High Pressure Recirculation (HPR)	Two charging pumps taking suction from residual heat removal (RHR) system discharge injecting to Loop 2 cold leg. Heat from the secondary side of the RHR heat exchangers is removed by the service water system (SWS).
	Low Pressure Recirculation (LPR)	Two RHR pumps taking suction from the sump and injecting into the core. Heat from the secondary side of RHR heat exchangers is removed by SWS.
Containment Overpressure Protection	Containment Air Recirculation (CAR)	Four 65,000 cpm fan cooler units. Service water system provides the cooling water.
	Containment Spray (CS) (During Injection)	LPSI pump(s) taking suction from RWST and delivering to spray header ring inside containment. The backup system is the two fire pumps taking suction from RWST and delivering to spray header rings. Fire pumps are also capable of taking suction from the river water.
	Containment Spray (CS) (During Recirculation)	RHR pumps taking suction from the sump and delivering coolant to the spray header ring.
Fission Product Removal	Containment Spray (CS)	Same as containment overpressure protection.

Table 2.2 Success Criteria for Front Line Systems Used to Mitigate the Consequences of LOCA Initiators

Initiator	Reactor Subcriticality	Emergency Core Cooling		Containment Overpressure Protection and Fission Product Removal
		Short Term	Long Term	
Large-break LOCA	None	1/2 LPSI	1/2 RHR	2/4 FANs OR Containment Spray (CS): 2/2 LPSI + 2/2 RHR + injection OR 1/2 LPSI + 1/2 RHR OR 1/2 Fire Pump + 2/2 RHR OR 1/2 Fire Pump + River Water
Medium-break LOCA	None	1/2 HPSI + 3/3 Loops OR 2/2 HPSI + 2/3 Loops	1/2 Charging + 1/2 RHR	Same as Large-break LOCA
PSS Small-break LOCA	RPS	1/2 MFW + 1/2 HPSI + 3/3 Loops OR 1/2 MFW + 2/2 HPSI + 2/3 Loops OR 1/2 AFW + 1/2 HPSI + 3/3 Loops OR 1/2 AFW + 2/2 HPSI + 2/3 Loops OR 1/2 MFW + 1/2 Charging OR 1/2 AFW + 1/2 Charging	Same as Medium-break LOCA	Same as CS function of Large-break LOCA

Table 2.2 Success Criteria for Front Line Systems Used to Mitigate the Consequences of LOCA Initiators (continued)

Initiator	Reactor Subcriticality	Emergency Core Cooling		Containment Overpressure Protection and Fission Product Removal
		Short Term	Long Term	
New Small-small Break LOCA Consequential Small-small LOCA (seals)	RPS	All the PSS Small-break LOCA OR Bleed-and-Feed:(1) (1/2 Charging + 1/2 PORVs OR 1/2 HPSI + 2/2 PORVs) OR Secondary Blowdown:(1) (1/2 MFW + SSR + 1/2 LPSI OR 1/2 AFW + SSR + 1/2 LPSI)	1/2 Charging + 1/2 RHR OR 1/2 MFW + SSR + 1/2 RHR OR 1/2 AFW + SSR + 1/2 RHR	Same as CS function of Large-break LOCA
New Small-break LOCA Consequential Small LOCA (PORVs)	RPS	1/2 HPSI + 3/3 Loops OR 2/2 HPSI + 2/3 Loops OR 1/2 Charging	Same as PSS Small-break LOCA	Same as CS function of Large-break LOCA
Unisolated Reactor Coolant Pump seal failure	RPS	1/2 MFW + 1/2 Charging OR 1/2 AFW + 1/2 Charging OR 1/2 MFW + SSR + 1/2 LPSI OR	1/2 Charging + 1/2 MFW OR 1/2 Charging + 1/2 AFW OR 1/2 MFW + SSR + 1/2 HPSI(1) OR 1/2 AFW + SSR + 1/2 HPSI(1)	

Table 2.2 Success Criteria for Front Line Systems Used to Mitigate the Consequences of LOCA Initiators (continued)

Initiator	Reactor Subcriticality	Emergency Core Cooling		Containment Overpressure Protection and Fission Product Removal
		Short Term	Long Term	
		1/2 AFW + SSR + 1/2 HPSI OR Bleed-and-Feed: (1/2 Charging + 1/2 PORV OR 1/2 HPSI + 2/2 PORV + 3/3 Loops OR 2/2 HPSI + 2/2 PORV + 2/3 Loops)		Same as Large-break LOCA
Steam Generator Tube Rupture Consequential Steam Generator Tube Rupture	RPS	1/2 MFW + 1/2 Charging OR 1/2 AFW + 1/2 Charging OR 1/2 MFW + 1/2 HPSI + 3/3 Loops OR 1/2 MFW + 2/2 HPSI + 2/3 Loops OR 1/2 AFW + 1/2 HPSI + 3/3 Loops OR 1/2 AFW + 2/2 HPSI + 2/3 Loops OR Bleed-and-Feed: (1/2 Charging + 1/2 PORV OR 1/2 HPSI + 2/2 PORV + 3/3 Loops OR 2/2 HPSI + 2/2 PORV + 2/3 Loops)	SG isolation + 1/2 MFW + PD OR SG isolation + 1/2 AFW + PD OR Loop isolation + 1/2 MFW OR Loop isolation + 1/2 AFW OR 1/2 RHR + PD(2) OR SG isolation + 1/2 RHR + PD(1)	Same as CS function of Large-break LOCA

(1) These success criteria were not used in the Haddam Neck PSS but were included in our model.

(2) This success criterion was not accepted in our review as discussed in Section 4.2.4.

The small-break LOCA in the Haddam Neck PSS corresponds to break sizes with equivalent diameter ranging from 3/8 inch, which approximately corresponds to the plant's normal make-up capability up to 2 inches. Included in this range is the small-break LOCA due to non-isolable spurious opening of the Pressurizer Power Operated Relief Valves (PORVs). For the lower end of this break size, from 3/8 inch to 3/4 inch, coolant flow out of the break is not sufficient to remove decay heat, so steam generator cooling is needed to remove the decay heat. Decay heat removal using steam generator cooling is not necessary in the upper end of this break range. In our review of the Haddam Neck PSS event trees, it was decided to divide the small-break LOCA into two ranges: 3/8 inch to 3/4 inch, where steam generator cooling is required, and 3/4 inch to 2 inches, where steam generator cooling is not required. The reason for this division is discussed in Section 4.1.1. The newly created lower range is called "new small-small break LOCA" and the upper range is the "new small-break LOCA."

For the PSS small-break LOCA, i.e., breaks from 3/8 inch to 2 inches equivalent diameter, the subcriticality function is provided by the successful insertion of the Reactor Protection System (RPS) control rods. The injection phase of emergency core cooling can be satisfied by a combination of HPSI or charging systems for injection and Main Feedwater (MFW) or Auxiliary Feedwater (AFW) systems for decay heat removal. The high pressure recirculation success criterion in this case is the same as for the medium-break LOCA. In this break range, containment heat removal is not necessary to prevent core melt due to containment failure. Fission product removal would be needed if the accident progresses to core meltdown due to failure of other emergency systems. The success criteria for the fission product removal function are the same as for the containment spray (CS) function of the large-break LOCA.

For the newly designated small-small break LOCA, the subcriticality function is provided by the RPS. The injection function in this case can be satisfied by all the combinations of systems mentioned above for the PSS small-break LOCA or by bleed-and-feed if injection by HPSI or charging pumps is available but steam generator cooling is lost. If injection by HPSI or charging pumps is not available but steam generator cooling is available, secondary blowdown can be performed to reduce the primary pressure so that Low Pressure Safety Injection (LPSI) could be used for the

injection phase. The success criteria for the recirculation function would depend on the condition of the core at the time recirculation is needed. If the core is at high pressure and charging pumps are available, high pressure recirculation would be used. If the core is at high pressure but charging pumps are unavailable, the primary pressure must be reduced by secondary blowdown so that low pressure long-term recirculation using the RHR system can be used. Finally, if the primary pressure is low at the time of recirculation, which would be the case if secondary blowdown is used, the RHR system can provide the long-term recirculation requirement. Containment overpressure protection is only needed if bleed-and-feed is used. If fission product removal is needed, the success criteria are the same as CS in large-break LOCA. The same functional success criteria apply to the consequential small LOCA, which occurs due to loss of coolant to all Reactor Coolant Pumps (RCPs) and subsequent failure of the seals. It should be noted that in the Haddam Neck PSS it was assumed that normal plant makeup can provide the lost primary coolant through RCP seals. In our review, the rate of RCP leakage was assumed to be higher than in the PSS. This resulted in categorization of the RCPs seal failure as a small-small LOCA. This subject is discussed in more detail in Section 4.1.2.

For the newly designated small-small LOCA, the subcriticality function is provided by the RPS. The injection function in this case can be provided by HPSI or charging systems. The recirculation function success criterion is the same as for the PSS small-break LOCA. There is no requirement for containment heat removal and fission product removal function success criteria are the same as for the PSS small-break LOCA.

The next LOCA initiator is the Unisolated Reactor Coolant Pump (RCP) seal failure. This event refers to random failure of one RCP seal where the leakage rate is lower than for the lower end of the new small-small break LOCA. The subcriticality function is provided by the RPS. The short-term cooling function can be provided by charging pumps providing the lost coolant and main or auxiliary feedwater systems for removing decay heat. Another method of providing injection to the core is by lowering the primary pressure sufficiently so that the high pressure safety injection system can be used. If steam generator cooling is unavailable, the bleed-and-feed procedure must be used to remove decay heat and depressurize the primary system. The long-term cooling function can be provided by the

charging system along with main or auxiliary feedwater systems or by HPSI along with main or auxiliary feedwater systems if secondary blowdown is used in the injection phase. This success criterion for long-term cooling was not credited in the PSS and was added in our model. The containment overpressure protection function is only needed when bleed-and-feed is used. In other cases, fission product removal is needed if core melt occurs. The success criteria for this function are the same as for large-break LOCA.

The next initiator that could lead to a LOCA is the Steam Generator Tube Rupture (SGTR). This category also includes consequential SGTR which can occur following a steamline break accident. The subcriticality function in this case is provided by the RPS. The short-term cooling function is provided by charging or HPSI systems injecting into the core to provide the lost coolant along with main or auxiliary feedwater systems for decay heat removal. In addition, the review determined that credit for bleed-and-feed cooling was warranted under certain conditions. The long-term decay heat removal function can be provided by several mechanisms. The first mechanism is steam generator (SG) isolation, primary depressurization (PD), and decay heat removal using main or auxiliary feedwater systems. Primary depressurization can be performed using normal pressurizer spray or auxiliary pressurizer spray (which requires 1 out of 2 charging pumps) or operation of 1 out of 2 PORVs. The second mechanism is loop isolation and decay heat removal using main or auxiliary feedwater systems. In the Haddam Neck PSS it was assumed that primary depressurization and decay heat removal using the RHR system is sufficient to keep the plant stabilized. In our review, this success criterion was not accepted and was replaced by the requirement of steam generator isolation along with primary depressurization and decay heat removal using the RHR system as discussed in Section 4.2.4. The containment heat removal function is only needed if bleed-and-feed is used. Fission product removal is needed if the accident progresses to core meltdown. The success criteria for this function are the same as for CS in the large-break LOCA.

2.2 Safety Functions and Front Line Systems Designed for Mitigation of Transient Initiators

The mitigation of an accident initiated by a transient requires successful performance of several functions. These include reactor

subcriticality, core cooling and inventory makeup, Reactor Coolant System (RCS) integrity, long term decay heat removal, containment overpressure protection and radioactivity removal. Table 2.3 lists the front line systems used for mitigating transients in this plant along with a description of their basic configuration. The success criteria for these front line systems for each of the transient initiators analyzed in the Haddam Neck PSS are shown in Table 2.4.

For the general plant transient, the subcriticality function would be satisfied by insertion of the RPS control rods. The core cooling function can be provided by successful operation of main or auxiliary feedwater systems. If both the MFW and the AFW systems fail, bleed-and-feed would be used for core cooling. The RCS integrity function consists of two subfunctions. The first subfunction is primary system overpressure protection, which can be satisfied by opening the PORVs and the associated block valves. If the PORVs fail to open, the Pressurizer Safety Relief Valves (SRVs) which are set to open at a higher pressure than the PORVs, could perform this function. The second subfunction of the RCS integrity is to make sure the primary system is intact following the initial stages of the transient. This function is performed by reclosure of PORVs, or associated block valves, and SRVs. Another event that could result in violation of RCS integrity is reactor coolant pump seal failure. This can be avoided by providing seal cooling using 1 out of 2 charging pumps or the metering pump or 1 out of 2 Component Cooling Water System (CCWS) pumps.

The long-term cooling function for this initiator can be provided by main or auxiliary feedwater systems. The RHR system would be used if the primary system is depressurized, which occurs after bleed-and-feed operation. Containment heat removal is only needed if the bleed-and-feed operation is used for core cooling. If steam generator cooling is available, then containment heat removal would not be necessary. The success criteria for this function are the same as for the large-break LOCA discussed in Section 2.1 and shown in Table 2.2. The fission product removal function, if necessary, would be provided by the CS subfunction of the containment heat removal function. The success criteria for this function are also the same as for the large-break LOCA. The same functional success criteria apply to the loss of DC Bus 1 and loss of DC Bus 2 initiators.

Table 2.3 Transient-Mitigating Functions and Front line Systems

Function	System (Abbreviation)	Configuration
Reactor Subcriticality	Reactor Protection System	
	Emergency Boration (EB) (In ATWS conditions)	Two charging pumps taking suction from 2 boric acid pumps and delivering to Loop 2 cold leg.
Core Cooling and Inventory Makeup	Main Feedwater (MFW)	Same as LOCA
	Auxiliary Feedwater (AFW)	Same as LOCA
	HPSI and charging systems along with PORVs in connection with Bleed-and-Feed (BAF)	Same as LOCA
	Charging	Same as LOCA
	HPSI	Same as LOCA
Reactor Coolant System Integrity		
a. Overpressure protection	PORVs and associated block valves SRVs	Same as LOCA
b. Primary Integrity	PORVs Safety Relief Valves (SRVs)	PORVs and SRVs must close after opening.
	Charging	Same as LOCA
	Metering Pump	Same as LOCA
	Component Cooling Water System (CCWS)	Three pump intermediate cooling system with heat transfer to SWS through CCW heat exchanger.
Containment Overpressure Protection	Containment Air Recirculation (CAR)	Same as LOCA
	Containment Spray (CS)	Same as LOCA
Fission Product Removal	Containment Spray (CS)	Same as LOCA

Table 2.4 Success Criteria for Front Line Systems Used to Mitigate the Consequences of Transient Initiators

Initiator	Reactor Subcriticality	Core Cooling and Inventory Makeup	RCS Integrity	Long Term Decay Heat Removal	Containment Overpressure Protection and Fission Product Removal
General Plant Transient Loss of DC Bus 1 Loss of DC Bus 2	RPS	1/2 MFWS OR 1/2 AFWS OR Bleed-and-Feed: (1/2 Charging + 1/2 PORVs OR 1/2 HPSI + 2/2 PORVs + 3/3 loops OR 2/2 HPSI + 2/2 PORVs + 2/3 loops)	1. PORV + block valves opening OR SRV opening 2. (PORV + block valve + SRV closing) + (1/2 charging OR metering pump OR 1/2 CCWS)	1/2 MFWS OR 1/2 AFWS OR 1/2 RHR	Same as large-break LOCA
Total Loss of Main Feedwater Loss of Offsite Power Loss of Offsite Power and MCC-5 Loss of Offsite Power and One Emergency Bus Loss of Control Air Loss of MCC-5 Loss of Semi-vital AC Total Loss of DC	RPS	1/2 AFWS OR Bleed-and-Feed: (1/2 Charging + 1/2 PORVs OR 1/2 HPSI + 2/2 PORVs + 3/3 Loops OR 2/2 HPSI + 2/2 PORVs + 2/3 Loops)	Same as general plant transient	1/2 AFWS OR 1/2 RHR	Same as large-break LOCA

Table 2.4 Success Criteria for Front Line Systems Used to Mitigate the Consequences of Transient Initiators (continued)

Initiator	Reactor Subcriticality	Core Cooling and Inventory Makeup	RCS Integrity	Long Term Decay Heat Removal	Containment Overpressure Protection and Fission Product Removal
Steamline Break Upsteam of NRVs Steamline Break Downstream of NRVs Main Feedline Break	RPS	SG isolation + 1/2 MFWS OR SG isolation + 1/2 AFWS OR Bleed-and-Feed: (1/2 Charging + 1/2 PORV OR 1/2 HPSI + 2/2 PORV + 3/3 Loops OR 2/2 HPSI + 2/2 PORV + 2/3 Loops)	Same as general plant transient	SG isolation + 1/2 MFWS OR SG isolation + 1/2 AFWS OR 1/2 RHR	Same as large-break LOCA
Station Blackout	RPS	1/2 AFWS + ER3 + 1/2 Charging OR 1/2 AFWS + ER3 + 1/2 HPSI + 3/3 Loops OR 1/2 AFWS + ER3 + 2/2 HPSI + 2/3 Loops OR ER2 + 1/2 Charging + 1/2 PORVs OR ER3 + 1/2 HPSI + 2/2 PORVs + 3/3 Loops OR ER2 + 2/2 HPSI + 2/2 PORVs + 2/3 Loops	Same as general plant transient	1/2 MFWS OR 1/2 AFWS OR 1/2 RHR	Same as large-break LOCA
Insufficient Flow of Service Water		1/2 AFW + Metering pump	Metering pump	1/2 AFW + Metering pump	None

Table 2.4 Success Criteria for Front Line Systems Used to Mitigate the Consequences of Transient Initiators (continued)

Initiator	Reactor Subcriticality	Core Cooling and Inventory Makeup	RCS Integrity	Long Term Decay Heat Removal	Containment Overpressure Protection and Fission Product Removal
Anticipated Transient Without Scram	Manual Trip OR EB: (1/2 Charging + 1/2 boric acid pumps)	EB + 1/2 MFWS OR EB + 1/2 AFWS OR Manual Trip + 1/2 Charging + 1/2 PORV OR Manual Trip + 1/2 HPSI + 2/2 PORVs + 2/3 Loops OR Manual Trip + 2/2 HPSI + 2/2 PORV + 3/3 Loops	Same as general plant transient	1/2 MFW OR 1/2 AFW OR 1/2 RHR	Same as Large-break LOCA

The next transient initiator is the total loss of main feedwater. The only difference between this initiator and the general plant transient discussed previously is that the MFW system is not available for heat removal. The success criteria for the five functions shown in Table 2.4 are the same except for the MFW system, which is not an option for core cooling and inventory makeup and long-term decay heat removal functions. The same functional criteria apply to loss of offsite power, loss of offsite power and MCC-5, loss of offsite power and one emergency bus, loss of control air, loss of MCC-5, loss of semi-vital AC, and total loss of DC. The only exceptions are that for the loss of offsite power situations, fire pumps cannot be used for containment heat removal.

The steamline break upstream of non-return valves (NRVs) can occur due to pipe ruptures, steam leaks, or stuck-open steam generator safety valves upstream of the NRVs. The subcriticality function is provided by the RPS. The core cooling function can be provided by isolation of the faulty steam generator and use of main or auxiliary feedwater systems for decay heat removal. The steam line break can occur either inside or outside the containment. If the break occurs outside the containment, adverse environmental conditions would disable the AFW pumps. If both MFW and AFW systems are unavailable, bleed-and-feed could be used for core cooling. The success criteria for this action are the same as for the general plant transient.

The RCS integrity function success criterion is the same as for the general plant transient. The long-term decay heat removal function can be provided by isolation of the faulty steam generator and operation of main or auxiliary feedwater systems for decay heat removal. If the primary system is depressurized, as would be the case after bleed-and-feed, long-term decay heat removal can be provided by successful operation of the RHR system. The success criteria for containment overpressure protection and fission product removal are the same as for the large-break LOCA. The same functional success criteria apply to steamline break downstream of NRVs and to main feedline break.

The next initiator is station blackout, which is defined as total loss of offsite and onsite AC power. The reactor subcriticality function is provided by the RPS. The only system available for core cooling is the AFW system. If the power is recovered within 15 minutes (EP1), RCP seal failure

is assumed to be avoided and the AFW system can remove the decay heat. If power is not restored before RCP seal failure, operation of AFW will not by itself prevent the core from melting. Offsite power must be restored at a later time to keep the core covered and remove decay heat. If AFW is available, uncovery of the core occurs after about 4 hours due to RCP seal failure. If AFW is not available, core uncovery occurs after about 50 minutes. Following this, an injection source from HPSI or charging pumps is needed to cover the core. If AFW is available, the power can be recovered as late as 4 hours (ER3), and the core cooling and inventory makeup can be provided by charging or HPSI systems. If AFW is unavailable, the power must be recovered before 50 minutes (ER2) and the core cooling and inventory makeup can be provided by bleed-and-feed operation.

Long-term cooling can be provided by main or auxiliary feedwater systems or the RHR system if the primary system is depressurized. The success criteria for containment overpressure protection and fission product removal are the same as for the large-break LOCA.

The next transient initiator is insufficient flow in the service water system (SWS). This initiator consists of loss of SWS and fire pumps as an alternative to this system. The reactor subcriticality function for this initiator is provided by manual reactor shutdown using the RPS. Since service water is used to cool the component cooling water system, which in turn cools the charging pumps, only the metering pump is available for seal cooling. The success criterion for the metering pump is operation of this pump taking suction from the RWST and delivering coolant to the four seals. Short and long-term decay heat removal can be provided by availability of the metering pump along with operation of the auxiliary feedwater system. No containment heat removal is assumed to be available following loss of SWS because both FANS and CS use the RHR system, which is dependent on SWS. The fire pumps can provide containment heat removal but are assumed unavailable as part of the definition of the initiator.

The final transient initiator shown in Table 2.4 is the Anticipated Transient Without Scram (ATWS). This transient occurs as a result of other initiators, such as the general plant transient, loss of control air, and loss of semi-vital AC, and is characterized by the failure of the RPS. The subcriticality function in this case is provided by manual trip of the

RPS or by Emergency Boration (EB). The success criterion for EB is defined as flow from 1 of 2 charging pumps taking suction from 1 of 2 boric acid pumps and delivering the borated water to the core through the loop 2 injection path. Short-term heat removal can be provided by operation of main or auxiliary feedwater systems. If steam generator cooling is lost, bleed-and-feed can be used only if the operator had successfully tripped the plant manually.

Long-term decay heat removal can be provided by main or auxiliary feedwater systems or the RHR system if bleed-and-feed has been used. Containment heat removal is required only if bleed-and-feed is used. The success criteria for this system are the same as for the large-break LOCA. Fission product removal, if necessary, would be provided by the CS subfunction of the containment heat removal function. The success criteria for this function are also the same as for the large-break LOCA.

3.0 INITIATING EVENTS

The initiating events considered in the Haddam Neck PSS were grouped into two major categories, Loss of Coolant Accident (LOCA) initiators and transient initiators. The LOCA initiator category consists of two classes of initiators. The first class includes those LOCA initiators which are due to primary system pipe rupture. The second class includes LOCA initiators with special features. Examples of the second group are unisolated reactor coolant pump seal failure, steam generator tube rupture, and LOCA outside containment.

The transient initiator category in the PSS consists of generic transient initiators common to all PWRs, and a series of plant-specific transient initiators that occur due to failures in the support systems. Each of these broad initiator groups was further broken down into subgroups based on common functions or systems required for mitigation of their progression. A discussion on each of these initiator groups follows.

3.1 Generic LOCA Initiators

The full range of possible primary system pipe ruptures in this plant was divided into different size LOCA initiators. The range in break size of these LOCA initiators was determined by performing a plant-specific best-estimate LOCA analysis to assess plant behavior following different break size LOCAs. This assessment was then combined with the capabilities of the plant's safety injection systems and the steam generators' cooling requirements to arrive at the appropriate break sizes.

Three ranges of primary pipe break sizes were identified which are labeled large-, medium- and small-break LOCAs.

The large-break LOCA category covers break sizes with equivalent diameters ranging from 6 inches up to a double-ended break of the largest pipe in the primary system. It is assumed that break sizes with equivalent diameter greater than a double-ended break of the largest primary pipe cannot be mitigated. This break range also includes reactor vessel ruptures that do not exceed the emergency core cooling system capabilities.

The medium-break LOCA covers break sizes with equivalent pipe diameters ranging from 2 to 6 inches. Included in this initiator are multiple failures of primary safety relief valves and steam generator manway leaks that fall in this break range.

The small-break LOCA covers break sizes with equivalent diameters ranging from 3/8 of an inch up to 2 inches. Non-isolable opening of the Power Operated Relief Valves (PORVs) or Safety Relief Valves and pipe breaks such as incore instrument tube ruptures that fall in this break range are included in this initiator. For breaks smaller than 3/8 inch equivalent diameter, the primary inventory can be maintained by the normal plant makeup flow, which is approximately 160 gpm.

For the large- and medium-break LOCAs, the frequencies used in the Haddam Neck studies are the same as those evaluated in the Millstone Unit 3 PSS (4). These frequencies were calculated in the Millstone Unit 3 PSS by performing a Bayesian updating of the generic Reactor Safety Study (WASH-1400) data (5). This was done by taking the 5th and 95th percentile values for each class of LOCA initiators as the 20th and 80th percentiles of the prior distribution to express greater uncertainty in pipe failure probabilities. These prior distributions were then updated based on the observation that no pipe breaks in these ranges have occurred in nuclear power plants so far. For the small-break LOCA, the median pipe break frequency suggested in WASH-1400 is converted to mean frequency and is used in this study. It is argued that the contribution of a stuck-open PORV to the frequency of this initiating event is negligible. This is due to the fact that such an event would consist of a spurious opening of PORVs combined with failure of PORVs to reclose and failure of the operator to stop the event by closing the appropriate block valves.

Table 3.1 shows the LOCA categories used in the Haddam Neck PSS along with the assigned frequency for the occurrence of each initiator in the PSS. Also shown in this table are our suggested LOCA initiation frequencies based on WASH-1400. The reason for suggesting the WASH-1400 frequencies for LOCA initiators is that it is not clear whether the Bayesian updating performed in the PSS provides a LOCA frequency that is more accurate or meaningful than the suggested frequencies in WASH-1400. This is

Table 3.1 Review of the Haddam Neck LOCA Initiators

LOCA Category	Approximate Break Diameter (inches)	Mean Frequency (per year)	
		PSS	Suggested WASH-1400 (5)
Large-Break	6"<D<Double-ended rupture of largest primary piping	3.9E-4	2.6E-4
Medium-Break	2"<D<6"	6.1E-4	7.9E-4
Small-Break	3/8"<D<2"	2.7E-3	-
New Small-Small Break	3/8"<D<2"		6.2E-4
New Small Break	3/4"<D<2"		2.0E-3

due to the fact that the basis for the prior distributions, i.e., WASH-1400 suggested frequencies, consists of some actual data and a lot of subjective judgment. Thus, it is not clear what meaningful information can be obtained from further updating this semi-subjective distribution.

As can be seen, for large and medium-break LOCAs the frequencies evaluated in Haddam Neck PSS are fairly close to the generic frequencies suggested in WASH-1400.

In the case of a small-break LOCA, the frequency used in the PSS was taken from WASH-1400. In reviewing the small-break LOCA event tree discussed in Sections 4.1.1 and 4.2.3, it was decided that the small break LOCA should be divided into two ranges of 3/8 inch to 3/4 inch equivalent diameter breaks which will be called small-small break LOCA, and 3/4 inch to 2 inches which will be called small-break LOCA.

For requantification of the Haddam Neck event trees in this review, the frequency of these newly created LOCA categories must be calculated. Due to the absence of any suggested probability distributions for the breaks in the range of 3/8" to 2 inches, it is assumed that the probability of breaks in this range is uniformly distributed. Thus,

$$\text{frequency of the LOCA over the small and small-small break range} = \int_{3/8"}^{2"} P_{SBL}\, dx = 2.7E\text{-}3 \qquad (3.1)$$

where P_{SBL} is the probability distribution of the small-break LOCA which is assumed to be uniformly distributed. From this P_{SBL} is equal to 1.6E-3.

For the small-small break LOCA, ranging from 3/8 inch to 3/4 inch equivalent diameter, the initiator frequency is:

$$\int_{3/8"}^{3/4"} P_{SBL}\, dx = 6.2E\text{-}4\ yr^{-1} \qquad (3.2)$$

For the small-break LOCA, ranging from 3/4 inch to 2 inches equivalent diameter, the initiator frequency is:

$$\int_{3/4"}^{2"} P_{SBL}\, dx = 2.0E\text{-}3\ yr^{-1} \qquad (3.3)$$

It is recognized that, based on the pipe break probabilities provided in WASH-1400, the probability of a pipe break increases as the diameter of the pipe decreases. Thus, the uniform distribution assumed in the above analysis might not be the most appropriate. But, due to lack of any other justifiable distribution, the uniform distribution is the simplest and most reasonable distribution that can be used for this purpose.

3.2 Special LOCA Initiators

Several potential LOCA initiators with special features were also analyzed in the Haddam Neck PSS which are reviewed in this section.

3.2.1 Unisolated Reactor Coolant Pump Seal Failure

This LOCA initiator consists of random failure of a single Reactor Coolant Pump seal. Depending on the seal leakage rate, this initiator could result in primary system inventory loss beyond the capability of the normal makeup system, in which case the high-pressure safety injection system would be required to maintain the primary system inventory. In Haddam Neck each reactor coolant pump seal includes a breakdown bushing that the utility claims would limit the leakage to 50 gpm per pump. This leakage rate would be within the capacity of the plant makeup system. However, following the review of Haddam Neck RCP seals, the NRC staff has concluded that the seal design is not sufficiently different to accept the 50 gpm per pump assumption (6). This flow rate could be as high as 480 gpm. But the results of some Westinghouse experiments show that the probability of seal leakage rate greater than 175 gpm is several orders of magnitude smaller than seal leakage below this rate, and most likely the seal leakage is about 100 gpm (6). Thus, with all the uncertainties involved, it can be assumed that a single RCP seal leakage is smaller than the lower boundary of the small-small break LOCA, i.e., 160 gpm.

The frequency of the unisolated reactor coolant pump seal failure was calculated by considering that the primary loops in this plant include motor-operated isolation valves that could be used to isolate any loop with a leaking reactor coolant pump seal.

Thus,

$$F_{US} = F_S \cdot (P_{MOV} + P_{OE}) \qquad (3.4)$$

where

F_{US} is the frequency of unisolated RCP seal failure;

F_S is the frequency of seal failure at Haddam Neck (0.25/year based on four actual events in 16 years of experience);

P_{MOV} is the probability of either MOV failing to close on demand (5.0E-2);

P_{OE} is an operator error of either failing to respond to annunciators, failing to follow the procedures, or selecting the wrong valve (3.1E-3).

Based on this equation, the frequency of unisolated reactor coolant pump seal failure is 0.013. It is interesting to note that the generic pump seal failure frequency used in different PRAs is 0.02 (7), which is an order of magnitude smaller than Haddam Neck experience. Thus, the existence of loop isolation valves is quite important in this plant for lowering the frequency of initiation of an unisolated reactor coolant pump seal failure.

3.2.2 Steam Generator Tube Rupture

The second LOCA initiator with special requirements considered in this study is the steam generator tube rupture. The special feature of this initiator is that it creates a path for LOCA outside containment and also affects secondary side heat removal. In the Haddam Neck PSS this initiator is defined as failure of one to five steam generator tubes. Larger numbers of tube ruptures or simultaneous tube ruptures in several steam generators are considered unlikely and are not included in the analysis.

The frequency with which this event occurs at the Haddam Neck Power Plant is calculated based on generic data suggested in NUREG-0844 (8). In this report, four single tube failures over 240 reactor years of experience are cited. This results in a steam generator tube rupture frequency of 1.7E-2 per year.

3.2.3 LOCA Outside Containment

The next initiator considered is the LOCA outside containment. This category includes all initiators that result in the creation of a direct path for loss of coolant outside the containment except for steam generator tube rupture, which is considered separately. The frequency of this event was evaluated by first considering low-pressure systems or paths that interface with the high-pressure primary coolant system, followed by identifying scenarios that could lead to LOCA outside containment in these systems or paths. Identified systems with possibility of initiating LOCA outside containment include the Chemical and Volume Control System (CVCS), the High- and Low-Pressure Safety Injection lines, and the Residual Heat Removal (RHR) System.

The frequency of a LOCA outside containment in the CVCS was calculated by looking at scenarios that could result in ruptures outside containment in the charging and letdown lines. The frequency with which the event could occur due to ruptures in the charging line outside containment was assessed to be very low because of multiple component failures that must occur. For the letdown line, the only credible initiator found was pipe rupture outside containment upstream of the normally open air operated valve FCV-202. The frequency of this event was calculated using the following relationship:

$$F_L = F_{PR} \cdot F_{MOV\text{-}200} \cdot F_{OE} \qquad (3.5)$$

where

F_L is the frequency of a LOCA outside containment due to ruptures in the CVCS letdown line;

F_{PR} is the frequency of pipe rupture = (11 pipe segments) * (8.5E-9 pipe segment failure/hr for pipe segments with a diameter less than 3 inches) * (8760 hrs/year) = 8.2E-4 per year;

$F_{MOV-200}$ is failure of MOV-200 to isolate the line = (1.25E-3 demand failure based on monthly tests) * (16 months between tests) = 2.0E-2;

F_{OE} is operator failure to close MOV-200 manually = 0.3.

Based on this equation, the frequency of a LOCA outside containment due to ruptures in the CVCS letdown line is 4.9E-6 per year.

Another initiator for this event which was not considered in the PSS analysis is the possibility of rupture of one of three orifices which are located right before the air operated valves. The failure frequency of this event can be calculated using the following relationship:

$$F_{OR} = 3 \cdot \lambda_{OR} \cdot T \qquad (3.6)$$

where

F_{OR} is the failure frequency of the one out of three orifices

λ_{OR} is the mean rupture failure rate of an orifice which is 3.0E-8/hr (7);

T is the number of hours per year, 8760 hrs/year.

Based on this equation, the failure frequency of any one of the orifices is 7.8E-4. This frequency should be added to the frequency of pipe rupture F_{PR} shown in equation 3.5. Combining these pipe segment and orifice failure probabilities with the failure of MOV-200 and operator error described in equation 3.5, the frequency of initiation of a LOCA outside containment due to ruptures in the CVCS letdown line is calculated as 9.6E-6 per year.

The total frequency of LOCA outside containment due to ruptures in the high and low pressure injection lines and the RHR discharge line is calculated as 2.8E-7 per year. This low frequency is primarily due to the fact that multiple component failures must occur in these lines before a LOCA outside containment can be initiated.

3.2.4 Catastrophic Pressure Vessel Rupture

The final special LOCA initiator considered is catastrophic pressure vessel rupture that is beyond the capability of the Emergency Core Cooling System (ECCS). The frequency of this event was taken from WASH-1400 as 2.7E-7 per year.

Table 3.2 lists these special LOCA initiators and the frequencies assigned to them in the Haddam Neck PSS and in the present review.

3.3 Transient Initiating Events

The transient initiating events in the Haddam Neck PSS consist of generic transient initiating events that occur due to causes common to most pressurized water reactors and some plant-specific transient initiating events that occur due to failures in the plant's support systems.

The generic transients in this study were grouped into the following categories:

1. General plant transients
2. Total loss of main feedwater
3. Main feedline break
4. Steamline break upstream of non-return valve
5. Steamline break downstream of non-return valve
6. Loss of offsite power

These initiators are reviewed in this section.

3.3.1 General Plant Transient

The general plant transient includes all the transient initiators that result in a trip with main feedwater system available. This category also includes some initiators that normally are included in the group of transients with power conversion system (PCS) unavailable. For example, full or partial closure of one or more Main Steam Isolation Valves (MSIV), loss of condensor vacuum, and loss of circulating water are included in this

Table 3.2 Review of Special LOCA Initiators Considered in the Haddam Neck PSS

Initiating Event	Frequency (per year) PSS	Suggested	Comments
Unisolated RCP Seal Failure	1.3E-2		
Steam Generator Tube Rupture	1.7E-2		
Interfacing System LOCA in CVCS Letdown Line	4.9E-6	9.6E-6	Addition of orifice rupture failure frequency
Interfacing System LOCA in Other Systems	2.8E-7		
Catastrophic Pressure Vessel Rupture	2.7E-7		

category because of a unique feature of the PCS in this plant in which the feedwater pumps do not trip on safety injection signal, high steam generator level or loss of condensor vacuum. Thus, this plant is much less likely than other PWRs to lose feedwater following a transient.

Table 3.3 lists the initiating events included in this category. The initiating event frequencies shown in this table are generic frequencies taken from EPRI NP-2230 (9). These frequencies are for all PWRs at all power levels excluding the events in the first two years of operation. In the Haddam Neck PSS the initiating frequency of this class of transients was calculated from the plant-specific data. Events that occurred during the first two years of the plant operation, generally thought of as the break-in period, were excluded and only the next 14 years (between 1970 to 1983) were considered. Based on 44 transients in the 14 years for which the data was evaluated, the frequency of general plant transient was calculated to be 3.14 per year. As comparison with the data in Table 3.3 shows, this plant has experienced a much smaller frequency of general plant transient than the generic experience.

3.3.2 Total Loss of Main Feedwater

The next transient category is the total loss of main feedwater. In this plant, this transient can occur due to total loss of the main feedwater system, closure of all main feedwater regulating valves or isolation valves, trip of both main feedwater or condensate pumps, or loss of control air to secondary plant components.

The frequency of this event was calculated using plant-specific data. Based on five events in 14 years, a frequency of 0.36 per year is determined. The generic frequency of this category for total loss of main feedwater and trip of both main feedwater condensate pumps using EPRI NP-2230 data is 0.10 per year.

Overall, it appears that the frequency derived from plant-specific experience for these two categories of initiating events at this plant is sufficiently large to justify using this data rather than generic transient frequencies.

Table 3.3 Transient Initiators Included in the General Plant Transient Category in the Haddam Neck PSS

Transient Initiator	Frequency (9) (per year)
RCP Trip	0.32
Multiple RCP Trip	0.02
RCP Locked Rotor	
RCP Shaft Failure	
RCP TC Isolation Valve Closure	
RCP TH Isolation Valve Closure	
Loss of 4160V Bus 1-1A or 1-1B	0.09
Instrumentation Faults Indicating Loss of Flow	
Loss of One FW or Condensate Pump	0.05
Closure of One or More MSTVs	0.14
Loss of Running and Standby FW Heater Drain Pumps	
Increase in FW Flow	0.57
Reduction in FW Flow	1.37
Reduction in FW Temperature	
Increase in FW Temperature	
Full or Partial Closure of one or more FW Regulating Valves or Isolation Valves	
Loss of Internal or External Load	
Excess Load	
Condenser Leakage	0.02
Moisture Separator Reheater Faults	
Instrumentation Faults, Erroneous Signals	
FW Flow Instability	0.29
FW Heater Faults	
Miscellaneous Leakage in Secondary System	0.09
Startup of an Idle RCS Loop	0.00
Spurious Opening of Atmospheric Steam Dump Valve	0.02
Spurious Opening of One High Pressure Steam Dump Valve	
Loss of a Vital Bus	
T4.1 Automatic Turbine Trip	0.98
T4.2 Loss of Condenser Vacuum	0.12
T4.3 Loss of Circulating Water	0.03
T4.4 Governor Valve Malfunction	
T4.5 Generator Trip	
T4.6 Turbine Generator Overload	0.27
T4.7 Turbine Stop Valve Closure	

Table 3.3 Transient Initiators Included in the General Plant Transient Category in the Haddam Neck PSS (continued)

Transient Initiator		Frequency (9) (per year)
T5.1	Automatic Trip	1.23
T5.2	Control Rod Problems	0.12
T5.3	High or Low Pressurizer Pressure	0.02
T5.4	High Pressurizer Level	
T5.5	Spurious Trip	0.08
T5.6	Manual Trip	0.54
T8.1	Control Rod Withdrawal	0.02
T8.2	CVCS Malfunction Baron Dilution	0.02
T8.3	Control Rod Drive Mechanism Malfunction	0.41
T8.4	Control Rod Ejection	
T8.5	High Power Trip	
T9.1	Inadvertent Safety Injection Signal	0.05
T9.2	High Containment Pressure Signal	0.00
T9.3	Spurious Low Pressurizer Pressure Signal	----
Total		6.87

3.3.3 Main Feedline Break

The next generic transient initiator is the main feedline break. The frequency with which this transient occurs was calculated by adding the number of pipe segments in the main feedwater lines and multiplying this figure by the pipe segment failure rates suggested in WASH-1400.

Based on 69 pipe segments and a mean pipe segment failure rate of 8.5E-10 per hour for pipe segments with a diameter larger than three inches, the frequency of main feedline break in this plant was calculated to be 5.1E-4 per year.

3.3.4 Steamline Break Upstream of the Non-Return Valve

There are two types of failures that contribute to the occurrence of this initiator. These include the possibility of pipe rupture upstream of the four non-return valves and spurious opening of steam generator safety valves.

In the PSS the pipe rupture contribution to this initiating event was calculated using a similar method as the main feedwater break frequency. Based on 64 pipe segments and a mean pipe segment failure rate of 8.5E-10, the frequency of steamline break upstream of the non-return valve due to pipe rupture was calculated to be 4.8E-4 per year.

The contribution from spurious opening of steam generator safety valves was not evaluated in the PSS. The frequency of this event can be calculated by noting that the maximum flow rate of each of the 16 steam generator safety valves is about 7%. The main steam isolation valves close at 110% flow. Thus, assuming that all the 16 valves have the same settings, simultaneous premature opening of at least two safety valves followed by failure of both valves to reclose is necessary to create an equivalent steam line break. The frequency of this event can be calculated using the following relationship:

$$F_{SR} = \frac{16!}{14!2!} [F_{SS1} * F_{FC1}] [P_{SS2} * F_{FC2}] \qquad (3.7)$$

where

F_{SR} is the frequency of any two of the steam generator safety relief valves getting stuck open;

F_{SS1} is the frequency of spurious opening of a steam generator safety relief valve;

F_{FC1} is the failure probability of the first safety relief valve to close, given it has opened;

P_{SS2} is the probability of spurious opening of a second safety relief valve at the same time or within a few hours after opening of the first one;

F_{FC2} is the failure probability of the second safety relief valve to close, given it has opened.

The first factor in Eq. (3.7) accounts for the fact that spurious opening and failure to reclose of any 2 relief valves out of the 16 relief valves can result in steam line break. The frequency of spurious opening of the first steam generator safety relief valve, F_{SS1}, based on an hourly failure rate of 6.06E-6 is equal to 5.3E-2 per year (10). For P_{SS2}, it was assumed that spurious opening of the second safety relief valve within 10 hours of the first one could create a steamline break. Based on this, F_{SS2} is equal to 6.06E-5. The mean failure probability of safety relief valves to close, given they have opened, is 2.0E-2/demand (11). Thus, the contribution from spurious opening of steam generator safety valves to the steamline break upstream of the non-return valve is 1.5E-7 per year. This is negligible compared to the contribution from pipe rupture to this initiator, thus the omission of this potential break path in the PSS does not affect the initiating event frequency.

3.3.5 Steamline Break Downstream of the Non-Return Valve

The frequency of steamline break downstream of the non-return valve in the PSS was calculated by considering the frequency of the pipe break downstream of the non-return valve and the frequency of spurious opening of two or more high-pressure steam dump valves. The number of high pressure steam dump valves that would constitute a steamline break was chosen based on the fact that each valve has a relief capacity of about 4% of the full flow. Main Steam Trip Valve (MSTV) closure occurs when the

steam flow is 110% of the rated flow. Thus, a single steam dump valve's opening will not lead to MSTV closure -- two or more valves must open.

The frequency with which spurious opening of two or more high pressure steam dump valves in the PSS occurs was calculated by considering the probability of common cause failure of two or more valves using the methodology and data suggested in NUREG/CR-2770 (12). The mean frequency of inadvertent opening of two or more valves was calculated at 4.2E-3 per year.

Because of the large number of pipe segments downstream of the non-return valve and difficulty in defining pipe segments, instead of multiplying the number of pipe segments by the frequency of pipe segment failure, a more subjective approach was used in the PSS to calculate the frequency of pipe break downstream of the non-return valves. From reference (4) it was found that the frequency of failure of turbine bypass valves is 3.8E-2 per year. This frequency is taken to represent steamline breaks due to valve failures. Then it is assumed that the frequency of pipe breaks is at least an order of magnitude smaller than the frequency of valve failures. Thus, the frequency of pipe breaks is calculated as 3.8E-3 per year and the total frequency of steamline break downstream of the non-return valve as 8.0E-3 per year.

In the above calculation, it is not clear why spurious opening of two or more high pressure steam dump valves (turbine bypass valves) is considered a steamline break. If the MSTVs close as a result of this event, the event would be similar to a general plant transient due to closure of all MSTVs. If the MSTVs do not close, the turbine and plant would adjust to the new steam flow rate. Also, in the PSS evaluation of this initiator, the basis for assuming that pipe break frequency is an order of magnitude smaller than turbine bypass valve frequency is not clear.

The frequency of steamline break downstream of the non-return valve can be calculated by considering the total number of pipe segments downstream of the non-return valves and the failure rate of pipe segments as discussed before. As mentioned earlier, it is indicated in the PSS that there was some difficulty in defining pipe segments downstream of the non-return valves. The licensee estimates that there are between 200 and 300 pipe segments downstream of the non-return valves (6). Using the largest

estimate of the number of pipe segments, 300, the upper bound frequency of steamline break downstream of the non-return valve is calculated to be 2.2E-3 per year.

3.3.6 Loss of Offsite Power

The last generic transient initiator is the loss of offsite power. This transient is defined as an event that leads to complete loss of offsite power to all 4160KV buses that originate onsite or offsite. The duration of this event should be long enough to result in a plant trip.

The frequency of occurrence of this event in the PSS was calculated using plant-specific data. Between 1/1/68 to 7/31/85 (17.6 years), seven loss of offsite power events occurred at this plant. Of these events, one was of very short duration and did not lead to a reactor trip. Three events occurred when the reactor was not at power and were due to causes that cannot occur during power operation. Thus, the plant-specific frequency of loss of offsite power was calculated to be 0.17 per year. The mean frequency of loss of offsite power for the ten operating plants in the northeast region is 0.154 per year (13).

Table 3.4 lists generic transient initiators used in the Haddam Neck PSS.

3.4 Plant-Specific Transient Initiators

In addition to the generic transient initiators discussed in the previous sections, a series of plant-specific or special transient initiators were identified in the PSS. These initiators occur as a result of failure of a support system and result in multiple failures of frontline or other support systems.

Table 3.4 Review of the Generic Transient Initiators Considered in the Haddam Neck PSS

Initiating Event	Frequency (per year) PSS	Suggested	Comments
General Plant Transient	3.14		
Loss of Main Feedwater	0.36		
Main Feedline Break	5.1E-4		
Steamline Break Upstream	4.8E-4		
Steamline Break Downstream of Non-Return Valve	3.8E-3	2.2E-3	Exclusion of failure frequency of the high pressure steam dump valves
Loss of Offsite Power	0.17		

The plant-specific transient initiators identified in the PSS include:

1. Insufficient flow of Service Water System
2. Loss of control air system
3. Loss of motor control center 5
4. Loss of DC Bus 1
5. Loss of DC Bus 2
6. Total loss of DC system
7. Total loss of semi-vital AC system

3.4.1 Insufficient Flow of Service Water System

The first plant-specific initiator analyzed is insufficient flow of Service Water System (SWS). This system provides cooling water to a large number of components and systems. One of the first effects of loss of SWS is the loss of turbine lube oil cooling. Following this, the main feedwater pumps will become unavailable due to loss of cooling. Loss of the SWS will also result in the loss of heat removal from component cooling and residual heat removal system heat exchangers. In addition, the containment air recirculation fan system will lose its heat removal capability. Finally, diesel generators are dependent on SWS for cooling. It is important to note that the Fire Pump System is capable of performing the same functions as the SWS and can be used as a backup for this system.

The SWS consists of four pumps. During the coldest months of the year, one SWS is sufficient to carry the plant load. During hot summer months operation of three pumps might be necessary, with one pump on standby.

To calculate the frequency of initiation of this event, the PSS conservatively assumes that three SWS pumps are running. The loss of heat removal from essential components that are serviced by the SWS is defined as failure of either two out of three or three out of three SWS pumps, followed by failure of either the fire pump system as backup to SWS or failure to isolate the SWS flow to the secondary plant components so that SWS could remove the essential heat load with only one pump. All necessary operator actions are included in the above scenario.

The total frequency of failure of the SWS, including the backup fire pump system and the necessary operator actions for isolation of secondary plant component, is calculated as 1.3E-4 per year. Our review indicates that modeling of the SWS failure as an initiator and the frequency of occurrence of this event was adequately analyzed in the PSS.

3.4.2 Loss of Control Air System

The next plant-specific transient initiator is the loss of Control Air System. This event is defined as non-recoverable failure of the instrument air, consisting of Control Air and Service Air Systems, to supply compressed air to the appropriate components. The service air can be used as a backup to the control air system normally used in the plant operation by manual lineup of the system. The definition of this initiator includes failure of service air due to operator error or hardware failures as a backup to the control air. Both of these systems are dependent on the Closed Cooling Water System for cooling of their air compressors.

Major consequences of loss of the instrument air system include closure of the feedwater regulating valves, lack of component cooling water flow to the reactor coolant pump thermal barrier and bearing oil, closure of main steam trip valves, and loss of atmospheric steam dump and steam dump to the condensor.

For simplicity, the PSS evaluation of the frequency of non-recoverable failure of the instrument air was performed very conservatively. This was done by looking at two major scenarios for complete loss of instrument air. The first scenario consists of loss of control air due to internal causes followed by failure of either service air or the operator error to align or recover the service air system. In this scenario, there are two sequences that contribute to the total loss of instrument air. These are:

$$S_1 = Fa * \overline{O_S} * S \qquad (3.8)$$

$$S_2 = Fa * O_S * S \qquad (3.9)$$

where

Fa is the failure frequency of the control air

O_S, $\overline{O}_S$ is operator failure, success in lining up the service air before plant trip

S is the operator failure to recover and line up the service air after the plant trip. This event includes the failure of service air due to hardware problems.

The failure frequency of the control air, Fa in the PSS, was calculated by assuming that the control air system failure is dominated by the common-cause failure of the compressors. Thus,

$$Fa = (1.9E\text{-}4 \text{ compressor failure/hr})(8760 \text{ hrs/yr})(0.1) = 0.17 \text{ yr}^{-1}$$

where 0.1 is assumed to be the Beta factor or common-cause coupling factor for two compressors. The operator failure to line up the service air before a plant trip, O_S, was calculated in the PSS by arguing that the number of challenges due to loss of control air which the operator had to respond to is equal to (16 yrs of operation)(0.17 failure/yr)=2.7 challenges. Then it is argued that if the operator would have failed once, the probability of O_S would be 1/2.7=0.37. The probability of failure of the operator to line up the service air after the trip, including the hardware failure of service air, i.e., event S, is assumed to be dominated by the operator error of about 1.3E-2. Based on these values, the contribution from sequences S_1 and S_2 to the frequency of total loss of instrument air is calculated to be 2.2E-2 per year.

In our review, we have recalculated these sequences using less conservative assumptions. For event Fa, the compressor failure frequency used in the PSS calculations is for very large compressors. In such a case, it is unlikely that such large compressors would be required to work continuously throughout the year. In fact, the product of the compressor failure rate used in the PSS calculation times the number of hours per year is larger than one indicating that more than one compressor failure per year must occur. This obviously has not been observed in this plant. A more reasonable failure rate for smaller compressors is 5.9E-5/hr (14). Using

this failure rate, and the same Beta factor of 0.1 used in the PSS, the frequency of Fa is equal to 5.1E-2 per year. The possibility of operator error O_S is taken from Table 7.5 of this report for cognitive operator error to shift control air supplies. The probability of this event is 0.1. For event S, similar to PSS, it is assumed that operator error dominates the failure of this event. From Table 7.7 of this report, the manipulative operator error for event AIR is 1.2E-2. Based on these values, the contribution from sequences S_1 and S_2 to the frequency of total Loss of Control Air is 6.2E-4 per year.

The second scenario for complete loss of instrument air in the PSS consists of loss of closed cooling system which fails the air compressors of both the control and service air systems, followed by either well water system failure or the operator error to align or recover the well water system.

Similar to the first scenario, there are two sequences that contribute to the total loss of instrument air. These are:

$$S_3 = F_b * \overline{O}_W * W \qquad (3.10)$$

$$S_4 = F_b * O_W * W \qquad (3.11)$$

where

F_b is the failure frequency of closed cooling system

O_W, $\overline{O}_W$ is operator failure, success in aligning well water to prevent reactor trip

W is the operator failure to recover the well water after the plant trip. This event includes the failure of well water due to hardware problems.

The frequency of failure of closed cooling system in the PSS is assumed to be dominated by common-cause failure of both pumps in this system. It is also assumed in the PSS that the two pumps are completely coupled, i.e., failure of the first pump results in the failure of the second pump. Based on this, the failure frequency of closed cooling system is calculated as

$$F_b = (7.99E\text{-}5 \text{ pump failure/hr})(8760 \text{ hrs/yr})(1) = 0.7 \text{ yr}^{-1}$$

The probability of operator error O_W is calculated in a similar way as O_S, based on an estimated number of challenges of 11.2 and one failure, i.e., 1/11.2=9E-2 per demand. For event W, similar to event S, it is assumed in the PSS that the operator error dominates the failure probability of the event and a value of 1.3E-2 is also assigned to this event. Based on these values, the contribution from sequences S_3 and S_4 to the frequency of total loss of instrument air is 9.0E-3. Thus, the total frequency of non-recoverable loss of instrument air calculated in the PSS is 1.1E-2 per year.

In our review of sequences S_3 and S_4, the frequency of failure of the closed cooling system is calculated based on Beta factor for the common-cause failure of the pumps. This value for most pumps is 0.03 (15). Thus,

$$F_b = (2.66E\text{-}5/\text{hr})(8700 \text{ hrs})(0.03) = 6.9E\text{-}3 \text{ yr}^{-1}$$

The probability of events O_W and W are taken to be the same as O_S and S since they are basically similar operator actions. Based on these values, the contribution to loss of control air from sequences S_3 and S_4 is calculated as 8.3E-5. Thus, the total frequency of non-recoverable loss of instrument air is reduced from 1.1E-2 per year calculated in the PSS to 7.2E-4 per year.

3.4.3 Loss of Motor Control Center 5 (MCC-5)

The last five plant-specific transient initiators are system or subsystem failures that have been modelled as part of the plant systems failure analysis for event tree quantification.

Review of the MCC-5 model in Section 5.0 on System Reliability Analysis resulted in reduction of the frequency of this initiator from 1.4E-2 per year to 2.1E-3 per year principally due to a lower failure rate for circuit breakers to remain closed. This change in the MCC-5 failure frequency is discussed in more detail in Section 5.

3.4.4 Loss of DC Bus 1

Results of the System Reliability Analysis review in Section 5.0 indicate that the frequency of initiation of this plant-specific initiator is correctly developed in the PSS.

3.4.5 Loss of DC Bus 2

Results of the System Reliability Analysis review in Section 5.0 indicate that the frequency of initiation of this plant-specific initiator is correctly developed in the PSS.

3.4.6 Total Loss of DC System

Results of the System Reliability Analysis review in Section 5.0 indicate that the frequency of initiation of this plant-specific initiator is correctly developed in the PSS.

3.4.7 Total Loss of Semi-Vital AC System

Results of the System Reliability Analysis review in Section 5.0 indicate that the frequency of initiation of this plant-specific initiator is correctly developed in the PSS.

3.5 Summary

Table 3.5 lists the results of the review of all the initiators considered in the Haddam Neck PSS. Our review of these initiating events indicates that selection and categorization of the LOCA initiators and the transient initiators in this study is reasonable. In our review, the PSS small-break LOCA was broken up into two ranges of small-small and small breaks for requantification of the event trees. This was the only change that was made to the classification of the initiating events. Quantification of the LOCA and transient initiators in this study included using both plant-specific and generic data. The use of plant-specific data for quantification of the initiators in this study was found to be appropriate. For the most part all initiator frequencies evaluated in this study are correct.

Several comments were made on some initiators that would result in small changes in the initiator frequencies. These changes are shown in Table 3.5.

Table 3.5 Review of All Initiating Events Used in Haddam Neck PSS

Initiating Event	Frequency (Per Year) PSS	Suggested
Large-Break LOCA	3.9E-4	2.6E-4[1]
Medium-Break LOCA	6.1E-4	7.9E-4[1]
Small Break LOCA	2.7E-3	-
New Small Break LOCA		2.0E-3[2]
New Small-Small Break LOCA		6.2E-4[2]
Unisolated RCP Seal Failure	1.3E-2	
Steam Generator Tube Rupture	1.7E-2	
Interfacing System LOCA in CVCS Letdown Line	4.9E-6	9.6E-6[3]
Interfacing System LOCA in Other Systems	2.8E-7	
Catastrophic Pressure Vessel Rupture	2.7E-7	
General Plant Transient	3.14	
Loss of Main Feedwater	0.36	
Main Feedline Break	5.1E-4	
Steamline Break Upstream of Non-Return Valve	4.8E-4	
Steamline Break Downstream of Non-Return Valve	8.0E-3	2.2E-3[4]
Loss of Offsite Power	0.17	
Insufficient Flow of Service Water	1.3E-4	
Loss of Instrument Air	1.1E-2	7.0E-4[5]

Table 3.5 Review of All Initiating Events Used in Haddam Neck PSS (continued)

Initiating Event	Frequency (Per Year) PSS	Suggested
Loss of MCC-5	1.4E-2	2.1E-3(6)
Loss of DC Bus 1	8.5E-3	
Loss of DC Bus 2	8.4E-3	
Total Loss of DC System	7.8E-6	
Total Loss of Semi-Vital AC System	1.7E-3	

(1) WASH-1400 suggested frequencies
(2) Calculated based on WASH-1400 frequences and assuming a uniform distribution.
(3) Orifice rupture failure frequency is added to the pipe rupture failure frequency in this event.
(4) Failure frequency of the high pressure steam dump valves is excluded from this event.
(5) Less conservative assumption used in the evaluation of this initiating event.
(6) Lower circuit breaker failure to remain closed failure rate used in calculation of this initiator.

4.0 REVIEW OF THE EVENT TREE ANALYSIS

The Haddam Neck PSS analysis team constructed 24 event trees to represent plant response to the initiators discussed in Section 3.0. These trees were reviewed to determine if they are a reasonable representation of this plant's response to the initiators. The assumptions employed in the tree construction were evaluated with respect to plant-specific thermal/hydraulic analyses performed by the utility (16) and were compared, where applicable, with assumptions used in previous PRAs. Where there were notable differences or uncertainties of interpretation, further analyses were conducted to assess whether the assumptions were reasonable. When necessary, modifications of the trees to reflect the results of these analyses are suggested. Each such modification is discussed in this section.

It is important to note that some of these modifications are needed to compensate for the PSS analysts' making conservative assumptions. While this practice is acceptable in most licensing analyses, it is not appropriate in a probabilistic context. The ISAP is intended to rank the importance of issues with respect to their contributions to core melt frequency. Conservative assumptions could distort the results. Conservative assumptions are only tolerable where they can be demonstrated to have no significant effects on the ranking of dominant contributors. Therefore, this review treats conservative assumptions with the same concern as optimistic ones, and every attempt is made to indicate how the realism of the event tree models can be improved.

The needed modifications fall into two categories. The first category addresses issues which are general in nature; that is, they affect more than one event tree. These are discussed in Section 4.1. The second category addresses issues which are specific to a particular initiator (event tree). These are discussed in Section 4.2. The plant damage states to which the core melt sequences are assigned are identified by a three-character designation (XYZ), as defined in Table 4.1.

Table 4.1 Definition of Various Plant Damage States for Core Melt Sequences

---

Three-Character Designation XYZ

X is the generic symbol for initiating event type and consists of one of the following cases:

A	indicates large or medium-LOCA
S	indicates a small-break-LOCA or Consequential-Small LOCA
T	indicates a transient or special initiator
V	indicates a LOCA-outside-containment
V2	indicates a LOCA-outside-containment due to steam generator tube rupture
R	indicates a catastrophic reactor vessel rupture

Y is the generic symbol for timing of the core melt and consists of one of the following two cases:

E	indicates an early core melt occurring 2 hours or less after the initiation of the accident
L	indicates a late core melt occurring more than 2 hours after the initiation of the accident

Z is the generic symbol for the availability of containment heat removal and consists of one of the following two cases:

C	indicates the availability of the containment heat removal based on either containment air recirculation fan coolers or the containment sprays

No Symbol indicates neither of the above two heat removal systems are available

---

4.1 General Event Tree Findings

The major concern regarding the event trees is the degree of simplification performed by the PSS analysts. While it is desirable to simplify the trees, a point can be reached where they are oversimplified. This can occur in a number of ways, but the result is an oversimplification of the logic structure which could be misleading and may eliminate sequences required for a proper engineering model.

One way oversimplification may occur is by the nonchronological representation of the event headings on the trees. This can help to simplify the trees and reduce the number of sequences, but in some cases the logical representation of the chronological sequences is not consistently preserved in the simplified tree. If there is not an equivalent sequence or sequences on the chronological tree for each sequence on the simplified tree, then an error has been made. Examples of this type of oversimplification are discussed later in this chapter, most notably in Section 4.2.4.

Another example of oversimplification occurs when a decision is made to reduce or combine trees based only on the decision that there is no quantitative effect on the final results. Although it is very important to have an accurate quantitative model, it is equally important that an accurate qualitative (or engineering) model be retained. This is especially true if the goal of the study is to create a "living model" which can be used for future analysis and sensitivity studies, as is the case for this PSS. It is impossible for the analysts to determine what may be important to have in the models for the purpose of further studies. In addition, it is important that the basis for the simplifications be apparent to anyone who may review or utilize the report, and that some level of consistency be maintained between the level of simplification of each tree. Without this, the models can become confusing and the basis for the final structure of the simplified models can be lost. There are a number of instances in the PSS where qualitative accuracy was sacrificed in the name of quantitative simplicity. These areas are confusing and inscrutable, and make model verification very difficult as well as limiting the capabilities of the model for future evaluation. This is poor PRA practice. Even if the only purpose of the analysis is a one-time answer, which is not the case here, confusing

oversimplification should be avoided. It is better to have too many sequences than too few. The specific occurrences of this type of oversimplification are discussed in detail throughout the remainder of this section and also in Section 4.2 as they apply to specific event trees.

The remainder of this section also presents the results of our evaluation of other notable areas of concern which pertain to more than one event tree.

4.1.1 Analysis of Random and Consequential Small LOCAs

The PSS considers a single size of small LOCA, ranging from an equivalent diameter of 3/8 inches to an equivalent diameter of 2 inches. The plant response and success criteria are based on the most restrictive (conservative) requirements across the break size range. For all breaks in this range, it is assumed that high-pressure injection and steam generator cooling are both required and that high-pressure recirculation is required within about one hour. However, in the best-estimate LOCA analysis performed for the Haddam Neck plant (16), it is shown that steam generator cooling is required only at the lower end of this range, i.e., for equivalent diameter less than 3/4 inch. Further, the analysis shows that alternative means of cooling are available for these smaller breaks. These are (1) bleed-and-feed cooling when steam generator cooling is unavailable, and (2) depressurization of the primary system to below the low-pressure injection initiation point by rapid blowdown of the steam generators (secondary depressurization) when high-pressure injection is unavailable. Secondary depressurization can also be utilized later in the accident sequence in situations in which high-pressure injection succeeds but high-pressure recirculation fails. In this case, the resultant depressurization of the primary allows use of low-pressure recirculation.

In the PSS, bleed-and-feed is inconsistently applied to the various small LOCAs (random and consequential) and secondary depressurization is not applied at all. The reason for the bleed-and-feed inconsistency was explained by the utility analysts as being a simplification. Bleed-and-feed was removed from trees where the unavailability was "sufficiently low" that there would be no impact on the results from retaining bleed-and-feed. This action is not explained or justified in the PSS, and is certainly not

easily verified without a comparative analysis. This is an example of an over-simplification which unduly distorts the engineering basis of the model and may affect its future use. Additionally, the response time assumed to be available for the operator to initiate recirculation for these breaks at the lower end of the range is quite a bit shorter than the actual available time since it is based on the time available for the 2-inch diameter breaks. These assumptions could lead to overestimation of the relative core melt contributions from these very small breaks because the success criteria are not consistent across the entire break size range.

A solution to this problem is to divide the small LOCAs into two new break size ranges, the small LOCAs (3/4-inch to 2-inches) and the small-small LOCAs (3/8-inch to 3/4-inch). This was done in the best estimate LOCA analysis but was not carried through to the PSS. In a meeting at the utility, the PSS analysts stated that the reasons for not dividing the small LOCAs into two ranges were two-fold. First, using one small LOCA category would simplify the analysis and the PSS analysts felt that there would be no significant effects on the final results of the analysis (despite the fact that the most restrictive success criteria were used). Second, the analysts were unsure of how to approach the issue of assessing the frequency of the two break size ranges since the available data was for a single small LOCA break size range. The accuracy of the first statement, that there would be no significant effect on the results, is impossible to determine without a comparative evaluation. Therefore, we have suggested a revision of the PSS event trees to provide a more accurate qualitative representation of the plant response to various small LOCA events (as specified in the best estimate LOCA analysis). Our requantification has verified whether the PSS simplification truly had no effect on the results, although we feel the PSS to have performed a confusing oversimplification. The results are discussed in Chapter 10. The manner of dealing with the assessment of the frequency of each small LOCA break size range is discussed in Section 3.1. The new small LOCA range would encompass random breaks and consequential LOCAs caused by stuck-open PORVs, as indicated by the PSS best estimate LOCA analysis. The success criterion for this break range requires high-pressure injection (HPSI or charging) for early core cooling and high-pressure recirculation for late core cooling. Methods for depressurizing and utilizing low-pressure systems would not be credited because LOCA analysis indicates that the pressure could not be sufficiently lowered prior to core

uncovery (for injection). No analysis has been provided that shows whether depressurization would work for recirculation. Even though secondary blowdown and depressurization is not adequate for injection, a case could be made for its use to reach low-pressure recirculation conditions when the time for switchover occurs, and this will be investigated further (in the review of ISAP issues) if high-pressure recirculation failure proves to be a significant core melt contributor for the small LOCA range. In keeping with the LOCA analysis, steam generator cooling would not be required for this break size.

The small-small LOCA range would encompass both random breaks and consequential LOCAs caused by RCP seal failure (see also Section 3.1.2). For these LOCAs, early core cooling could be provided by (1) steam generator cooling (SGC) in conjunction with high-pressure injection (HPSI or charging), (2) bleed-and-feed cooling (when HPI is available and SGC is unavailable), or (3) secondary depressurization and low-pressure injection (when SGC is available and HPI is unavailable). Late core cooling success would depend on the pressure at the time of recirculation, although it should be noted that when early core cooling is provided by SGC and HPI and high pressure recirculation cannot be provided due to charging system failure, then secondary depressurization can be utilized at the time of recirculation switchover to allow use of low-pressure recirculation.

For the small-small breaks, the time available for the operator to successfully initiate recirculation for LOCAs in this range is assumed to be much greater than the one hour allowed in the PSS. It would more likely take about 2-1/2 to 10 hours or so to reach the point at which recirculation could be established and that the low break flow rate would allow the operator a substantial amount of time, from about 3-1/2 hours to about 13 hours at the upper end of the range, after this point is reached to actually establish recirculation. (For further discussions of the timing, see Section 7.2.1b; if bleed-and-feed (BAF) cooling is utilized, then BAF assumptions apply.)

The event trees that contain random or consequential LOCAs have been modified to incorporate the changes discussed above. Two modifications to the PSS small LOCA tree were required, one to create a new small LOCA tree and one to create a revised small-small LOCA tree. It should be noted

that it is not necessary to have the event for adverse break size and location (which disables charging) on the small-small LOCA tree since none of these breaks fall within the new small-small break size range.

4.1.2 Treatment of Consequential RCP Seal LOCA

A problem related to the above discussion is the PSS treatment of the consequential RCP seal LOCA. This event results from a loss of cooling to the RCP seals, which causes seal failure and a subsequent LOCA. The design of the Haddam Neck RCP seals is such that the LOCA flow rate is limited to 50 gpm/seal. For this reason, the PSS argues that in some ways the RCP seal LOCA is not a real LOCA at all, since the total potential flow rate is only 200 gpm if all four seals fail and may actually be lower. Any leak of less than 160 gpm does not come under the definition of a LOCA, since normal makeup to the charging system can provide this much flow. (It is stated in the initiating event section of the PSS that the 3/8-inch diameter lower limit of the small LOCA range is based on this 160 gpm flow rate.) Another point made by the PSS is that there are a number of mitigating factors which come into play even with a 200 gpm seal LOCA. First, the operator can use loop isolation valves to stop the LOCA. Second, it would take a very long time to deplete the RWST and thus create the necessity for recirculation. For these reasons, the PSS assumes that if charging can be recovered after the seals have failed, the result is the same as if the seals had not failed at all. That is, the event is treated like a transient instead of a LOCA. This occurs mostly in certain occurrences of the event "primary integrity" (PIT), where seal failure with charging recovery is considered success of PIT.

We are concerned with this treatment of the RCP seal LOCA for several reasons. First, the 200 gpm is an approximation and, even with the uncertainties, indicates that the RCP LOCA may fall into the small-small LOCA range. Second, the NRC staff has reviewed the design of the Connecticut Yankee RCP seals and has concluded that they do not believe that the seal design is significantly different from other Westinghouse RCP seals and that seal flow would not be limited to 50 gpm/pump (4). In particular, they disagree with the utility's basis for that assumption, since the tests upon which the assumption is based were conducted using cold water and therefore

did not properly demonstrate the seal heatup phenomenon, which would lead to substantial seal breakdown and leakage (4).

The scenario is potentially much more complicated than assumed in the PSS since the leak rate could be as little as 50 gpm or as great as 480 gpm if the seals pop out, with the most probable range being between 80 and 150 gpm (4). The leak would not start at its maximum rate immediately, but would slowly build up to that level as the seals heated up. Depressurization of the primary may or may not have a significant effect on the total flow rate for all four pump seals. Operator actions to isolate one or two of the pumps (closing loop isolation valves) may or may not be a viable option, but the reduction in leakage rate may not be sufficient to make a significant difference in plant response. Overall, in the absence of a detailed analysis, it is reasonable to assume that the actual cumulative leakage rate would most likely average about 100 gpm per pump and thus be within the small-small LOCA range, close to the upper end of that range. For the purpose of requantification and comparison, this is the assumption we made and the significance to the overall results is assessed in Chapter 10 (Requantification).

The utility staff claims that, with 50 gpm leakage per pump, as assumed in all their analyses, normal depressurization would reduce the pressure sufficiently to initiate RHR cooling. This, they claim, would result in a sufficient reduction of the break flow rate that recirculation would not be required for at least 24 hours, and thus there would be no need to consider recirculation for breaks of this size. This could be true, but the analyses provided in the best estimate LOCA analysis do not demonstrate this to be the case and the utility has not provided other information to support its claim. In addition, no analysis for larger seal leakage rates have been done, and it is not clear at what pressure the seal leakage would stop, since critical flow conditions could exist down to quite low RCS pressures for a break of this size. Further, the PSS model essentially claims that the operator need not perform any actions for twenty-four hours if injection and feedwater are available during an RCP seal LOCA. This is clearly optimistic, since it appears that he must at least take actions to reduce pressure and possibly establish some form of long-term cooling. In the absence of a detailed plant-specific analysis, it seems logical to assume that the action required is to establish recirculation, since the

procedures would direct the operator in that direction as soon as 100,000 gallons were pumped from the RWST. It appears to be the most likely ultimate response path called for in these procedures. Alternatively. if it is possible to add coolant to the RWST, for example from the Condensate Storage Tank (CST), this could substantially delay any need for recirculation. It is important to note that addition of coolant to the RWST will result in subtantially more water in the containment. Thus, this option must include an analysis of the containment and equipment response to the larger addition of water to the containment.

We recognize and understand the reluctance of the PSS to categorize and treat this event with the same restrictive success criteria it applied across the range of its small LOCA category; however, this problem would not have occurred if the PSS had divided the small LOCA range as discussed in Section 4.1.1. Since the small-small LOCA range designated in this review more accurately fits the RCP seal LOCA than either the PSS small LOCA or the PSS RCP seal LOCA assumptions, the affected event trees have been modified so that the RCP seal LOCA is treated identically to the redefined small-small LOCA. In this way, it is determined through our requantification whether the PSS assumptions have a significant effect on the results due to underestimation of the contribution of RCP seal failures to core melt frequency.

In summary, the following changes have been implemented on trees involving RCP seal LOCAs. Failure of primary integrity (PIT) was originally defined in the PSS as failure of RCP seals and lack of charging makeup flow. It is redefined in this review as being failure of only the RCP seals. It should be noted that, for some trees, RCP seal failure is assumed and PIT failure in the PSS only requires further failure of charging makeup flow. For these trees in the review, the event PIT is removed and failure of PIT is assumed. In all cases, PIT failure is considered to be, and is treated as, a small-small LOCA requiring operator action and recirculation. Failure or inability to establish that will result in a core melt.

4.1.3 Need for Containment Heat Removal with Bleed-and-Feed

The PSS assumes that containment heat removal (CHR) using either fans or sprays is required for bleed-and-feed (BAF) scenarios. This

assumption is not consistent with other recent PWR PRAs which have shown that BAF followed by recirculation or RHR cooling is sufficient to prevent core melt without the use of CHR as long as heat is removed from the secondary side of the RHR heat exchanger. Additionally, the plant-specific LOCA analysis shows that the peak containment pressure during BAF without CHR is about 23 psi in the first 15 hours, a figure that is substantially lower than the containment failure pressure. However, a somewhat unique feature of the PORVs exists at Haddam Neck. The PSS states that "an adequate pressure [differential] must be maintained between the PORV receiver air tank and [the] containment [in order] to keep the PORVs opened." The PSS does not define "adequate," nor does it state at what time after the initiation of BAF "adequate pressure" is lost. However, in a meeting at the utility, the review team was told that the pressure in the containment must remain below 12.8 psi and the pressure would reach that point in about 40 minutes without CHR. Thus, the assumption appears reasonable for this plant.

It should be noted that planned changes to emergency procedures to utilize the low temperature over-pressure (LTOP) lines as a backup bleed path could reduce or eliminate this dependence under certain conditions. This will be investigated further if failure of CHR during BAF scenarios is shown to be a significant contributor to core melt frequency.

4.1.4 Treatment of Consequential Loss of Semi-Vital AC (SVA)

The semi-vital AC system (SVA) is an important support system at the Haddam Neck plant. Unlike the treatment of other support systems in the PSS, SVA was not considered in the support states evaluated. Rather, when it affected an event tree, SVA was included as an event on the tree. While this is an inconsistency in the approach, there is nothing inherently wrong with it if the analysis is handled properly. It is somewhat confusing in the PSS because SVA appears on some event trees and yet not on others which are similar and on which one would expect to find it. What the PSS did was to remove it from trees where the sequence frequencies through the SVA failure branch were less than the cutoff value (1E-6/year). This was done to simplify the trees. Again, there is nothing inherently wrong with this approach other than the fact that it is confusing and inconsistent. It would have been preferred, for the sake of scrutability, that SVA be handled

as part of the support state analysis, but there is no reason to modify the trees at this point because modification would be difficult and would not change the ultimate results with regard to consequential SVA failure.

4.1.5 Local Manual Control of Auxiliary Feedwater

For a number of initiators involving loss of certain support systems, it is necessary for an operator to take local manual control of the AFW system in the AFW pump room. This involves three steps; (1) a cognitive decision by the control room crew that local manual control is needed, (2) the necessary manipulative actions performed by an auxiliary operator dispatched to the pump room, and (3) successful functioning of the required equipment. This event is represented by node AF4 on the appropriate event trees.

For reasons discussed in detail in Section 7.3.1b, it appears necessary to separate the cognitive decision from the other parts of the event. Thus, a new cognitive action node, OA-21, is suggested to represent step 1 of AF4 as described above and is placed on each appropriate tree prior to the present AF4 node. The definition of AF4 has been changed to include only steps 2 and 3 as described above.

4.2 Specific Event Tree Findings

This section discusses areas of concern that pertain to specific event trees. In addition, the specific trees that are affected by the general comments discussed above are identified.

4.2.1 Large LOCA Event Tree

The large LOCA event tree was reviewed and found to be a proper representation of plant response. Our only comment would be that switching to two-path recirculation to prevent boron precipitation is probably not necessary. It is unlikely that boron precipitation sufficient to cause a problem would occur. However, this action is so simple and there is such a long time after the initiation of recirculation to perform it that it is not important to the results of the analysis. The PSS large-break LOCA event tree is shown in Figure 4.1.

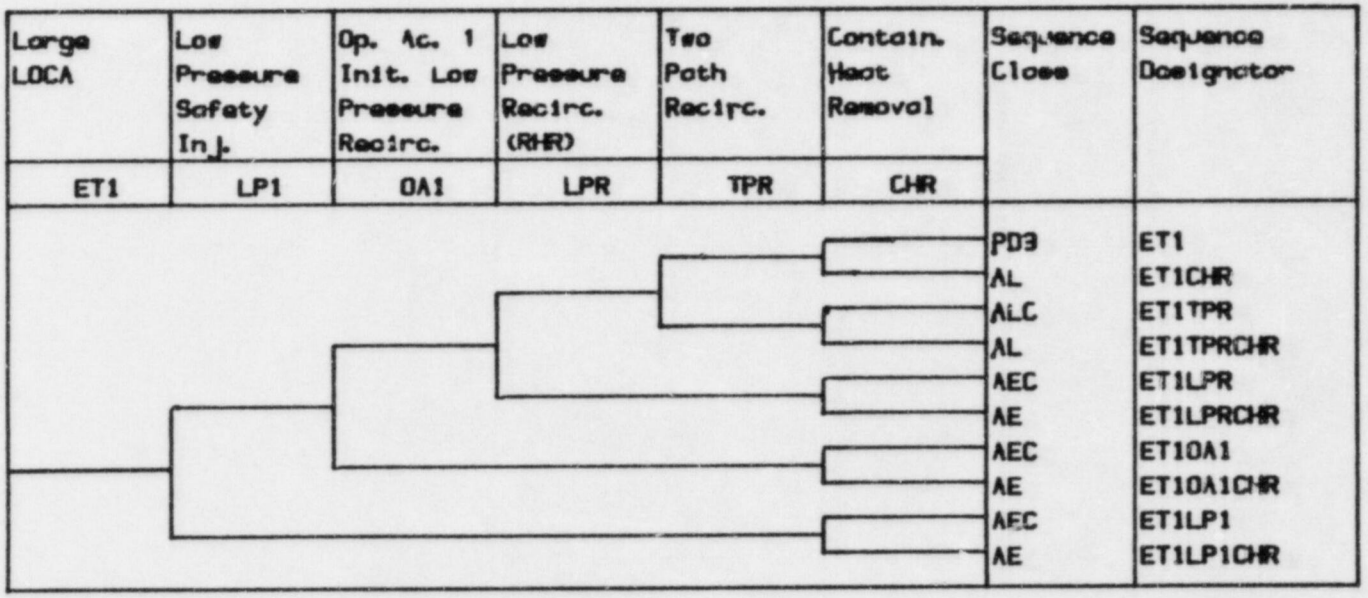


Figure 4.1 Large-Break LOCA Event Tree

4.2.2 Medium LOCA Event Tree

The medium LOCA event tree was found to be a proper representation of plant response. The PSS medium-break LOCA event tree is shown in Figure 4.2.

4.2.3 Small LOCA Event Tree

As discussed in Section 4.1.1, the analysis of small LOCAs should have been broken up into two size ranges and given success criteria as described in that section. Two trees have been developed to implement that conclusion. The small LOCA tree is shown in Figure 4.3 and the small-small LOCA tree is shown in Figure 4.4. The following event definition changes and additions (small-small LOCA tree only) should be noted:

- OA-8, Operator Cognitive Decision to Initiate Bleed-and-Feed. This action will take two forms. In cases where high-pressure injection of some kind (HPSI or charging) is available and steam generator cooling has failed, this action will involve the operator's recognition of those conditions and his decision to initiate bleed-and-feed by opening the PORVs. In cases where high-pressure injection capability has failed and steam generator-cooling is available, this action will involve the operator's recognition of those conditions and his decision to initiate low-pressure makeup through the reduction of primary pressure by opening secondary atmospheric dump valves.

- BLED, Procedural Actions and Equipment Required to Implement Bleed-and-Feed (Initiating Bleed-HPI already available). Applies to first case discussed above, i.e., where high-pressure injection is available.

- SBD, Procedural Actions and Equipment Required to Implement Secondary Blowdown and Low-Pressure Injection. Applies to second case discussed above, i.e., where high-pressure injection has failed.

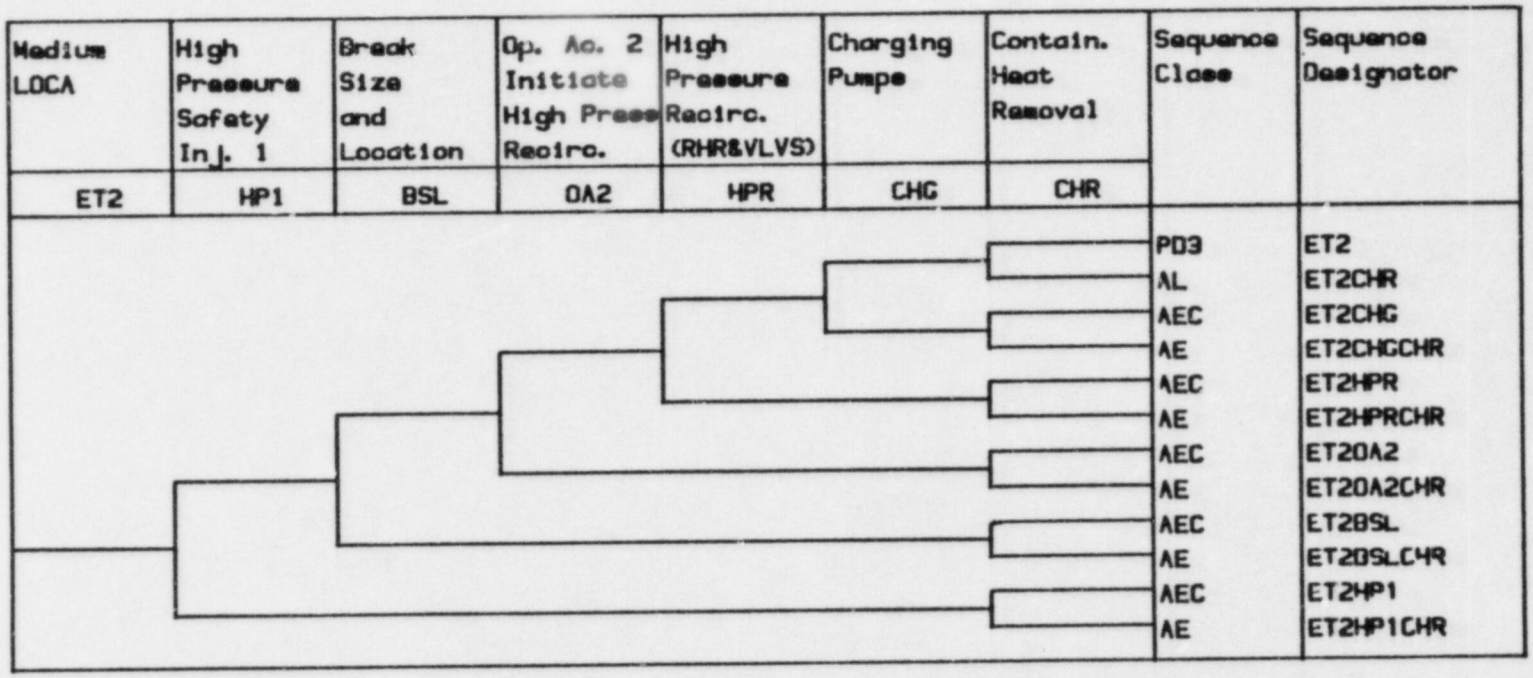


Figure 4.2 Medium-Break LOCA Event Tree

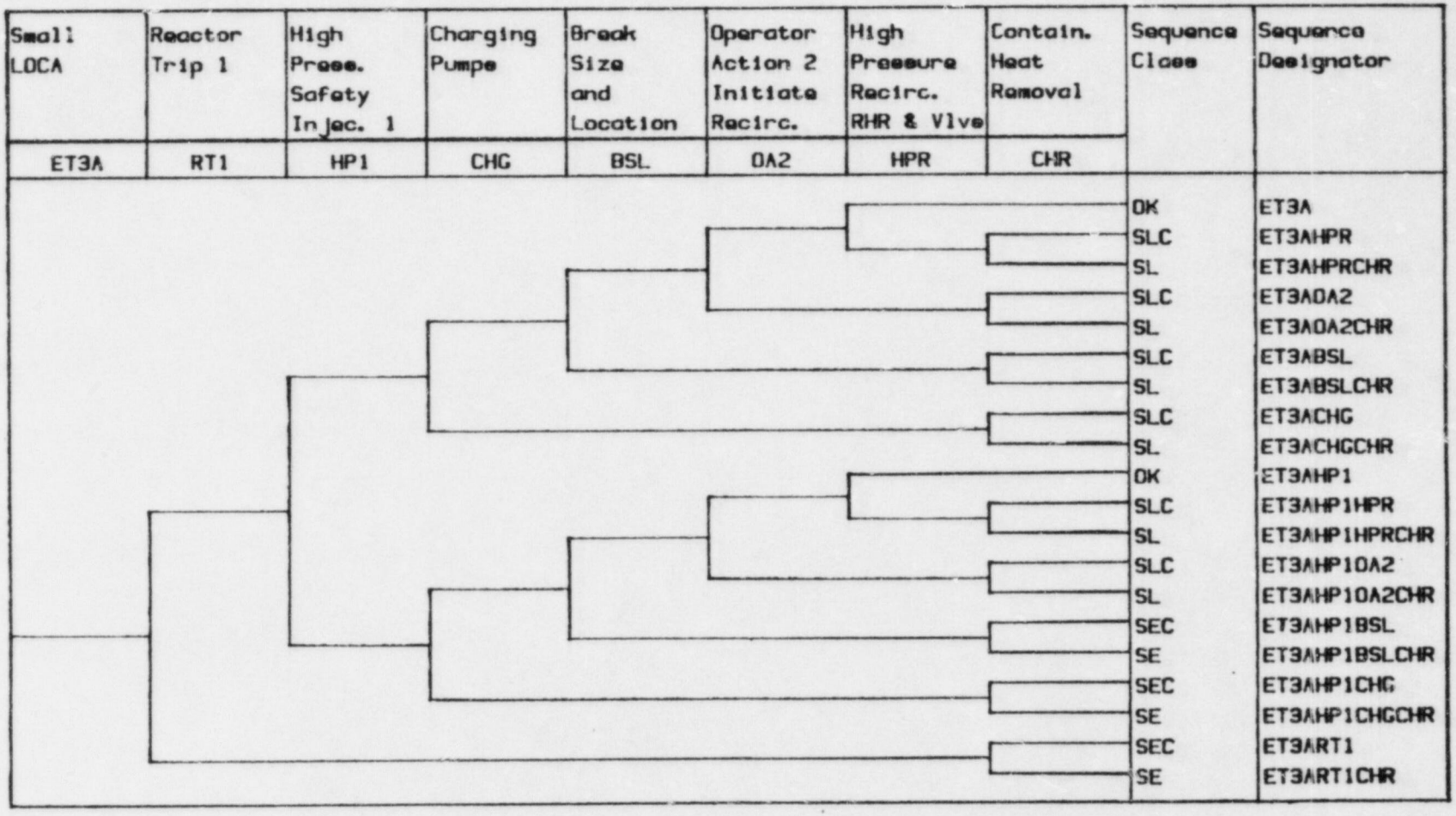


Figure 4.3 Small-Break LOCA Event Tree

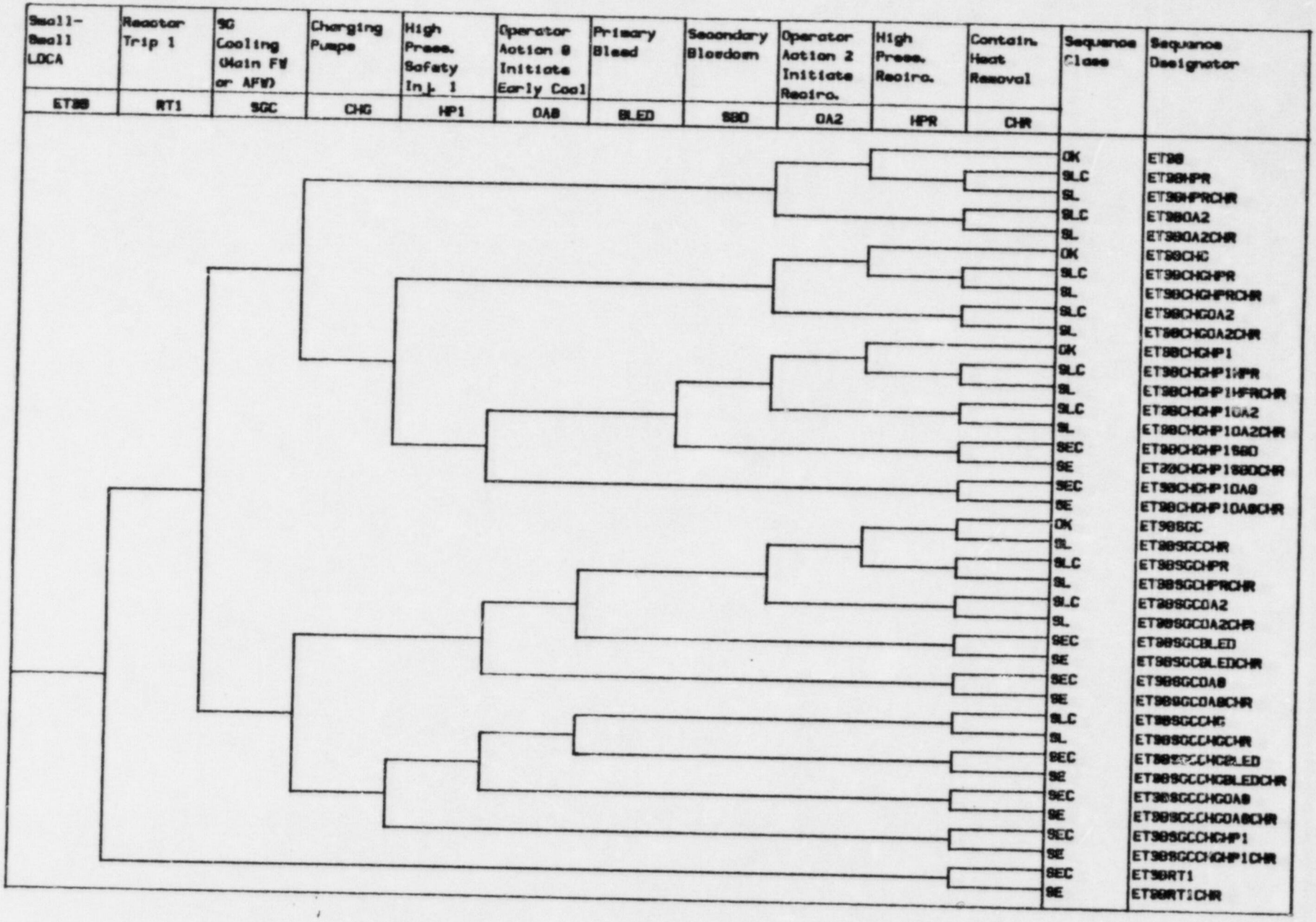


Figure 4.4 Small-Small Break LOCA Event Tree

- OA-2, Operator Cognitive Decision to Initiate Recirculation. Three cases would apply, depending on system availability and RCS pressure. In each case, this action would involve operator diagnosis of the conditions and decision to take the proper action. Case 1--high RCS pressure with charging system available: the proper decision is to initiate high-pressure recirculation. Case 2--high RCS pressure with charging system unavailable and steam generator cooling available: the proper action is to initiate secondary blowdown and low-pressure recirculation. Case 3--low RCS pressure: the proper action is to initiate low-pressure recirculation. For all other cases, no action is useful.

- HPR, Procedural Actions and Equipment Required to Implement Recirculation. As in the PSS, this event pertains only to the low-pressure (RHR) part of the recirculation equipment and its proper alignment. The exact equipment required and actions needed are based on the specific recirculation case under consideration as specified for action OA-2 above.

It should be noted that these event definitions also apply to the analysis of consequential small LOCAs in the transient event trees, as appropriate. The particular trees which have been modified to reflect the review comments on consequential small LOCA response are identified in subsequent sections as being affected by the general comments in Sections 4.1.1 and 4.1.2. The specific operator actions available for any particular support system initiating events will depend upon the specific support systems that failed.

4.2.4 Steam Generator Tube Rupture (SGTR) Event Tree

Before getting into details regarding this tree, some discussion regarding the initiating event is in order. As discussed in Section 3.2.2, the SGTR initiator is defined as a rupture of from one to five tubes. The best estimate LOCA analysis analyzed both the one tube and five tube cases. However, it is important to note that the data used for determining the initiating event frequency shows that only ruptures of one tube (equivalent diameter) have ever occurred. Thus, for the frequency used in the PSS, only the one-tube case should be represented on the event tree. Consequently,

our comments and revisions deal only with the event tree's representation of plant response to a single SGTR.

The SGTR event tree has a potentially significant problem regarding operator response under certain conditions. The problem comes from assuming that, for all conditions, the operator will eventually come to a step in a procedure that calls for determining whether an SGTR exists and that the first actions taken will be in response to the SGTR. This supposition is reflected on the tree by the positioning of this operator response prior to the steam generator cooling event (SGC). The PSS states that the success criterion for SGC is dependent on whether detection and isolation has occurred (based on potential degradation of the auxiliary feedwater (AFW) system if isolation is not accomplished), and assumes that this operator response is not dependent on whether SGC has succeeded. This statement is contrary to the actual sequence in which certain events occur. The failure of SGC is a critical preemptory failure in the symptom-oriented procedures. If steam generator cooling is not available and it is required (which is the case), the operator is instructed to go immediately to one of the emergency functional recovery procedures (FR-H.1, Response to Loss of Secondary Heat Sink). This occurs long before any step would be reached which calls for the operator to determine if an SGTR has occurred. Once in this emergency functional recovery procedure, failure to establish SGC would lead the operator to initiate bleed-and-feed. Again, this action would occur without the operator having come to any procedural step which would result in his discovering an SGTR. This is most likely acceptable, since initiating bleed-and-feed would appear to result in a drop in primary pressure below the secondary steam relief pressure in a relatively short period of time (based on the bleed-and-feed analysis included with the PSS). Thus, following the procedures for SGC failure would result in a safe condition (assuming successful bleed-and-feed response), but the SGTR condition would not be discovered. In any case, it appears that once the SGC failure occurred, the procedures would result in the operator never reaching a step at which he would determine that an SGTR existed. This is an example of a situation where setting up an event tree in nonchronological order alters the logic structure of the tree so that the nonchronological tree is not logically consistent with a chronological representation. In this case, the significance of the failure of SGC to subsequent operator response is completely missed. The PSS tree does not include the likely bleed-and-feed

response path or evaluate its ramifications. Thus, consistency of the logic structure is not maintained. In the reviewer's opinion, this effect on operator response is more significant and important than the effect on the success criteria of the AFW part of the SGC (loss of one auxiliary feedwater pump, which is discussed in the PSS), and it is more important that it be modeled as accurately as possible. Further, it could be argued that the loss of one of the auxiliary feedwater pumps will occur prior to operator diagnosis of the SGTR and isolation of the faulted steam generator. Thus, it should simply be assumed that one pump is unavailable when evaluating SGC availability following SGTR. Regardless, the potential for the operator to properly follow the procedures when SGC is lost and to initiate BAF must be included in the event tree. Thus, in order to properly represent the sequence of events, the SGC event has been moved up before the operator response node, the bleed-and-feed response path has been added, and the tree has been restructured.

Since SGTR is similar to small-small LOCA in flow rate, there was some question as to whether it might not be possible to use steam generator blowdown and low-pressure injection to provide makeup in those cases where both HPI and charging fail but steam generator cooling is available. No credit was taken for this in the PSS and the best-estimate LOCA analysis did not supply sufficient information to assess its credibility. However, subsequent responses by the utility to questions posed by the review team indicate that such credit is justified for a single SGTR. Thus, the event OA-8 has been redefined and event SBD added, as was done for the small-small LOCAs (Section 4.2.3), and the appropriate sequences added to the tree.

Finally, the PSS assumes that if the SRV fails (a secondary steam leak occurs) and the loop isolation valves are not closed, it is still possible to avert core melt by using long-term cooling (LTC). The thermal-hydraulic analysis provided in the PSS is not sufficient to justify this assumption. While the T/H analysis does evaluate this scenario, it carries the evaluation only out to the point at which the RWST is depleted (about 6 hours). However, what is important is what happens after the RWST is depleted. It is not clear how the RCS pressure could have been reduced sufficiently to preclude the continuous loss of coolant to a steam generator that is essentially at atmospheric pressure. This continuing loss should result in core uncovery and eventual core melt in less than 24 hours. The

use of LTC would not stop the coolant loss since there is no water source associated with this operating mode to provide makeup. Recirculation would not be available since the primary coolant was being lost into the secondary (and on to the atmosphere) and the sump would thus be empty. It appears, then, that the only way to prevent core uncovery when a secondary SRV is stuck open is by closing the loop isolation valves.

The tree has been modified to take these comments into account and is shown in Figure 4.5.

4.2.5 Steamline Break Upstream of the Nonreturn Valves (NRVs) Event Tree

The event tree for steamline break upstream of the NRVs was found to be a proper representation of plant response, with the possible exception of the assumption that CHR is required for these breaks. While this type of break will result in the blowdown of one steam generator into the containment, it is unlikely that the containment pressure will reach a level which could cause a problem. If the intact steam generators are isolated from the break and cooling is provided through these steam generators, there should be no additional steam added to the containment and therefore the pressure would remain relatively low. It appears, then, that for these scenarios the assumption of the need for CHR is conservative, although it should be noted that no best-estimate analysis was provided. It appears, however, that this assumption does not have a significant impact on the analysis. However, if requantification indicates that the effect of the assumption is greater than it appears, this issue will be investigated further. The event tree for this initiator is shown in Figure 4.6

4.2.6 Steamline Break Downstream of the NRVs Event Tree

The event tree for a steamline break downstream of the NRVs was found to be a proper representation of plant response. It should be noted that the general comments discussed in Sections 4.1.3 and 4.1.4 apply to this tree and to all other transient trees discussed in the remainder of Section 4.2. This fact will not be repeated in the discussion for each event tree because there is no effect on the tree structure, as discussed in those sections. The event tree for this initiator is shown in Figure 4.7.

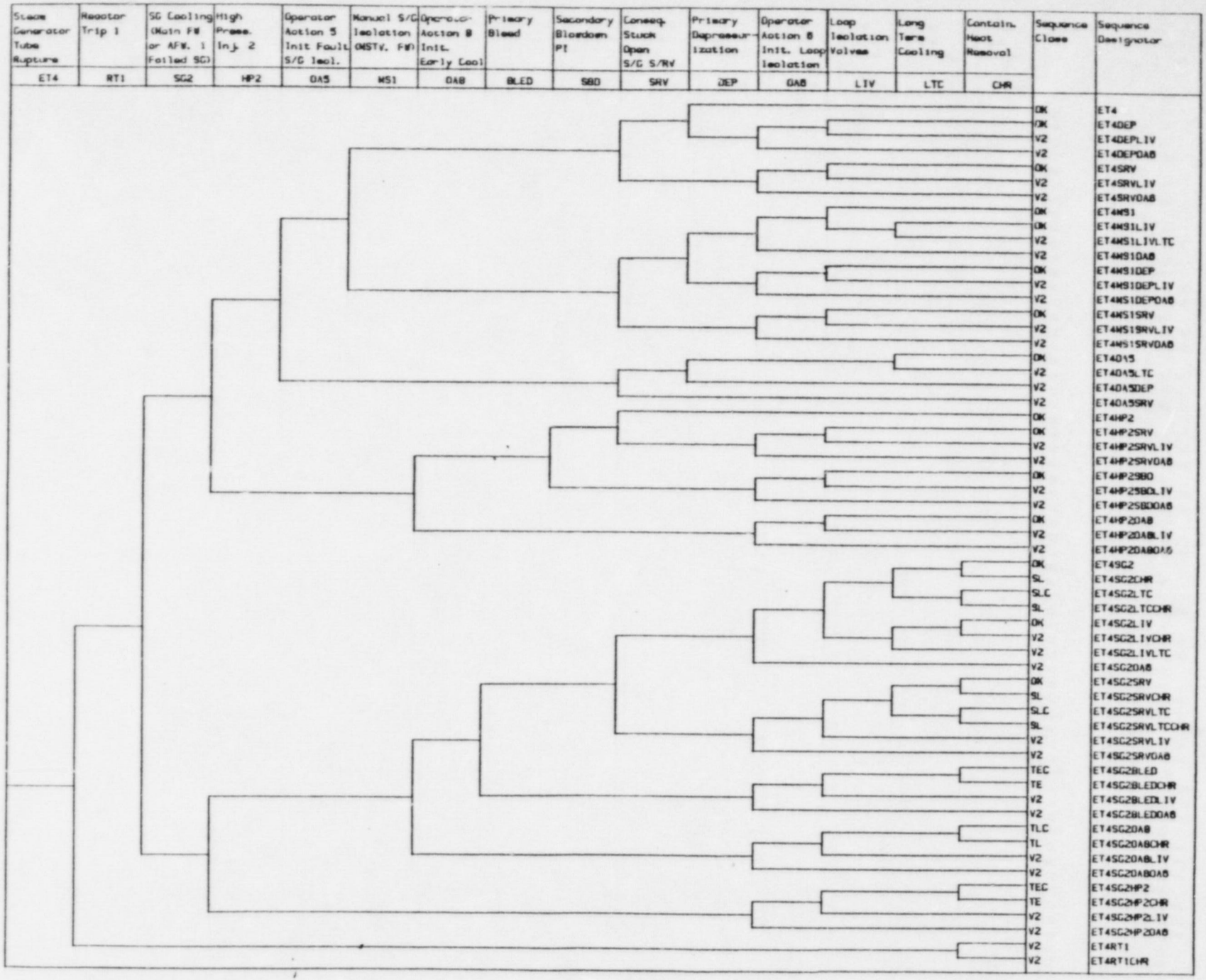


Figure 4.5 Steam Generator Tube Rupture Event Tree

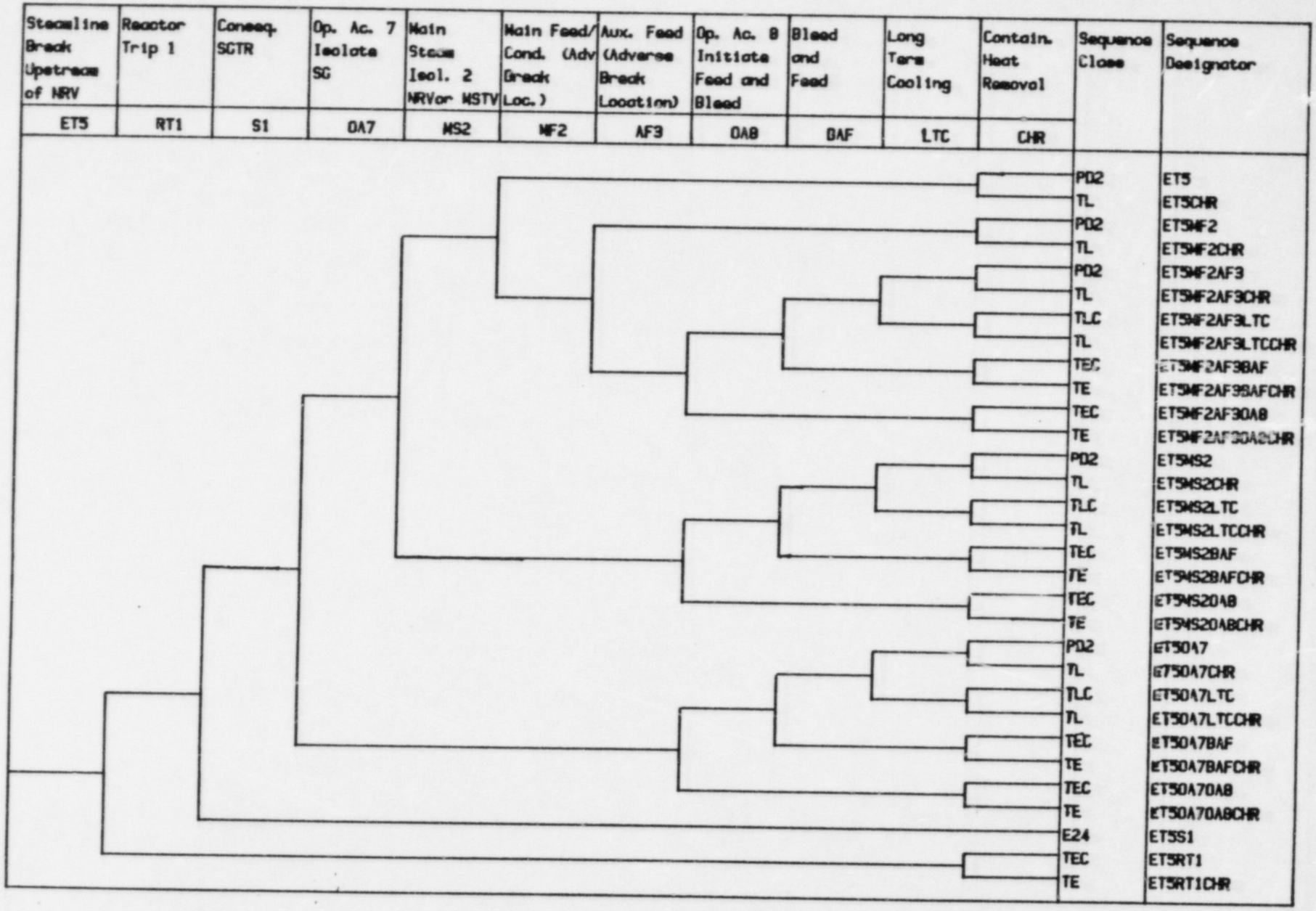


Figure 4.6 Steamline Break Upstream of the Nonreturn Valves (NRVs) Event Tree

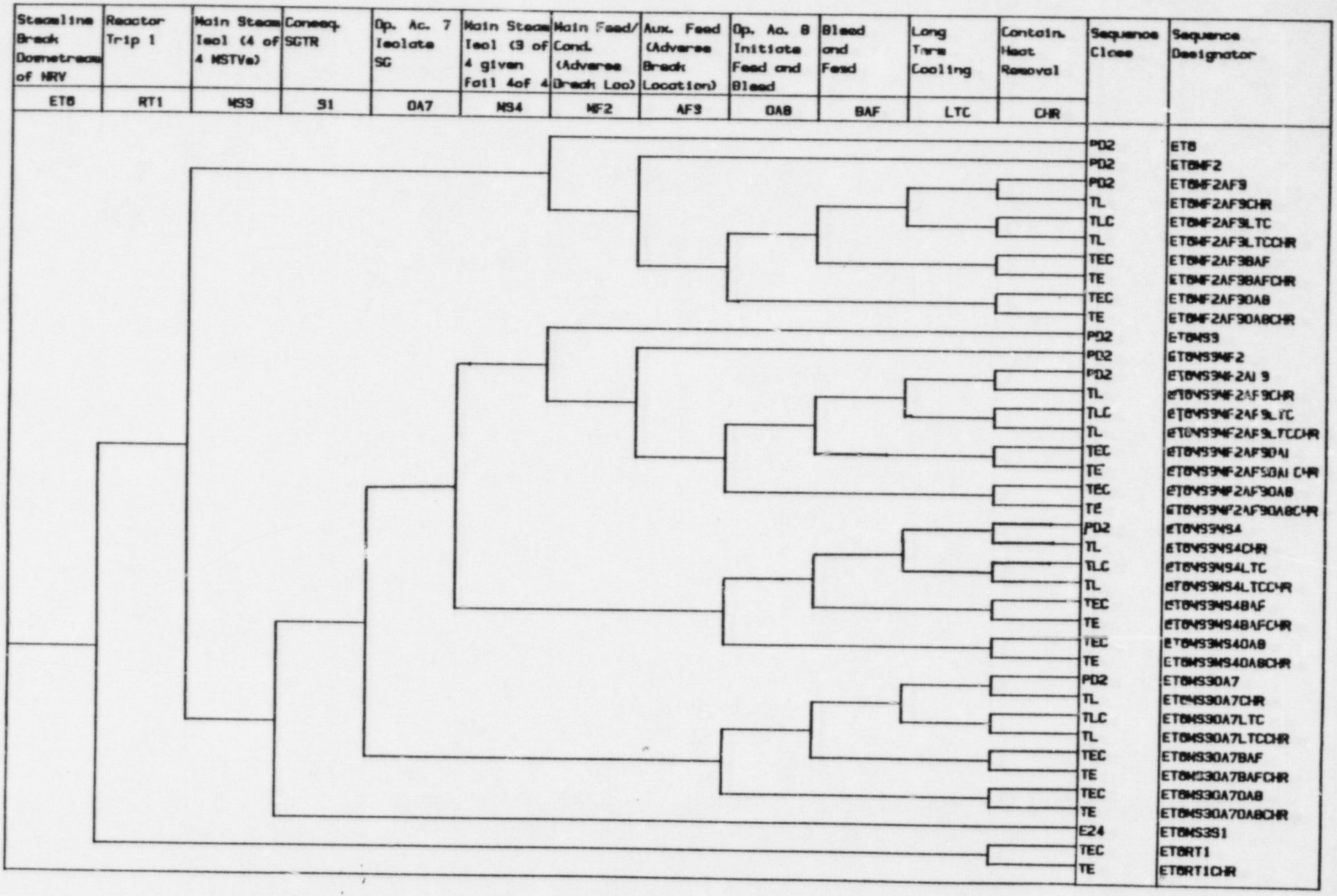


Figure 4.7 Steamline Break Downstream of the Nonreturn Valves (NRVs) Event Tree

4.2.7 Main Feedline Break Event Tree

The event tree for a main feedline break was found to be a proper representation of plant response. The PSS event tree for this initiator is shown in Figure 4.8.

4.2.8 Unisolated RCP Seal Leakage Event Tree

The unisolated RCP seal leak initiating event is not the same as the consequential RCP seal LOCA. The consequential RCP seal LOCA is generally caused by a loss of seal cooling to all four seals, as discussed in Section 4.1.2, which results in a flow rate in the small-small LOCA range. The unisolated RCP seal leak initiator refers to a random failure of a single seal which is not isolated by the operator. This failure most likely results in a leakage flow rate of about 100 gpm, which is below the lower limit of the definition of a small LOCA. Thus, the general comments in Sections 4.1.1. and 4.1.2 do not apply to this event.

In general, the unisolated RCP seal leak event tree is a reasonable representation of plant response to the event, with one exception. The PSS assumes that success of the charging system and steam generator cooling is sufficient to mitigate the event. This is a reasonable assumption since steam generator cooling is sufficient to remove decay heat and, at 100 gpm, the RWST contains enough water to provide makeup through the charging system for a substantial time period (over 35 hours). HPSI is also capable of providing this makeup from the RWST, but the RCS pressure must be lowered to do so. The method of lowering the RCS pressure depends on the actual systems available, and the particular case of interest is when charging has failed and steam generator cooling is available. As stated in the PSS and supported by the procedures, the preferred method of reducing RCS pressure in this case is by using secondary depressurization (steam generator blowdown). Logically, since all this method does is reduce pressure without causing additional loss of primary coolant, the plant response should be the same as when the charging system is operating. That is, the event is effectively terminated since the makeup required is about 100 gpm and the RWST capacity at that flow rate is over 35 hours. However, the PSS event tree treats this case in the same manner as the case where steam generator cooling fails, when the preferred method of cooling is bleed-and-feed.

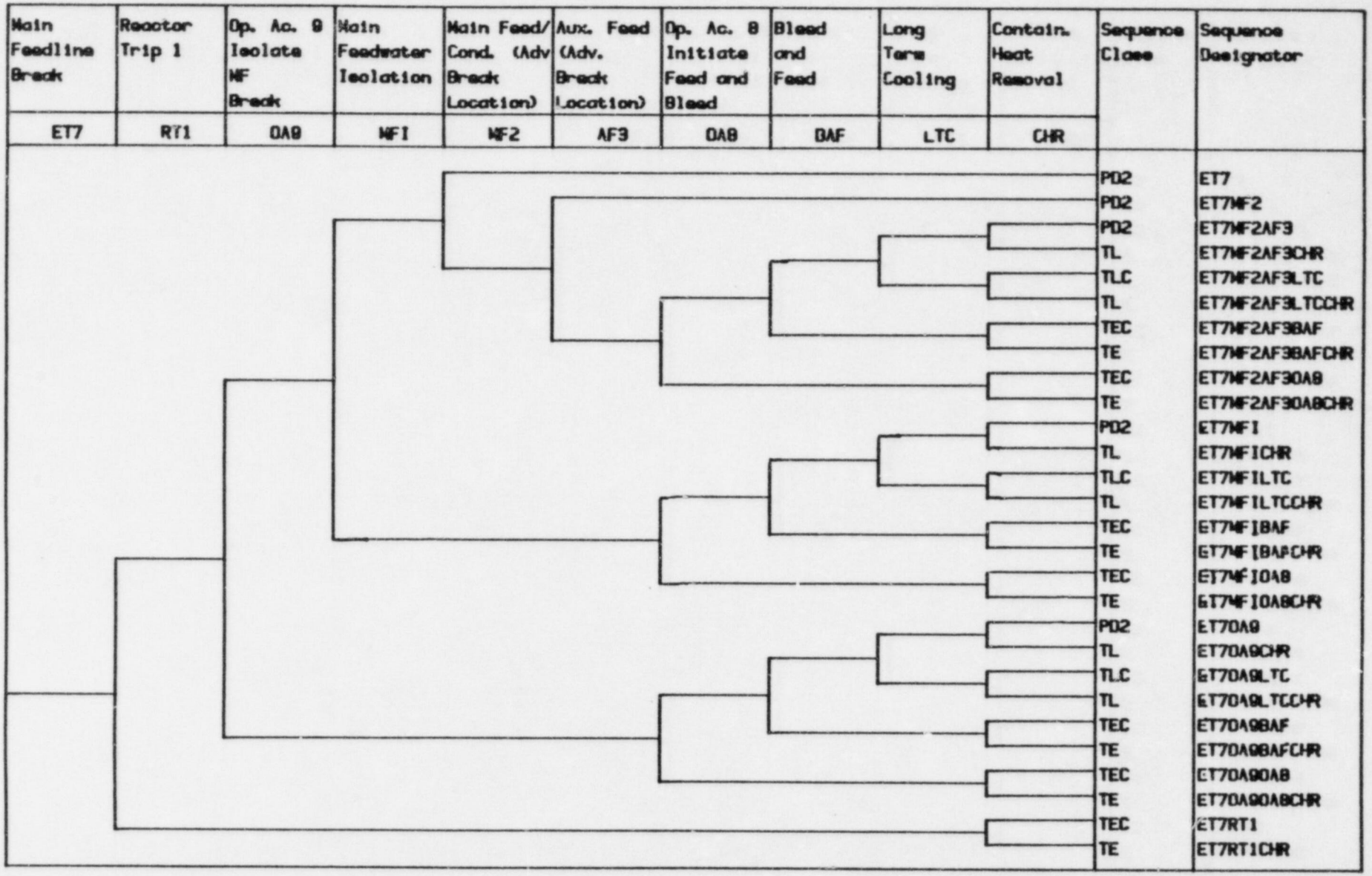


Figure 4.8 Main Feedline Break Event Tree

Thus, for both cases in the PSS, long-term (RHR) cooling and CHR are assumed to be required. This assumption is obviously conservative for the first case, where secondary depressurization is used. Therefore, the tree has been modified so that this conservatism is removed for that case. The revised tree is shown in Figure 4.9.

4.2.9 General Plant Transient Event Tree

The event tree for the general plant transient was found to be a proper representation of plant response. This event tree is shown in Figure 4.10.

4.2.10 Total Loss of Main Feedwater Event Tree

The event tree for total loss of main feedwater was found to be a proper representation of plant response. This event tree is shown in Figure 4.11.

4.2.11 Loss of DC Bus 2 Event Tree

There is a major problem with the event tree for loss of DC bus 2 with respect to the event PIT (primary integrity). The general comments discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response apply to this tree. In particular, failure of PIT and charging will result in core melt since high pressure recirculation will not be available and secondary blowdown cannot be used because the steam dump valves cannot function with loss of DC Bus 2. In addition, the comments in Section 4.1.5 regarding event AF4 also apply to this tree. The tree has been modified to take those findings into account. The revised tree is shown in Figure 4.12.

4.2.12 Loss of Offsite Power (LOSP) Event Tree

The loss of offsite power event tree is a proper representation of plant response to that event. This event tree is shown in Figure 4.13.

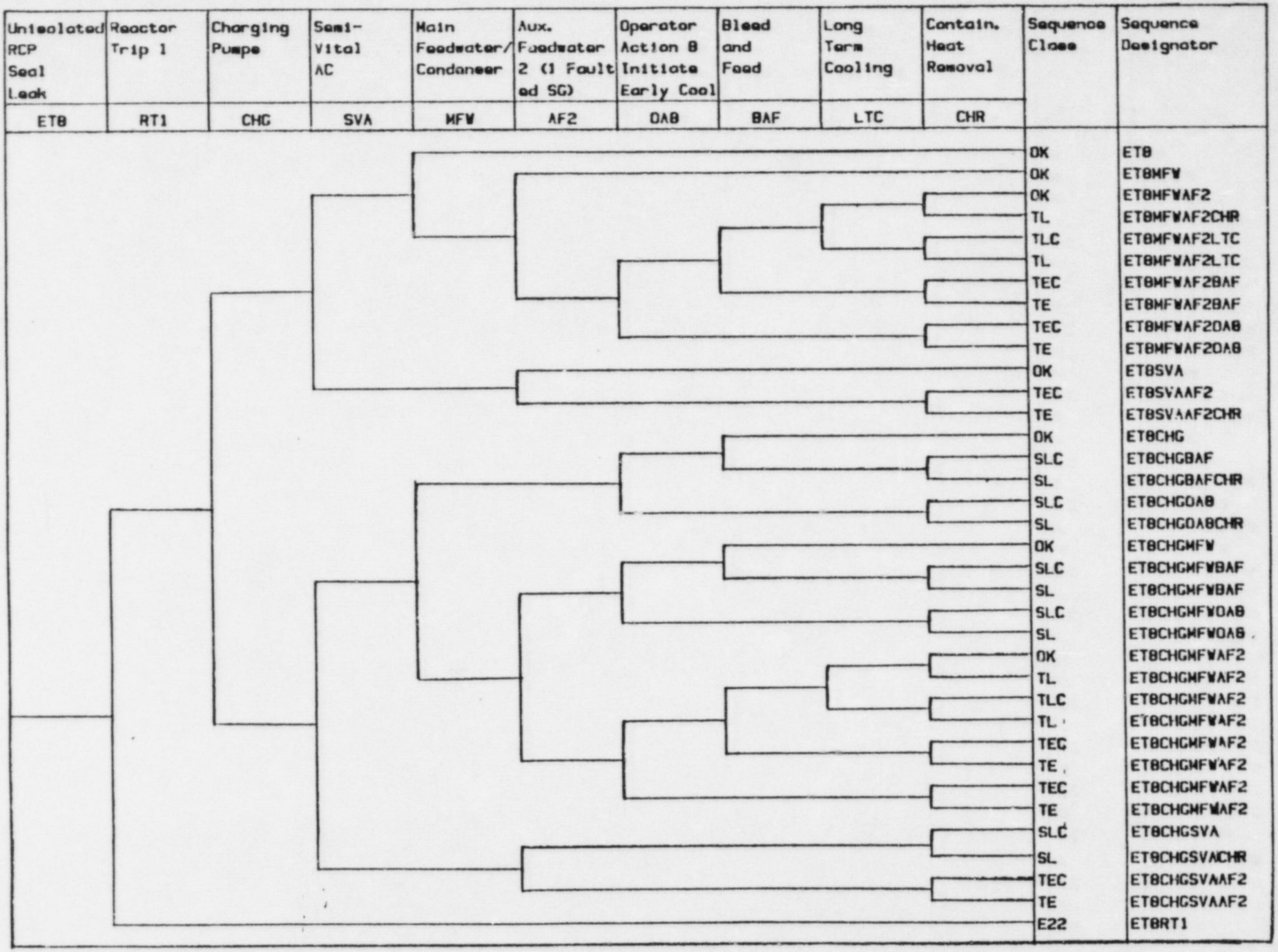


Figure 4.9 Unisolated RCP Seal Leak Event Tree

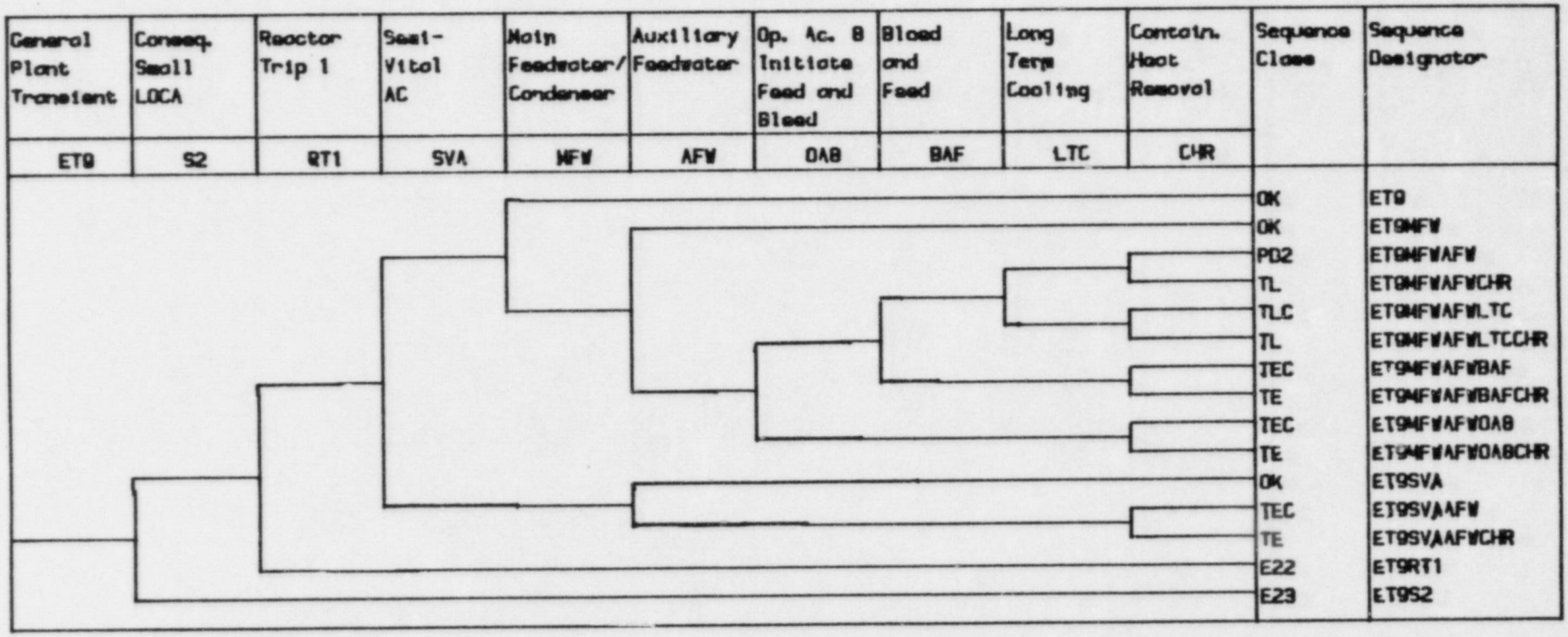


Figure 4.10 General Plant Transient Event Tree

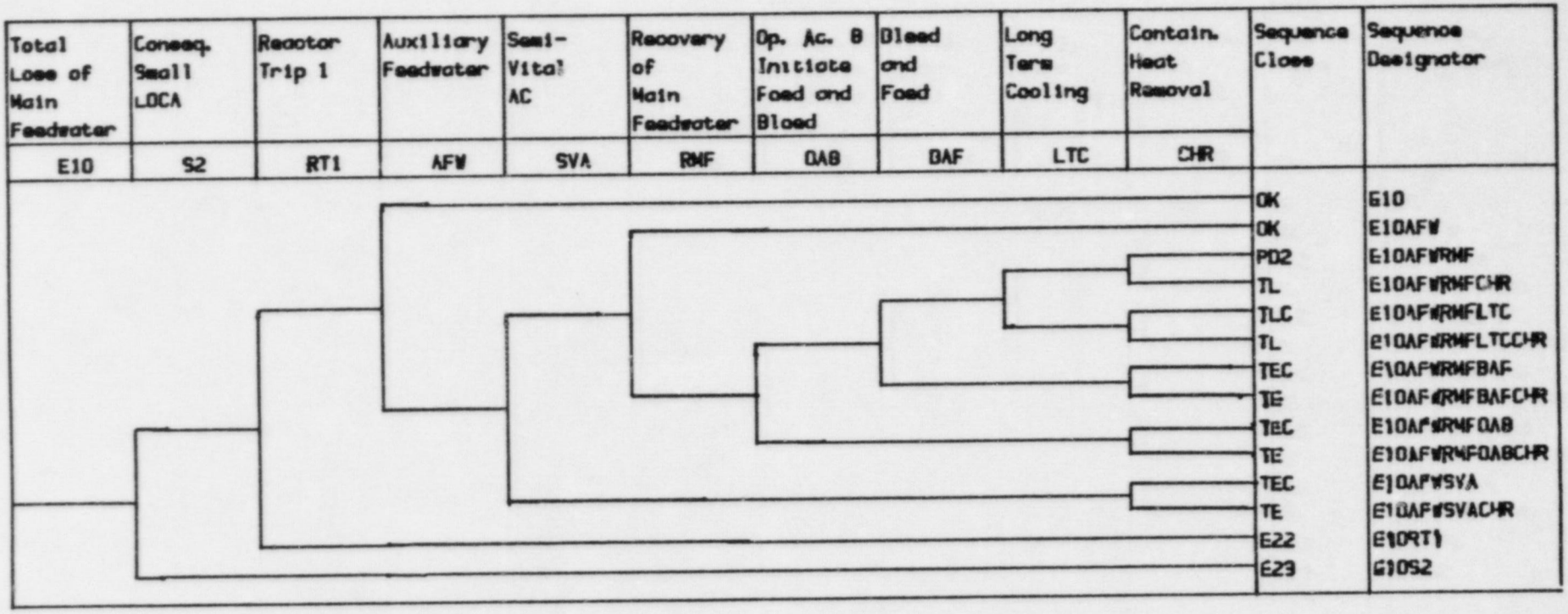


Figure 4.11 Total Loss of Main Feedwater Event Tree

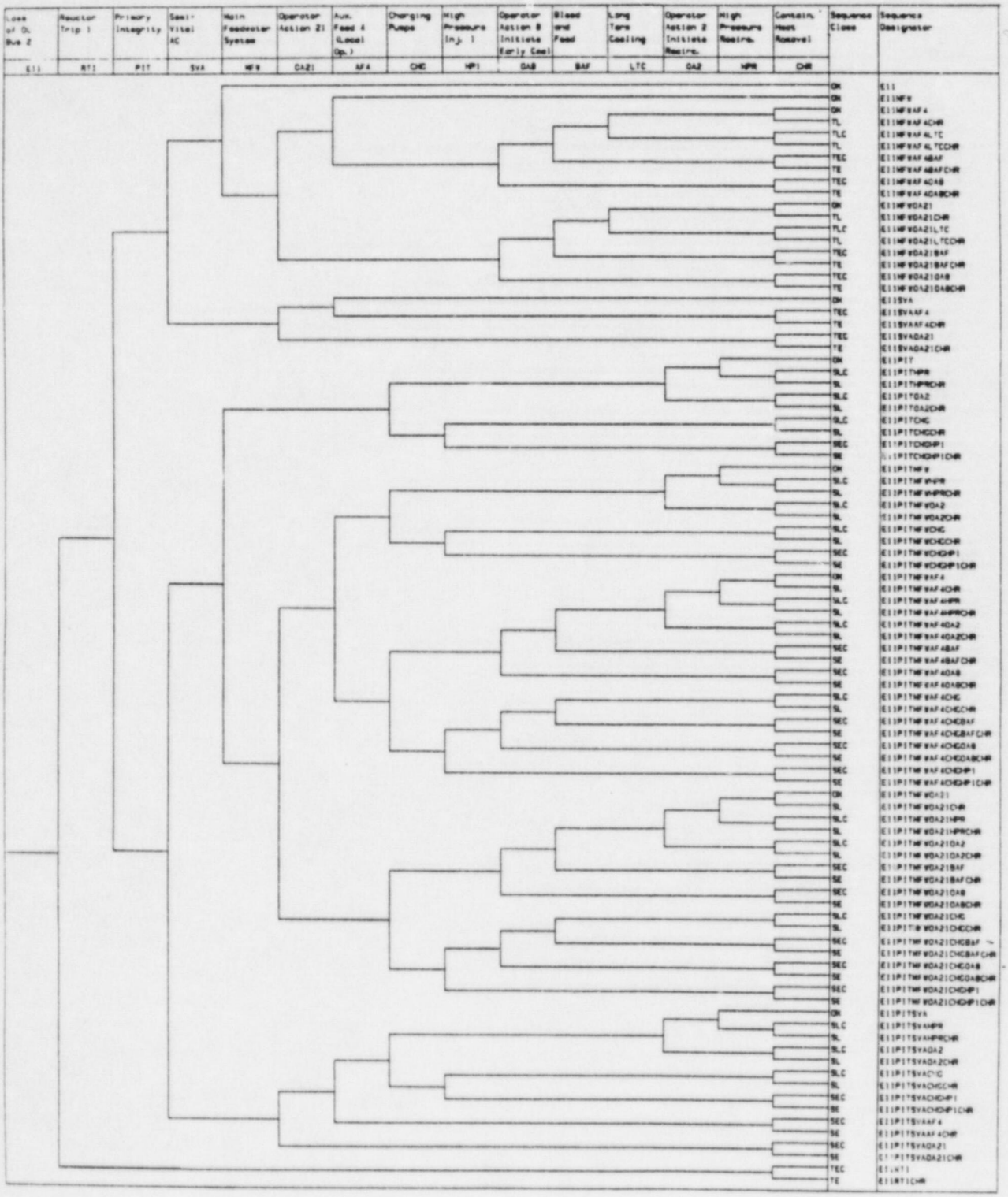


Figure 4.12 Loss of DC Bus 2 Event Tree

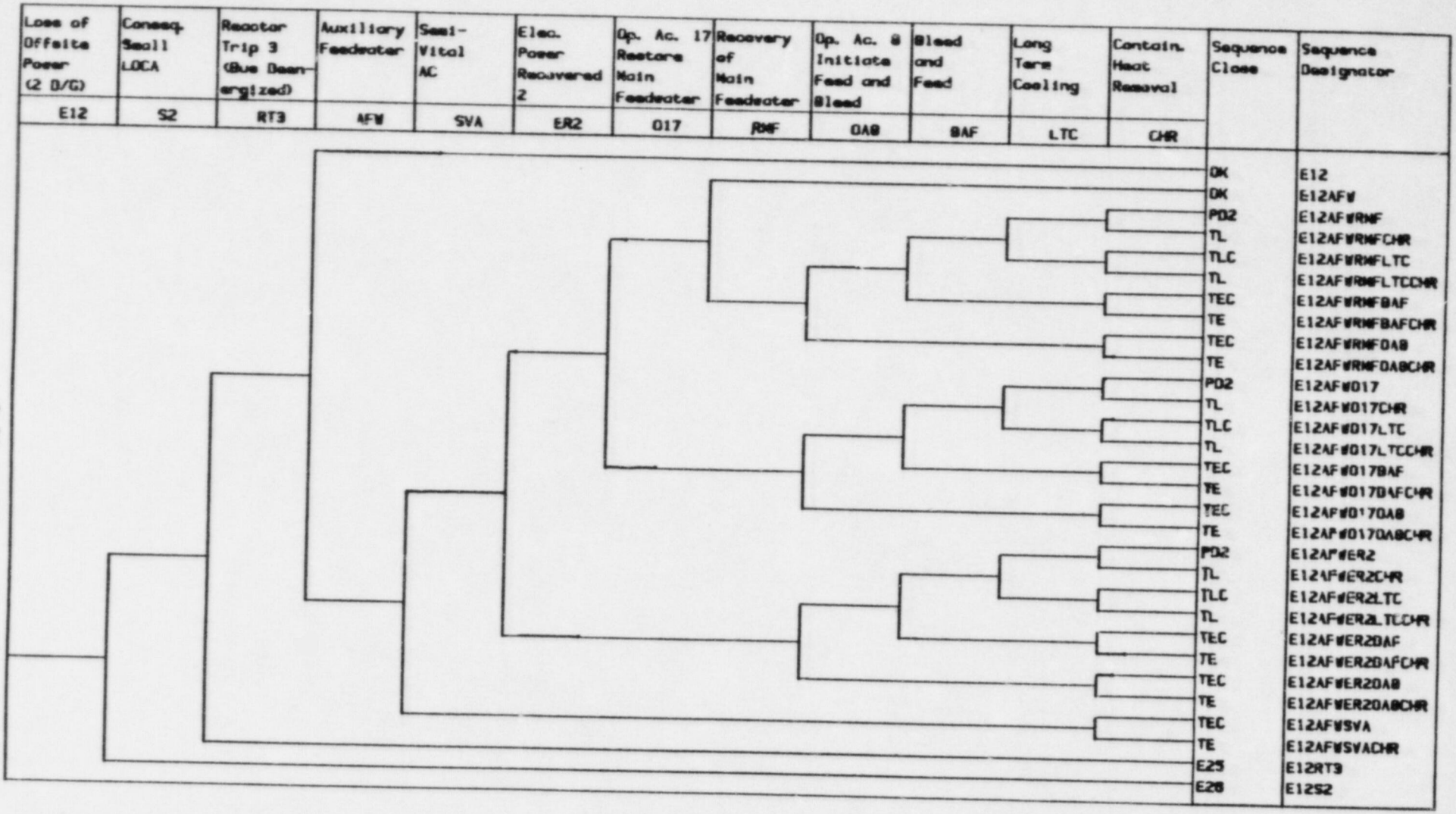


Figure 4.13 Loss of Offsite Power Event Tree

4.2.13 Loss of Offsite Power and MCC-5 Event Tree

A major problem with the event tree for loss of offsite power and MCC-5 pertains to the event PIT (primary integrity). The general comments discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response apply to this tree. In particular, RCP failure will occur as described in the PSS and thus, by the reviewer's definition, PIT automatically fails. Failure to recover MCC-5 will result in core melt since recirculation will be unavailable (see further discussion below). In addition, the comments in Section 4.1.5 regarding event AF4 also apply to this tree. The tree has been modified to take those comments into account and is shown in Figure 4.14.

For sequences where MCC-5 is not recovered in the short term (failure of events OA-18 or RMC, which have a 15-minute time limit), the only option for providing makeup is local manual recovery of the charging system through valve manipulation (as stated and considered in the PSS). If auxiliary feedwater is operating and charging is recovered, core melt is delayed for a significant period of time. As previously mentioned in Section 4.1.2, the PSS assumed that this was sufficient to prevent core uncovery past the 24-hour cutoff point (and presumably even longer). As also discussed in that section, the assumption may not be valid and some action to initiate long-term cooling (notably recirculation) may be required. Since this requires MCC-5 to be energized, the only way that core melt could be avoided is to manually initiate recirculation. It should be noted that the manual initiation of recirculation involves only the operation of valves, since MCC-5 does not affect the operation of the pumps. In addition, it would be unrealistic to assume that failure to recover MCC-5 within 15 minutes results in failure to recover MCC-5 in the long term when required for recirculation (within about 23 hours or so). Thus, even when events OA-18 or RMC fail, if AFW and charging are available, recirculation (event OA-2 and HPR) will be considered. In this case, these events will be redefined to include the decision and actions necessary to recover MCC-5. Since the cognitive decision (OA-2 for small-small LOCA) is already at the minimum human error probability (HEP) cutoff (discussed in Section 7.2.1b), the addition of another decision will not effect the HEP for this event. Thus, it will only be necessary to consider the fraction of MCC-5 faults which could reasonably be expected to be unrecoverable in the 23-hour time

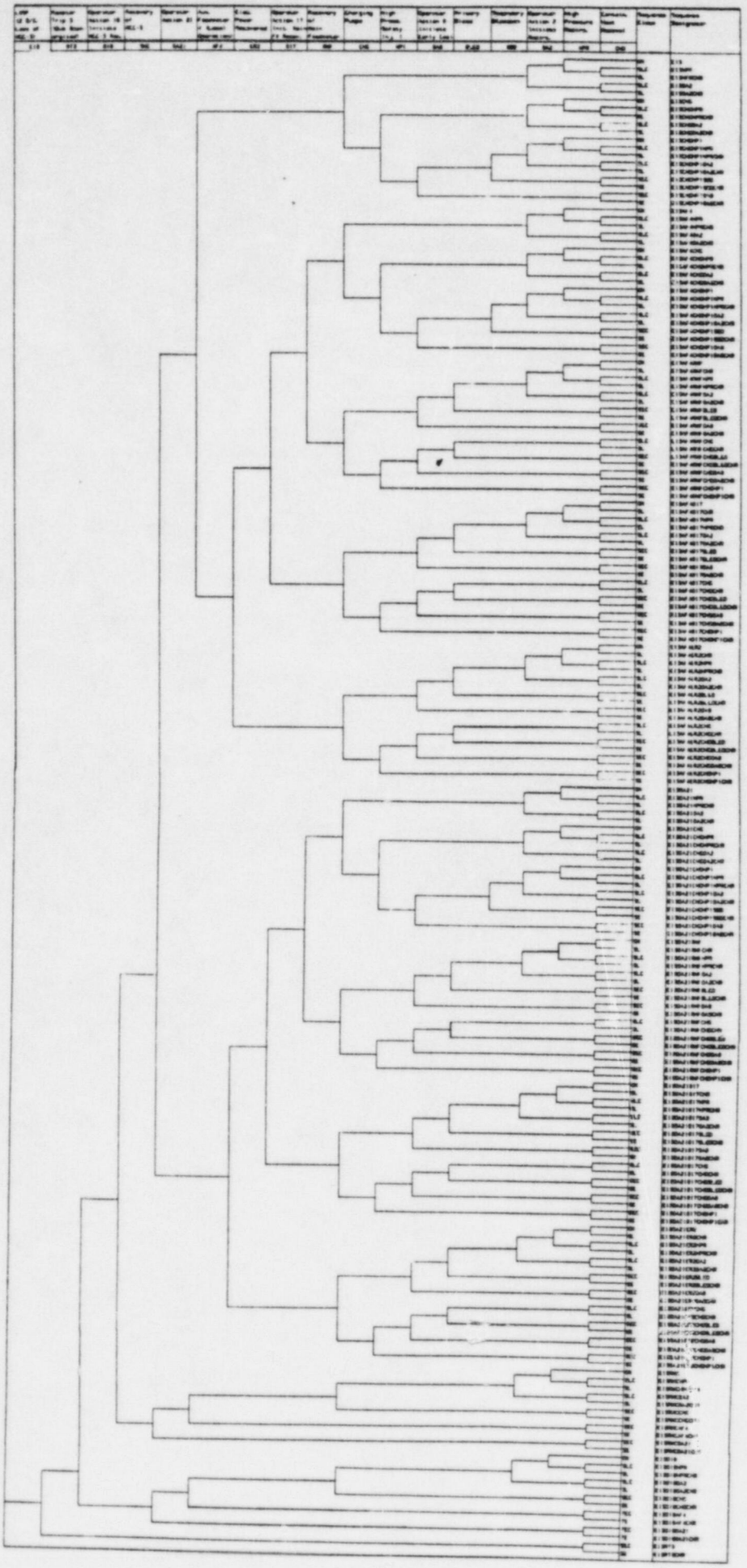


Figure 4.14 Loss of Offsite Power and MCC-5 Event Tree

frame and add that nonrecovery probability to the existing value for event HPR. It should be emphasized in this discussion that it is not important whether the recovery time limit is actually 23 hours or somewhat longer; the 24-hour sequence time cutoff should not be an absolute cutoff, but rather a guideline. What is important in this case is that there is a need to recover MCC-5 in a finite time period on the order of 24 hours, so that long-term heat removal can be established to prevent core melt.

4.2.14 Loss of Offsite Power and One Emergency Bus Event Tree

The event tree for loss of offsite power and one emergency bus was found to be a proper representation of plant response. This event tree is shown in Figure 4.15.

4.2.15 Station AC Blackout Event Tree

There is a major problem with the event tree for station AC blackout with respect to its treatment of plant response to an RCP seal LOCA. It is assumed (reasonably for this plant) that a seal LOCA will occur if the blackout persists for over fifteen minutes. Thus, the general comments discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response in the PSS would apply to this tree. In addition, the comments in Section 4.1.5 regarding event AF4 also apply to this tree. The tree has been modified to take those comments into account.

In addition to this problem, this tree is inconsistent with the other LOSP trees in two ways. First, when recovery of main feedwater following recovery of offsite power was considered in the other trees, two events appeared: OA-17 (operator cognitive decision to recover main feedwater), and RMF (mechanical and procedural failures in recovering main feedwater). These events were not included on the station blackout tree but were lumped together with the recovery of offsite power node since the failure to recover power was said to dominate the failure to recover main feedwater, in order to simplify the tree. Even if this were the case, this inconsistency is confusing. Further, the consideration of event OA-8 to represent operator response to the RCP seal (small-small) LOCA when steam generator cooling (all feedwater) has failed (that is, recognizing the need

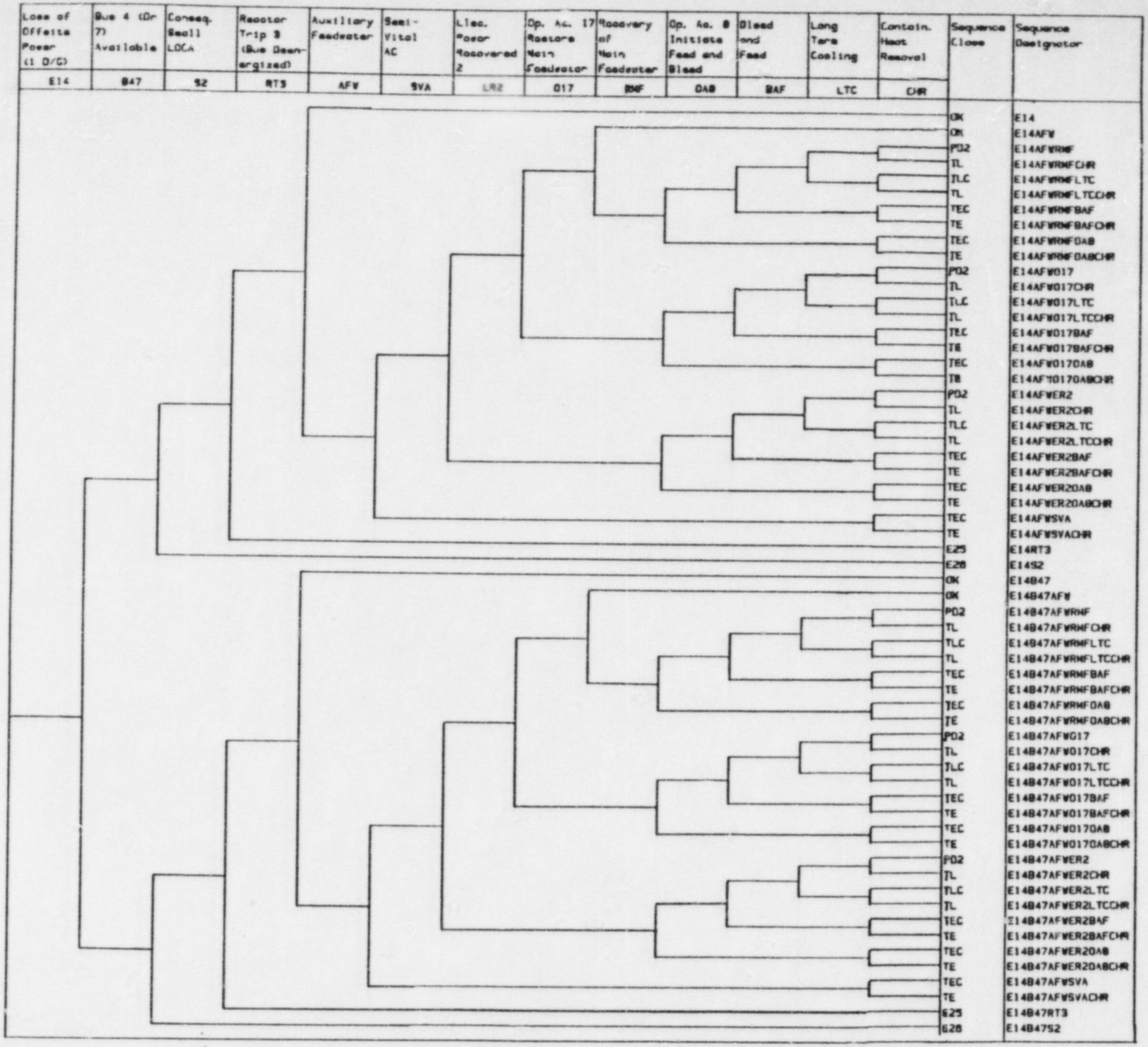


Figure 4.15 Loss of Offsite Power and One Emergency Bus Event Tree

for bleed-and-feed) requires separating out OA-17 since OA-8 is dependent on OA-17. Additionally, highlighting cognitive errors by modeling them on the event trees is an important tool in understanding plant response and combining them with other events would be counterproductive. Therefore, a modification of the tree is suggested to specifically identify these events.

The second inconsistency is the consideration of a 15-minute recovery period for offsite power. This was included because of the 15-minute time period to prevent RCP seal failure, which requires offsite power. However, it could be argued that if offsite power is recovered within fifteen minutes, it is almost as if the event had not occurred. That is, no adverse effects would have resulted from the LOSP (even including station blackout) other than a plant trip. Therefore, the initiating event LOSP should be redefined as meaning a LOSP of greater than 15 minutes' duration (as has been done in other PRAs such as the Millstone-3 PSS, where a 30-minute time period was used) and the initiating event frequency quantified to take that into account. LOSPs of less than 15 minutes' duration should be considered "general transients." The tree has been modified to reflect this change. The revised event tree is shown in Figure 4.16.

4.2.16 Insufficient Flow of Service Water Event Tree

The event tree for insufficient flow of service water exhibits a problem in that it assumes operator action is required to trip the reactor in order to prevent core melt. This is because it is assumed that much vital equipment would be lost due to overheating if the plant is not manually tripped. This assumption is extremely conservative and unrealistic. Even in the absence of a detailed analysis to determine what would fail and when the plant would trip, it is erroneous to assume such massive simultaneous failures, especially when some of the failures involve systems that do not even require service water for cooling. Reasonably, one would expect that overheating failure of the condensate and main feedwater system would cause plant trip before other systems were damaged. Even using a conservative approach and assuming that all operating systems cooled by service water would be irreparably damaged, the only result would be unrecoverable loss of feedwater, loss of the air compressors, loss of the operating charging pump, and loss of the operating containment air recirculation units. Other components cooled by service water could be recovered

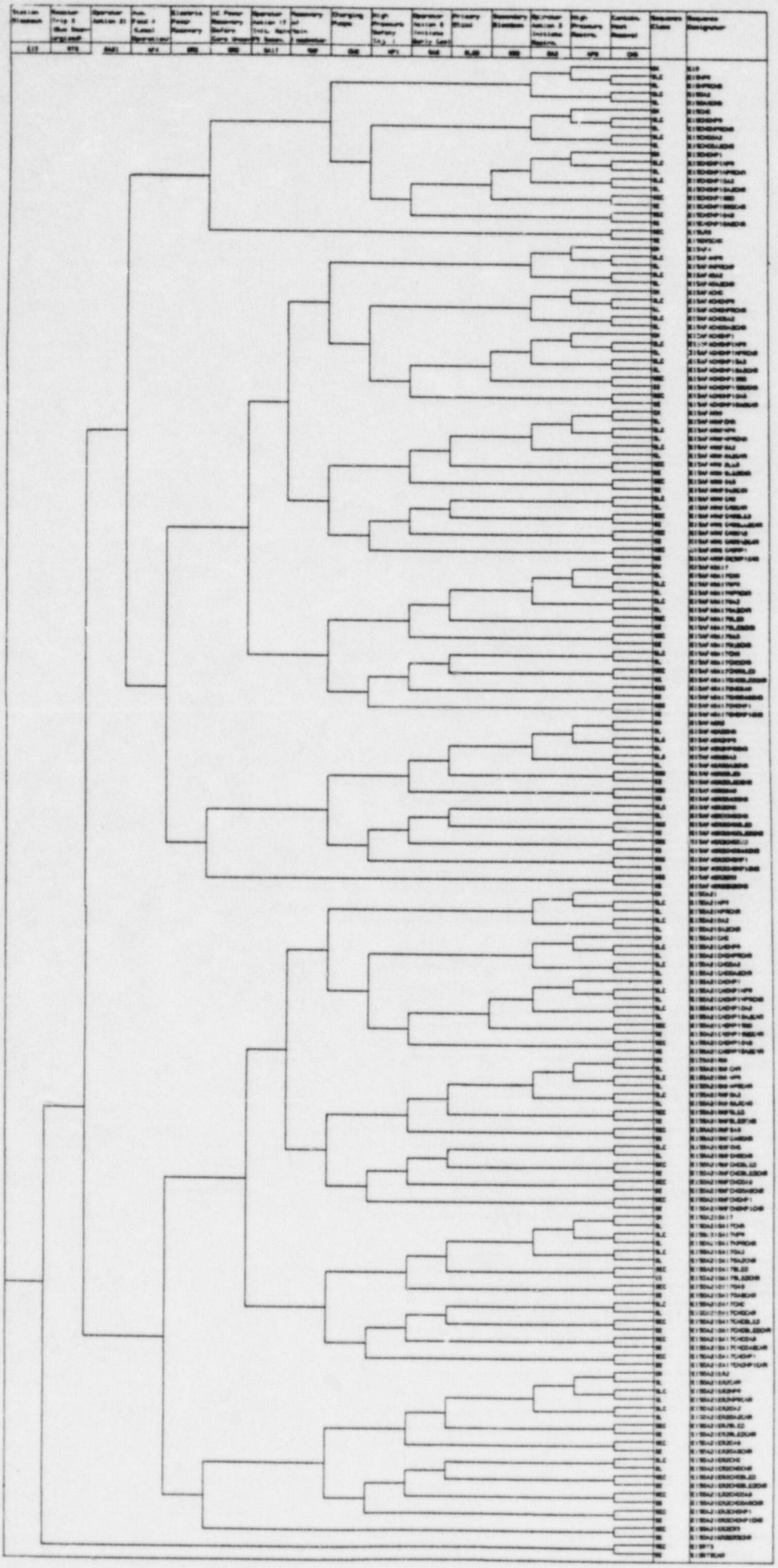


Figure 4.16 Station Blackout Event Tree

if service water is eventually restored. Therefore, the tree has been modified to reflect the availability of the unaffected systems if only automatic reactor trip occurs.

Another comment is that no credit is given for bleed-and-feed cooling if AFWS fails. Granted, if service water is not eventually recovered prior to the need for long-term cooling, the use of BAF would serve only to delay core melt. However, this ability to extend the time of melt, and credit for recovering service water within that time frame, should have been considered. One further point is that, since BAF requires success of CHR in order to be fully successful, the event CHR should always be evaluated assuming that service water is initially unavailable. That is, success of CHR would be defined as one of two fire pumps. The tree has been modified to reflect this change. The revised event tree is shown in Figure 4.17.

4.2.17 Loss of Control Air Event Tree

The major problem with the loss of control air event tree is with respect to the event PIT (primary integrity). The general comments discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response apply to this tree. In particular, failure of PIT and charging will result in core melt since high pressure recirculation will not be available and secondary blowdown cannot be used without control air. In addition, the comments in Section 4.1.5 regarding event AF4 also apply to this tree. The tree has been modified to take those comments into account. The revised tree is shown in Figure 4.18.

4.2.18 Loss of MCC-5 Event Tree

A major problem with the event tree for loss of MCC-5 occurs with respect to the event PIT (primary integrity). The general comments discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response apply to this tree. In particular, RCP seal failure will occur (as described in the PSS) and thus, by the present definition, PIT automatically fails. Failure to recover MCC-5 will result in core melt unless recirculation is established manually. The comments regarding long-term recovery of MCC-5 presented in Section 4.2.13 apply to

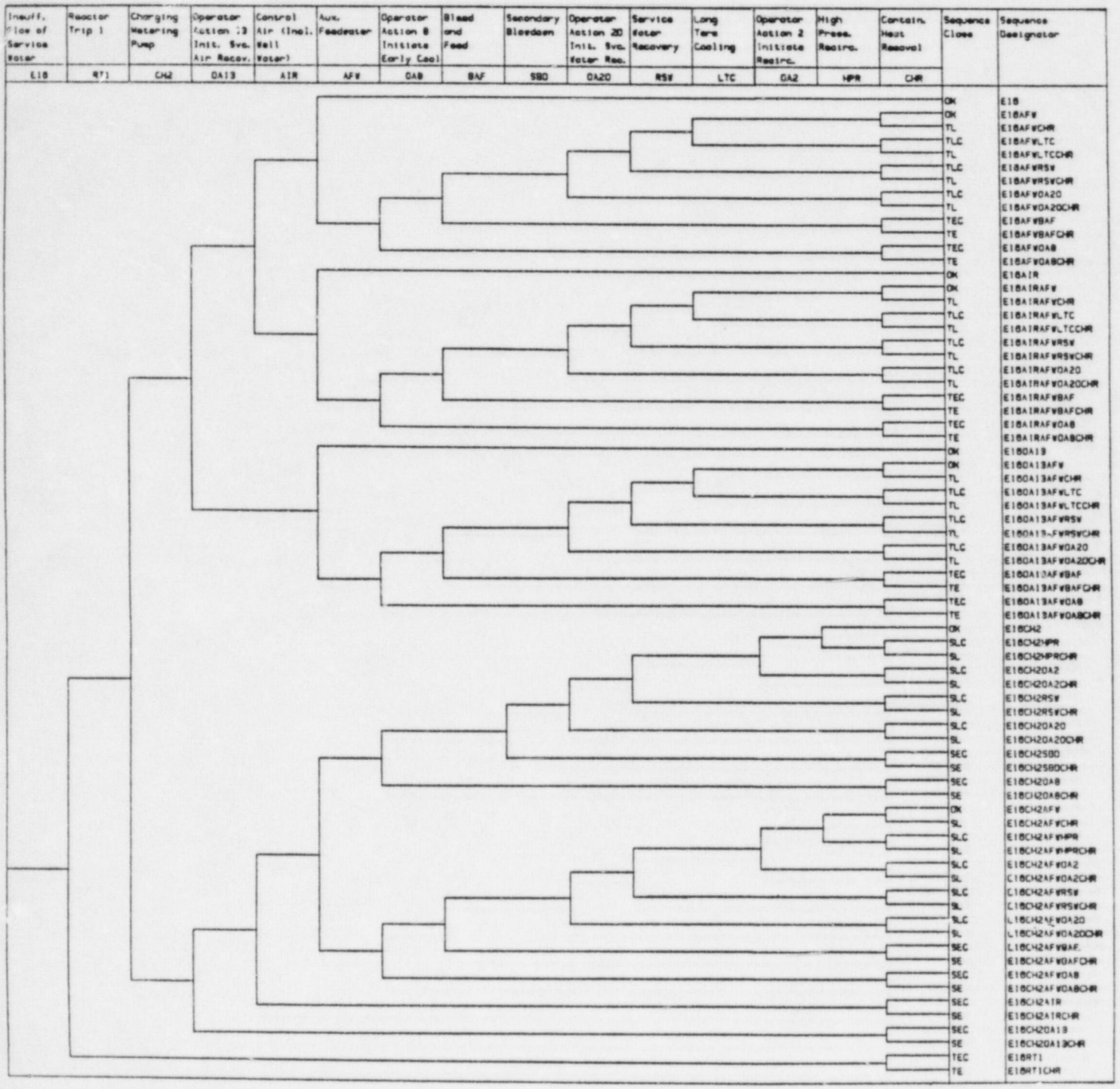


Figure 4.17 Insufficient Flow of Service Water Event Tree

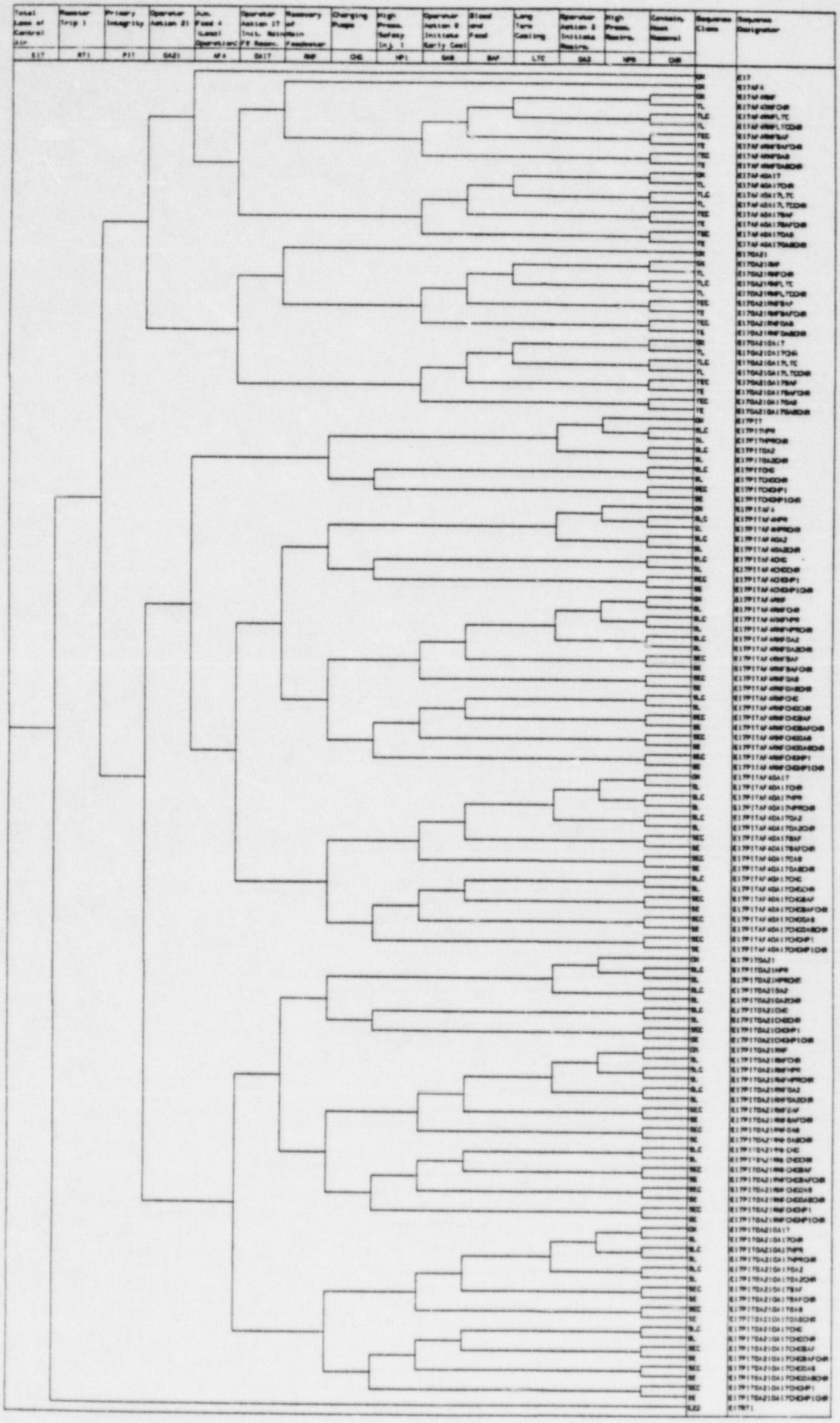


Figure 4-18 Loss of Control Air Event Tree

this tree, as well as the comments in Section 4.1.5 regarding event AF4. The tree has been modified to take those comments into account. The revised tree is shown in Figure 4.19.

4.2.19 Total Loss of DC Event Tree

The event tree for total loss of DC is based upon an assumption that a failure of the operator to control charging flow, which may result in a challenge to the SRVs, will result in a core melt. The PSS admits this is a conservative assumption, since the SRVs may not be challenged at all. This review has further concluded that the conservatism of the assumption is significant if it is assumed that the SRVs do lift, since it is by no means certain that they will fail to reseat. It would appear that the only difference between the case in which the operator fails to control charging and the case in which he succeeds is in the conditional probability of a consequential LOCA. In the case of operator failure, excess flow-induced opening and failure of an SRV to reseat would yield a higher consequential LOCA probability. In the opinion of the reviewers, the operator need take no action whatsoever if integrity is maintained and steam generator cooling functions. This is consistent with the analysis of all other transient initiators. The tree has been modified to reflect this conclusion.

A cosmetic problem with the event tree results from the inclusion of events OA-14 and RDC, which address recovery of DC power. The PSS determined that DC power cannot be recovered due to plant unique design features, a conclusion with which the review team concurs. However, that conclusion was not arrived at until after the tree was constructed, and the recovery events were not removed from the tree. This is confusing, and the review team corrected and simplified the tree by removing these events. The revised event tree is shown in Figure 4.20.

Although this tree contains event AF4, the comments in Section 4.1.5 do not apply because the subsequently affected events (as described in Section 7.3.1b) do not appear on this tree.

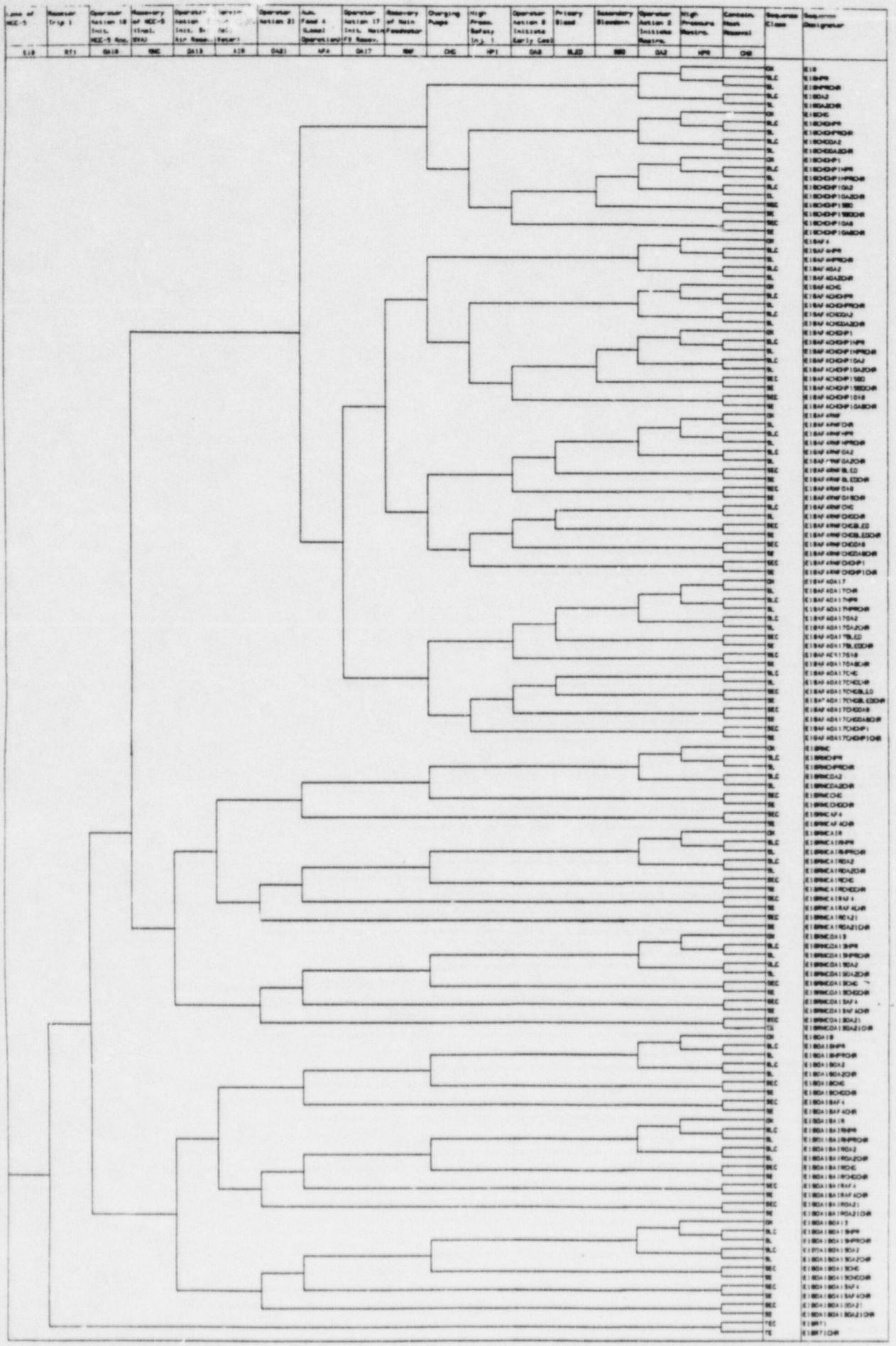


Figure 4.19 Loss of MCC-5 Event Tree

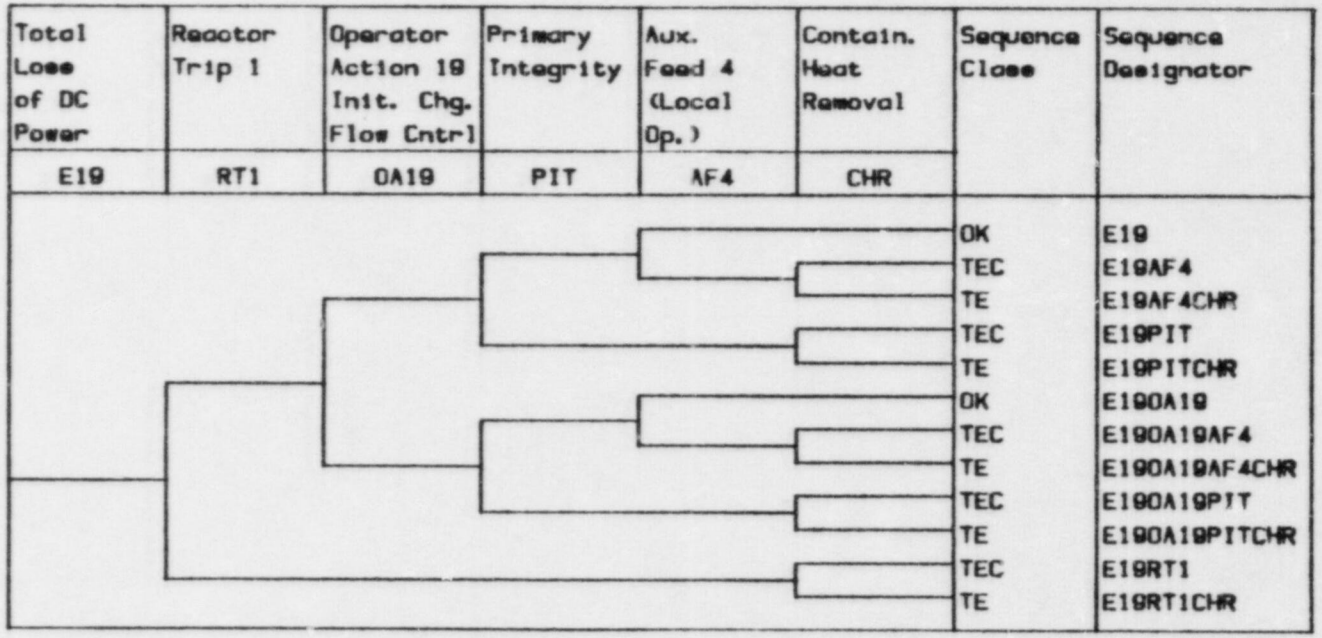


Figure 4.20 Total Loss of DC Power Event Tree

4.2.20 Loss of DC Bus 1 Event Tree

The event tree for loss of DC Bus 1 event tree also has a problem with respect to the event PIT (primary integrity). The general findings discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response apply to this tree. The tree has been modified to take those findings into account. The revised tree is shown in Figure 4.21.

4.2.21 Loss of Semi-Vital AC Event Tree

The only problem with the loss of semivital-vital AC event tree is with respect to the event PIT (primary integrity). The general findings discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response apply to this tree. In particular, RCP failure will occur (as described in the PSS) and thus, by the reviewer's definition, PIT will automatically fail. This results in a small-small LOCA. The tree has been modified to take those findings into account. The revised tree is shown in Figure 4.22.

4.2.22 Anticipated Transients Without Scram Event Tree

We have reviewed the anticipated transients without scram (ATWS) event tree and have found it to be a proper representation of plant response. This event tree is shown in Figure 4.23.

4.2.23 Consequential Small LOCA Event Tree

The only problem with the consequential small LOCA event tree is with respect to the handling of plant response to small LOCA events. The general findings discussed in Sections 4.1.1 and 4.1.2 regarding the treatment of RCP seal LOCAs and small LOCA plant response apply to this tree. The tree has been modified to take those findings into account. The revised tree is shown in Figure 4.24.

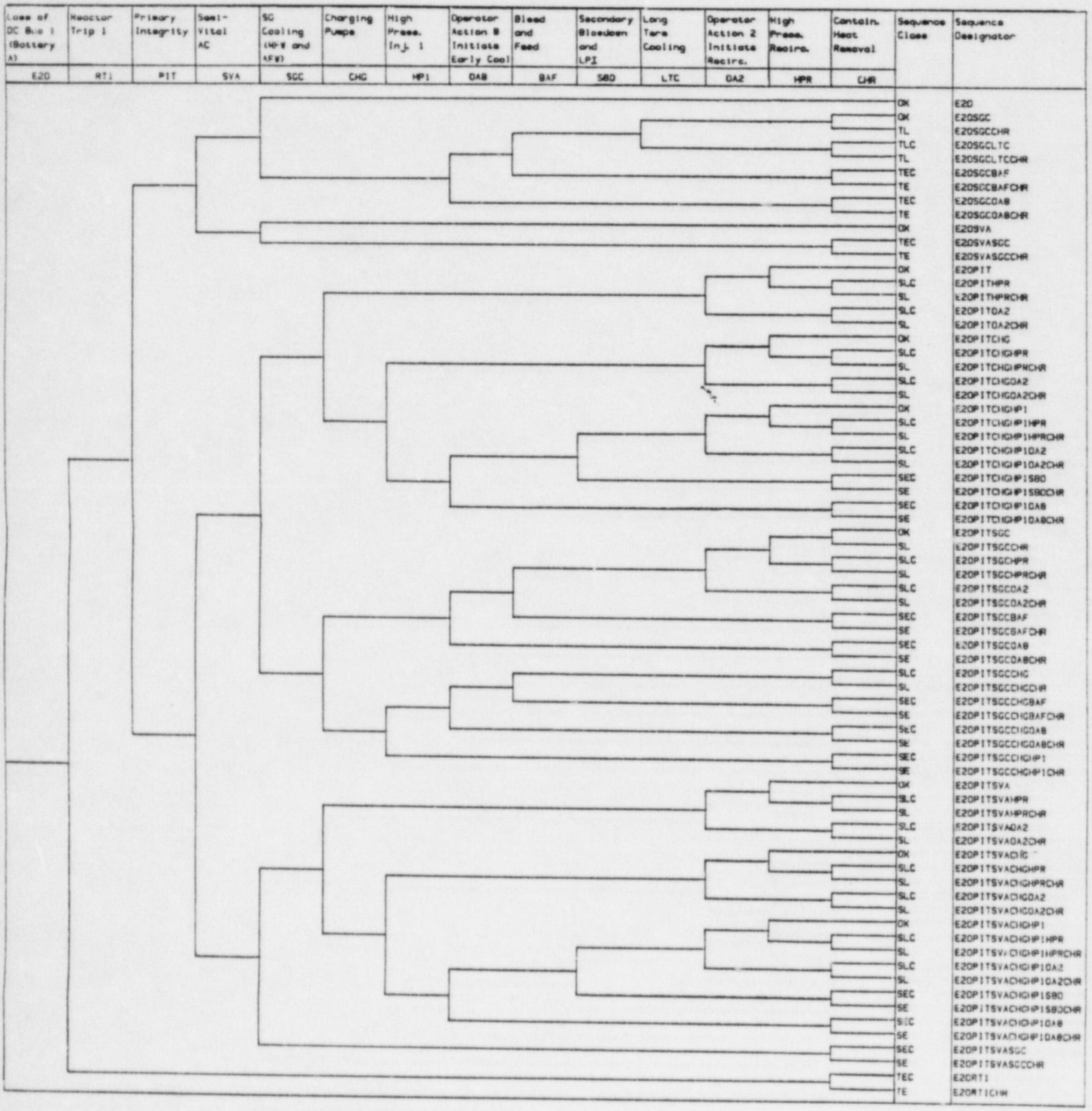


Figure 4.21 Loss of DC Bus 1 Event Tree

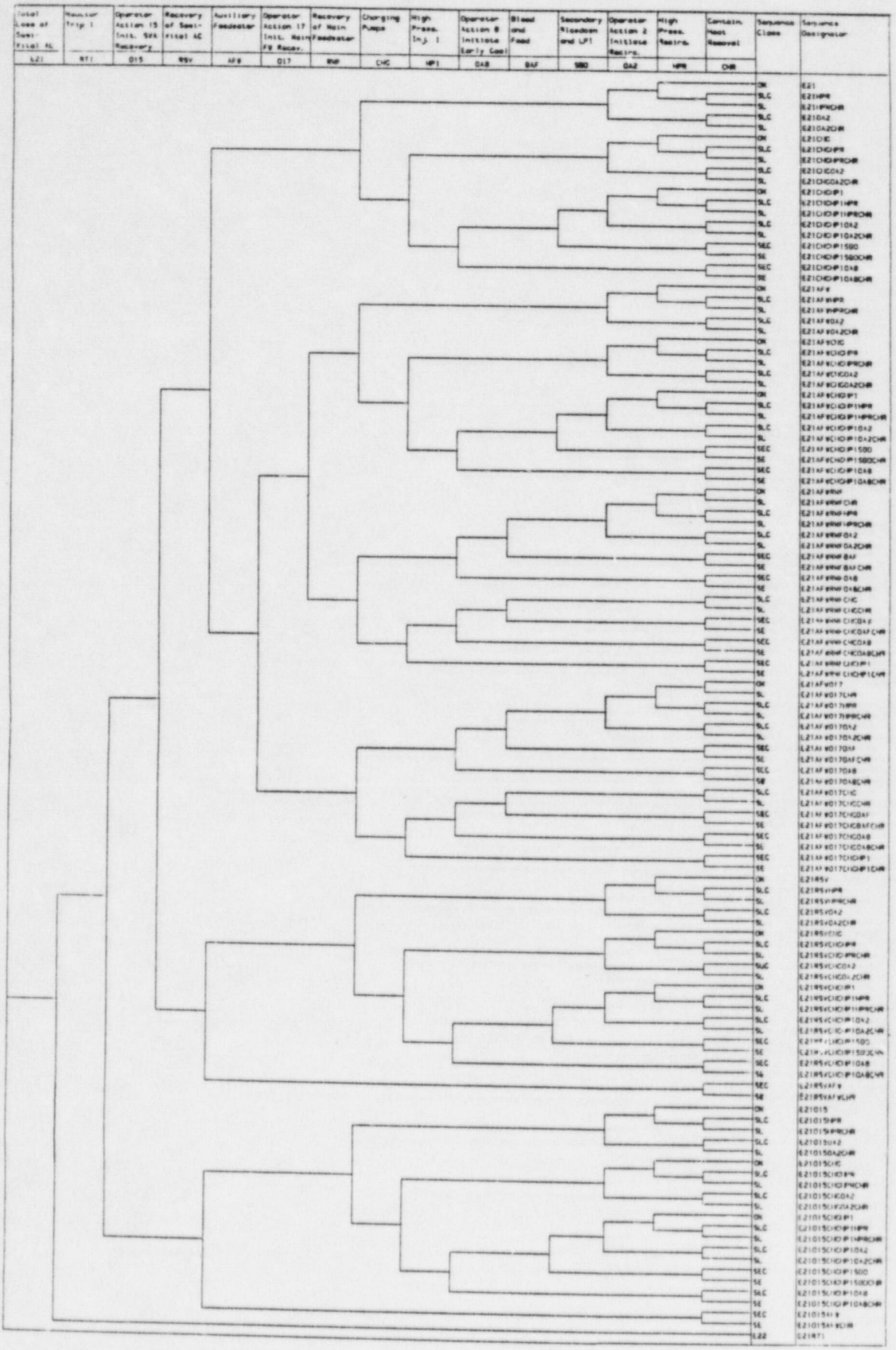


Figure 4.22 Loss of Semi-Vital AC Event Tree

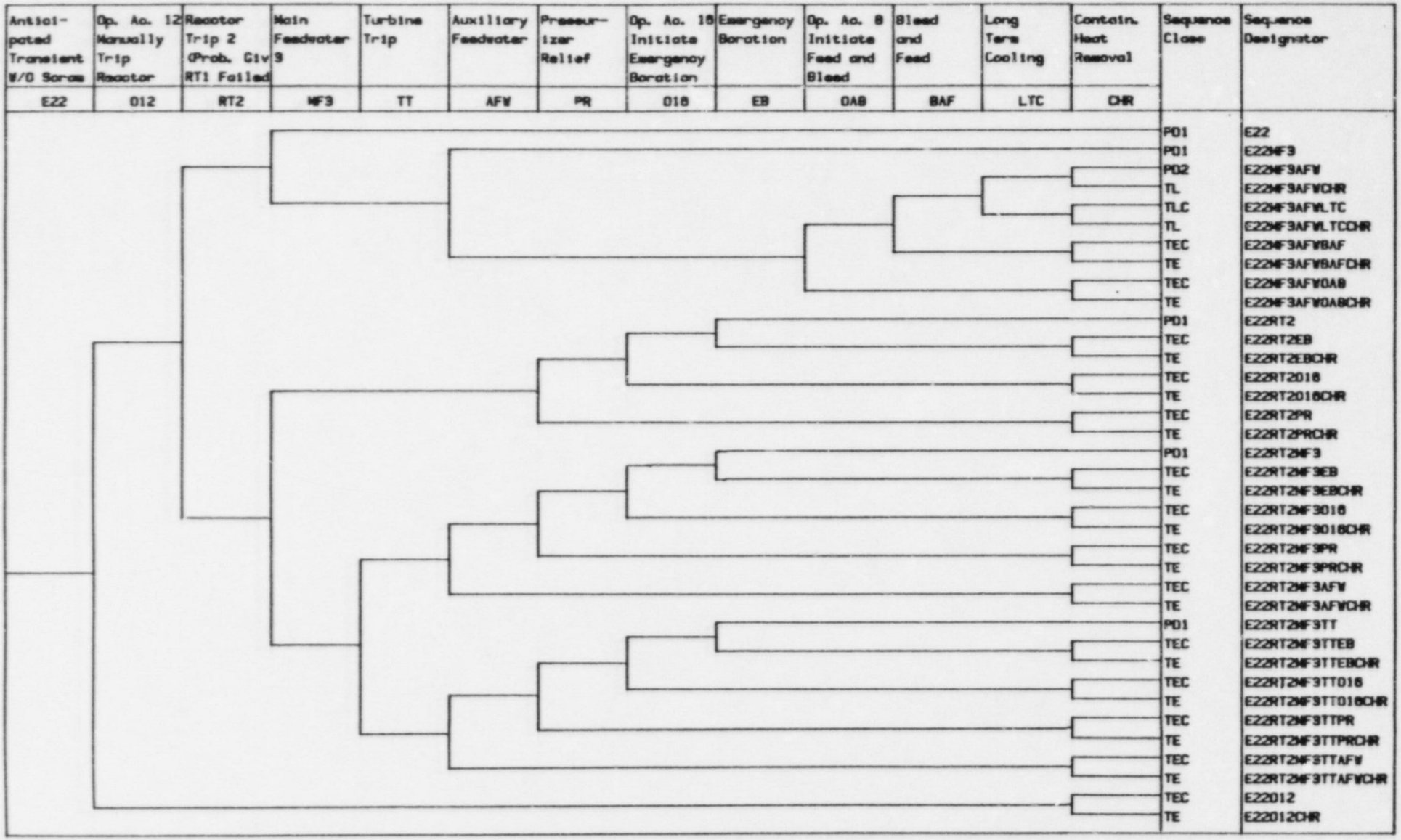


Figure 4.23 Anticipated Transient Without Scram Event Tree

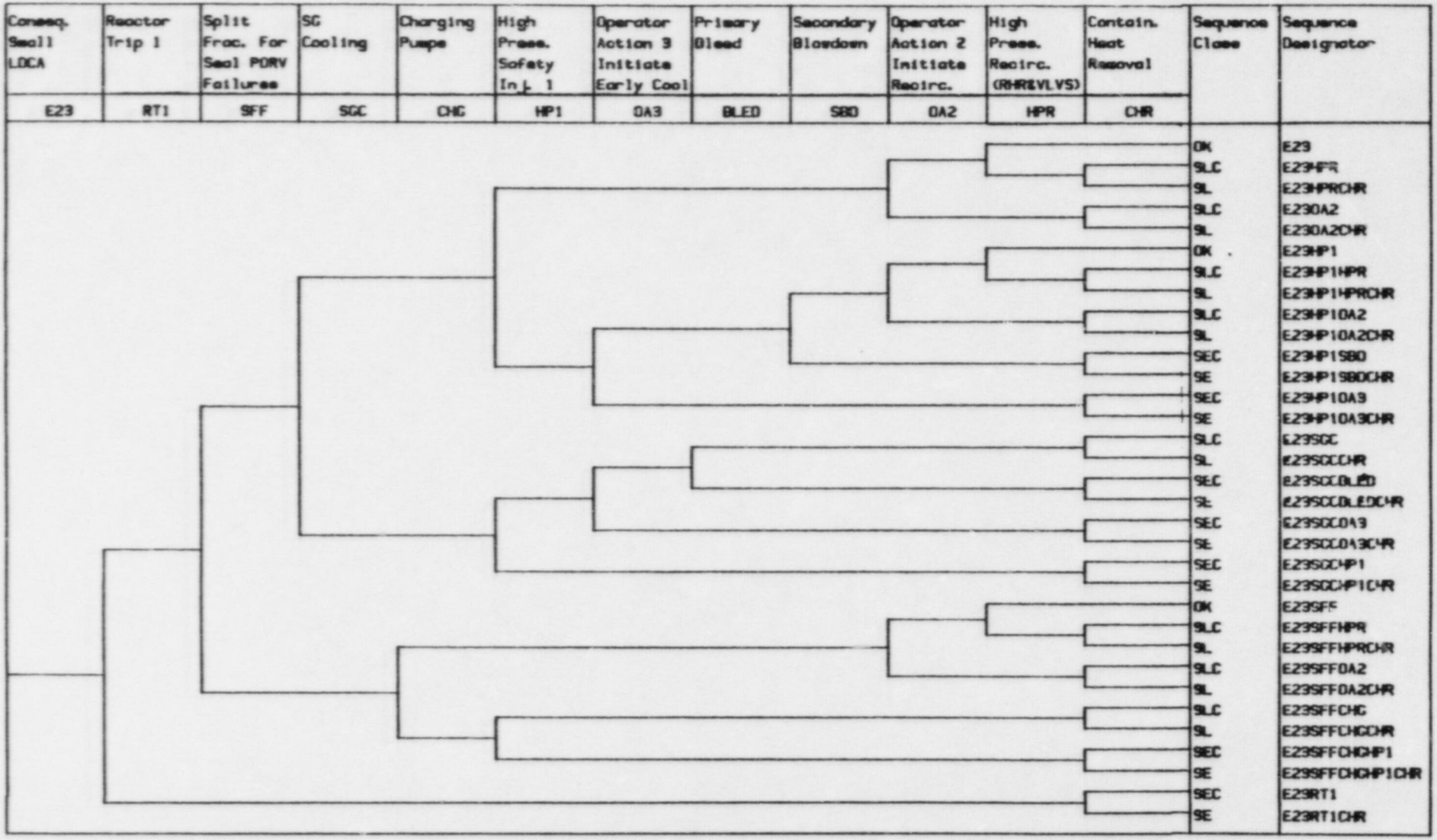


Figure 4.24 Consequential Small LOCA Event Tree

4.2.24 Consequential Steam Generator Tube Rupture (SGTR) Event Tree

The problem with this event tree is similar to that with the random SGTR tree (Section 4.2.4). That is, the sequence of events with respect to operator action and the conditions which affect these actions is not properly represented, resulting in a logical inconsistency between the likely response paths and the event tree representation. Once again, this is due to the nature of operator response to a failure of steam generator cooling (SGC). When SGC is successful, the procedures will cause the operator to take actions that will lead him to isolate the faulted steam generator secondary side and then eventually close the loop isolation valves. This sequence is properly represented on the event tree. However, when SGC is failed, the procedures will immediately set the operator on a course that will lead him to establish bleed-and-feed cooling before he determines that a steamline break and SGTR exists. Only after he has done this will he proceed to isolate the faulted steam generator and primary loop. This sequence is not properly represented on the event tree. The solution is to move the SGC and bleed-and-feed events so that they occur before the steam generator/loop isolation events on the tree and to restructure the tree accordingly.

It should also be noted that the assumption that all steam generator cooling will be lost if the operator fails to perform steam isolation of the unfaulted steam generator (MS4) is overly conservative. This action should occur automatically (except for the isolation of feedwater from the faulted steam generator, which has little effect on the eventual result of the sequence). Thus, whether isolation occurs is just a part of the mechanical equipment required for steam generator cooling, and MS4 is not required on the tree, since it serves no other purpose in the model other than the preservation of SGC. The revised event tree, which also incorporates other comments from Section 4.2.4, is shown in Figure 4.25.

In summary, the review team has suggested modifications to 14 of the 24 event trees, with a corresponding increase in the number of accident sequences. Many of these modifications are suggested in the interest of qualitative accuracy, as is appropriate for a "living PSS." The quantitative impacts of the modifications are estimated in Chapter 10.

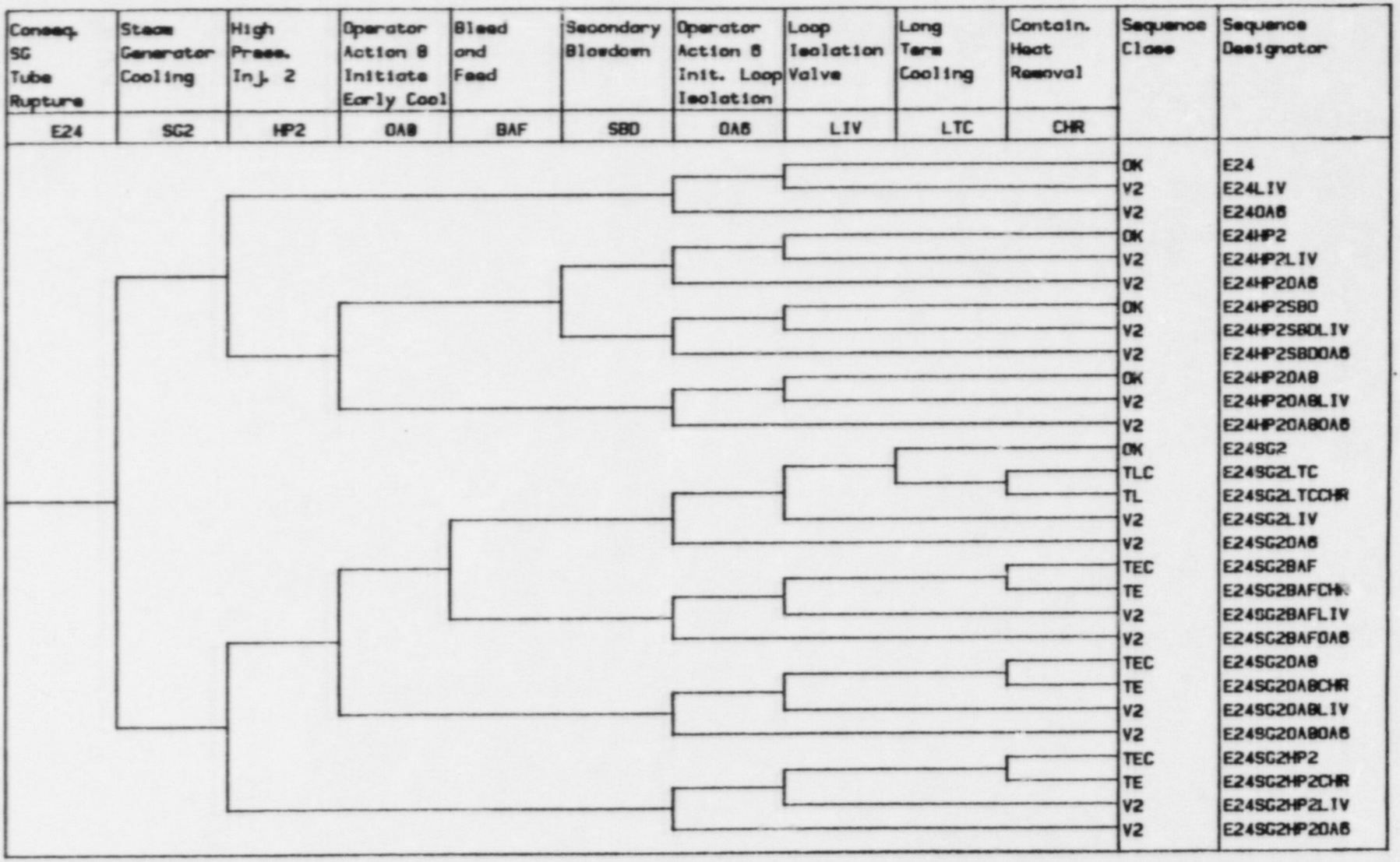


Figure 4.25 Consequential Steam Generator Tube Rupture (SGTR) Event Tree

5.0 SYSTEM RELIABILITY ANALYSIS REVIEW

This section contains the results of the review of the systems modeled using fault tree techniques in the Haddam Neck PSS. The intent of this review was to assess:

- the accuracy of the fault tree logic,
- the consistency in the level of detail of the systems modeled,
- the assumptions used and the impact of system model simplifications
- the modeling of system dependencies, both between systems and between the initiating events and the systems modeled,
- the comprehensiveness of the faults addressed by the PSS (human errors, test and maintenance errors, component faults); and
- the accuracy of the system model quantifications.

The review of each system fault tree consists of a system description and comments on the system model. The system description includes the system configuration, the system dependencies, and the system success criteria. The system dependencies are depicted in system dependency diagrams, which model the dependency fault logic. Comments are divided into those that we feel are significant and those that we feel are relatively minor observations. Significant comments deal with modeling assumptions, errors, and omissions that could affect the system quantification. As part of the system analysis review, a check of the fault tree models results was performed by verifying the calculated system unavailabilities and dominant contributors to the system unavailability. Comments on the system quantification are also included.

Finally, as part of each system analysis review, a limited requantification of the system unavailability was performed to assess the impact of the recommended changes. This includes the comments on the system analysis presented in this section and the recommended changes to the component reliability data presented in Section 6. However, data changes were limited to components that were significant contributors to the system unavailability except for where the component failure data increased by nearly an order of magnitude or more.

The fault tree models supplied in the PSS are reduced fault trees that contain what was determined to be the majority of the dominant system faults. The reduced fault trees have been developed to the component level (pumps, valves, relays, sensors, etc.) which in some cases have been recombined into developed events which were used in the reduced system fault trees. Some of the simpler system fault trees have been included in their entirety.

Fault trees were provided in the PSS for the following systems:

- DC Power System
- AC Power System
  - MCC-5
  - Semi-Vital AC
- Service Water System
- Component Cooling Water System
- Instrument Air System
- Steamline/Feedline Isolation
- Charging System
- Safety Injection Actuation System
- High-Pressure Safety Injection System
- Low-Pressure Safety Injection System
- Residual Heat Removal System
- Integrated Injection for SGTR
- Containment Spray System
- Auxiliary Feedwater System

Some systems, such as th Reactor Protection System (RPS), Power Conversion, and Primary Depressurization, were analyzed using methods other than fault tree analysis. The methods used to evaluate these systems also have been reviewed.

Some human errors are evaluated in the system fault tree analysis. Those human errors that are the result of manipulative actions, actions required to properly align equipment for use, or that occur prior to an initiating event are included as part of the system analysis. This second type of error includes failure to restore equipment after test or maintenance and errors committed during maintenance. Many human errors are

incorporated directly into the event trees. These are primarily the cognitive human errors (those involving recognition of what is happening) and of the actions necessary to respond to the situation.

In the Haddam Neck PSS, system interactions are primarily modeled through the use of a support state methodology. Each of the front-line systems, as determined by the event tree analysis, and the support systems are evaluated (quantified) for various combinations of support system successes and failures. The support states modeled in the PSS are presented in Table 5-1. The system dependencies are not explicitly modeled on each system fault tree. For example, the emergency AC power system requires service water cooling for the diesel generators. The emergency AC power system fault tree is quantified once assuming that the service water system is available and a second time assuming the service water system is unavailable. In the second case those components that need service water cooling in order to operate are assumed to have failed.

As a result of the use of the support state methodology, the system fault trees are intended to be completely independent of each other. System boundaries are defined so that components are modeled in one system only.

The use of detailed fault trees in the system analysis significantly reduces the potential for missed support system interdependencies often cited as a weakness of the support state methodology. The argument is that the support state methodology does not provide the mechanism to identify potential component failures that could affect more than one division of a support system or set of support systems. This is true if detailed models of the support system are not used or if the system is not completely modeled. The use of complete detailed fault trees, with the proper system success criteria, greatly reduces the potential to omit the subtle but important component failures that affect more than one support system division. It is important that the systems be completely modeled and that system success criteria include the requirement for successful operation of multiple support system divisions. (For example, the AC power system should be modeled to require that both divisions provide power to their loads so that single failures that fail both divisions can be identified.) The example cited is the one case where the PSS analysis was

Table 5-1 Haddam Neck PSS Support States

Support State	Notes	Support Systems Unavailable
1		All support systems available
2		Service Water
3		One DC Bus
4		One DC Bus and Service Water
5		Both DC Buses and Service Water
6	A	Both DC Buses and MCC-5
7	B	Both DC Buses and MCC-5 and Service Water
8		Offsite Power
9		Offsite Power and MCC-5
10	C	Offsite Power and 1 AC or DC Bus
11	D	Offsite Power and Service Water or Offsite Power and Both DC Buses
12		MCC-5
13		Both DC Buses
14	D	Offsite Power and Both AC Buses
15	D	Offsite Power and 1 AC Bus and 1 DC Bus
16	C	Offsite Power and MCC-5 and 1 AC or DC Bus

Notes:

A - Support state is quantified as either DC bus fails or both fail and MCC-5 fails. Impact on front line systems is always treated as both DC buses and MCC-5 fail.

B - Support state quantifications is dominated by service water system and MCC-5 failure probabilities.

C - Support state quantification includes failure of single AC or DC bus. Event tree quantification assumes that in this support state a DC bus is failed. (This assumption impacts the ability to recover power given a recovery of offsite power.)

D - These 3 support states are station blackout scenarios. The event tree quantification assumed, for support state 11, that both DC buses were unavailable.

not as complete as necessary. Only one train of the emergency AC power system was completely modeled; the second was assumed to be identical to the first. For this support system, component failures, if they exist, that could fail both AC divisions were not found. In all other cases, the models appear adequate to identify such support system interdependencies.

The Haddam Neck PSS system reliability analysis is generally well done and accurately models the plant systems. This is best illustrated by the relatively few major comments generated by this review and the small impact of those comments. Most of the modifications to system unavailabilities result from component data modifications rather than system model changes. Details of the system analysis review are contained in the following sections.

5.1 AC Power System

A simplified one-line diagram of the AC power system is provided in Figure 5.1. Two offsite AC power supplies are available at Haddam Neck Plant. These two sources of power are crosstied in the switchyard so that all essential loads can be supplied by either offsite power source. (This is not the system configuration described in the PSS; however, the differences between this arrangement and the arrangement described in the PSS have no impact on the system reliability analysis.) In the event that both offsite power sources are lost, each AC power division is loaded onto one of two emergency diesel generators. The support systems required for operation of the emergency AC power system are shown in the system support diagram in Figure 5.2. (This diagram, as in all of the system support diagrams, models the fault logic. The diagram shows support system failure combinations required to fail the top event system.)

Fault trees were constructed for the failure of one of the two emergency AC buses and for the failure of both emergency AC buses. Fault trees were also constructed for the loss of power (either with or without offsite power) at particular 480V buses and Motor Control Centers (MCCs). Common cause failure of the diesel generators is included in the fault tree for the loss of both AC trains.

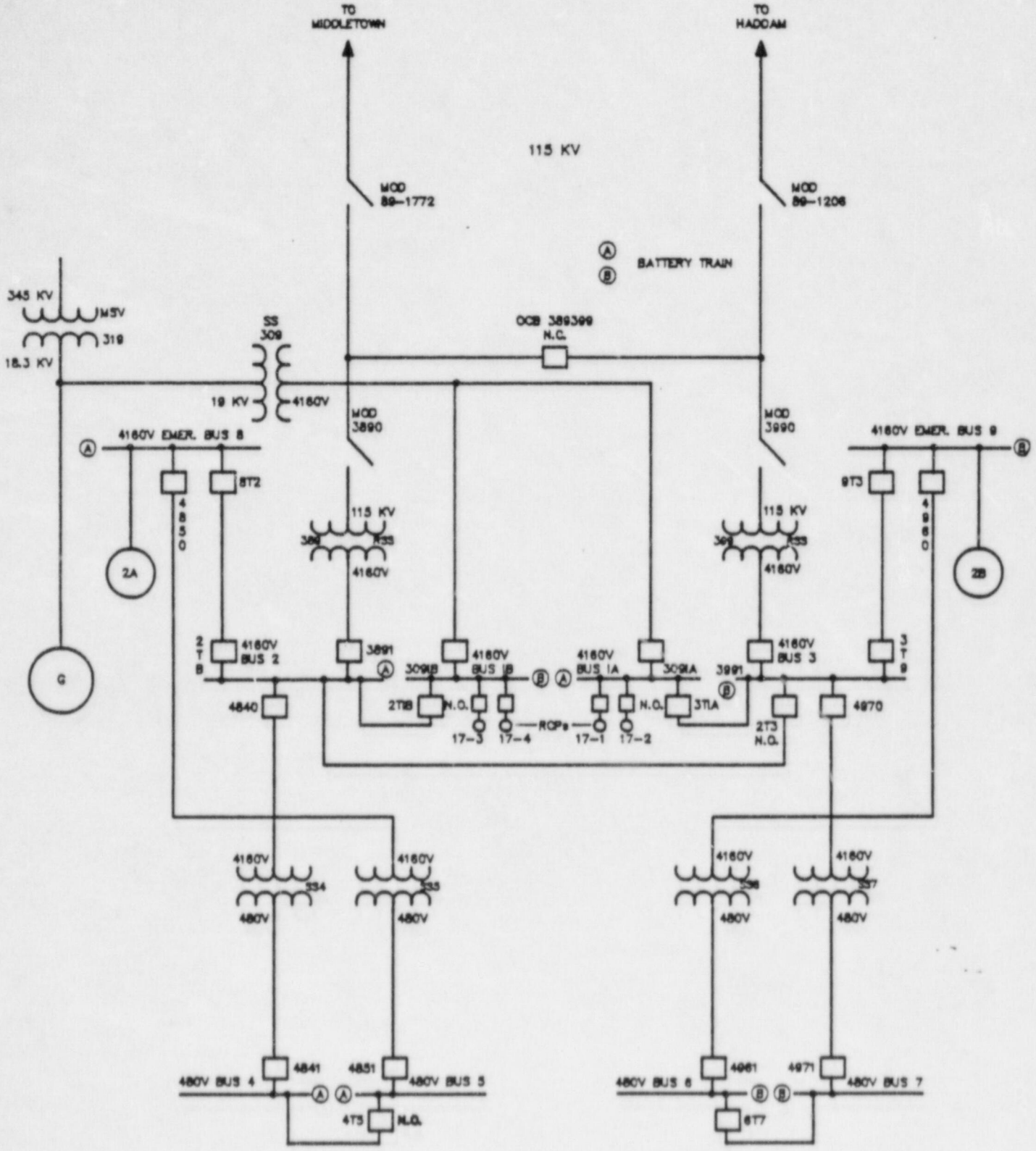


FIGURE 5.1. Simplified Schematic of the CY Electrical Distribution System.

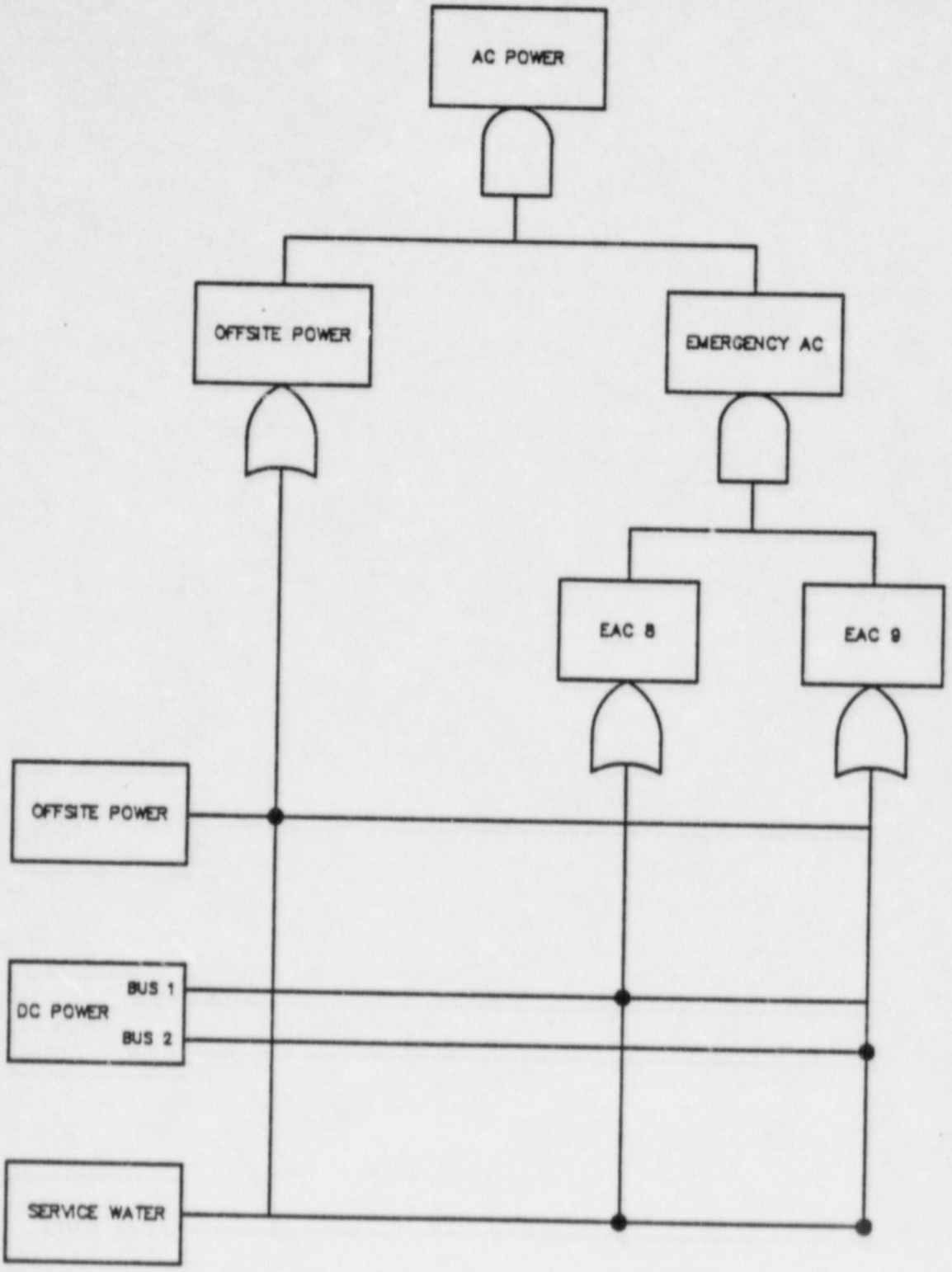


FIGURE 5.2. AC Power Dependency Diagram.

5.1.1 Comments

The load shed logic for disconnecting the plant electrical system from the offsite sources and the emergency 480V buses from those that are load-shedded is not explicitly modeled in the version of the fault trees provided in the PSS. The breakers that must open would not be tested except during refueling outages and could affect the probability of failure of one or both AC power trains. Also, the need for room ventilation is not discussed in the PSS. Based on comments received from Northeast Utilities, these two items were considered during the AC power system analysis (17). A failure of the load shed logic requires multiple failures which should not significantly contribute to the system unavailability. The ventilation system for the diesel generators was analyzed and has a much lower failure probability than the diesel generator itself.

Only one train of AC power has been modeled completely; the second is assumed to be identical to the one modeled. It is therefore not possible to determine if any common cause failures exist in the control logic. Such failures would greatly impact the probability of a loss of both AC power trains following a loss of offsite power. A single component failure would be of the same order of magnitude as the random failure of both diesel generators or the common cause failure of both diesel generators. It is beyond the scope of this review to determine if such common cause logic failures do exist at Haddam Neck.

5.1.2 Other Observations

When Bayesian updating of generic data based on plant-specific observations is used for diesel generators, it is not appropriate to combine the diesel generator faults and the control logic faults into a single failure mode as was done in the PSS. Generic diesel generator failure data does not include the control logic faults. However, logic components tested monthly should not significantly affect the availability of the emergency AC power system. For example, if there is one single relay, tested monthly, whose failure will result in the failure of one emergency AC power train, then the system unavailability will increase by less than 1% due to the relay failure.

5.1.3 Requantification

The requantification of the AC power system is performed to assess the impact of system modeling changes and component data modifications as recommended in Section 6.0. The impact of suggested system model changes on the emergency AC power system unavailabillity is negligible. Data changes did reduce the calculated unavailability of both AC power trains by approximately 1E-3, from 3.9E-3 to 2.9E-3. Most of this reduction was due to the reduction of common cause failures of both diesel generators to start and run.

The effect of data modifications on the unavailability of individual 480V buses and MCCs is not discussed in this section. Since these portions of the AC power system are input into other system models, the impact of the data changes will be discussed in the analysis of each system model.

5.2 MCC-5 and Semi-Vital AC Power

Both MCC-5 and semi-vital AC power are subsets of the AC power system. Due to the importance of the consequences of losing either bus, as a failure following an initiating event or as initiators, these portions of the AC power system are discussed separately from the remainder of the AC power system.

The success criterion for both of these buses is to provide power to their respective loads. The semi-vital AC power supply is fed directly from MCC-5 through two stepdown transformers as shown in Figure 5.3. These normal and emergency power supplies are interlocked through an automatic bus transfer. MCC-5 has two possible sources of power; bus 8 (via bus 1-5) is the normal supply, and bus 9 (via bus 1-6) is the alternate source of power. An automatic transfer from bus 1-5 to bus 1-6 occurs when power to bus 1-5 is lost. The system dependencies for these two portions of the AC power system are shown in Figure 5.4. In addition to the initiator fault trees, fault trees were developed for the loss of MCC-5 for the following support state combinations: (1) all AC and DC power available, (2) one or both DC buses unavailable, (3) a loss of offsite power and all AC and DC available,

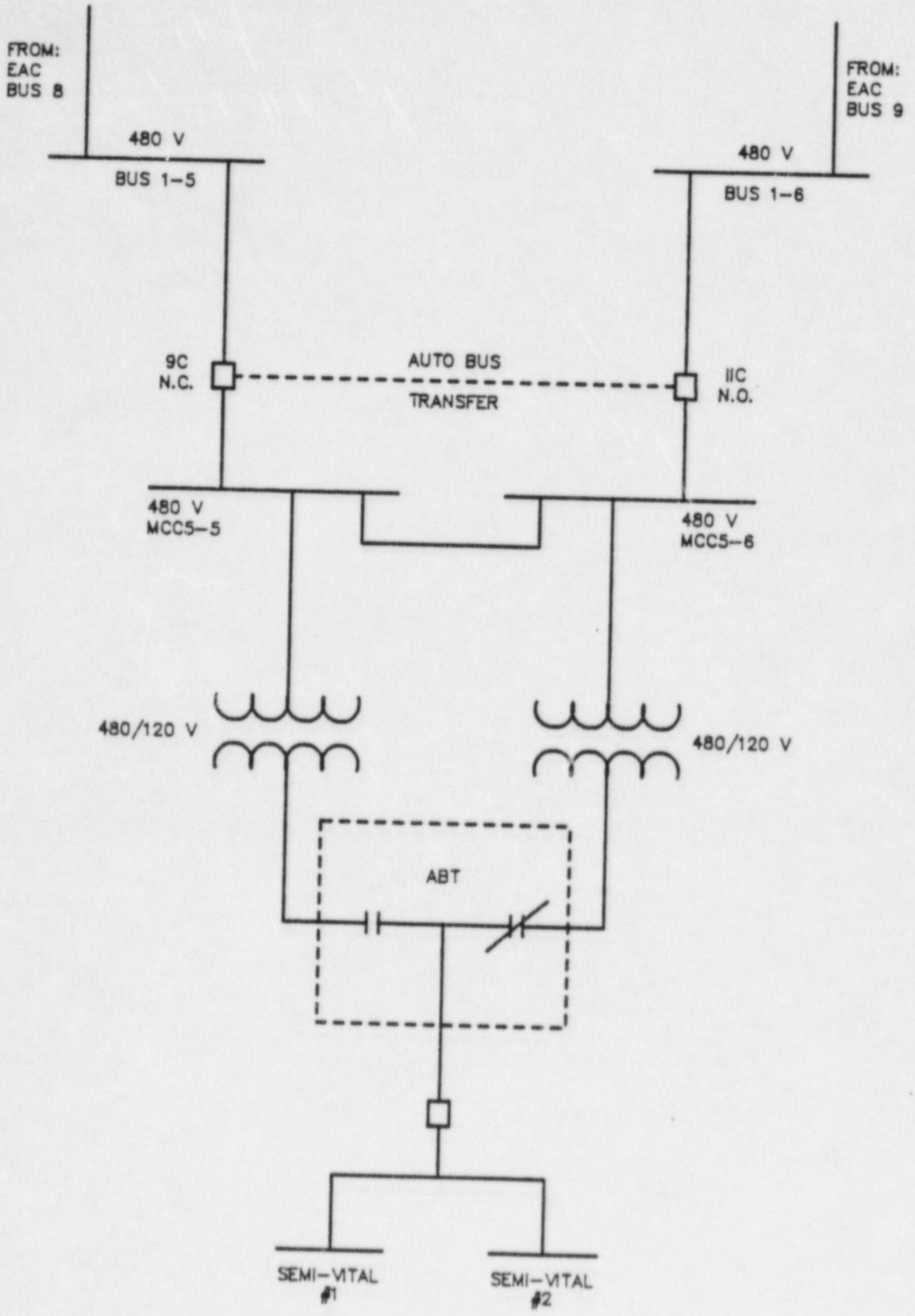


FIGURE 5.3. MCC-5 and Semi-Vital AC System Diagram.

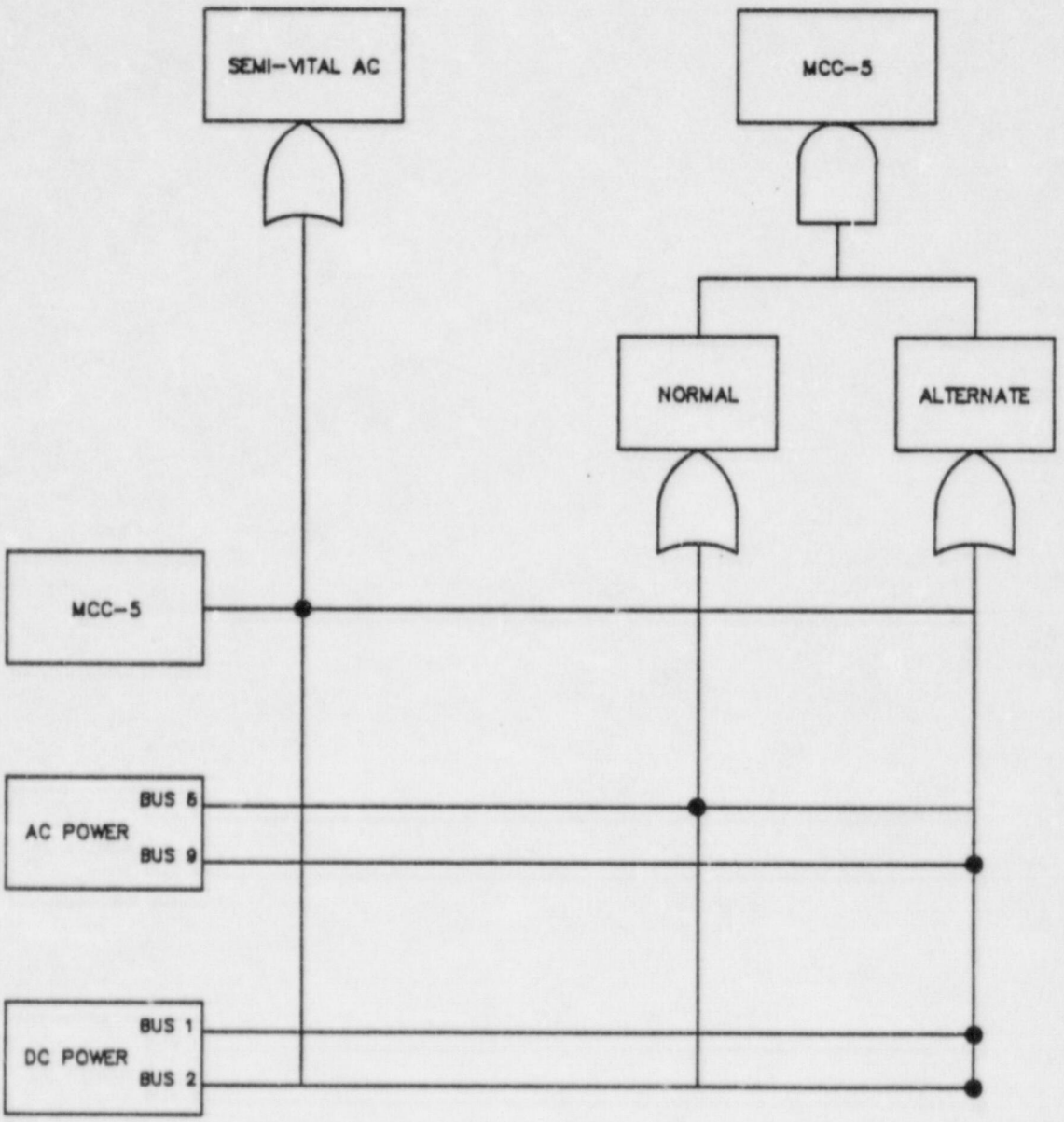


FIGURE 5.4. Semi-Vital AC and MCC-5 Dependency Diagram.

(4) a loss of offsite power and emergency AC bus 8 (EAC 8) unavailable, and
(5) a loss of offsite power and emergency AC bus 9 (EAC 9) unavailable.

5.2.1 Comments

In general, the PSS modeling of these two systems is correct. We have no significant comments on the system analysis.

5.2.2 Other Observations

The fault tree model did not include maintenance failures on the alternate power supply to MCC-5. This power source is not normally energized, and failure to restore after maintenance is a possible failure mode. The probability of this type of failure would be the product of component failures, principally a breaker fault discovered during one of the tests performed during shutdown, and the probability of a failure to restore the equipment after maintenance. Since the component failures are already considered as part of the fault tree, the additional human errors would result in the maintenance related faults being orders of magnitude less than the equipment failures themselves. Therefore, the contribution of such errors are not significant.

5.2.3 Requantification

The major effect of the data modifications recommended in Section 6.0 of this report is to reduce the frequency of a loss of MCC-5 initiator from 1.4E-2/yr to approximately 2.0E-3/yr. The changes to MCC-5 unavailability are shown in Table 5.2. This reduction is due almost entirely to the reduction (by a factor of nearly 20) in the breaker failure to remain closed probability. Failure of the feed breaker on the preferred source of power was the dominant contributor to the loss of MCC-5 initiator frequency. This failure is still a significant contributor to the loss of MCC-5 initiator but it is now of the same order of magnitude as several other failures, including bus faults and combinations of failures that include failure of the automatic bus transfer.

Table 5.2 MCC-5 Modified System Unavailabilities

Failed Support Systems	System Unavailability PSS	Suggested
As an initiator	1.4E-2/yr	2.0E-3/yr
None	4.3E-5	6.7E-6
DC 1 or DC 2 or both DC	1.8E-4	4.4E-5
Offsite power and EAC 8	1.2E-2	1.7E-2
Offsite power	9.7E-3	1.2E-2

For the most part, the data changes did not significantly affect the system failure probabilities for the loss of offsite power cases. When these three fault trees were reevaluated using the recommended data, only the system failure probability for the case of a loss of offsite power and EAC 9 increased by as much as 40%, due primarily to increased relay failure probabilities. The other two loss of offsite power cases were virtually unaffected.

The reduction in the breaker fails to remain closed probability reduced the MCC-5 system failure probability for the remaining two fault tree models. The reduction in the system unavailability for the all support systems available model and the loss of DC (one or both buses) model did not have a significant effect on the PSS results. Both impact support state split fractions that are relatively small already and contribute little to the total core melt frequency.

5.3 DC Power System

The DC power system is a two-train system. Each train consists of a battery charger, a battery, and a distribution switchboard. During normal operation the system is powered from the AC power system via the battery chargers. On a loss of AC power the batteries become the source of DC power. Successful operation of the system has been defined as supplying power to the DC buses, from either power supply, for a minimum of 9 hours. Fault trees were developed for five situations: loss of either DC bus following an initiating event, loss of either bus as an initiator, or loss of both buses as an initiator. No fault tree was developed for the loss of both buses following an initiating event since it was judged that the two trains of power were sufficiently independent that the probability of a failure of both trains is the product of the failure probability of each. The system dependencies are shown in Figure 5.5.

5.3.1 Comments

In general, the PSS modeling of the DC power system is correct. There are some areas of the analysis, however, that are subject to a large degree of uncertainty.

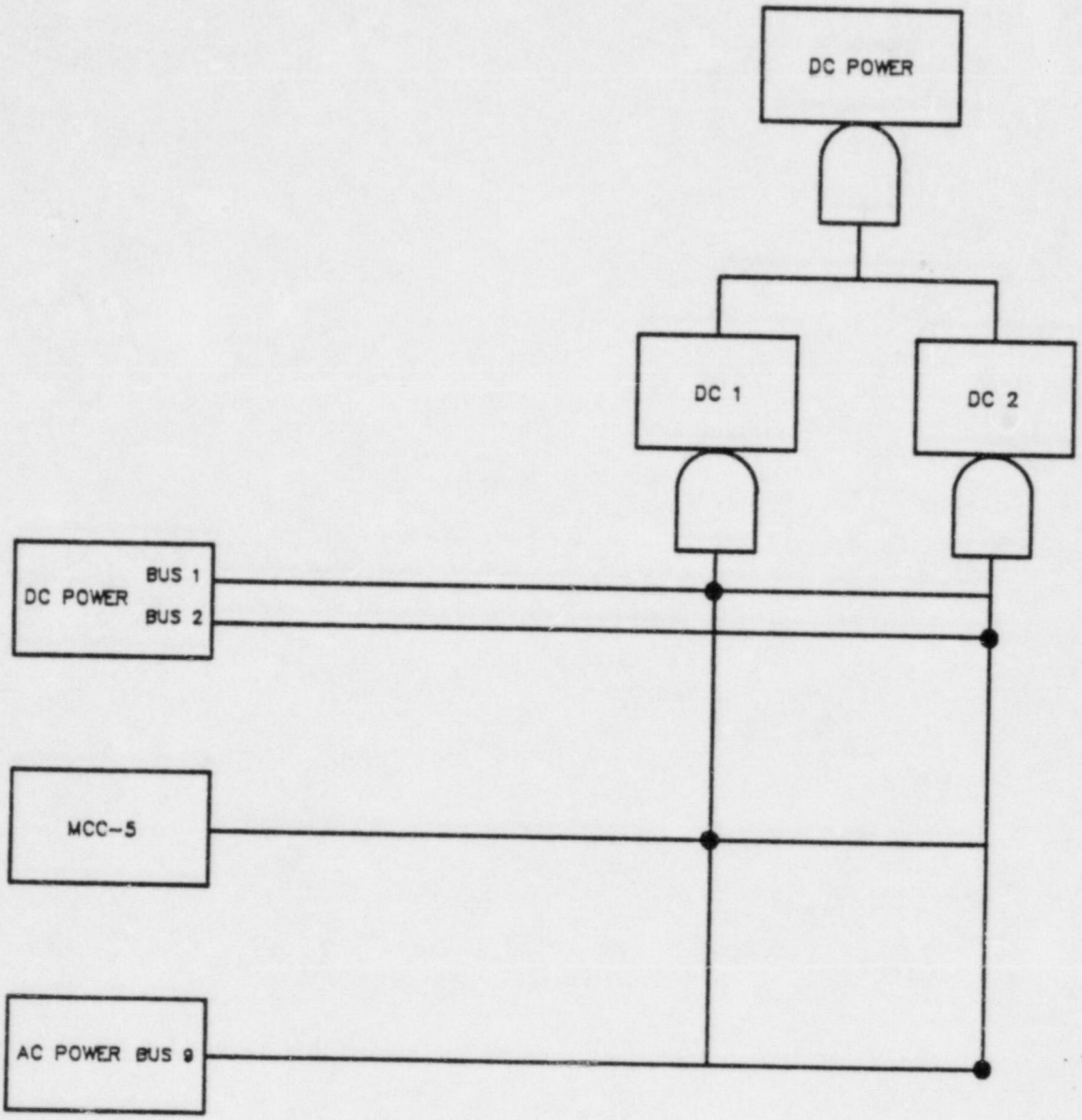


FIGURE 5.5. DC Power System Dependency Diagram.

Common cause faults for the batteries are not considered in the PSS. The utility claims their maintenance practices would eliminate all possible common cause faults. Data on common cause battery faults is limited, but there are indications that not all battery common cause faults are maintenance related, i.e., due to human faults. The claim that common cause faults can be completely eliminated through good maintenance practices appears to be overly optimistic.

An accurate determination of the common cause battery failure probability would be difficult to assess, and the uncertainties associated with that probability would be very large. Use of a particular value, especially if inappropriately chosen, could unfairly bias the results of the PSS. (Due to the large number of equipment failures resulting from a loss of DC power, any uncertainty associated with total DC power failures would propagate nearly unchanged to the core melt probability.) This effect in conjunction with the effect of good test and maintenance procedures leads us to recommend that for the moment no change be made to the treatment of battery common cause failures in the PSS. However, the topic should not be forgotten, and as part of the maintenance of the PSS, it should be revisited on a periodic basis to assess the effect of any advances in the assessment of battery common cause faults.

In evaluating battery faults it is assumed that 14% of all battery faults would result in a loss of a DC bus as an initiating event. These are the faults deemed severe enough to cause battery charger instabilities and trips. Northeast Utilities admits this is a highly uncertain number and variations would affect the frequency of a loss of DC power.

5.3.2 Other Observations

As with the diesel generator output breakers, the battery charger breakers have been assumed to be part of the battery chargers. However, due to the configuration and function of these breakers, their failure probability would not be a significant contributor to DC power unavailability.

5.3.3 Requantification

There were no system model or data changes that would affect the calculated system unavailabilities of 4.6E-4 for the failure of a single DC bus and 2.1E-7 for the failure of both DC buses.

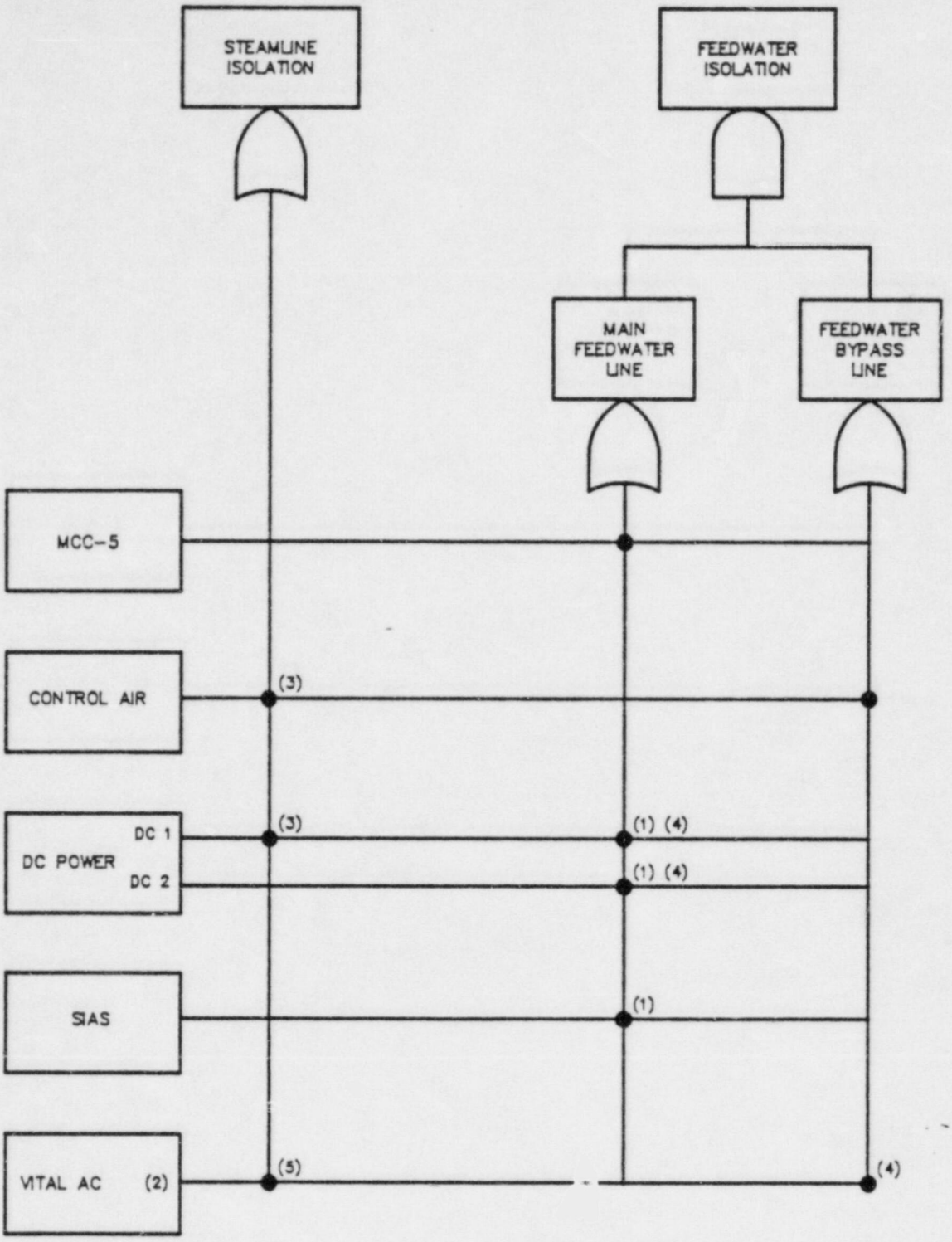
5.4 Steamline/Feedline Isolation

Steamline or feedline isolation is required for three types of events: a steamline break, a feedline break, or a steam generator tube rupture. If the feedline break is downstream of the common feedwater header, isolation of that one feedline only is necessary. But, if the break is between the feed pumps and the common header, isolation of all four feedlines would be necessary. Steam generator tube ruptures require isolation of both the steam and the feed lines to the affected steam generator. Steamline breaks require isolation of all four steamlines for breaks downstream of the non-return valve, or isolation of the steam and feedlines to the affected steam generator for breaks upstream of the non-return valve.

Depending upon the type of break, the isolation may be either automatically or manually initiated. Feedwater isolation is automatic on a steam generator tube rupture, but steamline isolation is completely manual. Feedwater breaks must be manually isolated. Steamline breaks should generate an automatic isolation signal, although the feedwater isolation in response to a steamline break, if required, is manual.

The components used to isolate the breaks include feedwater bypass valves, main feedwater isolation valves, the steamline non-return valves (NRV), and the main steam trip valves (MSTV). Depending on the location of the break, local manual isolation actions may be possible. A steam generator tube rupture, for example, could be manually isolated locally.

System dependencies for the steamline/feedline isolation are shown in Figure 5.6. (The components used to isolate any break are part of the power conversion system which is shown in Figure 5.21.)



(1) Required only for automatic actuation which occurs only for an SGTR.
(2) Vital AC – 4 panels: 1 and 2 are powered from DC 1, 3 and 4 from DC 2.
(3) Loss of support system results in MSTV closure and isolation.
(4) Train of DC power required depends on which SG loop is affected.
(5) Required for automatic isolation only.

FIGURE 5.6. Steamline/Feedline Isolation System Dependencies Diagram.

5.4.1 Comments

For the case of a steamline break downstream of the non-return valve and a loss of DC bus 1, the PSS lists the dominant cut sets as combinations of valve failures and actuation logic failures. Combinations of solenoid valve failures and failure of the feedwater bypass valve (due to the DC power failure) are not listed. These faults produce a system failure probability about 10% greater than the failure probability listed in the PSS (9.9E-2 versus 9.1E-2).

5.4.2 Other Observations

In the PSS it is assumed that a loss of service water results in a loss of isolation capability due to failures resulting from the loss of control air. However, control air is not lost automatically on the loss of service water. This conservative assumption affects the importance of this system only in those support states where service water is unavailable. The resulting overall sequence frequency (initiator, loss of service water, system failure) is very small.

For a steamline break upstream of the NRV, one steam flow sensor may not see a high-steam flow condition, depending on sensor location and type and the break location. In the event of a loss of DC bus 2, this means that a high-steam flow signal may not be generated even if there are no further component failures. This occurs if the break affects the output of a sensor that, through the vital AC bus, is powered from DC bus 1. As in the previous comment, the combined impact of initiator frequency, support state split fraction, and system unavailability is very small, so this is not a significant omission.

5.4.3 Requantification

The requantification of the steamline/feedline isolation system is based on the comments in this section and the results of the component data review of Section 6.0. The results of the requantification are summarized in Table 5.3. In all five fault tree models the data modifications resulted in increased system unavailabilities in the support states where all support systems are available. For the main steamline break and SGTR isolation

Table 5.3 Steamline/Feedline Isolation System: Modified System Unavailabilities

Break Type and Location	Failed Support Systems	Unavailability PSS	Unavailability Suggested
Main Feedwater Break			
Feedstation to Containment	None(1)	3.3E-2	5.5E-2
Feedpumps to Feedstation	None(1)	1.1E-2	2.0E-1
Steam Generator Tube Rupture	None(1)	9.3E-5	1.6E-4
Steamline Break			
Upstream of Non Return Valve	None(1)	3.0E-4	3.4E-4
Downstream of Non Return Valve	None(1)	1.6E-2	3.0E-2
	DC Bus 1	9.1E-2	1.3E-1
	DC Bus 2	1.8E-1	2.0E-1

Note (1) Also applies to the loss of offsite power support state

fault trees, the increased unavailability is due primarily to an increase in the main feedwater isolation valve failure probability. The steamline break isolation failure probabilities increase primarily due to an increase in the main steam trip valve failure to close probability. Only for the isolation of a steamline break downstream of the nonreturn valve do the system unavailabilities increase in any other support state. For this case, the system unavailability increased on the loss of one DC bus due to the additional fault combinations identified in Section 5.4.1 and the increase in relay failure to operate and MOV failure to close probabilities.

5.5 High Pressure Safety Injection (HPSI) System

The HPSI system consists of two redundant pump trains and four motor-operated isolation valves. The system is designed to auto-actuate upon receiving a safety injection actuation system (SIAS) signal, and to inject borated water from the Refueling Water Storage Tank (RWST) to the cold leg of each loop. Figure 5.7 illustrates a simplified diagram of the HPSI system.

Success criteria include one of two HPSI trains if three of three unfaulted injection loops are available or two of two HPSI trains if two of three unfaulted injection loops are available. (It is assumed that the HPSI system is required after a pipe break, and that the pipe break occurs in one of the four injection paths, leaving three unfaulted paths.) During an emergency, the HPSI system automatically starts upon receiving an actuation signal from the safety injection actuation system. The HPSI pumps require DC power to start, and 4160V AC to run. Also, MCC-5 provides motive power to open the MOVs on the injection loops. Figure 5.8 shows the support systems required for HPSI operation.

5.5.1 Comments

In general, the model developed for the HPSI system is adequate for system analysis purposes.

Maintenance faults were handled in an inconsistent manner in the HPSI system. The same probability was used to represent the maintenance unavailability due to pump A or pump B being in maintenance and for the

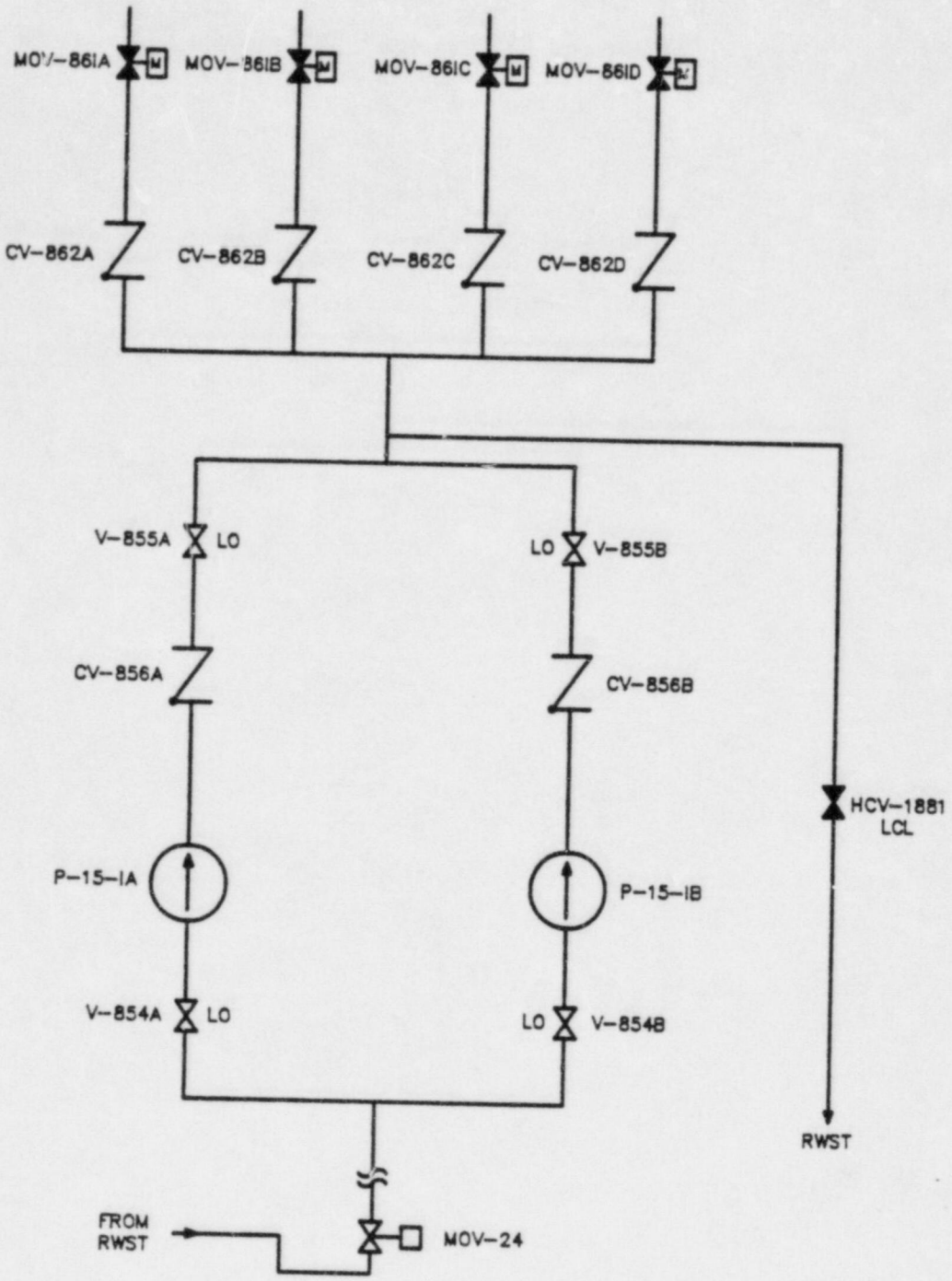
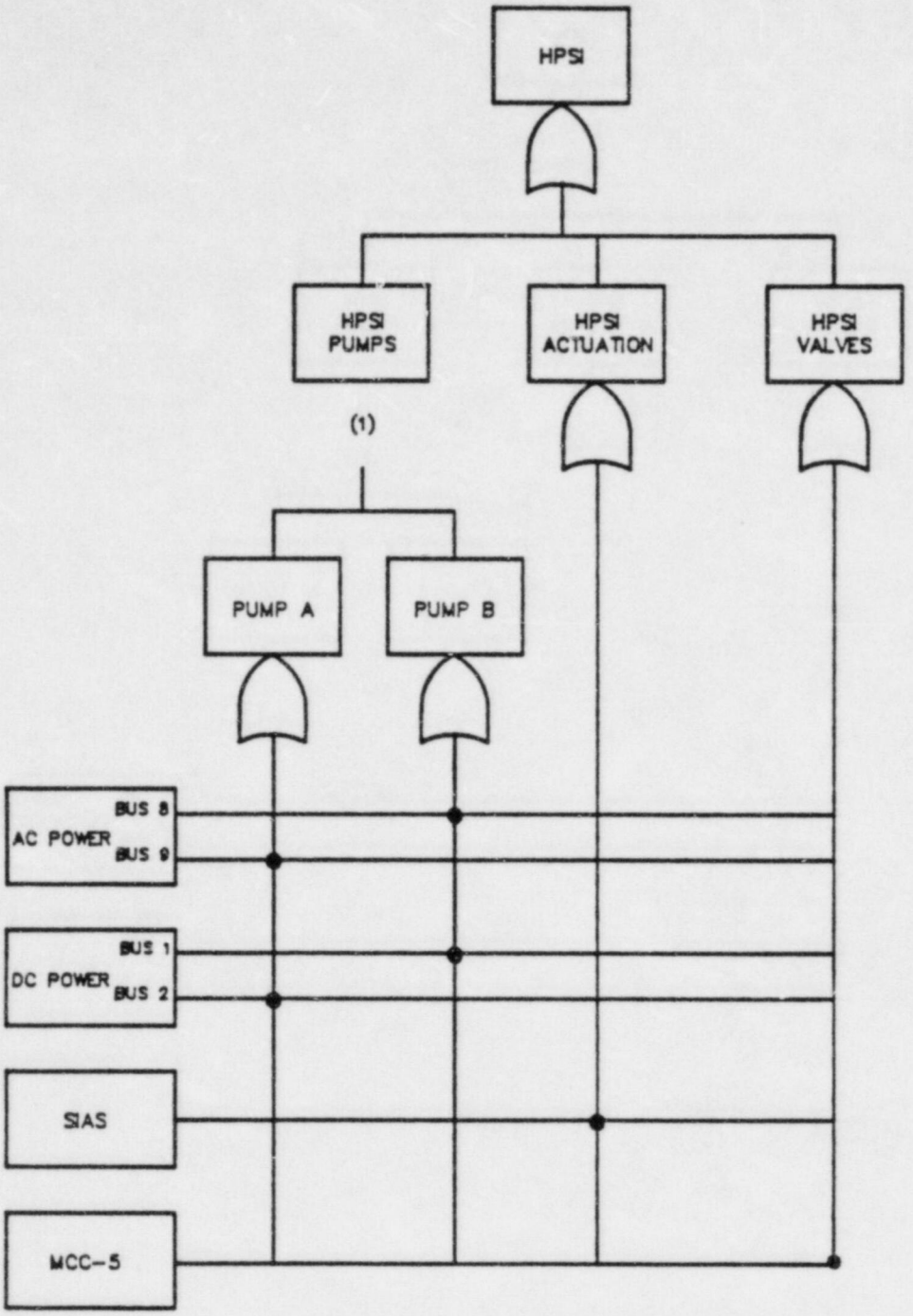


FIGURE 5.7. Simplified Flow Diagram for HPSI System.



(1) If 3 of 3 injection loops are available this is an "and" gate.
If 2 of 3 injection loops are available this is an "or" gate.

Note: PAB ventilation may be needed but this dependency is not modeled for short-term use of the HPSI system.

FIGURE 5.8. High-Pressure Safety-Injection System Dependency Diagram.

maintenance unavailability of pump A alone. Further clarification from the utility indicates that the maintenance data were applicable to individual pumps. Thus, the PSS treament understates the contribution of the maintenance unavailability of one pump train coupled with the random failure of the second pump train to the system failure, when both HPSI pumps are required to operate, by about 3.6E-4.

Common cause failure of the HPSI pumps to start was not considered in the PSS. Only common cause failures to run were considered. As described in Chapter 6.0, common cause failures to start for HPSI pumps are estimated at about 1.22E-4/demand. The above changes in component data and system analysis will be incorporated in the requantification of the system unavailability as described in Section 5.5.3.

5.5.2 Other Observations

The HPSI system takes suction from the RWST. However, this suction path was not considered in the analysis of the HPSI system. This suction path appears to be normally open (i.e., no closed valves) but failures on this flow path may or may not affect other systems. Further information obtained from the licensee indicates that the MOV located on the HPSI suction path is locked open, and indeed, the PSS analysis did consider this path as a pipe segment. Thus, this additional clarification has satisfactorily resolved our concern.

In the PSS it is stated that the Primary Auxiliary Building (PAB) ventilation may be required for HPSI, LPSI, and charging system operation but the failure probability of this ventilation system is so small that it would be a negligible contributor to the system failure probabilities. Based on our understanding of the PAB ventilation system operation and the layout of the equipment in the PAB, ventilation may not be required for the short-term operation of the HPSI, LPSI, and charging systems. Even if ventilation is required, not modeling the PAB ventilation system in the HPSI, LPSI, and charging systems does not appear to impact the quantification of these systems' failure probabilities.

5.5.3 Requantification

The HPSI system reliability data was requantified to reflect changes both in component failure data and modification to the fault tree models. For the case where both DC buses are available, it is estimated that the system unavailability increases from 4.1E-3 to about 1.0E-2. This increase consists of changes in MOV and HPSI pump failure probability, requantification of the maintenance contribution to the system failure, and addition of common cause failures to start HPSI pumps. For a loss of one DC bus scenario, the system failure probability increases from 9.1E-2 to about 1.6E-1 due to changes in MOV and the SIAS unavailability.

5.6 Low Pressure Safety Injection (LPSI) System

The LPSI system is designed to automatically inject borated water (from the RWST) into the reactor vessel head following a large break LOCA. It is designed for injection at reactor vessel pressures below 350 psig. The system consists of two redundant pump trains and two core deluge valves. The LPSI system is activated upon receiving an actuation signal from the SIAS. The LPSI pumps require DC power to start and AC power to operate. MCC-5 is also required to provide motive power to the MOVs (core deluge valves). Figures 5.9 and 5.10 show the simplified diagram and the system dependencies for the LPSI system, respectively. Successful system operation requires that one of two LPSI pumps start automatically and inject water into the reactor vessel through one of two core deluge valves.

5.6.1 Comments

In general, the model developed for the LPSI system is adequate for system analysis purpose. However, as described in the HPSI system review, the utility only provided data for common cause failures to run the pumps without data for LPSI pumps to start. As presented in Chapter 6.0, the common cause failures to start LPSI pumps are estimated at 1.22E-4/demand. This results in an increase in the system unavailability as indicated in Section 5.6.3.

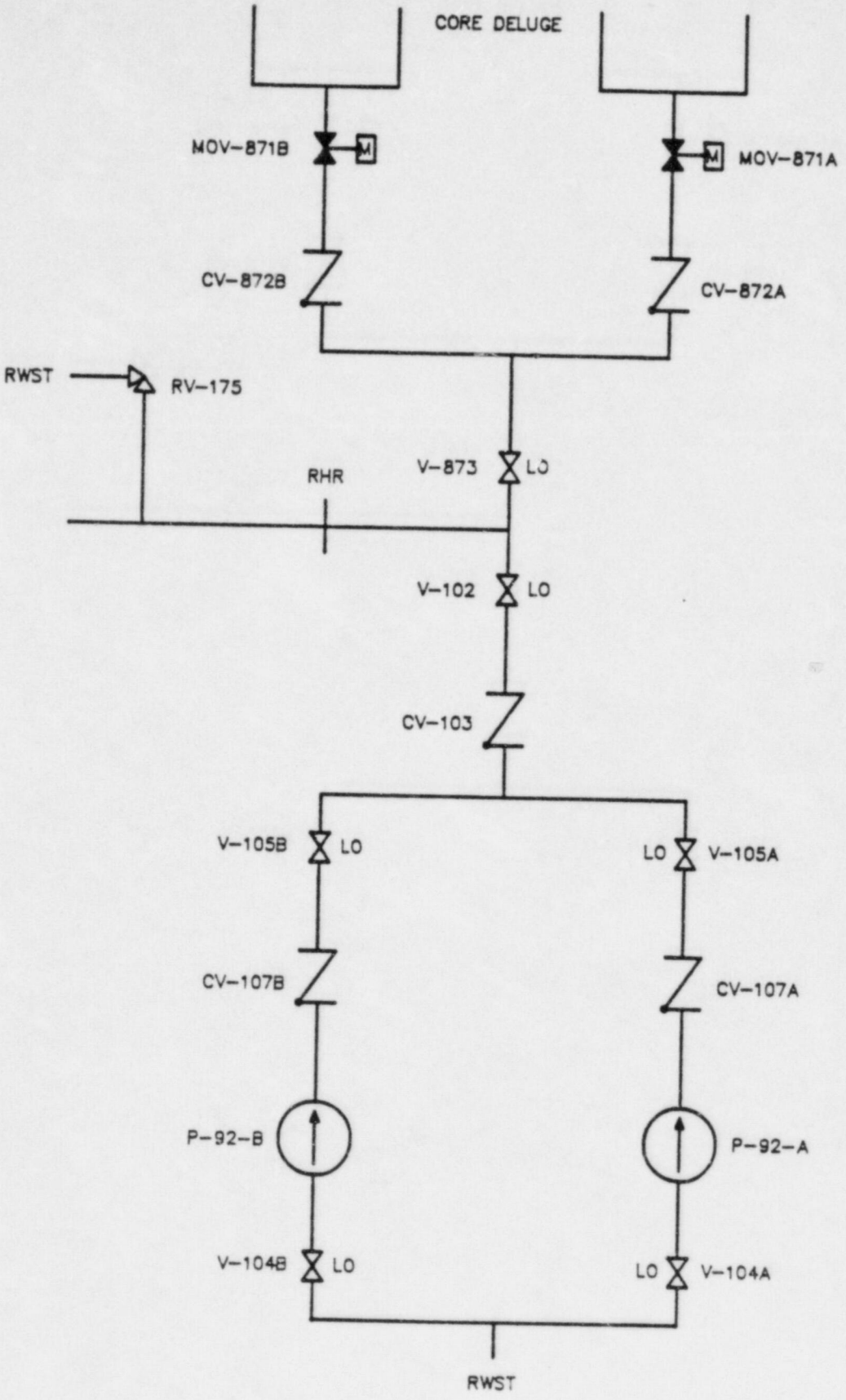
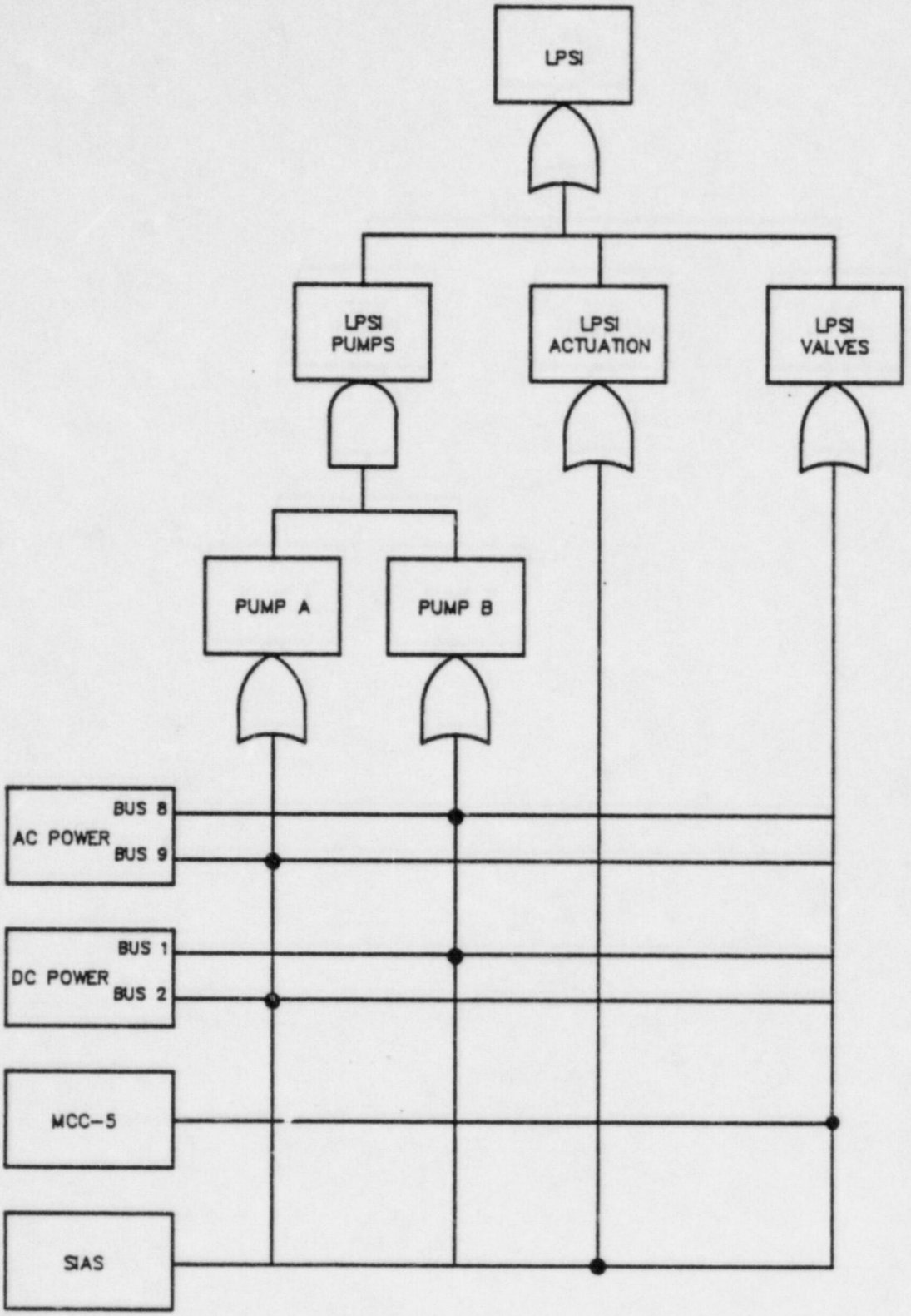


FIGURE 5.9. Simplified Flow Diagram for LPSI System.



Note: PAB ventilation may be required but this dependency is not modeled for the short-term use of the LPSI system.

FIGURE 5.10. Low-Pressure Safety-Injection System Dependency Diagram.

5.6.2 Other Observations

The fault trees are intended to be independent of each other. However, we found that failure of a single relief valve will cause failure of the LPSI system and also of the RHR system. (This valve is located on a pipe segment common to the suction lines of the LPSI and RHR systems.) A review of the event trees indicates this system dependency would not have any impact on the Haddam Neck dominant core melt sequences and therefore is not significant.

5.6.3 Requantification

The system unavailability was reevaluated to reflect the impact of changes in commponent data and in the system analysis. This requantification effort indicates that the LPSI system unavailability increases from 7.9E-3 to 9.4E-3 for the case where both buses are available, and from 2.9E-2 to 3.2E-2 for the case where one DC bus is available. The change in the first case is dominated by the MOV failure probability followed by the addition of common cause failures to start LPSI pumps. For the second case, the increase in system unavailability is mainly due to increase in the SIAS unavailability data.

5.7 Residual Heat Removal (RHR) System

The RHR system consists of two redundant pump trains and is designed to remove decay heat during plant shutdown, after a loss of coolant accident (LOCA), and to supply water from the containment sump to the containment spray valves.

During normal plant shutdown, the RHR system draws coolant from hot leg of Loop 1, and injects back into cold leg of Loop 2 after rejecting heat through the RHR heat exchangers. This system is designed to operate at reactor pressure of less than 400 psi. During a large LOCA, the RHR system provides the capability for low pressure recirculation by withdrawing coolant from the sump, rejecting heat through the heat exchangers, and delivering to the core deluge valves in the Low Pressure Safety Injection (LPSI) system. During a medium or small LOCA, high pressure recirculation uses the RHR system to circulate coolant from the containment sump to the

charging system through the heat exchangers. The RHR system also is designed to provide long term cooling following the use of bleed-and-feed and following an unidentified steam generator tube rupture accident. For the use of the RHR system as a means to remove containment heat, refer to the discussion presented in Section 5.15 of this report. A simplified diagram of the RHR system is shown in Figure 5.11.

Each RHR pump requires DC power to start and 480V AC power to run. The RHR system is dependent on service water to provide heat removal operation (indirectly through the component cooling water (CCW) system except during LOCA conditions, where the RHR heat exchangers are cooled directly by the service water system). It also depends on the Semi-Vital AC to provide the power to operate the pressure interlock between the RHR system and the reactor pressure. MCC-5 controls the operation of the MOVs contained in the RHR system, while PAB ventilation will provide cooling to the RHR pumps. System dependencies are shown in Figure 5.12.

5.7.1 Comments

In the analysis of the cold shutdown mode for the RHR system, the PSS does not give credit to the "core deluge valves" as an alternate path for the RHR system injection. This means of injecting water into the core is used in other low pressure applications of the RHR system. This apparent omission results in a significantly higher RHR system unavailability in the cold shutdown mode. The dominant faults in the fault tree for this RHR mode of operation are listed as a failure of the suction or discharge valves. Crediting an additional injection path would effectively eliminate half of the system cut sets. However, this cold shut-down mode of the RHR system apparently did not affect any core-melt sequences, and therefore would not impact core melt frequency.

5.7.2 Other Observations

There is no discussion of the possibility of one RHR heat exchanger being out of service due to maintenance at the same time the other heat exchanger fails to work due to mechanical or valve alignment failure. However, the impact on core melt frequency is expected to be negligible.

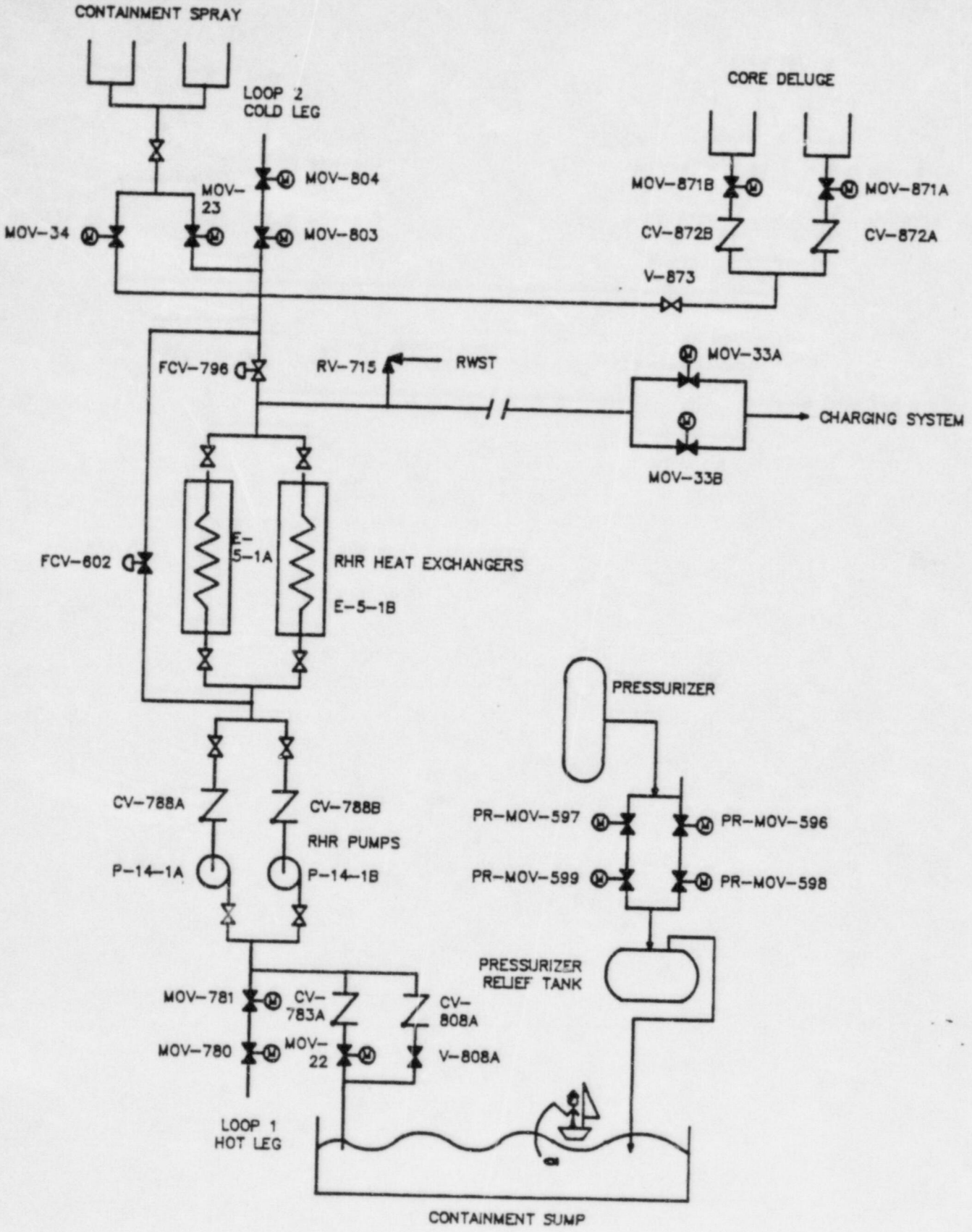
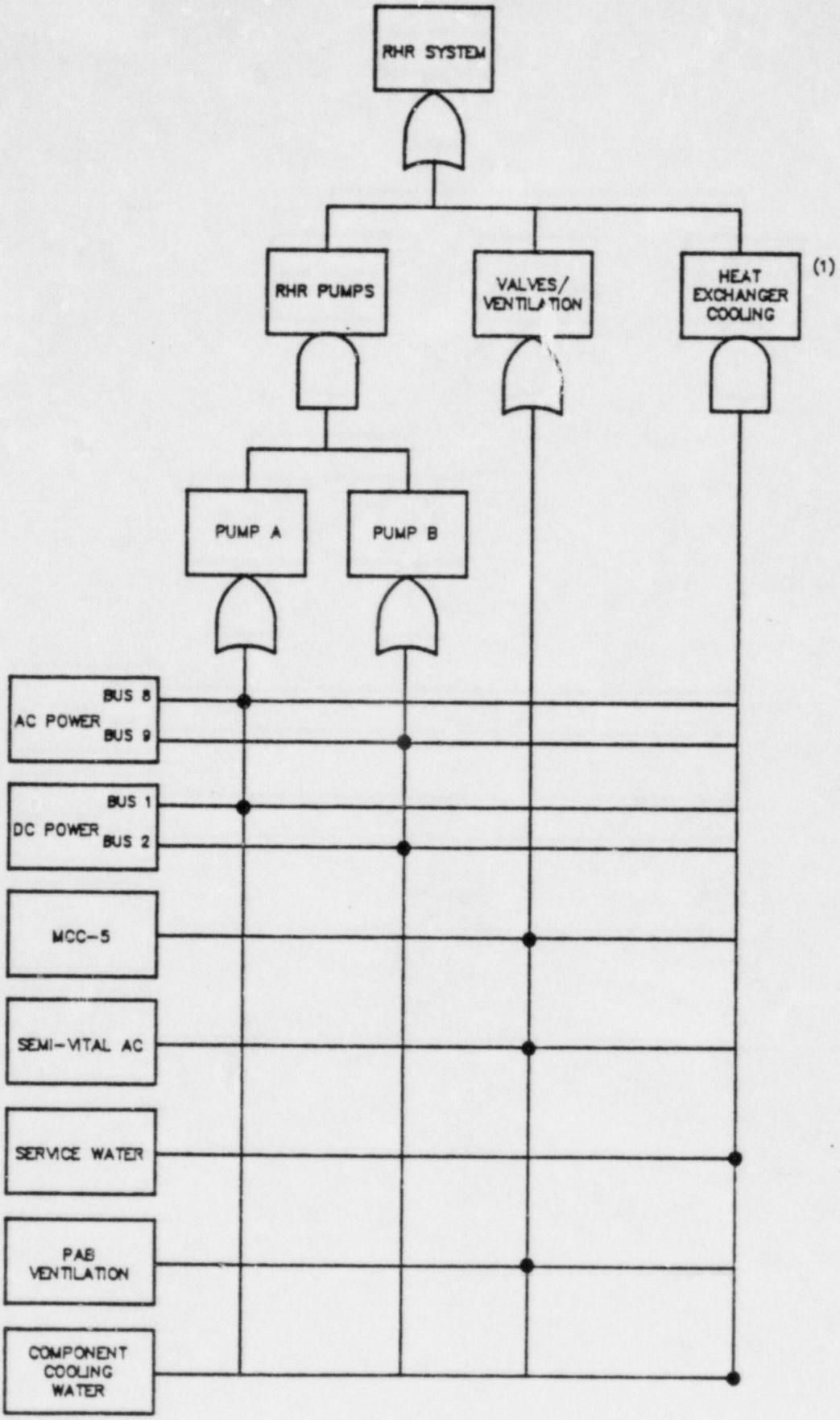


FIGURE 5.11. Simplified Flow Diagram for RHR System.



(1) Heat Exchanger Cooling is provided by Component Cooling Water System under normal conditions; Service Water in post-LOCA conditions.

FIGURE 5.12. RHR System Dependency Diagram.

5.7.3 Quantification

Due to the modifications to the component reliability data as suggested in Chapter 6.0 of this report, the RHR system unavailability was requantified and the results are presented in Table 5.4.

The increases in the high and low pressure recirculation modes are primarily due to an increase in the MOV failure probability. In the long-term cooling modes, the increases in system unavailabilities are primarily due to the increase in air-operated valve failure probability. Additionally, for the loss of offsite power and one DC bus support state, the failure of an RHR pump train is a significant contributor to the system unavailability and this failure probability increases due to component data changes.

5.8 Charging System

The charging system consists of two redundant pump trains (A and B) which are rated at 360 gpm at a design pressure of about 2800 psig, and a positive-displacement metering pump which is capable of delivering about 30 gpm for the Reactor Coolant Pump (RCP) seal cooling after a transient.

During normal operation, the charging system is designed to provide vessel make-up and RCP seal cooling. Normal charging flow path is from the Volume Control Tank (VCT) through the charging pump, to the RCP seal and the reactor vessel, and back to the VCT. After a small or medium loss of coolant accident (LOCA), the charging system is required to provide high pressure injection and high pressure recirculation. During the injection mode, the charging path is automatically transferred from the VCT to the Refueling Water Storage Tank (RWST). For the recirculation mode, it is used in conjunction with the Residual Heat Removal (RHR) system to remove decay heat, taking suction from the containment sump. In addition, this system configuration is also used to provide the two-path recirculation (TPR) capability after a large LOCA, with the exception that the charging pumps are not required to run. In this TPR mode, the charging injection flow path is required for the RHR to inject about 50 gpm to the reactor to prevent boron precipitation. Figure 5.13 shows a simplified diagram of the charging system.

Table 5.4 RHR System Modified System Unavailabilities

System Operational Mode	Failed Support Systems	Unavailabilities	
		PSS	Suggested
Low pressure recirculation	None or offsite power	1.5E-3	3.1E-3
	One DC Bus	4.0E-3	5.3E-3
	Offsite power and one DC Bus	5.1E-3	6.4E-3
High pressure recirculation	None or offsite power	4.9E-3	6.3E-3
	One DC Bus	7.4E-3	8.7E-3
	Offsite power and one DC Bus	8.5E-3	9.9E-3
Long-term cooling after bleed-and-feed	None	1.3E-3	5.8E-3
	Offsite power and one DC Bus	4.9E-4	9.7E-3
Long-term cooling after SGTR	None	9.1E-4	5.4E-3
	Offsite power and one DC Bus	4.7E-3	9.5E-3

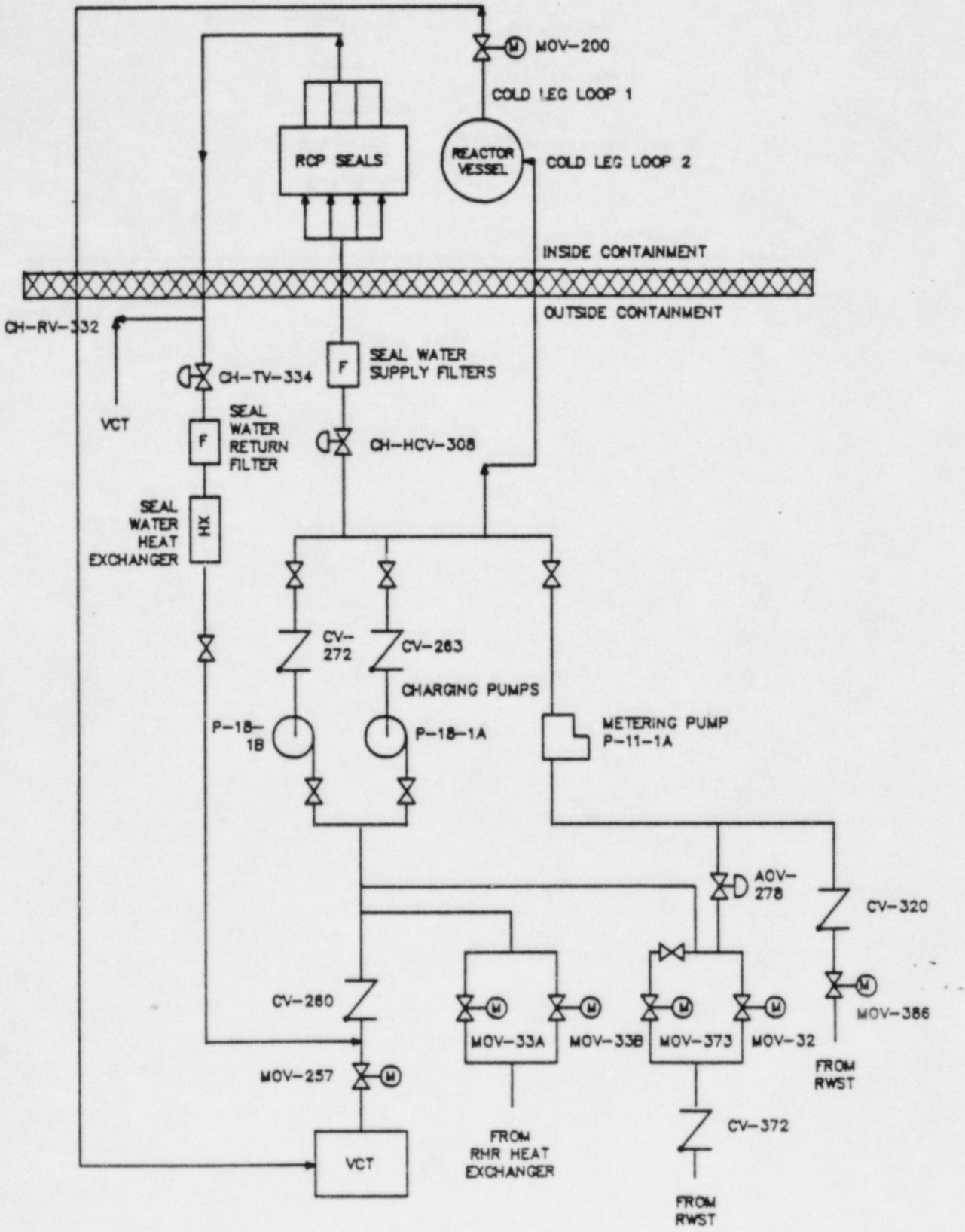


FIGURE 5.13. Simplified Flow Diagram for Charging System.

In the RCP seal cooling mode, the charging system requires Component Cooling Water System (CCWS), semi-vital AC, and Control Air to maintain a normal flow path to and from the charging system and heat removal. MCC-5 provides motive power to MOVs which can be opened as an alternate path when the normal flow path is not available. The success criterion for the charging system in this mode of operation is one of three pumps. DC Bus 1 and AC Bus 2 (via 480V-AC Bus 4) provide power for the startup and operation, respectively, of the metering pump. For charging pumps A and B, DC buses are required for starting and AC buses for running the pumps. In addition, lube oil is also required to provide cooling to the charging pumps. Lube oil pumps require component cooling water (CCW) for heat removal, and either MCC-5, which provides motive power to the main lube oil pump, or AC Bus 9 (via MCC-8) for the auxiliary lube oil pump.

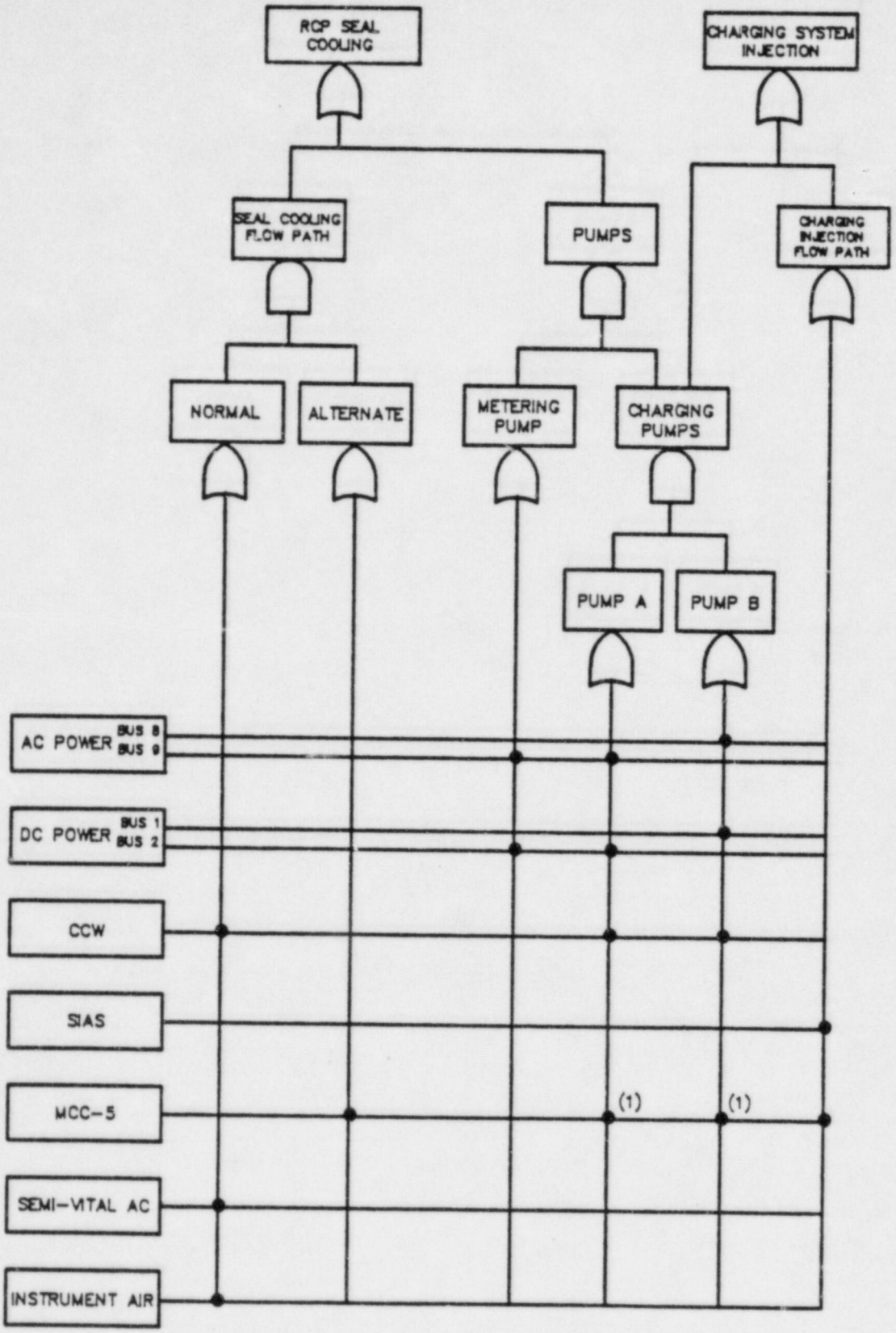
In the injection and recirculation mode, the success criterion for the charging system is one of two charging pumps providing injection flow. The charging system is activated when it receives an actuation signal from the safety injection actuation system (SIAS). MCC-5 is required to provide motive power to the MOVs on the injection flow path. For the charging pumps, all dependencies are the same as described previously and shown in Figure 5.14.

5.8.1 Comments

A review of the charging system fault tree for "vessel make-up after a loss of MCC-5, Control Air or Semi-vital AC" indicates that the PSS has omitted the system unavailability contribution due to failure of a check valve on the charging system suction line from the RWST. In this case, the valve failure probability should increase the system unavailability from 5.3E-3 to 7.3E-3. It is recommended that this fault be included in the above fault tree. Additional modifications to the system unavailability are discussed in Section 5.8.3.

5.8.2 Other Observations

It is noted that the system unavailability calculated for the loss of both DC buses support state, presented in Table 4.2.10-1, page 4.2-145 of the PSS, is incorrectly documented. A verification of the fault tree



(1) MCC-5 and AC power train powered from Bus 8 or 9 supply power to the charging pump lube oil pumps. The loss of MCC-5 alone will not fail the lube oil pumps.

FIGURE 5.14. Charging System Dependency Diagram.

indicates that this value should be 1.6E-2 instead of 3.6E-2. Reviews of the system and support state quantification indicate that the impact of this discrepancy on the total core melt frequency is negligible.

5.8.3 Requantification

The charging system was requantified to determine the impact on the system unavailability due to the modifications to component reliability data suggested in Chapter 6.0, and those affecting system modeling as discussed in Section 5.8.1. The information presented in Table 5.5 represents recalculated system failure probabilities of the charging system for the different modes of operation.

For all modes of charging system operation except for the vessel makeup after the loss of MCC-5, control air, or semi-vital AC, the changes in the system unavailabilities are due primarily to increased MOV failure rates. The fact that these three modes of operation differ primarily only in valve lineup differences, that is, different injection and discharge points, is the main reason the same type of failures are responsible for the increase in system unavailabilities for each mode. The remaining mode of operation involves more manual operation of components and is intended for use under special conditions, following plant-specific initiators. For the vessel makeup after a loss of MCC-5, control air, or semi-vital AC, several factors contributed to the increase in system unavailability. These include the addition to the model of a check valve failure as described in the comments section above, an increase in the charging pump failure probability, a reduction in the CCW system unavailability, and the common cause failure rate for MOVs.

5.9 Component Cooling Water System

The Component Cooling Water (CCW) system is an intermediate closed loop cooling water system designed to transfer heat from certain components to the Service Water (SW) system. CCW is comprised of three pumps (in parallel), two heat exchangers (in parallel), a surge tank and associated valves, piping, and instrumentation. The major cooling loads include the Residual Heat Removal (RHR) heat exchangers and the Reactor Coolant Pump (RCP) thermal barriers. Two fault tree models were constructed for the CCW

Table 5.5 Charging System Modified System Unavailabilities

System Operational Mode	Failed Support Systems	Unavailabilities	
		PSS	Suggested
RCP Seal Cooling	DC 1	1.1E-2	1.7E-2
	Service Water	3.4E-2	5.6E-2
	Both DC	1.5E-2	2.0E-2
	Offsite Power and DC 1	1.1E-2	1.7E-2
	DC 2	4.5E-5	4.2E-5
	None	2.3E-5	2.2E-5
High pressure injection	One DC bus	2.4E-2	3.9E-2
	Offsite power	2.9E-2	4.3E-2
	Offsite power and one DC bus	7.1E-2	8.0E-2
	None	2.3E-2	3.8E-2
Two path recirculation		2.2E-3	3.5E-3
Vessel Makeup after a loss of MCC-5, Control Air, or Semi-Vital AC	None	5.3E-3	6.7E-3
	Offsite power	6.5E-3	7.4E-3
	Offsite power and MCC-5	5.0E-3	6.4E-3
	One DC bus	2.6E-2	4.0E-2

system. One modeled the failure to provide cooled water to the main CCW piping. The second was developed to model the failure of the CCW system to provide reactor coolant pump thermal barrier cooling.

During normal plant operation, only two CCW pumps and one heat exchanger are operating. CCW is pumped through the shell side of the CCW heat exchanger where it is cooled by SW. Pressure detection equipment on the CCW discharge header automatically starts the standby pump if the pressure falls below a certain point. (This requires failure of both normally operating pumps). Operation of the standby heat exchanger requires operator action (it is isolated by a normally closed manual valve). Two CCW pumps and one heat exchanger are required for successful function of the CCW system. A simplified schematic of the CCW system is shown in Figure 5.15.

CCW pumps A, B, and C depend on 480V buses 4, 6, and 7, respectively for motive power. CCW pump A depends on DC bus 1 for control power and pumps B and C on DC bus 2. CCW also depends on Control Air and 120V semi-vital AC to keep the thermal barrier return valve (CC-FCV-608) open. After a loss of offsite power (LOSP), the motor operated valves (MOVs) on the SW discharge side of the CCW heat exchangers automatically close. They have to be reopened by the operator in order to reestablish SW cooling. A dependency diagram of the CCW system is shown in Figure 5.16.

5.9.1 Comments

In general, it appears that the PSS modeling of the CCW system is correct. We have no significant comments on this fault tree model.

5.9.2 Other Observations

No credit for the standby CCW pump was given in the analysis. Inclusion of the operator failing to start the standby pump would only reduce the unavailability of the CCW system but would probably have little effect on the overall analysis. For those fault trees where only two CCW pumps were available, common cause failure of the pumps was not included. The single failure of one pump is a higher contributor than the common cause failure (success criteria is <u>two</u> pumps) and this simplification has no effect.

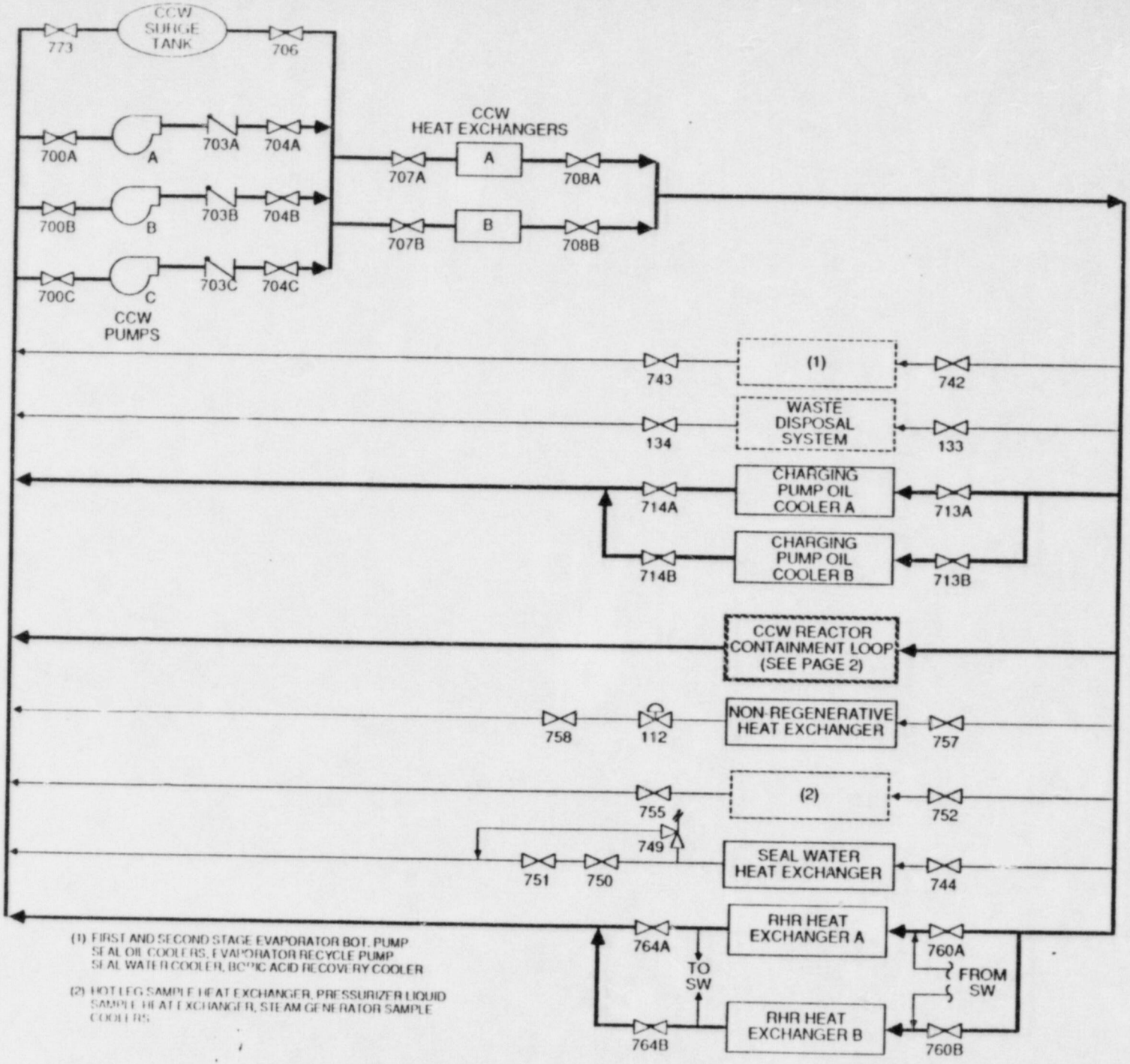


FIGURE 5.15. Simplified Flow Diagram for CCW System (sheet 1).

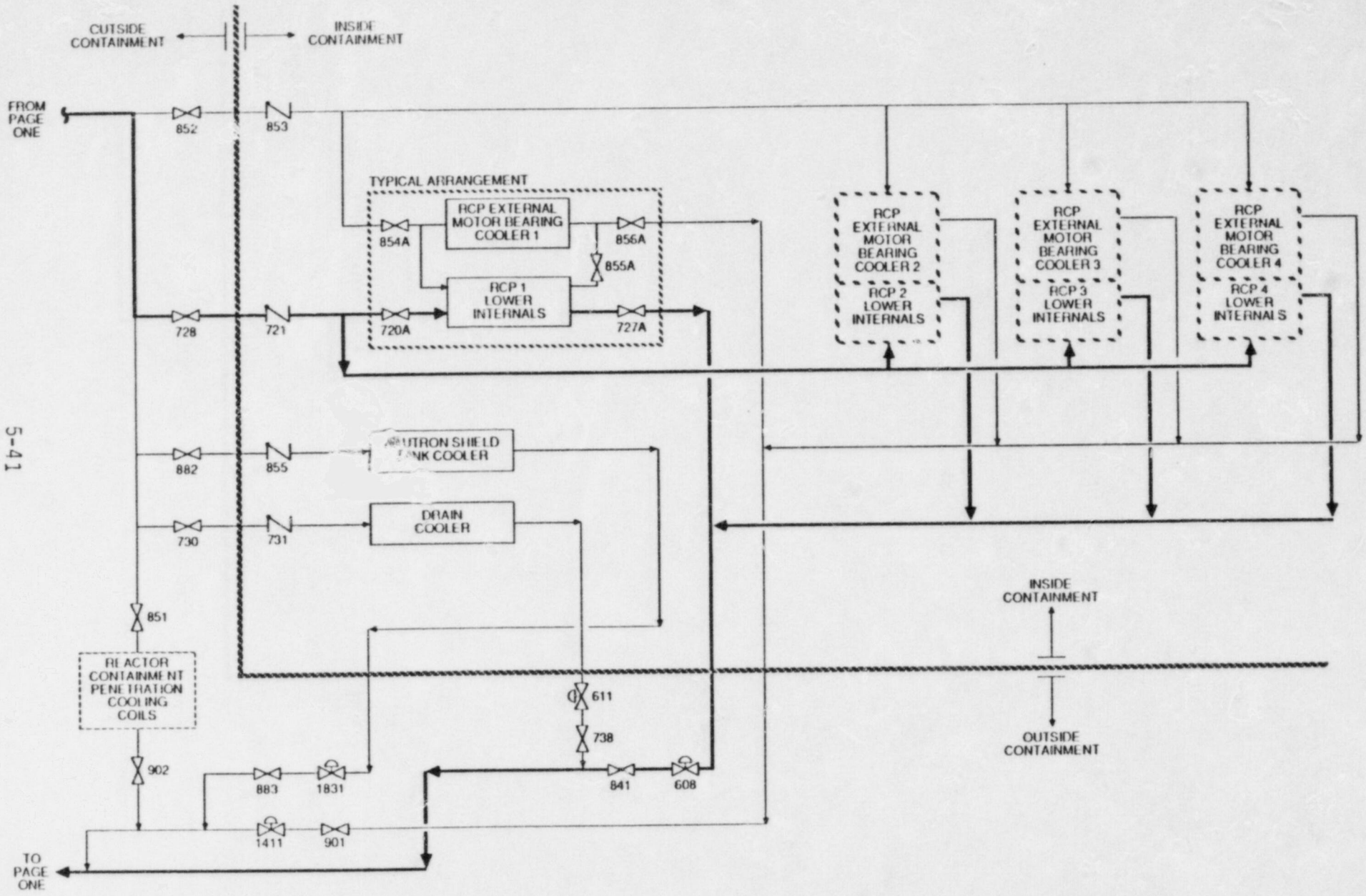
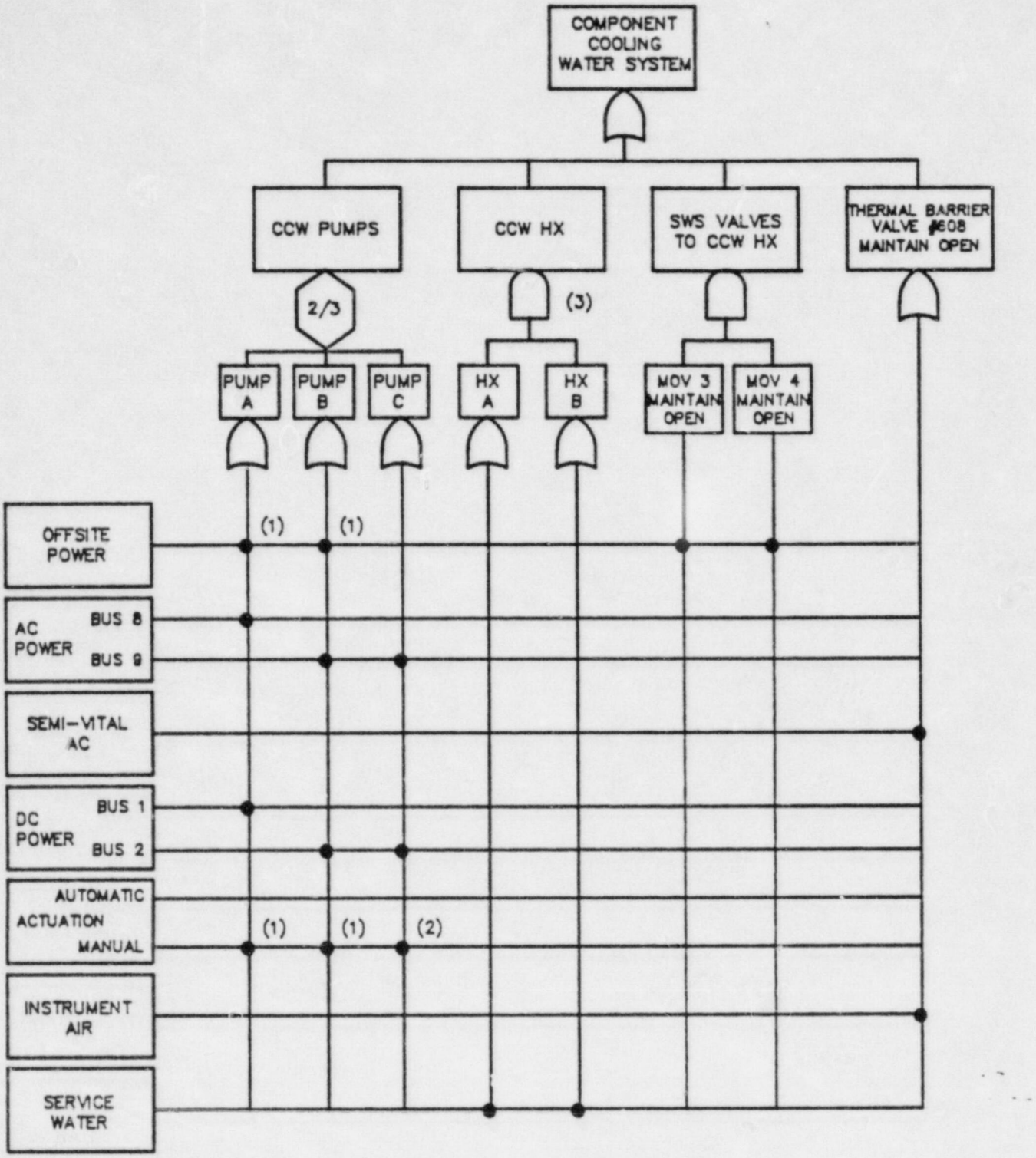


FIGURE 5.15. Simplified Flow Diagram for CCW System (sheet 2).



(1) CCW pumps A and B are normally operating (using offsite power), must be manually restarted after LOSP.
(2) Automatically starts if pumps A AND B fail; otherwise must be manually started.
(3) HX train A normally operating; HX train B, valves must be manually opened.

FIGURE 5.16. CCW System Dependency Diagram.

5.9.3 Requantification

The data modifications outlined in Section 6.0 of this report result in some relatively minor changes in the component cooling water system unavailability. The data changes result in a reduction in the system unavailability for the failure to provide flow to the main component cooling water piping. These reductions are primarily the result of a lower common cause pump failure probability and a lower transformer failure probability. The system unavailability changes are shown in Table 5.6.

The system unavailability increases for the CCW system when it is used to supply thermal barrier cooling after a loss of offsite power. This increase is due almost entirely to an increase in the air operated valve failure to open probability. Failure of one air operated valve will fail the thermal barrier cooling capability of the CCW system.

5.10 Service Water System

The Service Water (SW) system is an open loop cooling water system designed to supply cooling water to both the primary and secondary plant loads. SW is comprised of four pumps (in parallel) which take suction from the Connecticut River, two parallel full capacity headers and associated valves, piping, and instrumentation. The major primary cooling loads include the Residual Heat Removal (RHR) heat exchangers, the emergency diesel generators, and the CCW heat exchangers.

During normal plant operation, two to four SW pumps are operating. (Three pumps are assumed to be normally operating.) Pressure detection equipment on the SW discharge header automatically starts the standby pump(s) if the pressure falls below a certain point. The success criteria of the SW system is dependent on its configuration. If the secondary plant loads are isolated (SW MOVs 1 and 2 are closed), only <u>one</u> SW pump is required; however, if the secondary plant loads are not isolated (SW MOV 1 or 2 is open), then <u>two</u> SW pumps are required. A simplified schematic of the SW system is shown in Figure 5.17.

Table 5.6 Component Cooling Water System Modified System Unavailabilities

Mode	Failed Support Systems	Unavailability PSS	Unavailability Suggested
Normal	None	6.8E-4	4.5E-4
	Offsite power	1.9E-3	1.3E-3
	Offsite power and MCC-5	4.2E-4	2.5E-4
	Offsite power and DC 1	1.9E-2	1.7E-2
Thermal Barrier Cooling	Offsite power	1.2E-2	4.9E-2

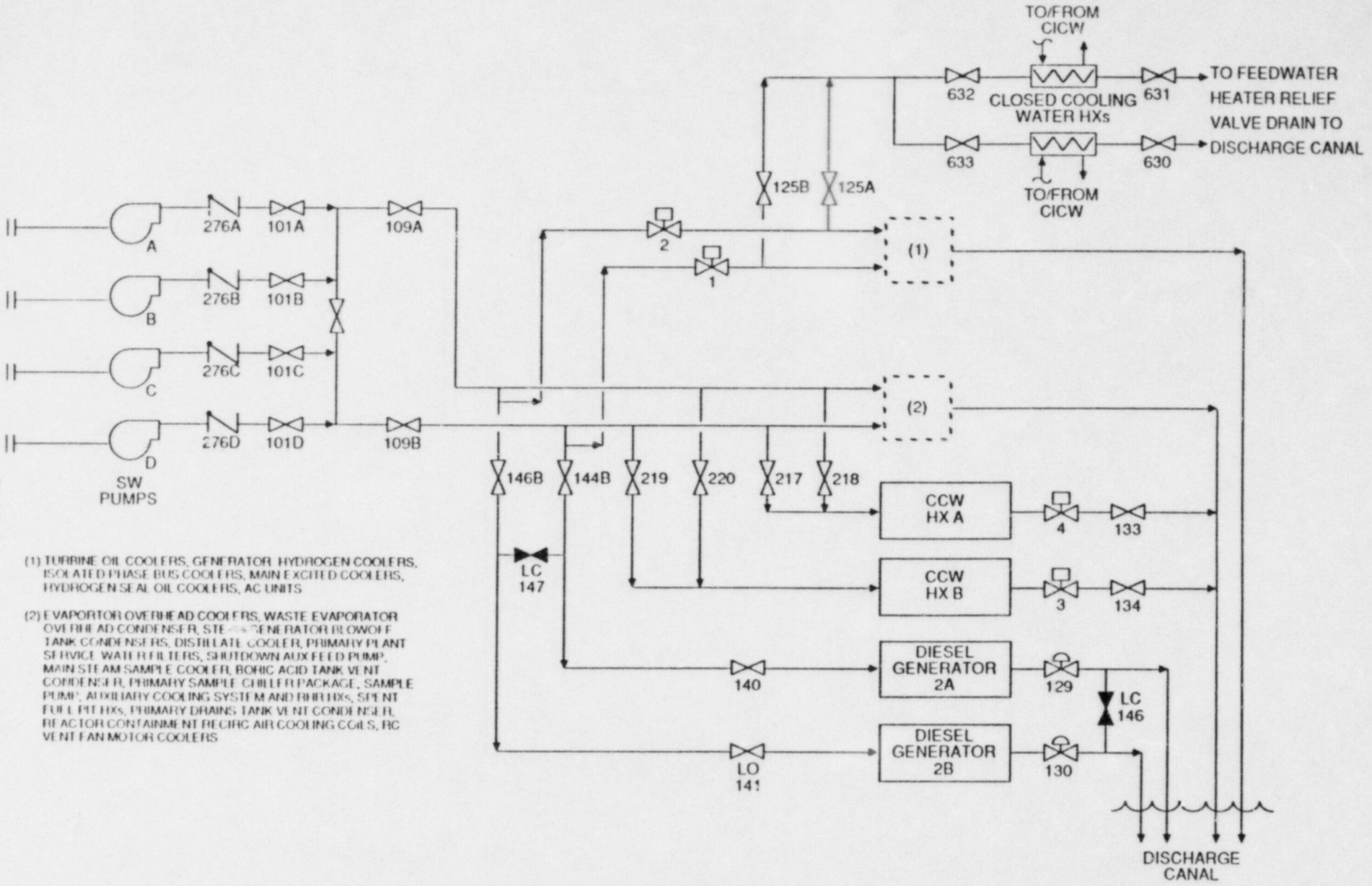


FIGURE 5.17. Simplified Flow Diagram for SW System.

SW pumps A, B, C, and D depend on 480V buses 4, 5, 6, and 7, respectively for motive power. SW pumps A and B depend on DC bus 1 for control power and pumps C and D on DC bus 2. Auto pump starts are dependent on availability of offsite power. With LOSP, only one pump is auto started per each emergency bus (i.e., emergency buses 8 and 9). SW MOVs 1 and 2 are powered (both motive and control power) by MCC-5 and close on LOSP. A dependency diagram of the SW system is shown in Figure 5.18.

5.10.1 Comments

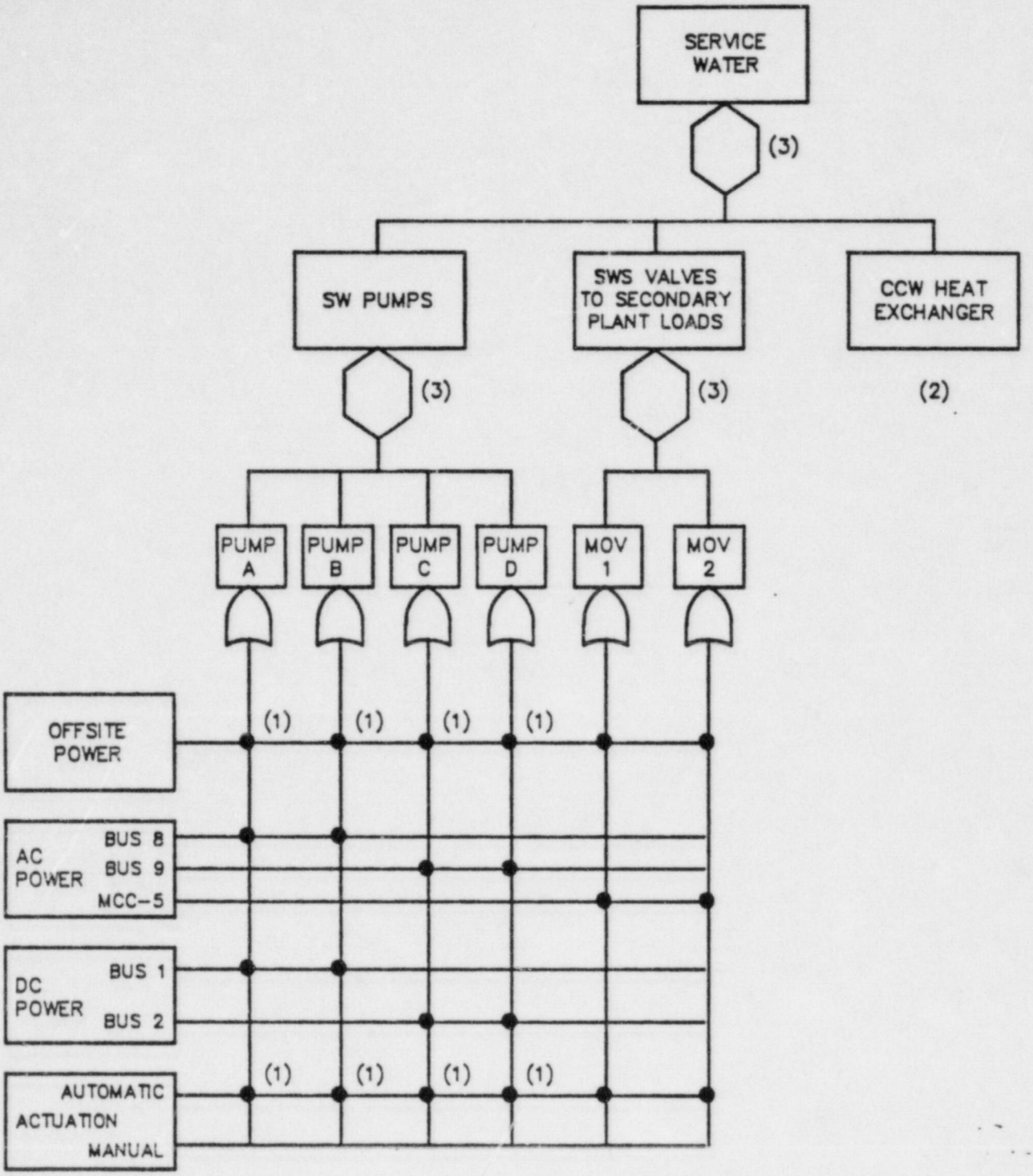
In general, it appears that the PSS model of the SW system is correct. We have no significant comments on this fault tree model.

5.10.2 Other Observations

No credit for the operator closing SW MOVs 1 and 2 in certain models was given in the analysis. This exclusion also affects the success criteria. If the operator were to close the valves, then only one SW pump would be required instead of two. Inclusion of the operator failing to close the valves would only reduce the unavailability of the SW system but would probably have little effect on the overall analysis. On Fault Tree 5, failure of contact pairs 2-2C 27/X4 and X5 to close which then fails to automatically close SW MOV 2 was not included. Since failure of only one valve to close is required, this omission has negligible effect on the analysis.

5.10.3 Requantification

The system unavailability of the service water system in three-support states was affected by the component data modifications outlined in Section 6.0 of this report. For the loss of offsite power support state, the service water system failure probability increased to 5.1E-5 from 9.5E-5 due almost entirely to the increase in the service water pump common cause failure probability. The doubling of the motor operated valve failure to open probability resulted in a doubling of the service water system unavailability, to a value of 3.0E-3, for the loss of offsite power and one emergency AC power train support state. The only other case where the data changes had a noteworthy effect on the service water unavailability was for



(1) With loss of offsite power, one pump per each emergency bus is automatically started. Pumps A, B, and C are normally operating; pump D is standby.
(2) Modeled as part of CCW; see CCW dependency.
(3) Two valves close and any one SW pump OR two or one valve opens and any two S W pumps.

FIGURE 5.18. SW System Dependency Diagram.

the loss of offsite power and MCC-5 support state. In this case, the system unavailability was reduced from 6.0E-4 to 4.0E-4 due primarily to the reduction of the transformer failure probability and the circuit breaker failure to remain closed probability.

5.11 Instrument Air System

The Instrument Air (IA) system consists of two subsystems: Control Air and Service Air. The IA system is designed to supply control air to normal plant loads with service air as a backup. The Control Air system is comprised of three air compressors and the Service Air system of two compressors and each with associated valves, piping, and instrumentation.

The compressors from both systems are cooled by the Closed Cooling Water (ClCW) system. The ClCW is comprised of two pumps (in parallel), two heat exchangers (in parallel) -- normally cooled by SW, a surge tank and associated valves, piping, and instrumentation. If ClCW is lost, well water from a hydro-pneumatic tank can supply cooling water to the compressors. Additionally, if SW is lost, well water can also be supplied to the ClCW heat exchangers. Well water is comprised of two pumps (in parallel), a flow control valve (FCV-1870), a well water compressor, normally closed manual valves (for alignment either directly to air compressors or to the ClCW heat exchangers), a hydro-pneumatic tank and associated valves, piping, and instrumentation.

During normal plant operation, only two control air compressors are operating. Compressor A is supplying air to normal plant loads with compressor B in standby. Compressor C supplies air to the primary auxiliary building and control room header. The major normal plant loads include the Main Feedwater (MFW) regulating valves, the MFW regulating valve bypass valves, the Auxiliary Feedwater pump steam control valves, the high pressure steam dump (turbine bypass) valves, the atmospheric steam dump valve, the main steam isolation valves, the CCW isolation valve to the RCP thermal barrier, and the charging pump flow control valves. Upon loss of the Control Air system, service air acts as a backup. It requires manual action to line up the Service Air system to the control air main headers. Only one air compressor is required for successful fucntion of IA.

One ClCW system pump is normally operating. The second pump is in a standby mode and requires operator action for actuation. Both heat exchangers are also normally operating. The SW system is normally operating (see Section 5.10 for a detailed discussion of SW). The well water system is normally isolated and requires operator action for actuation. One ClCW pump and heat exchanger or one well water pump is required for compressor cooling. A simplified schematic of IA, ClCW, SW, and well water is shown in Figure 5.19.

Control air compressors depend on MCC-5 for motive and control power. Service air compressors depend on 480V buses 5 and 7, respectively, for motive power and DC buses 1 and 2, respectively, for control power. However, they are not normally powered by the emergency buses during a LOSP. The ClCW pumps depend on MCC-5 for both motive and control power. Well water pumps C and D are dependent on MCC 3-4 and MCC 3-7, respectively, for motive power and DC bus 2 for control power. Well water FCV-1870 depends on air from the well water air compressor for motive power and MCC 3-7 for control power. The well water compressor depends on MCC 3-7 for motive power and DC bus 2 for control power. A dependency diagram of the IA, ClCW, SW, and well water systems is shown in Figure 5.20.

5.11.1 Comments

In general, it appears that the PSS has modeled the IA system correctly. We have no significant comments on this fault tree model.

5.11.2 Other Observations

The level of detail modeled for the IA system was quite different than seen for the other systems. A "smart" approach was taken here in that not all components were modeled. An attempt was made beforehand to identify those components that would dominate the system unavailability. Only the air compressors, the ClCW pumps and specific ClCW and well water valves were modeled in the fault tree. (Some of these models were not included in the PSS.) No other components were included. We feel that this simplification more than adequately encompasses the dominant failures of IA.

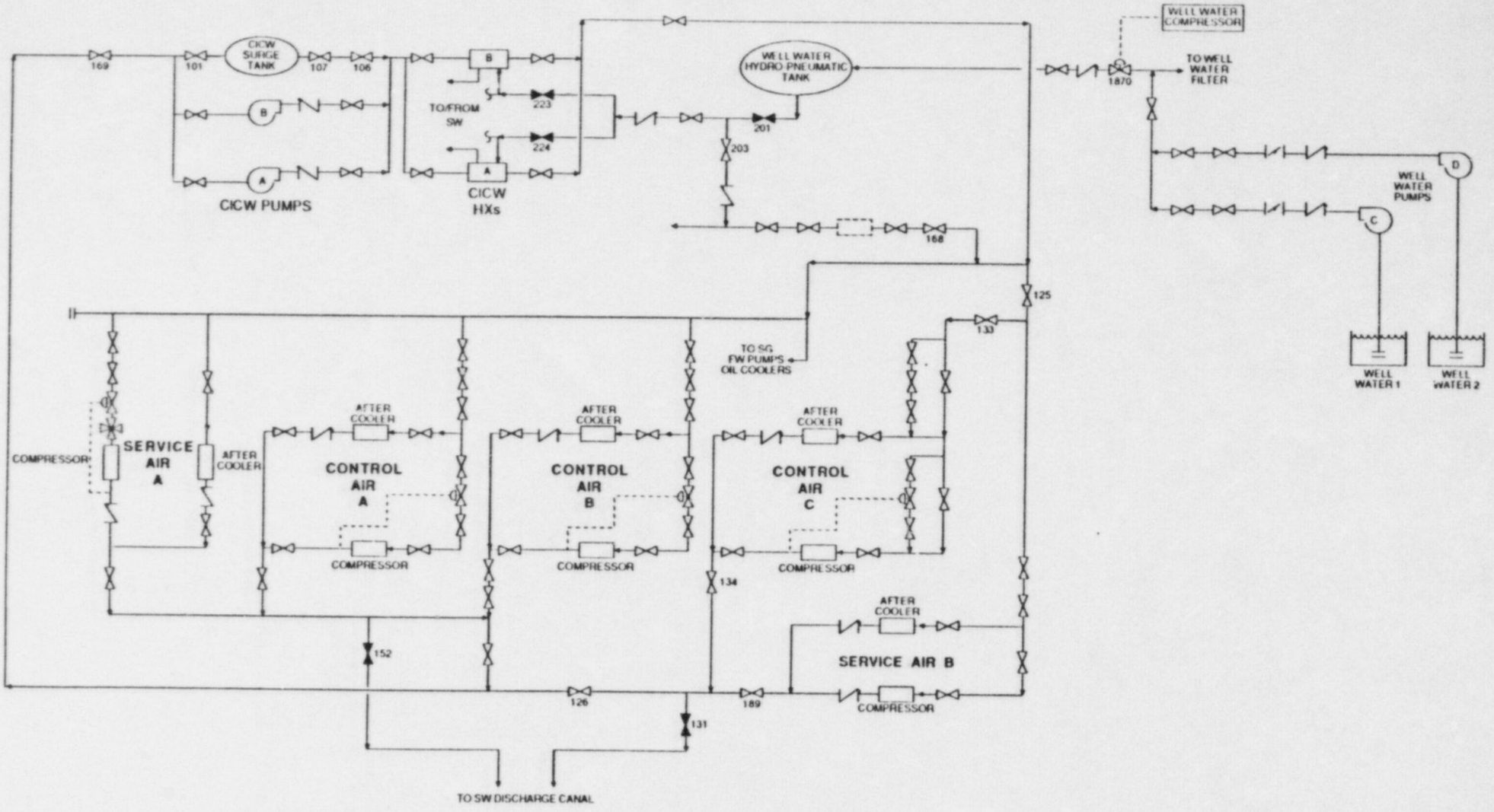
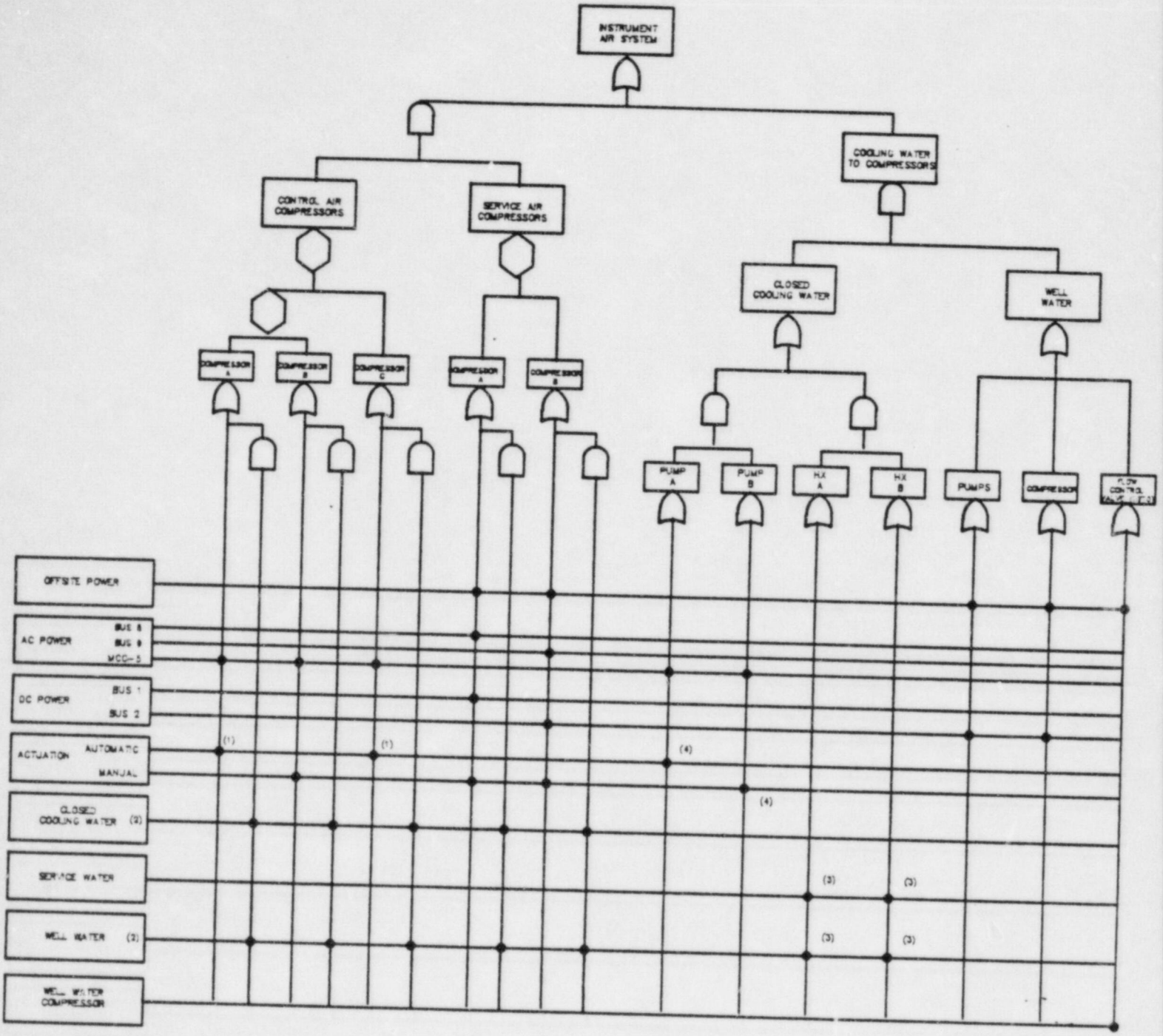


FIGURE 5.19. Simplified Flow Diagram for Control Air System.



(1) Control air compressors A and C are normally operating, compressor B requires manual operation.
(2) All compressors are normally supplied by closed cooling water; well water requires manual action.
(3) Closed cooling water heat exchangers are normally supplied by service water; well water requires manual action.
(4) Closed cooling water pump A is normally operating, pump B requires manual operation.

FIGURE 5.20. Control Air System Dependency Diagram.

For the state in which all support systems are available, no credit was given for the use of well water if the ClCW system was lost. This addition would lower the system unavailability, but have little effect on the overall analysis.

The ClCW and well water valves that were modeled were those that required the operator to change state for "successful" operation of the well water system. If the operator failed to isolate the ClCW system surge tank, failure of well water occurred because of flow diversion to the surge tank. However, there are other valves that the operator could also close if he were unable to close ClCW valves 101 and 107. No credit was given for closure of other valves such as ClCW-169 or ClCW-106 and others. This addition would decrease the system unavailability, but would have negligible effect on the overall analysis.

5.11.3 Requantification

The instrument air system unavailability was impacted primarily by one component data modification. The failure probability for an air operated valve was increased by nearly an order of magnitude. (See Section 6.0.) In the air system the failure of a single air operated valve will fail the well water supply to the system compressors. For the support states, a loss of service water or a loss of MCC-5, where well water is required for instrument air operation, the failure of this air operated valve now dominates the system failure probability. For the loss of service water support states the instrument air unavailability increases from 2.3E-2 to 4.7E-2, and for the loss of MCC-5 support states it increases from 2.5E-2 to 4.9E-2.

5.12 Main and Auxiliary Feedwater System

The Main Feedwater (MFW) system, also referred to as the Power Conversion System (PCS) during normal plant operation, is the main system for secondary heat removal and feedwater. PCS is comprised of three subsystems: Main Steam (MS), Feedwater (FW), and Condensate. The major components of the MS system include the steam generators (SG), MS isolation valves, MS safety relief valves, the atmospheric steam dump valve, the high pressure steam dump valves, the high and low pressure turbines, the moisture

separator reheaters, other miscellaneous equipment and associated valves, piping, and instrumentation. The feedwater system is comprised mainly of two turbine driven pumps (in parallel), heaters and associated valves, piping, and instrumentation. The condensate system is comprised mainly of two pumps (in parallel), main condenser, and associated valves, piping, and instrumentation.

During normal operation, the feedwater and condensate pumps are each operating. The Haddam Neck design is different from most other Westinghouse plants in that the MFW pumps do not trip on a safety injection signal, a high steam generator level, or a loss of condenser vacuum. (On a safety injection signal, the MFW isolation valves close and the auxiliary feedwater bypass valves open.) If a trip does occur, the first MFW pump will restart automatically. This is also true for the condensate pumps. Trip of a condensate pump, low voltage on the associated 4160V AC bus, sustained low suction pressure or electrical fault protections make up the trip functions for the MFW pumps.

After a MFW pump trip, secondary side heat removal is usually through the ten high pressure steam dump valves (i.e., the turbine bypass valves), then alternately through the air-operated atmospheric steam dump valve (which requires operator action), or via four one-inch vent lines (which requires the operator to open two manual valves, in series, on each line). If each of the above fails, four safety relief valves on each SG are available. Additionally, the level in the SGs is controlled by four variable position air-operated valves (MFW regulating valves), one for each SG.

If MFW or condensate is unavailable, the Auxiliary Feedwater (AFW) system can supply feedwater to the SGs. AFW is comprised of two turbine driven pumps (in parallel), an air-operated bypass valve (FW-1301-1, -2, -3, -4) to each SG, an alternate feed path MOV (FW-MOV-35), an air-operated valve (MS-PICV-1206a, B) to each AFW turbine and associated valves, piping, and instrumentation. The AFW system is initiated automataically when either both MFW pump breakers are open or two of four SG wide range level indications in train A or B indicate less than a forty-five percent level. A simplified schematic of the PCS and AFW system is shown in Figure 5.21.

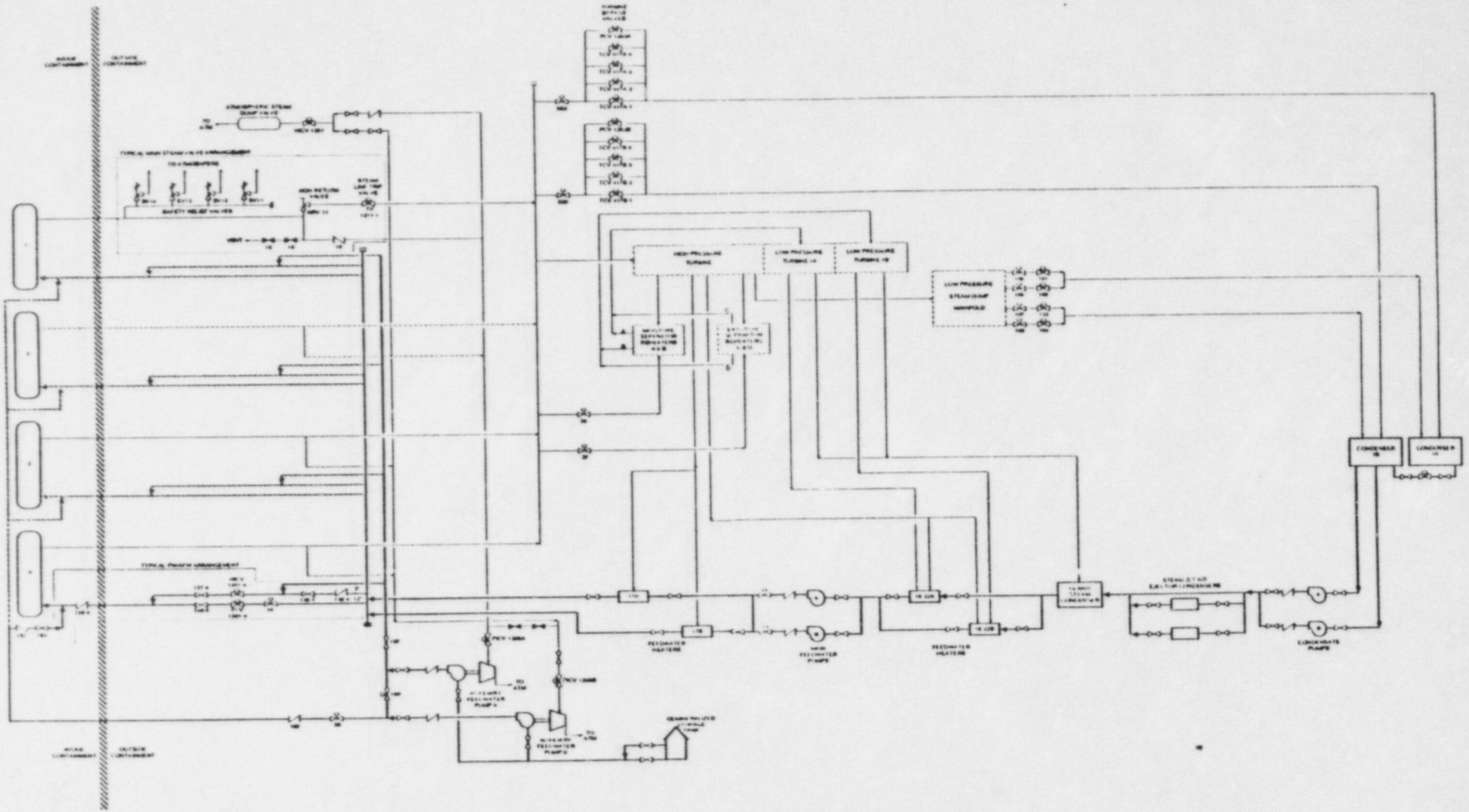


FIGURE 5.21. Simplified Flow Diagram for PCS/AFW System.

Upon loss of instrument air, the PCS valves each fail close in a fail safe position; the AFW valves each fail open. The MFW pumps are dependent on offsite power for motive power and DC power for control. The pumps also require seal and lube oil cooling. Seal cooling is powered and controlled by MCC 3-7 and lube cooling by MCC 6-7 and 6-6, respectively. The ClCW system is also required for lube oil cooling. The condensate pumps require offsite and DC power for motive and control power, respectively. The high pressure steam dump valves are dependent on instrument air for motive power and DC bus 2 for control. The atmospheric dump valve is dependent on instrument air for both motive and control power. The main steam isolation valves are dependent on instrument air for motive power and DC bus 1 for control power. The MFW regulating valves are dependent on semi-vital AC for motive power and DC power for control power. The AFW system is dependent on DC power for control (actuation) and instrument air for feedwater control flow to the SGs. The alternate AFW bypass valve is dependent on offsite power for motive and control power. The pumps are dependent on steam for motive power and DC power for control. A dependency diagram of the PCS and AFW system is shown in Figure 5.22.

5.12.1 Comments

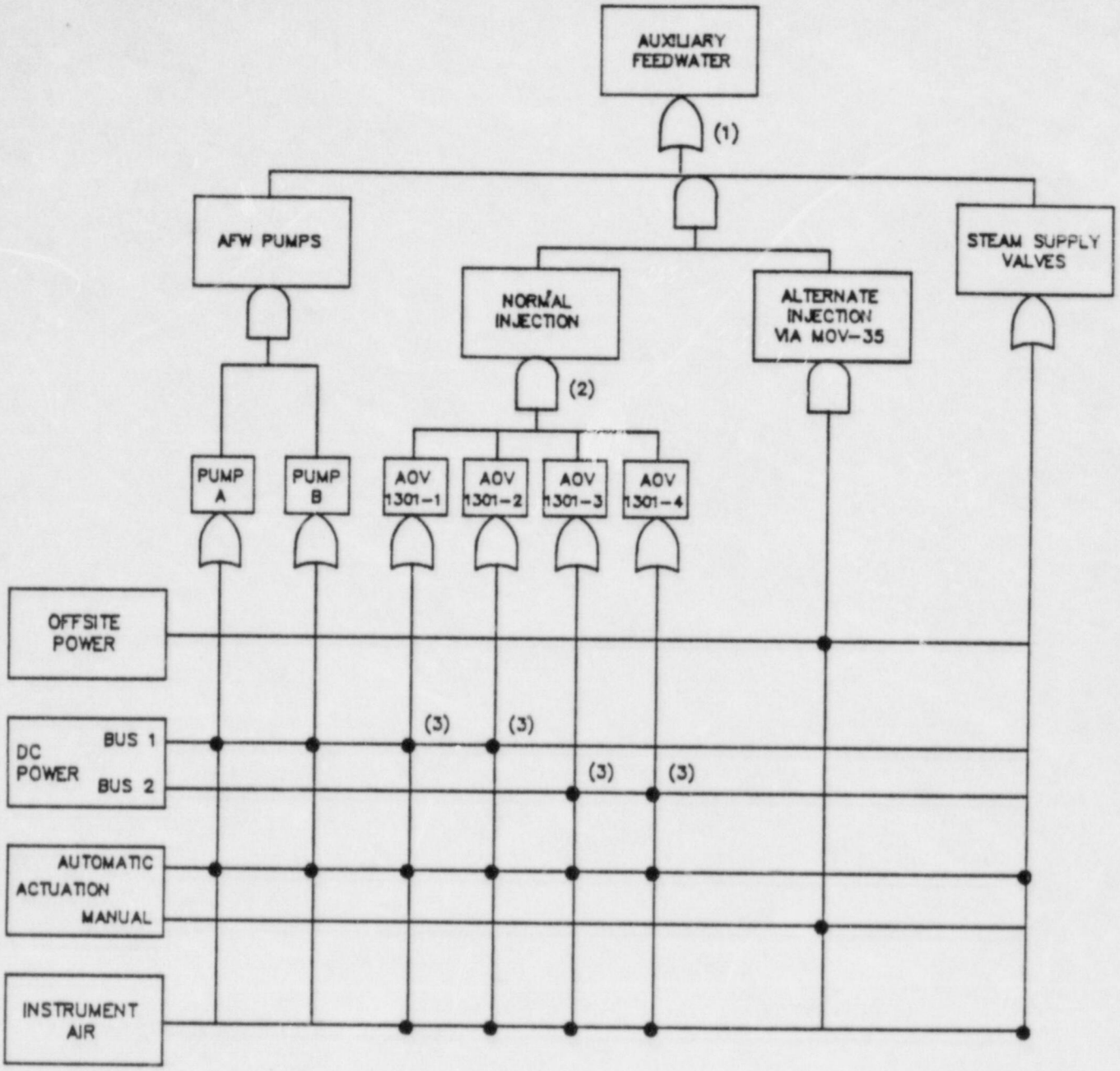
In general, it appears that the PSS model of the MFW and AFW system is correct. We have no significant comments on this fault tree model.

5.12.2 Other Observations

The cooling dependencies of the MFW pumps are listed in the PSS; however, these failure are not accounted for in the fault tree models. This addition would increase the unavailability, but have negligible effect on the overall analysis.

5.12.3 Requantification

The recommended component data changes presented in Section 6.0 of this report had little or no impact on the auxiliary feedwater system unavailability calculations, and only a minor impact on the integrated feedwater, auxiliary and main feedwater, system analysis. The requantification



(1) Success criteria does not include ATWS.
(2) Valves open on loss of air or DC power.
(3) Dependency is through the vital DC power system.

FIGURE 5.22. AFW System Dependency Diagram.

results are presented in Table 5.7. In two support states, all support systems available and the loss of DC bus 2 support state, the change to motor operated valve failure data resulted in an increase in the system failure probability. The unavailability of the feedwater system after an ATWS is reduced due to the reduction in the auxiliary feedwater pump random failure probability.

5.13 Safety Injection Actuation System

The safety injection actuation system (SIAS) consists of the sensors and relays used to automatically actuate the high pressure, low pressure, and charging systems when emergency makeup water is required. The signals required to automatically initiate safety injection are high containment pressure or low pressurizer pressure. Figure 5.23 shows the logic used to generate a safety injection signal. The six containment pressure sensor outputs are arranged in two trains of three signals each. One half of a safety injection signal is generated if two of the three sensor outputs in either train indicate a high containment pressure condition; train B containment pressure actuates relay 4B, train A actuates relay 4A. Two of three low pressurizer pressure signals will also generate a safety injection signal. A safety injection signal results in two relays (relays 4A and 4B) becoming energized. Each relay generates a start signal to one low pressure, high pressure, and charging pump.

In the PSS fault tree analysis, the system boundary is defined as these two relays. The components, including contact pairs off of these two relays, used to transfer the safety injection signal to each pump is considered in the fault tree for each injection system.

Two sets of fault trees were developed in the PSS. One was for post LOCA situations where both high containment pressure and low pressurizer pressure conditions would be expected. In this case, either signal would generate an SI signal. The second set of fault trees was developed for post transient conditions where no high containment pressure would occur. For this set of fault trees, only the low pressurizer pressure signal was modeled. In both cases, system success was considered to be the energization of relays 4A and 4B.

Table 5.7 Main and Auxiliary Feedwater Systems
Modified System Unavailability

Mode	Failed Support Systems	Unavailability PSS	Unavailability Suggested
Four Steam Generators Available	None	5.0E-5	8.0E-5
One faulted Steam Generator	None	5.6E-5	9.0E-5
	DC 2	6.3E-5	8.0E-5
Post ATWS		1.7E-4	1.4E-4

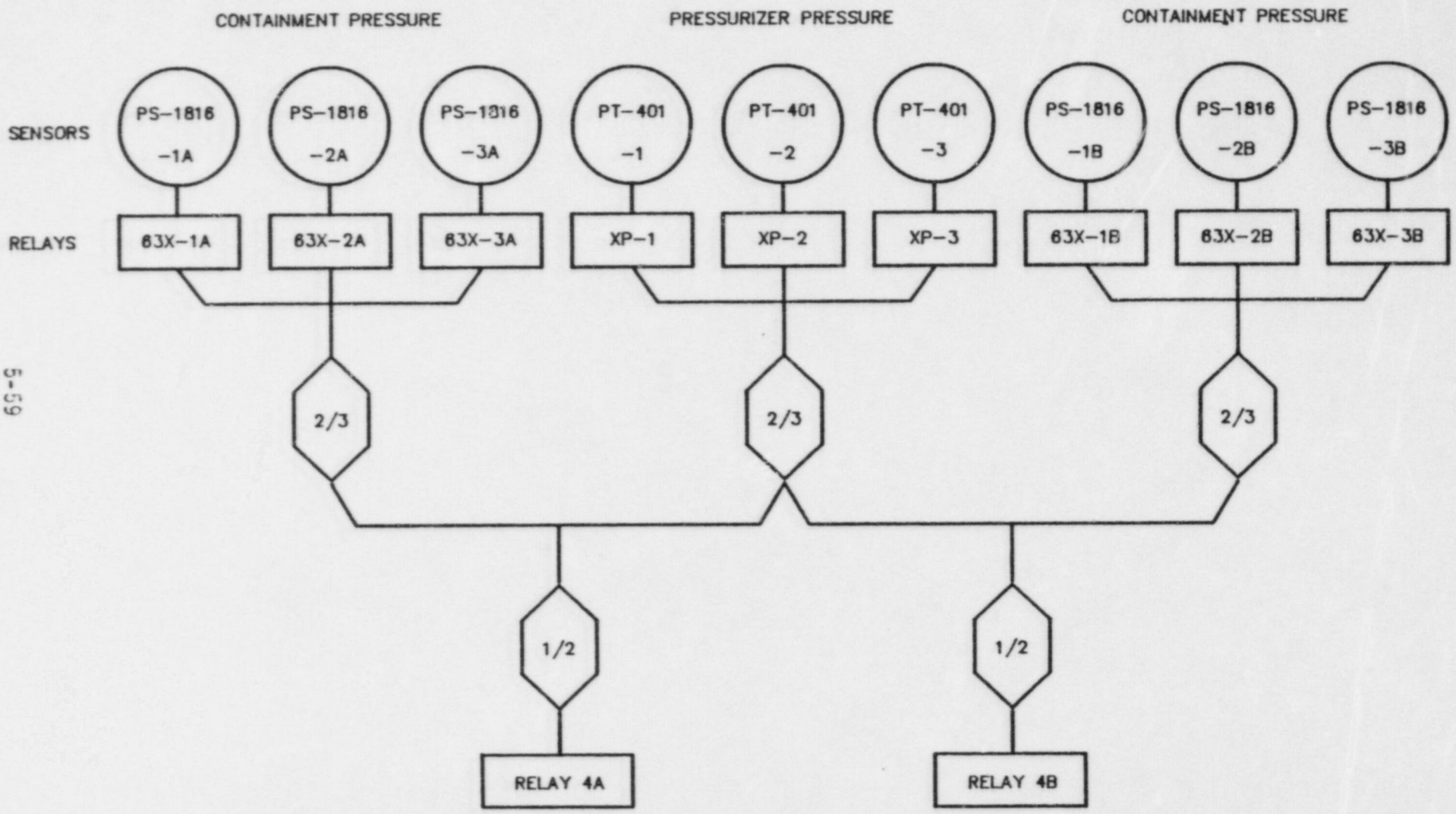


FIGURE 5.23. SIAS Logic Diagram.

The only system dependencies modeled were the dependencies in DC power and Vital AC power, which is dependent on DC power only. Relays 4A and 4B are dependent on DC trains 1 and 2, respectively. Each train of containment pressure relays is dependent on one of the two DC power supplies. Loss of power to the pressurizer pressure sensors and their associated relays results in the generation of a low pressure signal. Since two pressurizer pressure relays are powered by DC bus 1, a loss of DC bus 1 results in the generation of an SI signal. System dependencies are shown in Figure 5.24.

5.13.1 Comments

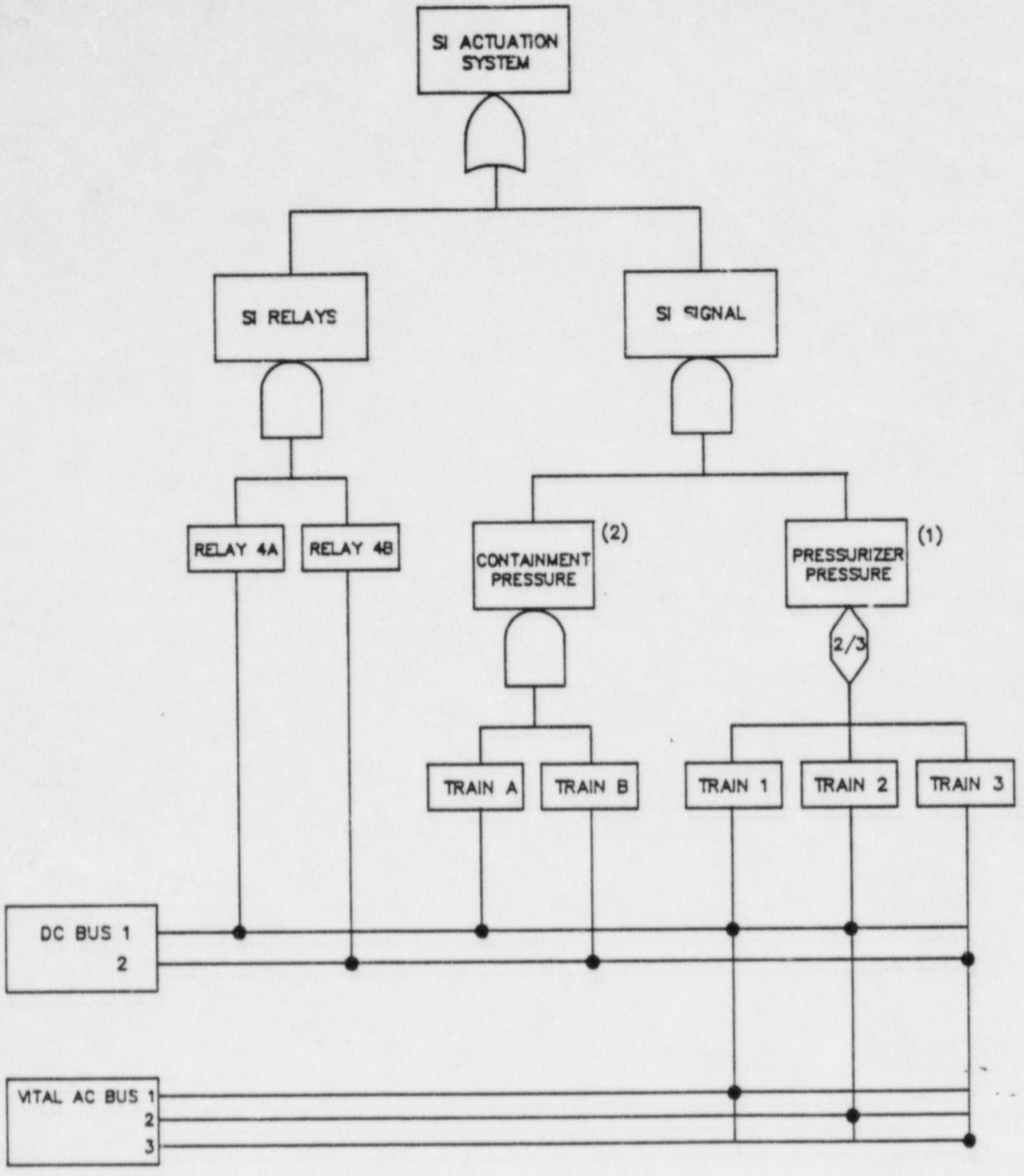
In general, it appears that the PSS model of the SIAC is correct. We have no significant comments regarding this system analysis.

5.13.2 Other Observations

This system model is input to the models for high and low pressure injection systems and integrated safety injection system. The system boundary as defined by the PSS in the SI actuation system analysis is not necessarily the boundary as defined in the other system analyses. In general, parts of the SIAS were modeled both in the actuation system analysis and in the injection system analysis. However, for those cases where the injection system analyses included parts of the actuation system modeled in the SIAS analysis, the actuation system analysis was revised to eliminate duplication of component failures in the final system (actuation plus injection systems) analysis. From our review, we conclude that the system interfaces of the safety injection systems with the actuation system were properly handled in all cases.

5.13.3 Requantification

The review of this system did not result in any modifications to the system model that would impact the system unavailabilities as calculated in the PSS. The system model was requantified to assess the impact of the data modifications discussed in Section 6.0.



(1) Loss of DC results in generation of low pressurizer pressure signal; therefore, loss of DC 1 generates an SI signal.
(2) High containment pressure will not exist for all accident sequences.
(3) Vital AC buses 1 and 2 are solely dependent on DC1.
Vital AC buses 3 and 4 are solely dependent on DC2.

FIGURE 5.24. SIAS Dependency Diagram.

The major change in the system unavailability is due to the increase in the relay failure to energize probability. This change in the failure probability results in an increase of 1.4E-5 in the system failure probability from 1.1E-5 to 2.5E-5 for the case where high containment pressure does exist and all support systems are available. The impact of data modifications on the other support states and system models, i.e., SI actuation where no high containment condition occurs, is not as pronounced as for this case. (The changes in system unavailability range from no impact to approximately a 30% increase.)

As stated earlier, the results of this system analysis were input into the system models for low pressure, high pressure, and integrated injection. The changes in the system unavailabilities calculated for the SIAS had little impact on the unavailabilities of these injection systems.

5.14 Containment Spray System

The containment spray system is used in conjunction with the containment air recirculation fans to provide the containment heat removal function for containment depressurization or for post-core melt situations. The containment spray system is a manually operated system. The LPSI pumps or the fire protection system pumps are manually aligned to the containment spray valves during the early part of the spray system operation. The LPSI pumps take suction from the RWST and the fire pumps draw water from the Connecticut River. Later, the RHR pumps are used to supply water to the containment spray valves. This water is drawn from the containment sump and cooled by the service water system in the RHR heat exchangers. A simplified system diagram is shown in Figure 5.25.

Five different models were created in the PSS for the containment spray system. These models represent use of the system under varying conditions which result in different combinations of system equipment necessary to ensure successful operation. The five models created in the PSS are as follows. In the first case, LPSI is being used for injection into the core. Administrative procedures require that both LPSI pumps and both RHR pumps be operable before the LPSI and RHR systems can be used for containment spray. One of the two fire pumps can be used in place of the LPSI system pumps. In the second case, the LPSI system is not being used to

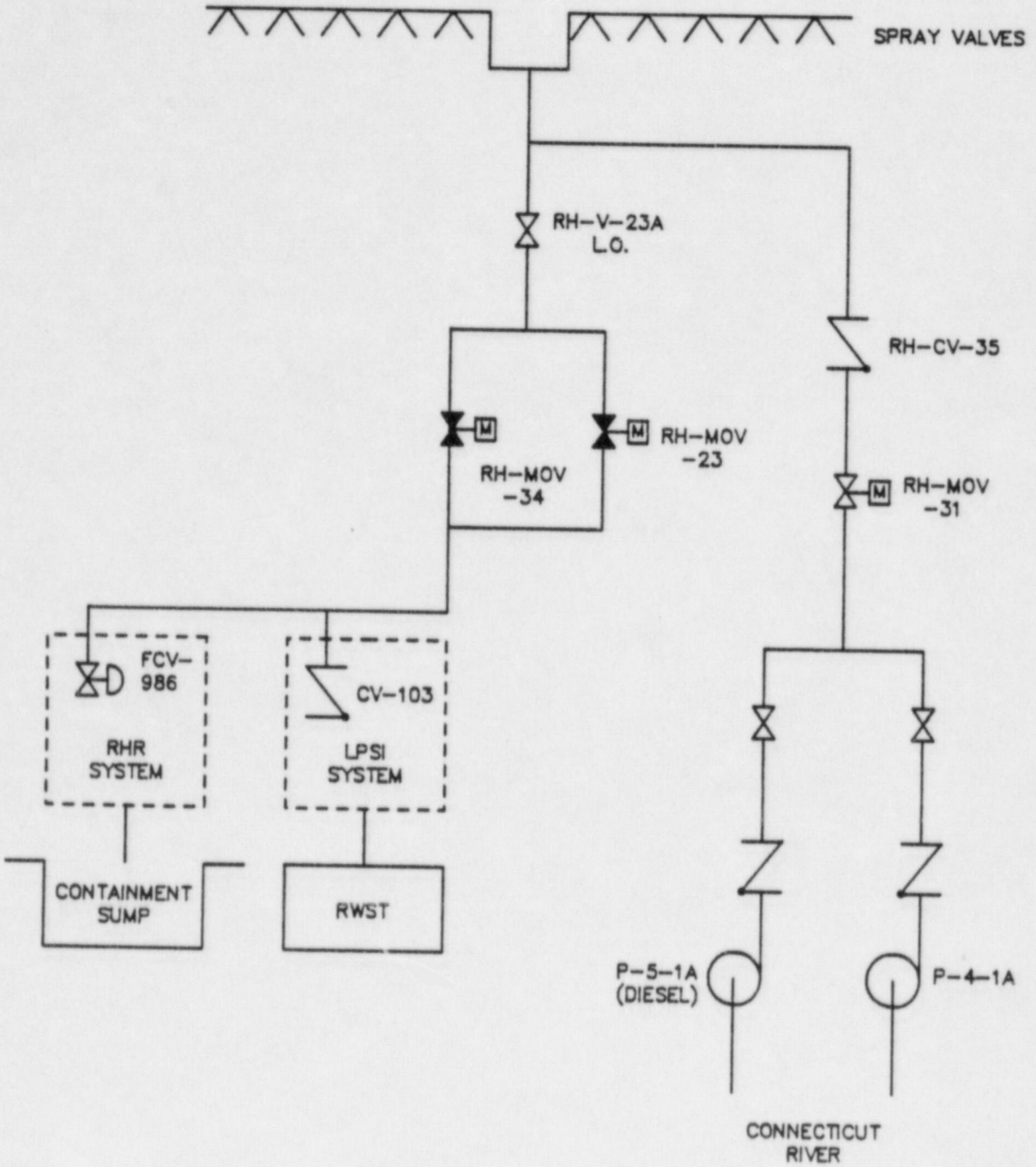


FIGURE 5.25. Containment Spray System.

inject into the core. In this case, the success criteria for the containment sprays is one of two LPSI or fire pumps and one of two RHR pumps. The system dependency diagram in Figure 5.26 represents this case. Case three is nearly identical to case two except that it is used when the LPSI system is explicitly modeled in an event tree and the event sequence being modeled includes LPSI failure. In this case, the conditional probability of LPSI failure to provide containment spray given that the LPSI system has failed in the injection mode is used. The success criteria for cases 2 and 3 are the same. Case 4 corresponds to the use of the containment spray system in a post-core melt environment where both LPSI and RHR have failed. For this case, the system success criteria was defined as one of two fire pumps providing flow to the containment spray valves. Case 5 is a special version of case 4, used during a station blackout. It considers manual actions to align the diesel driven fire pump to the containment spray system.

5.14.1 Comments

In general, the PSS model appears to be a reasonable analysis of the containment spray system. The review of this system analysis did not result in any suggested modifications that would have a significant impact on the system unavailabilities.

5.14.2 Other Observations

In case 5, failure of MOV-31 (see Figure 5.25) is not considered as part of the dominant failure contributors to the system failure probability. For this case the dominant failures are listed as failure of check valve CV-35 (3E-2) and failure of the diesel driven fire pump (5.1E-3). The total system failure probability is given as 3.7E-2. In all other cases, the failure probability for MOV-31 is given as 2.0E-2, which, if included, would raise the case 5 system failure probability to 5.7E-2. No justification was provided for reducing the valve failure probability although it appears that the valve was treated as a manual valve or only non-recoverable faults were considered when manual operation of the MOV was considered. (This reduction of the MOV failure probability was not done for other valves operated manually, in particular not in the charging system analysis.) Such

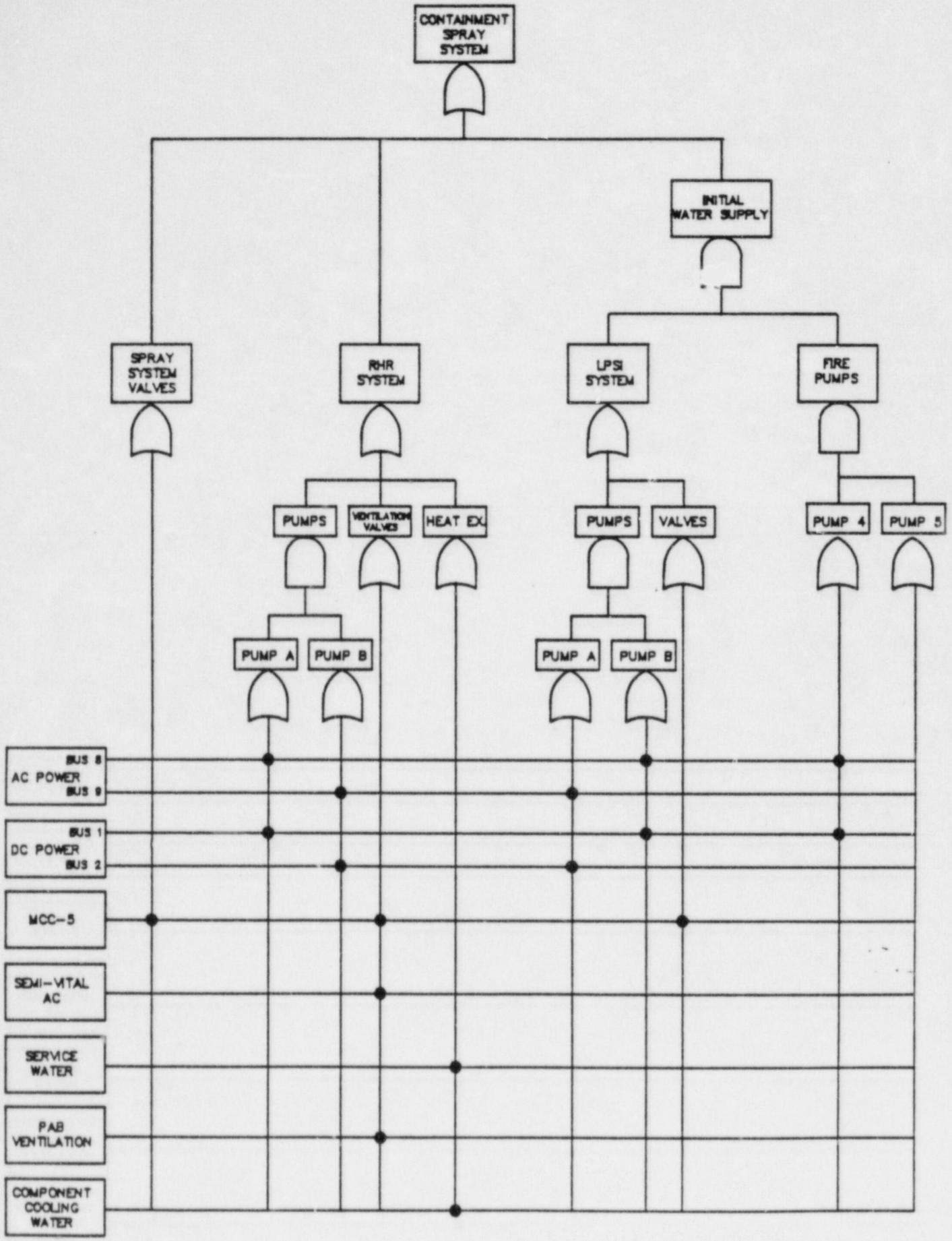


FIGURE 5.26. Containment Spray System Dependency Diagram.

a treatment of the valve is not unprecedented but, since used in this case, should have been more consistently applied throughout the PSS.

5.14.3 Requantification

The system models developed for the containment spray system were not changed as a result of this review. This requantification assesses the impact of data changes recommended in Section 6.0 of this report.

The largest change in any system unavailability occurred in case 2 for the loss of offsite power support state. This system unavailability doubled. In no other case did the system unavailability change by more than 50%. For this system, these system unavailability changes are not really significant. The primary reason for the insensitivity of the PSS to changes in the containment spray system is that this system is always used in conjunction with the containment air recirculation fans (CARFANs). In most situations, the CARFANS or operator errors, modeled at the event tree level, dictate the value of the containment heat removal function used in the event trees. The changes calculated in the containment spray probabilities do not significantly impact the containment heat removal system unavailabilities.

5.15 Containment Air Recirculation Fan System

The containment air recirculation fan (CARFAN) system consists of four 65,000 cfm fan coolers and a system of distribution ductwork and instrumentation and control. The system is used in conjunction with the containment spray system to remove heat from the containment during normal operation and during post accident conditions which result in containment pressurization. Under normal conditions three or four fans are operating; the PSS assumed in all cases that three fans were normally operating. Under accident conditions one (for bleed-and-feed operation) or two (for post LOCA, steamline break, or post core melt situations) fans are required. For simplicity, the PSS assumed that two CARFANs were required for all situations.

The cooling water for the CARFAN system is provided by the service water system. The fans are powered from AC buses 4, 5, 6, and 7. The two fans normally powered from AC buses 5 and 6 can be cross connected to buses

6 and 5, respectively. This means that for situations where one emergency AC bus is unavailable, three fans are available, two through normal power supplies and a third through alternate power supplies. DC power is required to start each fan (DC1 for the fans on AC buses 4 and 5, DC2 for the fans on AC buses 6 and 7). On a LOSP all running fans are tripped. Only one fan on each emergency bus is automatically started; a sequencer is used to attempt to start one fan, and only if it fails is the attempt to start the second fan made.

No detailed system model was developed in the PSS for the CARFAN system. The only failures considered were common cause failures of the fans to start and run. Failures of the actuation system were not considered since the system is not required immediately after an initiating event and operator action to start the CARFAN system is possible in all cases where the fans would be operable. Even in those cases where operator action to start, or in some cases after a LOSP, to restart the fans, the failure probability of the system is modeled using the common cause failure probability for the fans.

5.15.1 Comments

The system analysis, although not detailed, appears to adequately model the CARFANs system. We have no comments that would significantly affect the system unavailabilities.

5.15.2 Requantification

Neither the system analysis review nor the data review had any significant impact on the PSS values for the unavailability of this system.

5.16 Integrated Safety Injection for SGTR

The integrated safety injection system consists of four subsystems: (1) the charging system, (2) the high pressure safety injection (HPSI) system, (3) the low pressure safety injection (LPSI) system, and (4) the safety injection actuation system (SIAS). The integrated safety injection function was analyzed for the steam generator tube rupture (SGTR) accident scenario.

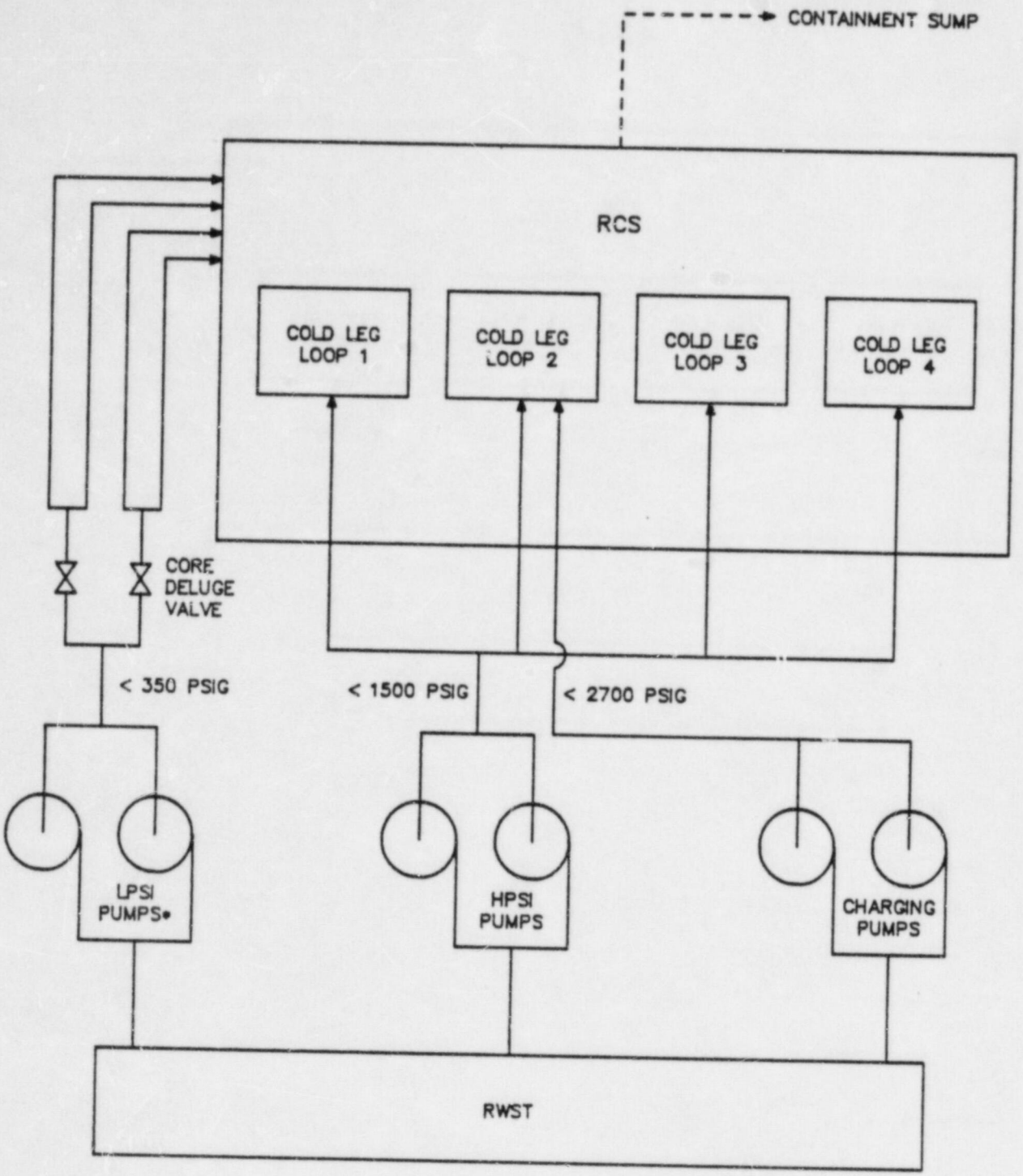
Following a SGTR event, the SIAS injection actuation signals will be generated as a result of two out of three low pressurizer pressure signals. All safety injection systems including charging will be automatically initiated and deliver borated water from the refueling water storage tank (RWST) to the reactor coolant system (RCS). Specifically, the charging system suction will be switched from the volume control tank (VCT) to the RWST and delivered to the cold leg of loop 2 at about 270C psig or less. At the same time, the HPSI will also be actuated and ready to inject borated water from the RWST into one of the cold legs of each loop, but at a lower pressure condition (<1500 psig). The LPSI system, which operates at less than 350 psig, will also be actuated; however, it would not be used in this scenario since the RCS pressure condition will still be too high for it to function properly. A simplified schematic of the integrated safety injection system is illustrated in Figure 5.27.

Success criteria for this system include SIAS signals being generated and automatically initiating HPSI and charging system, including the success criteria associated with the HPSI and the charging system. Figure 5.28 shows the support system required for this integrated safety injection system.

The integrated safety injection system was evaluated for four different support states: (1) all support systems are available, (2) either service water (SW) system is unavailable or a loss of offsite power (LOSP) has occurred, (3) a loss of either DC Bus 1 or DC Bus 2, and (4) a loss of either DC Bus 1 or DC Bus 2 and service water system. For each of the first three cases, fault tree models were developed and analyzed. For the fourth case, the analysis was based on the fault tree modeled for case 3 with the omission of the charging system branch.

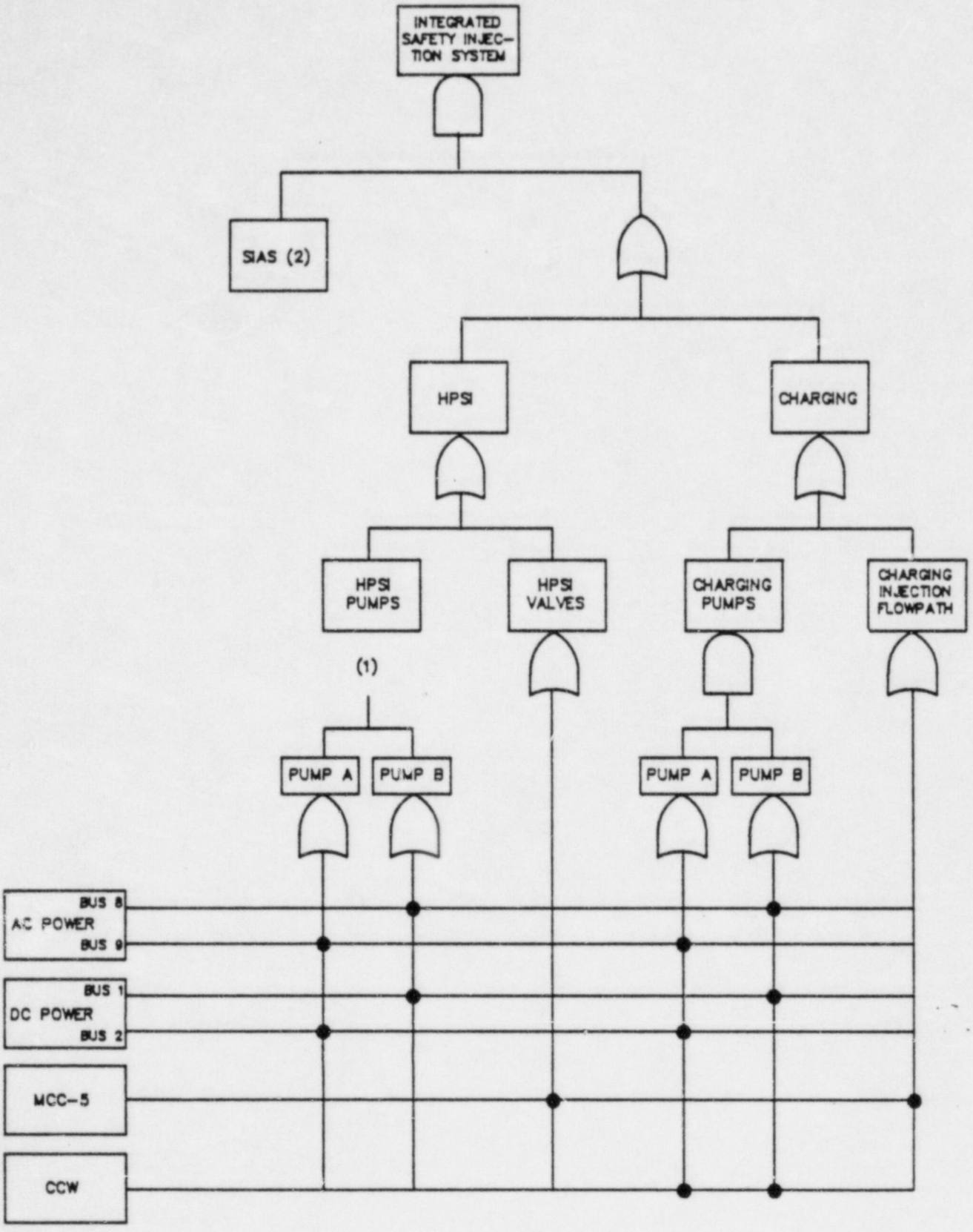
5.16.1 Comments

Reviews of these models and information available in the PSS and at the Northeast Utilities Headquarters indicate that the system analysis is satisfactory.



*LPSI system would not be used in the SGTR event.

FIGURE 5.27. Simplified Diagram of the Integrated Safety Injection System.



(1) If 3 of 3 injection loops are available this is an "and" gate. If 2 of 3 injection loops are available this is an "or" gate.
(2) SIAS is illustrated in Figure 5.24 and is dependent on DC power and vital AC power.

FIGURE 5.28. Integrated SI System Dependency Diagram.

5.16.2 Requantification

As a result of changes in component unavailability data, the system failure probability values are requantified using suggested data presented in Chapter 6.0.

For the loss of SW or LOSP support state, it is estimated that the system unavailability will increase from 7.6E-3 to 1.2E-2 due to changes in MOV and HPSI pump reliability data. For the loss of either DC Bus 1 or Bus 2, the system failure probability will increase from 7.0E-3 to 1.3E-2 as a result of changes in MOV and relay data. For the support state in which SW and either DC Bus 1 or DC Bus 2 have failed, the system unavailability also increases from 9.3E-2 to 1.5E-1 due to an increase in MOV failure probability.

5.17 Additional Event Quantifications

Several events that appear on the Haddam Neck PSS event trees were not quantified using system fault tree analysis. Most of these events were classified as additional quantifications in the Haddam Neck PSS. These events include such items as loop isolation, recovery of offsite power (including a time dependent station blackout analysis) and primary depressurization. Still other events were quantified using the results of the system reliability analysis. Such events include bleed-and-feed, consequential LOCAs and primary integrity. Table 5.8 lists the systems modeled using different quantification techniques along with the two systems, reactor protection and power conversion, presented as part of the system analysis but not modeled using fault tree techniques. The methods used to quantify these systems and events are also presented in this table.

5.17.1 Comments

In general, the models used for each of these events was found to be acceptable and to adequately model the system or event. We have no significant comments regarding these event models.

Table 5.8 Additional Quantification Methodologies

Event/System	Method of Analysis
Reactor Protection System	generic data and Northeast Utility reliability analyses
Power Conversion System	historical industry data and simple pump failure model to generate feedwater recovery probabilities
Recovery of Offsite Power	Northeast region and site frequency and duration of offsite power loss
Emergency Boration	fault tree
Pressurizer Relief	fault tree
Feed and Bleed	results of HPSI and charging system analyses plus fault tree model of manual "bleed" operation
Loop Isolation Valves	simple valve failure model (FMEA)
Primary Depressurization	simple comoponent failure model (FMEA)
Consequential Small LOCA and Primary Integrity	results of charging system analysis for seal failures and simplified component analysis for PORV and S/RV failures to close
Consequential Stuck Open Steam Generator Safety Relief Valve	estimate of number of valve cycles per initiator and valve failure per cycle
Consequential Steam Generator Tube Rupture	generic data
Adverse Break Size and Location	estimate of the fraction of pipe segments whose rupture would disable mitigating systems
Turbine Trip for ATWS	Millstone 3 analysis
Time Dependent Station Blackout Analysis	time dependent diesel generator failure analysis

5.17.2 Requantification

Changes in the unavailability of each event listed in Table 5.8 are due to the recommended data changes of Section 6.0. The changes listed in Table 5.9 are limited to those that are significant to the event tree analysis quantification effort. As with most of the system analyses, the change in the motor operated valve failure probability is the single most significant data change. For the quantification of the bleed-and-feed event, the increase in the air operated valve failure probability is also important. The changes in the primary integrity and consequential LOCA unavailabilities result primarily from the changes in the charging system unavailabilities and the PORV failure to release probability, which is dominated by a relay failure.

Table 5.9 Additional Events Requantification Results

Event	Failed Support Systems	Unavailability PSS	Unavailability Suggested
Emergency Boration	None	3.0E-2	5.2E-2
	Offsite Power and 1 AC Bus	3.6E-2	5.8E-2
Loop Isolation Valves	-	5.0E-2	9.0E-2
Bleed-and-Feed	None	1.8E-2	2.9E-2
	Service Water (SW)	1.3E-1	2.5E-2
	1 DC Bus	3.0E-2	4.4E-2
	1 DC Bus and SW	2.1E-1	4.0E-1
	Offsite power	1.8E-2	3.5E-2
	Offsite power and 1 AC Bus	6.8E-2	9.2E-2
Primary Integrity			
1. Loss of DC Initiator	Offsite power and 1 AC Bus	8.1E-4	3.4E-3
2. Loss of Control Air Initiator	None	6.6E-3	9.5E-3
Consequential LOCA			
1. General Plant Transient	None	2.9E-4	6.0E-4
	SW	3.4E-2	5.6E-2
2. Loss of Main Feedwater	None	3.5E-4	7.2E-4
	SW	3.4E-2	5.7E-2
	Offsite Power	1.1E-3	1.5E-3
3. Loss of Offsite Power	Offsite power	8.8E-4	1.0E-3

6.0 COMPONENT RELIABILITY ANALYSIS

The component reliability analysis for the Haddam Neck PSS consists of development of component failure data, common-cause failure analysis, and component unavailability analysis due to test and maintenance outages. The component failure data was developed using a combination of plant-specific and generic component failure rates. This data base is reviewed in Section 6.1. The common-cause calculations were performed for a series of components using the binomial failure rate model (12). This analysis is reviewed in Section 6.2. The component unavailabilities due to test and maintenance outages are discussed in the Haddam Neck PSS component Data Collection and Reliability Analysis section but are included more explicitly on the system fault trees. Comments about these calculations are provided as part of the System Reliability Analysis Review presented in Section 5.0.

6.1 Review of the Component Data Base

Because of the relatively long operating history of the Haddam Neck Nuclear Power Plant, a substantial amount of plant-specific data has been collected for a series of components. For these components in the Haddam Neck PSS, the generic data was updated using the Bayes theorem and the plant-specific component failure data. For the rest of the components with insufficient or no plant-specific experience, generic failure rates were used in the PSS. Thus, the component failure data developed in the Haddam Neck PSS consists of a combination of plant-specific and generic data.

In performing Bayesian updating of generic data using plant-specific experience, proper choice of prior distribution for the generic data and likelihood function for the plant-specific data can result in an updated or posterior distribution that has a closed-form or analytical solution. Specifically, if the prior distribution is a Beta distribution and the likelihood function is a Binomial distribution, the posterior distribution is also a Beta function. Since Binomial distribution is appropriate for component failure on demand, in the PSS, the plant-specific component failures on demand were assumed to fit a Binomial distribution and

a Beta distribution was assumed for the generic component failures on demand.

Similarly, if the prior distribution is a Gamma distribution and the likelihood function is a Poison distribution, the posterior distribution is also a Gamma distribution. For the component's hourly failure rates in the PSS, a Poison distribution was assumed for the plant-specific failure rates and a Gamma distribution was assumed for the generic component failure rates.

The choice of Beta and Binomial distributions for the prior distribution and likelihood function when dealing with Bayesian updating of demand failure data is appropriate. Similarly, the choice of Gamma and Poison distributions for the prior distribution and likelihood functions when dealing with Bayesian updating of hourly component failure rates is also appropriate (18). The basic question raised is whether it is appropriate to Bayesian update all the plant-specific component failure data irrespective of differences between the plant-specific and generic evidence. This point can be better explained by looking at the plant-specific, generic, and Bayesian updated component failure data developed in the Haddam Neck PSS and shown in Tables 6-1 and 6-2 for component failures on demand and hourly component failure rates.

As can be seen, for most components the plant-specific experience is fairly close to the generic data. But there are several components where plant-specific data is substantially different than the generic data. These components include diesel generators failure to start, turbine driven auxiliary feedwater pump failure to start, charging pumps failure to start, battery chargers no electric output, inverters no electric output, component cooling water pumps failure to run, and service water pumps failure to run. For these components, there is an order of magnitude difference between the plant-specific and generic data.

If the difference between the plant-specific and generic failure rates for these components is due to the statistical dispersion of the data, then Bayesian updating of these components is appropriate. But if the observed differences are due to non-statistical reasons, i.e., they are due to differences in equipment quality, environment, or test and maintenance

Table 6-1. Review of the Haddam Neck Plant-Specific Components Failure on Demand

Component Failure Mode	Plant-Specific Data: Failures	Plant-Specific Data: Demands	Mean Failure on Demand	Generic Mean Failure on Demand WASH-1400 (5)	Updated Mean Failure on Demand
1. Diesel Generators Failure to Start	2	642	3.12E-3	3.75E-2	5.35E-3
2. Diesel Fire Pumps Failure to Start	2	790	2.53E-3	1.40E-2(1)	3.12E-3
3. Electric Fire Pumps Failure to Start	1	654	1.53E-3	1.25E-3	1.34E-3
4. Turbine-Driven Auxiliary Feedwater Pumps Failure to Start	2	479	4.18E-3	2.58E-2(2)	1.32E-2
5. LPSI Pumps Failure to Start	1	279	3.58E-3	1.25E-3	1.64E-3
6. HPSI Pumps Failure to Start	1	321	3.12E-3	1.25E-3	1.60E-3
7. RHR Pumps Failure to Start	0	358	<2.79E-3	1.25E-3	1.0E-3
8. CCW Pumps Failure to Start	0	136	<7.35E-3	1.25E-3	1.14E-3
9. Boric Acid Pumps Failure to Start	2	1069	1.87E-3	1.25E-3	1.52E-3

Table 6-1. Review of the Haddam Neck Plant-Specific Components Failure on Demand (cont'd)

Component Failure Mode	Plant-Specific Data: Failures	Demands	Mean Failure on Demand	Generic Mean Failure on Demand WASH-1400 (5)	Updated Mean Failure on Demand
10. Service Water Pumps Failure to Start	1	539	1.86E-3	1.25E-3	1.42E-3
11. Charging Pumps Failure to Start	5	259	1.93E-2	1.25E-3	4.04E-3
12. C.A.R. Fans Failure to Start	0	337	<2.97E-3	3.75E-4	3.50E-4

1. Source of generic data is IEEE Std 500 (14)
2. Source of generic data is Millstone Unit 3 Probabilistic Safety Study (4)

Table 6-2. Review of the Haddam Neck Plant-Specific Hourly Components Failure Rate

Component Failure Mode	Plant-Specific Data: Failures	Hours	Mean Failure Rate (Per Hour)	Generic Mean Failure on Rate (Per Hour) WASH-1400 (5)	Updated Mean Failure Rate (Per Hour)
1. Battery Chargers No Electrical Output	6	175,200	3.43E-5	1.83E-6[1]	1.28E-5
2. Batteries No Electrical Output	2[3]	175,200	1.14E-5[3]	3.75E-6	5.82E-6
3. Invertors No Electrical Output	1	350,400	2.85E-6	2.39E-5[2]	4.41E-6
4. Diesel Generators Failure To Run	1	880	1.14E-3	7.99E-3	1.29E-3
5. RHR Pumps Failure to Run	0	14,400	<6.94E-5	7.99E-5	9.72E-6
6. C.A.R. Fans Failure to Run	0	262,800	<3.81E-6	2.66E-5	6.09E-7
7. Component Cooling Water Pumps Failure to Run	1	175,200	5.71E-6	7.99E-5	6.57E-6

Table 6-2. Review of the Haddam Neck Plant-Specific Hourly Components Failure Rate (cont'd)

Component Failure Mode	Plant-Specific Data: Failures	Plant-Specific Data: Hours	Plant-Specific Data: Mean Failure Rate (Per Hour)	Generic Mean Failure on Rate (Per Hour) WASH-1400 (5)	Updated Mean Failure Rate (Per Hour)
8. Service Water Pumps Failure to Run	1	219,000	4.57E-6	7.99E-5	5.27E-6
9. Charging Pumps Failure to Run	1	74,997	1.33E-5	7.99E-5	1.51E-5

1. Source of generic data is IEEE Std 500 (14)
2. Source of generic data is Millstone Unit 3 Probabilistic Safety Study (4)
3. In Section 4.1 of PSS two failures for batteries are shown. Later in Section 4.2.1 of PSS it is indicated that only one failure is appropriate. This was not corrected in Section 4.1 of PSS. In our analysis we assumed one failure for batteries.

procedures, then the plant-specific data might not belong to the generic population, in which case Bayesian updating of the data would not be appropriate.

To examine this, it is proposed to test a null hypothesis that all the components' mean plant-specific failures are the same as the generic failures, i.e., any difference between the two means are merely due to chance or random dispersion of the data. If the test is positive, the hypothesis is accepted, which means that there is no statistical difference between plant-specific and generic data. In this case, Bayesian updating of the generic data using plant-specific data as performed in the Haddam Neck PSS would be appropriate.

If the hypothesis is rejected, this implies that there is a significant difference between the two groups of data and in this case Bayesian updating of the generic data using plant-specific data would not be appropriate. For those components in which the null hypothesis is rejected, it is recommended that plant-specific data with no modifications be used.

Let λ_g and λ_{ps} represent the generic and plant-specific mean component failure rates. In this analysis it is assumed that both generic and plant-specific component failure data are lognormally distributed (18). The null hypothesis in this case is that $\lambda_s = \lambda_{ps}$, i.e., the generic and plant-specific samples are taken from two populations with the same mean.

Since both the generic and plant-specific mean failure rates are assumed to be normally distributed in log space, the difference between the means would also be normally distributed in log space. The mean of this normal distribution in log space would be:

$$\mu_D = \mathrm{Ln}\lambda_g - \mathrm{Ln}\lambda_{ps} \qquad (6.1)$$

and the standard deviation of this normal distribution in log space would be:

$$\sigma_D = \sigma_g^2 + \sigma_{ps}^2 \qquad (6.2)$$

where σ_g and σ_{ps} are the variances of the log of the generic and plant-specific failure rates.

The generic data that is assumed to be lognormally distributed is usually presented in tables containing a median value, a mean value (λ_g) and an error factor (EF). The lognormal variances of the generic data are found using the following relationship.

$$\sigma_g = EF/Z_{1-\gamma} \tag{6.3}$$

where

EF is the error factor of the lognormal distribution for the generic data, and $Z_{1-\gamma}$ is the 100(1-) percentile of standard normal distribution

For the plant-specific data, the observed component failure rate, λ_{ps}, is considered to be the mean value of the distribution. The variance of the means of the plant-specific data is assumed to be equal to the square of the standard error (SE) of the plant-specific data (19). Assuming the plant-specific data to be lognormally distributed, the lognormal variance of the plant-specific data can be found using the following relationships:

$$\lambda_{ps} = \exp(\xi + \sigma_{ps}^2/2) \tag{6.4}$$

$$SE^2 = \exp(2\xi + \sigma_{ps}^2) \quad \exp(\sigma_{ps}^2)-1 \tag{6.5}$$

$$\text{median} = \exp(\xi) \tag{6.6}$$

Equations 6.4, 6.5, and 6.6 are also used to determine the variance of the generic data.

The normal distribution for the difference between the two means in log space can be transformed to a standardized normal distribution using the standardized variable Z given by

$$Z = \frac{\left| \text{Ln } \lambda_g - \text{Ln } \lambda_{ps} - 0 \right|}{\sqrt{\sigma_g^2 + \sigma_{ps}^2}} \qquad (6.7)$$

To test how well the plant-specific and generic data match, the "significance level" for each pair of plant-specific and generic failure on demand or failure rates can be calculated using the relationship

$$SL = 2(1-\gamma) \qquad (6.8)$$

where γ is the cumulative area under a standardized normal curve from $-\infty$ to the value of Z calculated using Eq. 6.7. Thus, the higher the significance level the better is the match between the generic and plant-specific data. If there is a perfect match, Z is equal to zero and the area under the curve would be half of the normal distribution 0.5 and SL is 1.0, i.e., 100% match. If there is no match, Z would be a very large number and the area under the curve would be equal to 1.0 and SL would be zero, i.e., 0% match.

The next step is to choose different levels of significance for accepting or rejecting the hypothesis. The criteria chosen for deciding whether a plant-specific component is part of the generic population or not is as follows:

a. The null hypothesis that there is no difference between the generic and plant-specific means will be rejected if SL is less than 1%. This implies that if the difference between the means of the generic and plant-specific data represented by the variable Z falls in the lower range of 0 to 0.5% or upper range of 99.5% to 100% of the standard normal distribution, then the hypothesis is rejected, i.e., there is significant difference between the two populations. In this case it is recommended that the plant-specific data be used without any Bayesian updating.

b. If the SL is between 1% and 10%, i.e., the variable Z falls in the lower range of 0 to 5% or upper range of 95% to 100% of the standard normal distribution, the analyst should not use statistical considerations to decide if the hypothesis should be accepted or not. The decision whether to Bayesian

update or to use plant-specific data is normally a qualitative engineering judgment. The analyst's confidence in both the generic and the plant data should enter into his decision, but the main input will normally be based on his knowledge of the plant. Issues such as relative magnitude of the failure rates, perceived test adequacy, equipment location and environment, and the effected system characteristics (temperature, pressure, voltage, etc.) will influence the determination as to whether the equipment should be perceived as part of the "generic" population.

c. If the SL is above 10%, the null hypothesis will be accepted. This implies that if the difference between the plant-specific and generic means represented by variable Z falls between 5% to 95% of the standard normal distribution, it is concluded that both means are part of the same population. In such cases, Bayesian updating of the generic data using plant-specific failure rates as performed in the Haddam Neck PSS would be appropriate.

For cases in which no failures have been observed in the plant-specific data, a failure rate estimator developed by E. Welker and M. Cipow (20) is used in conjunction with the generic information. The failure rate estimator essentially assigns one-third of a single failure to the equipment with no observed failures, then divides this by the actual time or number of demands observed in the plant to estimate the failure rate of the component. Reference 20 shows that this estimator is numerically reasonable for cases with adequate plant data but no observed failures. This method clearly produces a more reasonable point estimate for components with no observed failures than other methods such as the upper bound 95% χ^2 approximation that has been used in other studies.

It is important to note that the "one-third failure" estimator cannot logically be used for cases in which there is inadequate plant experience (run time or demands) to establish a failure rate. Additionally, since the plant experience is inconclusive, it also should not be used as a prior in a Bayesian update. Therefore, if the plant experience in terms of number of demands or run time for a component is so small that the one-third

estimator produces failure rates larger than generic data, the generic failure rates or failure on demand should be used. Once the plant experience indicates better than generic equipment performance, then the failure rate or failure on demand produced by the one-third estimator should be used for the component.

Before discussing the results, it should be noted that the generic component failure data used in the PSS is based on the WASH-1400 suggested data. This generic data base was updated during the Interim Reliability Evaluation Program (IREP) and some of the component failure rates and error factors were changed (11). Table 6-3 shows the generic data used in the PSS based on WASH-1400 data and the updated IREP data which is our suggested generic data. In testing the differences between plant-specific and generic component failure rates mentioned above, and Bayesian updating of the generic data using plant-specific component failure rates, we have used the updated IREP generic data base.

Table 6-4 shows the results of the test. As can be seen, for three components, namely diesel generator failure to start, inverters no electric output, and battery charger failure to operate, the null hypothesis that the mean plant-specific and generic failure rates are from the same populations are rejected at 1% significance level. Thus, for these components the plant-specific failure rates are recommended without any modifications. For batteries chargers, no electric output, the null hypothesis is rejected at 10% significance level. This means that it is up to the analysts to decide if plant-specific data should be used without any modifications or if Bayesian updating would be more appropriate. In this case the significance level is 2% and it is recommended that plant-specific data be used.

In addition, Table 6-4 shows that for RHR pumps, CCW pumps, and CAR fans failure to start and failure to run, there are no observed plant-specific failures. Except for the CAR fans failure to start, for the rest of these components and failure modes, one-third failure estimator is smaller than the generic failure rates. Thus, the one-third failure estimator is recommended for these components. In the case of CAR fans failure to start, the one-third estimator is larger than the generic failure rate. In this case the generic failure to start is recommended for this component.

Table 6-3. Review of the Generic Failure Data Used in the Haddam Neck PSS

Component Failure Mode	Failure Data Used in the PSS WASH-1400 (5) Mean	Median	Error Factor	Suggested Failure Data based on IREP (11) Mean	Median	Error Factor
1. Pumps (Motor Driven)						
Failure to Start	1.25E-3/D	1.0E-3/D	3	2.66E-3	1.0E-3/D	10
Failure to Run	7.99E-5/Hr	3.0E-5/Hr	10	2.66E-5/Hr	1.0E-5/Hr	10
2. Pumps (Diesel Driven)						
Failure to Start	1.40E-2/D(1)			1.25E-3/D	1.0E-3/D	3
Failure to Run	7.99E-5/Hr	3.0E-5/Hr	10	8.48E-4/Hr	1.0E-4/Hr	30
3. Pumps (Turbine Driven)						
Failure to Start	2.58E-2/D(2)			2.66E-2/D	1.0E-2/D	10
Failure to Run	6.15E-4/Hr(2)			1.25E-5/Hr	1.0E-5/Hr	3
4. Manual Valves						
Failure to Operate	1.25E-4/D	1.0E-4/D	3		Same	
5. Motor Operated Valve Failure to Operate	1.25E-3/D	1.0E-3/D	3	2.66E-3/D	1.0E-3/D	10
6. Check Valve						
Failure to Open	1.25E-4/D	1.0E-4/D	3		Same	
Reverse Leakage	3.75E-7/Hr	3.0E-7/Hr	3	5.03E-7/Hr	1.0E-8/Hr	100
7. Air-Operated Valve						
Failure to Operate	3.75E-4/D	3.0E-4/D	3	2.66E-3/D	1.0E-3/D	10
8. Solenoid-Operated Valve						
Failure to Operate	1.25E-3/D	1.0E-3/D	3		Same	

Table 6-3. Review of the Generic Failure Data Used in the Haddam Neck PSS (cont'd)

Component Failure Mode	Failure Data Used in the PSS WASH-1400 (5) Mean	Median	Error Factor	Suggested Failure Data Based on IREP (11) Mean	Median	Error Factor
9. Relief Valve						
Failure to Open	1.25E-5/D	1.0E-5/D	3	2.66E-4/D	1.0E-4/D	10
Premature Open	1.25E-5/Hr	1.0E-5/Hr	3	-		
Failure to Close, given Open	-			2.5E-2/D	2.0E-2/D	3
10. Bus, MCC, Switchgear Faults	7.49E-8/Hr(3)			1.25E-8/Hr	1.0E-8/Hr	3
11. Circuit Breakers >480V						
Failure to Close	3.38E-4/D(3)				Same	10
Failure to Open	1.58E-4/D(3)				Same	10
Failure to Remain Closed	1.52E-6/Hr(3)			7.38E-8/Hr(4)	2.31E-7/Hr(4)	10
12. Circuit Breaker <480V						
Failure to Remain Closed	1.4E-7/Hr(3)				Same	
13. Manual Switch						
Failure to Operate	1.25E-5/D	1.0E-5/D	3	2.66E-5/D	1.0E-5/D	10
14. Pressure & Level Switch						
Failure to Operate	1.25E-4/D	1.0E-4/D	3		Same	
15. Transformer						
No Output	2.5E-6/Hr			1.25E-6/Hr	1.0E-6/Hr	3

Table 6-3. Review of the Generic Failure Data Used in the Haddam Neck PSS (cont'd)

Component Failure Mode	Failure Data Used in the PSS WASH-1400 (5) Mean	Median	Error Factor	Suggested Failure Data Based on IREP (11) Mean	Median	Error Factor
16. Relay						
Failure to Operate	1.25E-4/D	1.0E-4/D	3	2.66E-4/D	1.0E-4/D	10
Failure to Remain Energized	2.66E-7/Hr	1.0E-7/Hr	10	2.66E-6/Hr	1.0E-6/Hr	10
17. Electric Fan						
Failure to Start	3.75E-4/D[1]				Same	
Failure to Run	2.66E-5/Hr[3]			1.21E-6/Hr[1]		
18. Alarms						
Failure to Operate	2.3E-6/Hr[1]					
19. Contact Pair						
Failure to Close	1.35E-4/D[1]					
Failure to Remain Closed	1.25E-7/Hr[1]					
Failure to Open or Remain Open	2.66E-8/Hr[1]					
20. Diesel Generator						
Failure to Start	3.75E-2/D	3.0E-2/D	3		Same	
Failure to Run	7.98E-3/Hr	3.0E-3/Hr	10	2.66E-3/Hr	1.0E-3/Hr	10
21. Battery						
No Electric Output	3.75E-6/Hr	3.0E-6/Hr	3	1.25E-6/Hr	1.0E-6/Hr	3
22. Battery Charger						
No Electric Output	1.83E-6/Hr[1]			1.25E-6/Hr	1.0E-6/Hr	3

Table 6-3. Review of the Generic Failure Data Used in the Haddam Neck PSS (cont'd)

Component Failure Mode	Failure Data Used in the PSS WASH-1400 (5) Mean	Median	Error Factor	Suggested Failure Data Based on IREP (11) Mean	Median	Error Factor
23. Inverter						
No Electric Output	2.39E-5/Hr(2)			1.25E-4/Hr	1.0E-4/Hr	3

(1) Source of generic data is IEEE Standard 500 (14)

(2) Source of generic data is Millstone Unit 3 PSS (4)

(3) Source of generic data other than WASH-1400

(4) Converted from demand failure probabilities of 2.66E-5 and 1.0E-5 assuming monthly tests.

Table 6-4. Results of the Test on Compatibility of the Plant-Specific Data with the Generic Data

Component Failure Mode	Plant-Specific Data Failure Rate or Failure on Demand	Plant-Specific Data Variance	Generic Data Failure Rate or Failure on Demand	Generic Data Variance	Significance Level	Comments
1. Diesel Generator						
Failure to Start	3.12E-3/D	4.84E-6	3.75E-2/D	7.90E-4	0.0	Plant-specific data recommended
Failure to Run	1.14E-4/Hr	1.29E-6	2.66E-3/Hr	4.32E-4	0.6	Bayesian updating recommended
2. Diesel Fire Pump						
Failure to Start	2.53E-3/D	3.2E-6	1.25E-3/D	8.78E-7	0.46	Bayesian updating recommended
3. Electric Fire Pump						
Failure to Start	1.53E-3/D	2.33E-6	2.66E-3	4.32E-5	0.74	Bayesian updating recommended
4. Turbine-Driven Auxiliary Feedwater Pumps						
Failure to Start	4.18E-3/D	8.68E-6	2.66E-2	4.32E-3	0.24	Bayesian updating recommended
5. LPSI Pumps						
Failure to Start	3.58E-3/D	1.28E-5	2.66E-3/D	4.32E-5	0.86	Bayesian updating recommended
6. HPSI Pumps						
Failure to Start	3.12E-3/D	9.67E-6	2.66E-3/D	4.32E-5	0.93	Bayesian updating recommended

Table 6-4. Results of the Test on Compatibility of the Plant-Specific Data with the Generic Data (cont'd)

Component Failure Mode	Plant-Specific Data Failure Rate or Failure on Demand	Plant-Specific Data Variance	Generic Data Failure Rate or Failure on Demand	Generic Data Variance	Significance Level	Comments
7. RHR Pumps						
Failure to Start	0.0	-----	2.66E-3/D	4.32E-5	N/A	1/3 Est. = 9.31E-4/D < generic 1/3 Est. recommended
Failure to Run	0.0	-----	2.66E-5/Hr	4.32E-9	N/A	1/3 Est. = 2.31E-5/Hr < generic 1/3 Est. recommended
8. CCW Pumps						
Failure to Start	0.0	-----	2.66E-3/D	4.32E-5	N/A	1/3 Est. = 2.45E-3/D < generic 1/3 Est. recommended
Failure to Run	5.71E-6/Hr	3.30E-11	2.66E-5/Hr	4.32E-9	0.35	Bayesian updating recommended
9. Boric Acid Pumps						
Failure to Start	1.87E-3/D	1.75E-6	2.66E-3/D	4.32E-5	0.82	Bayesian updating recommended
10. Service Water Pumps						
Failure to Start	1.86E-3	3.44E-6	2.66E-3	4.32E-5	0.83	Bayesian updating recommended
Failure to Run	4.57E-6	2.10E-11	2.66E-5	4.32E-9	0.29	Bayesian updating recommended

Table 6-4. Results of the Test on Compatibility of the Plant-Specific Data with the Generic Data (cont'd)

Component Failure Mode	Plant-Specific Data Failure Rate or Failure on Demand	Plant-Specific Data Variance	Generic Data Failure Rate or Failure on Demand	Generic Data Variance	Significance Level	Comments
11. Charging Pumps						
Failure to Start	1.93E-2	7.31E-5	2.66E-3	4.32E-5	0.19	Bayesian updating recommended
Failure to Run	1.33E-5	1.78E-10	2.66E-5	4.32E-9	0.67	Bayesian updating recommended
12. C.A.R. Fans						
Failure to Start	0.0	-----	3.75E-4	N/A	N/A	1/3 Est. = 9.89E-4/D > generic Generic failure on demand recommended
Failure to Run	0.0	-----	2.60E-6	4.30E-11	N/A	1/3 Est. = 1.26E-6/Hr < generic 1/3 Est. recommended
13. Battery Chargers						
No Electric Output	3.42E-5/Hr	1.95E-10	1.25E-6/Hr	1.0E-12	0.0	Plant-specific data recommended
14. Inverters						
No Electric Output	2.85E-6/Hr	8.0E-12	1.25E-4/Hr	8.78E-9	0%	Plant-specific data recommended
15. Batteries						
No Electric Output	1.14E-5/Hr	6.5E-11	1.25E-6/Hr	1.0E-12	0.0	Plant-specific data recommended

Based on the results of the test discussed above and the updated IREP generic data base, a set of recommended component failure data for all appropriate components was developed. Table 6-5 shows the component failure data used in the PSS and the recommended failure data based on our review and analysis. Because of the statistical differences in component failure data, it was decided that any difference between the PSS component failure data and our suggested component failure data that is less than a factor of 2 should not be considered in the requantification process.

6.2 Review of the Common Cause Failure Analysis

The common cause failure analysis in the Haddam Neck PSS was performed using the binomial failure rate model (12). Common cause failure of similar components in this model can occur due to a common cause shock which randomly fails several components and a lethal shock that fails all the components. The common cause shock rate and lethal shock rates for a given component are assumed to be fixed and are generated from actual data. Data for common cause calculation of pumps (21), valves (12), diesel generators (22), and instrumentation and control assemblies (23) have been collected using actual plant experience. These data are used to generate the parameters necessary for calculation of common cause failure rate for each of the above components in the binomial failure rate model. The period of time covered in the data for different components varies. For example, the data for the pumps covers the actual experience from January 1, 1972 through September 30, 1980 whereas the valve data covers the period from 1976 to 1980. The basic methodology presented in this model is appropriate for common cause calculations, but the data presented in the references cited above is somewhat limited.

To assess the accuracy of the common cause failure probabilities calculated in the PSS for various components, the same calculation was performed using an alternative method and source of data. The alternative method, which is much simpler than the binomial factor method, is the Beta factor methodology (15). The Beta factor in its simplest form is defined as

$$\beta = \frac{n_{ac}}{n_{ac} + n_{ai}} \qquad (6.9)$$

Table 6-5. Review of the Component Failure Data Used in the Haddam Neck PSS

Component Failure Mode	PSS Data Base: Mean Failure Rate or Mean Failure on Demand	PSS Data Base: Source	Suggested Data Base: Mean Failure Rate or Mean Failure on Demand	Suggested Data Base: Source
1. Diesel Generator				
Failure to Start	5.35E-3/D	Bayesian Updating	3.12E-3/D	Plant-Specific data
Failure to Run	1.29E-3/Hr	Bayesian Updating	1.23E-3/Hr	Bayesian Updating
2. Diesel Fire Pump				
Failure to Start	3.12E-3/D	Bayesian Updating	1.71E-3/D	Bayesian Updating
Failure to Run	7.99E-5/Hr	Generic, WASH-1400	2.66E-5/Hr	Generic, IREP
3. Electric Fire Pump				
Failure to Start	1.34E-3/D	Bayesian Updating	1.63E-3/D	Bayesian Updating
Failure to Run	7.99E-5/Hr	Generic, WASH-1400	2.66E-5/Hr	Generic, IREP
4. Turbine-Driven AFW Pumps				
Failure to Start	1.32E-2/D	Bayesian Updating	4.41E-3/D	Bayesian Updating
Failure to Run	6.15E-4/Hr	Millstone 3 PSS	2.66E-5/Hr	Generic, IREP
5. LPSI Pumps				
Failure to Start	1.64E-3/D	Bayesian Updating	3.42E-3/D	Bayesian Updating
Failure to Run	7.99E-5/Hr		2.66E-5/Hr	Generic, IREP
6. HPSI Pumps				
Failure to Start	1.60E-3/D	Bayesian Updating	3.04E-3/D	Bayesian Updating
Failure to Run	7.99E-5/Hr		2.66E-5/Hr	Generic, IREP
7. RHR Pumps				
Failure to Start	1.0E-3/D	Bayesian Updating	9.31E-4/D	1/3 Estimator
Failure to Run	9.72E-6	Bayesian Updating	2.31E-5/Hr	1/3 Estimator
8. CCW Pumps				
Failure to Start	1.14E-3/D	Bayesian Updating	2.45E-3/D	1/3 Estimator
Failure to Run	6.57E-6/Hr	Bayesian Updating	6.42E-6/Hr	Bayesian Updating

Table 6-5. Review of the Component Failure Data Used in the Haddam Neck PSS (Cont'd)

Component Failure Mode	PSS Data Base: Mean Failure Rate or Mean Failure on Demand	PSS Data Base: Source	Suggested Data Base: Mean Failure Rate or Mean Failure on Demand	Suggested Data Base: Source
9. Boric Acid Pumps				
Failure to Start	1.52E-3/D	Bayesian Updating	1.91E-3/D	Bayesian Updating
10. Service Water Pumps				
Failure to Start	1.42E-3/D	Bayesian Updating	1.94E-3/D	Bayesian Updating
Failure to Run	5.27E-6/Hr	Bayesian Updating	5.17E-6/Hr	Bayesian Updating
11. Charging Pumps				
Failure to Start	4.04E-3/D	Bayesian Updating	1.62E-2/D	Bayesian Updating
Failure to Run	1.51E-5/Hr	Bayesian Updating	1.43E-5/Hr	Bayesian Updating
12. C.A.R. Fans				
Failure to Start	3.5E-4/D	Bayesian Updating	3.75E-4/D	Generic Data
Failure to Run	6.09E-7/Hr	Bayesian Updating	1.26E-6/Hr	1/3 Estimator
13. Battery				
No Electric Output	5.82E-6/Hr	Bayesian Updating	5.70E-6/Hr	Plant-Specific data
14. Battery Chargers				
No Electric Output	1.28E-5/Hr	Bayesian Updating	3.43E-5/Hr	Plant-Specific data
15. Inverter				
No Electric Output	4.41E-6/Hr	Bayesian Updating	2.85E-6/Hr	Plant-Specific data
16. Manual Valve				
Failure to Operate	1.25E-4/D	Generic, WASH-1400	Same	
17. Motor Operated Valve				
Failure to Operate	1.25E-3/D	Generic, WASH-1400	2.66E-3/D	Generic, IREP

Table 6-5. Review of the Component Failure Data Used in the Haddam Neck PSS (cont'd)

Component Failure Mode	PSS Data Base: Mean Failure Rate or Mean Failure on Demand	PSS Data Base: Source	Suggested Data Base: Mean Failure Rate or Mean Failure on Demand	Suggested Data Base: Source
18. Check Valve				
Failure to Open	1.25E-4/D	Generic, WASH-1400	Same	
Reverse Leakage	3.75E-7/Hr	Generic, WASH-1400	5.03E-7/Hr	Generic, IREP
19. Air-Operated Valve				
Failure to Operate	3.75E-4/D	Generic, WASH-1400	2.66E-3/D	Generic, IREP
20. Solenoid-Operated Valve				
Failure to Operate	1.25E-3/D	Generic, WASH-1400	Same	
21. Relief Valve				
Failure to Open	1.25E-5/D	Generic, WASH-1400	2.66E-4/D	Generic, IREP
Premature Open	1.25E-5/D	Generic, WASH-1400	-	
Failure to Close, given Open	-		2.5E-2/D	Generic, IREP
22. Bus, MCC, Switchgear				
Faults	7.49E-8/Hr	Generic, Other	1.25E-8/Hr	Generic, IREP
23. Circuit Breaker >480V				
Failure to Close	3.38E-4/D	Generic, Other	Same	
Failure to Open	1.58E-4/D	Generic, Other	Same	
Failure to Remain Closed	1.52E-6/Hr	Generic, Other	7.38E-8/Hr(1)	Generic, IREP
24. Circuit Breaker <480V				
Failure to Remain Closed	1.4E-7/Hr	Generic, Other	Same	
25. Manual Switch				
Fails to Operate	1.25E-5/D	Generic, WASH-1400	2.66E-5/D	Generic, IREP

Table 6-5. Review of the Component Failure Data Used in the Haddam Neck PSS (cont'd)

Component Failure Mode	PSS Data Base: Mean Failure Rate or Mean Failure on Demand	PSS Data Base: Source	Suggested Data Base: Mean Failure Rate or Mean Failure on Demand	Suggested Data Base: Source
26. Pressure & Level Switch				
Failure to Operate	1.25E-4/D	Generic, WASH-1400	Same	
27. Transformer				
No Output	2.50E-6/Hr	Generic, WASH-1400	1.25E-6/Hr	Generic, IREP
28. Relay				
Failure to Operate	1.25E-4/D	Generic, WASH-1400	2.66E-4/D	Generic, IREP
Failure to Remain Energized	2.66E-7/Hr	Generic, WASH-1400	2.66E-6/Hr	Generic, IREP
29. Electric Fans				
Fails to Start	3.75E-4/D	Generic, IEEE Std 500	Same	
Fails to Run	2.60E-5/Hr			
30. Alarms				
Failure to Operate	2.3E-6/Hr	Generic, IEEE Std 500	Same	
31. Contact Pair				
Failure to Close	1.35E-4/D	Generic, IEEE Std 500	Same	
Failure to Remain Closed	1.25E-7/Hr	Generic, IEEE Std 500	Same	
Failure to Open or Remain Open	2.66E-8/Hr	Generic, IEEE Std 500	Same	

(1) Converted from demand failure probability of 2.66E-5 assuming monthly tests.

where

n_{ac} is the number of actual common cause failurres observed for a particular component

n_{ai} is the number of independent failures observed for a particular component

Potential common cause or independent failures defined as events that could have resulted in a failure but were detected before the failure can also be included in the definition of the Beta factor using some weight factors:

$$\beta = \frac{n_{ac}+W_c n_{pc}+1}{(n_{ac}+W_c n_{pc}+1)\ (n_{ai}+W_i n_{pi}+1)} \qquad (6.10)$$

where

n_{ac} and n_{pc} are the number of actual and potential common cause events observed for a particular component

n_{ai} and n_{pi} are the number of actual and potential independent events observed for a particular component

W_c and W_i are the weights associated with the potential common cause and potential independent events, which are basically the analyst's judgment of the probability of each of these potential events leading to an actual failure.

The latest Beta factor data base covers between 10 to 12 years of data for a select number of components (15). This corresponds to about 394 to 503 reactor-years of experience. Table 6.6 shows the Beta factor for the components included in this data base. Using these Beta factors, the common-cause failure probability of the components considered in the PSS was evaluated and is shown in Table 6.7. Because of large uncertainties involved in the common cause calculations, it was decided that any difference between the PSS results and our calculations that is less than a factor of 4 should not be considered in the requantification process.

Based on this criteria, the PSS common cause results for service water system pumps, component cooling water system pumps, charging pumps, residual heat removal system pumps, and auxiliary feedwater system pumps are

Table 6.6 Generic Beta Factors for a Select Group of Components

Component	Generic Beta Factor
Reactor Trip Breakers	0.19
Diesel Generators	0.05
Motor-Operated Valves	0.08
Safety Relief Valves	
PWR	0.07
BWR	0.22
Pumps	
Safety Injection	0.17
RHR	0.11
Containment Spray	0.05
Auxiliary Feedwater	0.03
Service Water	0.03
All	0.10

Table 6.7 Review of the Haddam Neck PSS Common Cause Analysis Results

System Component Failure due to common-cause	PSS Common-cause Unavailability	Non Common-cause Unavailability	Beta Factor ( )	Suggested Common-cause Unavailability
1. AC Power System				
Diesel failure to start	1.3E-3	3.1E-3	0.05	3.0E-4[1]
Diesel failure to run		2.9E-3		
		6.0E-3		
2. Service Water System				
Failure of 3/4 or 4/4 pumps to run	1.7E-6	1.2E-4	0.03	3.7E-6[2,3]
Failure of any 2/3 pumps to run	2.3E-6	1.2E-4	0.03	3.7E-6
Failure of 2/2 pumps to start	2.5E-5	1.9E-3	0.03	5.7E-5
Failure of 2/2 pumps to run	2.1E-6	1.2E-4	0.03	3.7E-6
4/4 pumps fail to start	1.6E-5	1.9E-3	0.03	5.7E-5
4/4 pumps fail to run	1.4E-6	1.2E-4	0.03	3.7E-6
3. Component Cooling Water System				
Failure of 2/3 pumps to start	1.1E-4	1.1E-3	0.03	3.4E-5[4]
Failure of 2/3 pumps to run	5.7E-6	1.5E-4	0.03	4.6E-6[4]
Common cause failure of 2 MOVs to open	1.2E-3	4.2E-3	0.08	3.4E-3
4. Charging System				
Failure of 2/3 to run	2.0E-6	3.4E-4/Hr	0.17	5.8E-5[2]
5. Safety Injection Actuation System				
Failure of 2/3 containment pressure sensors	8.1E-4		-	
Failure of 2/3 pressurizer pressure sensors	3.1E-3		-	

Table 6.7 Review of the Haddam Neck PSS Common Cause Analysis Results (continued)

System Component Failure due to common-cause	PSS Common-cause Unavailability	Non Common-cause Unavailability	Beta Factor ( )	Suggested Common-cause Unavailability
6. HPSI System				
Failure of 2/2 pumps to start	-	3.0E-3	0.17	5.1E-4
Failure of 2/2 pumps to run	2.1E-6	1.0E-4	0.17	1.8E-5(5)
Failure of 2/3 MOVs	7.0E-4	5.4E-3	0.08	4.3E-4
7. LPSI				
Failure to start	-	3.4E-3	0.17	5.8E-4
Failure of 2/2 pumps to run	2.1E-6	5.3E-5	0.17	9.1E-6(6)
Failure of 2/2 MOVs	5.7E-4	4.2E-2	0.08	3.4E-3
Failure of 4/4 air-operated valves (AOVs)	7.0E-4			
Failure of 3/4 AOVs	7.1E-4			
Failure of 2/4 AOVs	8.8E-4			

1. Common cause diesel failure in the PSS includes both failure to start and failure to run.
2. Since only one pump is on standby, only failure to run was considered.
3. Beta factor for the third and fourth pumps is assumed to be 1.0.
4. Service Water system Beta factor was used for component cooling water system.
5. The longest mission time for HPSI is assumed to be 4 hours in the PSS.
6. The longest mission time for LPSI is assumed to be 2 hours in the PSS.

acceptable. The common cause failure probability of diesel generators calculated using Beta factor is smaller than the PSS results, principally due to the fact that the Beta factor methodology links the independent and common cause failure probabilities. Since the Haddam Neck plant-specific diesel failure probability is much lower than generic values, the common cause portion also becomes smaller. Alternataively, the binomial failure rate data corresponds to the generic experience which is worse than the Haddam Neck experience and thus results in a larger common cause failure probability. Other differences include lower common cause failure probability for MOVs using Beta factor methodology and higher common cause failure probability for safety injection pumps which are directly related to the data base used in the two methodologies.

7.0 REVIEW OF THE HUMAN RELIABILITY ANALYSIS (HRA)

The HRA performed in the PSS is a detailed, state-of-the-art, generally well-documented analysis. Two major categories of human actions are considered. The first consists of cognitive actions in response to plant accident conditions. A cognitive action is the detection/diagnosis/decision process which the operator goes through in determining the plant condition and the proper response to that condition. The second category consists of manipulative (or procedural) actions in response to plant accident conditions. A manipulative action is composed of the actual tasks required to control and actuate the pieces of equipment necessary to implement the chosen response. In general, it can be stated that for each cognitive action there is at least one corresponding manipulative action. The analyses of the actions in each category are modeled and quantified differently. A detailed review of the PSS analysis of each category is given in Sections 7.2 and 7.3, respectively. Section 7.1 discusses the overall structure of the HRA pertaining to both categories.

7.1 General Comments on the HRA

An important point to keep in mind regarding the HRA performed in the PSS and this review of it is that HRA is still an art requiring much in the way of analyst judgment. The tools available can provide only guidance in determining human error probabilities (HEPs), and the analyst must temper that guidance with common sense when attempting to incorporate the effects of various performance shaping factors and other parameters. Both the PSS and the review contain substantial amounts of judgment, and no rigid rules were adhered to other than that both have as their goal the reasonable estimation of HEPs which will reflect the contribution of human error to core damage frequency. In keeping with this, in the instances where the reviewers disagreed with the judgments of the PSS analysts, every effort was made to address only those areas which appeared to have the <u>potential</u> to significantly change the HEPs used or the final results of the PSS.

7.1.1 The Overall HRA Process and Documentation

The HRA was performed using the Systematic Human Action Reliability Procedure (SHARP) taken from EPRI NP-3583 (24). SHARP is not an HRA

modeling technique, but rather a structured process for the selection, integration, quantification and documentation of human errors in a PRA. The SHARP process is the most complete and scrutable tool available to assist in the structuring of an HRA. Table 7.1 presents a description of the steps used in SHARP. The application of this process in the PSS is quite complete and the analysis is clear, concise, and, with one exception, complete in its presentation of the HRA process and results. The exception pertains to the quantification of cognitive errors, in which the raw data required by the quantification model is not fully presented or explained. The detailed information does exist, in an understandable and usable form, in an analysis file at the utility offices, but no summary is given in the PSS. Considering the importance of these errors in the results of the PSS, the information should have been included. Despite this problem, the human reliability analysis presented in the PSS is the most complete application of the best available HRA process (SHARP) of any nuclear plant PRA performed to date. This statement holds true in the overall sense, and the specific review comments contained in Sections 7.2 and 7.3 regarding disagreements in the treatment of individual operator responses should not in any way be construed to contradict our conclusion regarding the high quality and state-of-the-art nature of the HRA process and modeling techniques used in the PSS.

7.1.2 Treatment of the Effect of Loss of Instrumentation

For a long time, it has been recognized that failures which result in a loss of plant instrumentation can affect the ability of the operators to successfully respond to accident conditions. Thus, it is possible that, given the same initiating event and desired plant response, the human error probability for a particular action may be different if in one case all instrumentation is available and in another case some instrumentation has failed. The failure of single instruments is most likely not cause for concern; the real problem comes about when an accident is accompanied by the failure of a major instrumentation bus or emergency AC power train. This phenomenon has generally not been treated in PRAs. The PSS, however, has made a concerted effort to "get a handle on it;" the treatment of the effect of loss of instrumentation on human reliability is substantially more advanced than in any other PRA, including those performed by the same utility for Millstone 1 and Millstone 3.

TABLE 7.1 Description of SHARP Steps (Ref. 24)

STEP 1 - DEFINITION

OBJECTIVE: Ensure that potentially important human influences are included in the plant logic models.

INPUT: Initiating events, preconstructed event trees and fault trees.

ACTIVITIES

(1) Identify functions that humans perform at each branch point in preconstructed event trees.

(2) Select a classification system suitable for describing the types of human interactions modeled in PRA studies (e.g., before, at, and after initiating events) in operation, maintenance and test.

Use the classification system to ensure that significant human interactions are identified (i.e, evaluate for each type of human interaction each fault tree to enhance completeness).

(3) Perform additional completeness checks by examining other key human interactions through review of additional information (e.g., emergency procedures, maintenance and test operations, incident writeups, past PRA studies, reports/data from simulator training, and interviews with plant personnel).

OUTPUT: Enriched tentative logic structure for human interactions (e.g., ETs and FTs) to achieve reasonable degree of completeness.

This step is led by the systems analysts.

STEP 2 - SCREENING

OBJECTIVE: Reduce the number of human interactions for more detailed examination by applying a screening technique.

ACTIVITIES

(1) Establish a screening technique to rank and select key interactions for detailed analysis. The typical techniques are based on (1) judgment (e.g., location in the tree logic), (2) coarse screening (e.g., by evaluation of the human impact in hardware cut-sets) or (3) fine screening (e.g., quantifying both generic hardware failures and human interactions based on behavior type).

(2) Apply the selected screening technique to the plant logic models from Step 1.

(3) Select those interactions which are above an identified cut-off parameter that is compatible with the initial screening technique (e.g., 1% impact on the frequency of events, relative probability is less than 1% of other human interactions, or likelihood of affecting core-melt is judged to be small).

OUTPUT: A list of key human interactions identified by screening process for more detailed examination.

This step is typically performed by the systems analyst with support from the human reliability data base or data analyst.

STEP 3 - BREAKDOWN

OBJECTIVE: Provide a detailed description of each key human interaction by task and subtask and include influence parameters.

ACTIVITIES

(1) Breakdown the types of human interactions into specific tasks and subtasks associated with specific equipment or procedures.

(2) Scrutinize operating experience (e.g., plant specific event writeups, licensee event reports and events from other plants) for these tasks and subtasks to identify mishaps and corrective actions taken.

(3) Enhance the task/subtask descriptions by including the appropriate influence parameters (e.g., the behavior type, method of detection, time allowed, alarms available, feedback for action, coordination required, stress level, and performance factors) to establish the basis for selecting a model or representation of the human interaction.

OUTPUT: Details of the breakdown of each key human interaction in matrix format of tasks/subtasks versus influence parameters.

This step is typically led by a system analyst having significant HRA experience with support from the cognitive psychologists, plant or training personnel and other system analysts.

STEP 4 - REPRESENTATION

OBJECTIVE: Represent key human interactions for subsequent quantification and examination of impact in event and fault trees.

ACTIVITIES

(1) For each human interaction select a representation (e.g., THERP, OAT, etc.).

(2) Determine availability of data and/or expert opinion to support selected representation. If not available, consider alternate representations.

(3) Apply selected representation to develop specific descriptions of human interactions (e.g., alternate choices or mistakes).

OUTPUT: A representation describing human interaction successes and mistakes suitable for assessing the impact on associated dependencies in the fault trees and event trees.

This task is led by the human reliability analyst.

TABLE 7.1 Description of SHARP Steps (Continued)

STEP 5 - IMPACT ASSESSMENT

OBJECTIVE: Assess and incorporate impacts of insights derived from the representations of human interactions.

ACTIVITIES

(1) Evaluate derived human interactions (e.g., alternative choices or mistakes) for their impact on initiating events, common-cause failures, system reliabilities, event tree logic, and sequence quantification. Choose candidates for re-screening and grouping.

(2) Analyze the impact of derived human interactions by applying the screening techniques of Steps 1 and 2, to help group and screen in particular those affecting equipment reliability, dependencies between redundant system elements, initiating event groupings and linking event trees.

(3) Define how the derived human interactions should be grouped for quantification (e.g., coalesce many actions into a few by impact on consequences).

OUTPUT: Fault tree and event tree structures refined to include the key human interactions and recommended groupings for quantification.

This step is typically led by the systems analyst with input and discussion with the human reliability analyst.

STEP 6 - QUANTIFICATION

OBJECTIVE: Provide probabilities of success and failure of human interactions.

ACTIVITIES

(1) Quantify the probability for the key human interactions identified in Steps 4 and 5 by selecting the most appropriate data base, which might include:

a) Time-reliability curves

b) Direct data from events

c) Published human-error data

d) Opinions of experts

(2) State the key dependencies, uncertainties, and sensitivities in the quantification, based on results of representation and influence factors.

OUTPUT: Quantified probabilities of human interaction related to fault and event trees, including uncertainties and sensitivities.

This step is performed by the human reliability analyst and is reviewed by the systems analyst. It may be reviewed by plant operating personnel and others as needed.

STEP 7 - DOCUMENTATION

OBJECTIVE: Produce an accurate description of the process used to develop the quantitative assessments.

ACTIVITIES

For each event tree:

(1) Document data, assumptions, models, and representations.

(2) List important dependencies and sensitivities such as decisionmaking, quantification, times for action, etc.

(3) Develop a quantitative statement of the human impact on core-melt frequency.

OUTPUT: A document describing the human interactions modeled in the PRA study.

This step is carried out by the human reliability analyst in conjunction with the system analyst. Support from all others involved may be needed.

Since the PSS uses a support state methodology (discussed elsewhere in this report), the state of the various instrumentation and AC power busses is explicitly identified and known for quantification of each event tree. Therefore, just as the mechanical failure probability of a system is adjusted based on the support state, so too can the HEPs be adjusted for the various cognitive and manipulative actions. (It should be added that this is one area in which the support state method, notwithstanding its other faults mentioned elsewhere in the report, is preferable to fault tree merging. While fault tree merging better handles the support system interfaces with other support systems and front-line systems, it would be extremely difficult to adjust the HEPs since they would not only be sequence-dependent but cut set dependent as well. This would necessitate a cut set-by-cut set adjustment of the HEPs.)

The HEP adjustment factors used are applied to both the cognitive and manipulative errors. The adjustment factors are x2 (for partial loss of instrumentation), x5 (for various station blackout conditions), and a ceiling HEP of 0.5 (for almost complete loss of instrumentation). The PSS table giving the adjustment factors is reproduced in this report as Table 7.2. The factors are apparently based primarily on judgment with some consideration of basic information contained in Chapter 17 of NUREG/CR-1278 (25), and thus their accuracy could be argued based on a different interpretation of the available information. Further, the use of a single adjustment factor for all actions during a given support state is an oversimplification, since some actions would likely be affected more than others. However, nothing would be gained by disputing the exact numbers chosen since there is really no experience data base upon which to base a particular set of numbers. It is obvious that some level of adjustment is more realistic than no adjustment at all, and the values selected are certainly within the range of believability. Further, any attempt to "fine tune" the factors would be inappropriate considering the level of uncertainty in the HRA to begin with. What is important is that the PSS has attempted to deal with a significant deficiency in previous HRAs. In doing so, it has used a reasonable approximation of the relative HEPs for identical actions taken under various conditions and therefore provides a valuable insight regarding the importance of these support states to the overall study results. We find the approach and the selected model to be acceptable and a very good effort compared to previous PRAs.

TABLE 7.2 Adjustment to HEPs for Support State

Support State Description	Stress Modifier (Factor)
Nothing Failed	None
Service Water	None
Single DC Bus	2
Single DC Bus and Service Water	2
Both DC Buses and Service Water	0.5*
Both DC Buses and MCC-5	0.5*
Both DC Buses, Service Water and MCC-5	0.5*
Offsite Power	None
Offsite Power and MCC-5	5
Offsite Power and either: DC Bus 1 and EAC Bus 8, or DC Bus 2 and EAC Bus 9	5
All Support Systems	0.5*
MCC-5	5
Both DC Buses	0.5*
Offsite Power and Both EAC Buses	5 before AC recovery, None after recovery
Offsite Power and either: DC Bus 1 and Both EAC Buses, or DC Bus 2 and Both EAC Buses	5 before AC recovery, 2 after AC recovery
Offsite Power, MCC-5 and either: EAC Bus 8, or DC Bus 1, or EAC Bus 9, or DC Bus 2	5 except for 018 and RMC (no stress factor)

* represents absolute error probability rather than a factor

7.1.3 Consideration of Operator Misdiagnosis

In the PSS, the evaluation of human errors deals generally with whether the operator will make the proper response or will make no response at all. That is, the error is considered to be one of failing to take action to improve the plant conditions. This does not account for the possibility that the operator will take an action which he believes correct but which is in reality incorrect because he has not properly diagnosed the plant conditions. In this case the operator could turn a relatively stable situation into a serious accident. The analysis of this type of mistake is quite complex, and is complicated by the fact that there is no quantification tool available that indicates how to estimate the probability of these errors. Nonetheless, the PSS should have provided a discussion of potential errors of this type and indicated whether they might be significant. This review identifies and discusses these errors in an abbreviated manner.

The first step in the process is to consider which events could reasonably be expected to be misinterpreted by operators. For example, it is not reasonable to assume that the operator could misdiagnose a large LOCA as a turbine trip transient. Nor is it likely that he would misdiagnose a station blackout as a reactor trip (or, for that matter, as anything else given the highly unique and obvious symptoms of station blackout). However, he could misdiagnose a steam generator tube rupture as a small-small LOCA, since many of the symptoms are similar and the operator could potentially miss those symptoms which are different.

The second step in the process is to determine which potential misdiagnoses could affect the operator's response significantly enough to degrade a situation. Again, by way of example, the operator could easily confuse a turbine trip with a loss of main feedwater, or a small-small LOCA with a small LOCA. However, these events can easily be confused precisely because they are so similar that any operator response would follow the same pattern and utilize the same procedures regardless of which event had occurred. Thus, the misdiagnoses in these cases would have no adverse affect on either operator or plant response.

After applying these two steps, three potential misdiagnoses were identified which might be a problem at the plant, but upon further

examination were found not to constitute a problem. The three potential errors are:

1. Operator misdiagnoses a small-small LOCA as a transient with inadvertent safety injection.

2. Operator misdiagnoses a steam generator tube rupture (SGTR) as a small-small LOCA.

3. Operator misdiagnoses a SGTR as a transient with inadvertent safety injection.

In each of the above cases, the procedures used to respond to the plant upset condition were reviewed and the operator was assumed to have missed the key symptoms that would have indicated the proper condition. That is, the assumption is that the operator was initially aware only of the symptoms shared by the two events in each case. In every case, the actions that would be taken in response to the common symptoms would not degrade the situation to the point of imminent core damage, and in fact in some cases the actions taken would be sufficient to terminate the event successfully even if the operator never properly diagnosed the event. (This is particularly notable in sequences involving SGTR.) In all cases, backup verifications in the procedures to check certain symptoms repeatedly (in some cases even prior to taking any actions significant to the misdiagnosis scenario) would provide ample opportunity for recovery. Finally, continual monitoring of the critical safety functions by the shift supervisor provides a final backup for functional recovery.

Thus, it is highly unlikely that operator misdiagnosis would occur. Stated another way, it is more likely that the operator will fail to respond in time (fail to take action) than that he will take erroneous actions based on a misdiagnosis. Therefore, the fact that the PSS treated all cognitive operator response errors as nonresponses rather than improper responses is not expected to materially affect the results. This is due in large part to the symptom-oriented procedures being implemented at the plant which formed the basis for the HRA in the PSS. In most cases, the diagnosis of the exact cause of the plant condition is not required for proper operator response. In those cases in which eventual exact diagnosis is

required, the symptomatic responses called for in the procedures, along with backup verification and critical safety function monitoring, are sufficient to reduce the likelihood of significant misdiagnosis error to below the point at which it would affect the results.

7.2 Review of the Cognitive Human Error Analysis

The PSS has identified a series of cognitive human errors associated with the diagnoses and decisions that may be required from the operator to assess plant conditions and select a course of action in response to the initiators (and subsequent system failures) modeled in the PSS. The cognitive errors evaluated are listed in Table 7.3. In addition to these cognitive errors, there are some other cognitive errors that were incorporated into the evaluation of manipulative errors. These are discussed in Section 7.3. This review indicates that the errors evaluated constitute a generally complete list of those decisions that are (a) desirable in one or more event sequences and (b) clearly called for in the plant procedures. No credit is given in the PSS for "creative" decisions that are not included in the procedures. There are two areas which do not fit into this general conclusion. These include the need to add credit for an additional cognitive action and the need to specifically call out a cognitive error that was incorporated into a manipulative action in the PSS. These two areas are discussed further in Section 7.2.3.

Cognitive errors are generally incorporated into the PSS at the event tree level. That is, each error is used as a distinct top event on the appropriate event trees and is defined as such. The only exceptions to this are the cognitive errors that are incorporated into manipulative errors. These are discussed in Section 7.3. Incorporating cognitive errors at the event tree level helps to clearly identify the decisions required of the operators and to easily assess the contribution of these errors to core damage frequency. Further, it simplifies the modeling of dependencies between various cognitive errors and between the errors and the plant systems.

The approach used in the SHARP process (discussed in Section 7.1) calls for conducting a screening analysis to determine which decisions are potentially important to the final estimate of core melt frequency and then

TABLE 7.3 Cognitive Operator Actions Evaluated in the PSS

Operator Action	Description
OA-1	Operator Recognizes Need to Initiate Low-Pressure Recirculation
OA-2	Operator Recognizes Need to Initiate High-Pressure Recirculation
OA-3	Operator Recognizes Need to Depressurize the RCS in Response to an Unisolable RCP Seal Failure
OA-4	Not Used
OA-5	Operator Correctly Identifies and Decides to Isolate the Affected Steam Generator Following an SGTR Event
OA-6	Operator Decides to Use Loop Isolation Valves to Isolate the Affected Loop Following an SGTR Event
OA-7	Operator Correctly Identifies, Locates and Decides to Isolate a Steamline Break
OA-8	Operator Recognizes Need to Perform Bleed-and-Feed Cooling
OA-9	Operator Correctly Identifies, Locates and Decides to Isolate a Main Feedline Break
OA-10	Not Used
OA-11	Not Used
OA-12	Operator Decides to Manually Trip the Reactor Following a Total Loss of Service Water or an ATWS
OA-13	Operator Recognizes Need to Shift Control Air Supplies and Provide Well Water Cooling
OA-14	Operator Recognizes Need to Restore Both D.C. Power Supplies (Not Credited)
OA-15	Operator Recognizes Need to Restore Semi-Vital A.C. Power

TABLE 7.3 Cognitive Operator Actions Evaluated in the PSS (Continued)

Operator Action	Description
OA-16	Operator Recognizes Need to Initiate Emergency Boration
OA-17	Operator Recognizes Need to Recover Main Feedwater
OA-18	Operator Recognizes Need to Recover Power to MCC-5
OA-19	Operator Recognizes Need to Manually Control Charging Flow Given a Total Loss of DC Power

refining the analysis of the important decisions by performing a detailed analysis of those decisions. This generally was done in the PSS for the cognitive decisions considered. This review is structured in the same manner. A detailed review has been performed of the cognitive decisions found to be important in the PSS (OA-1, OA-2, OA-8, and OA-18) in an attempt to confirm that appropriate estimates of the HEPs were used in the final quantification. (Note that the PSS uses three-character abbreviations of these actions because of limitations in their computer codes. Thus, OA-1 becomes OA1 and OA-18 becomes O18.) For the other cognitive decisions, the review was simply intended to assure that the screening HEP values used were not overly optimistic. For cognitive decisions added by this review, or for cognitive decisions for which changes in assumptions or parameters are suggested by the review, the HEP values were developed by the review team in a manner consistent with a PSS final (rather than screening) quantification.

The human error probabilities for the cognitive decisions were estimated in the PSS by using four different models and combining them based on the judgment of the analysts. The primary model used was the human cognitive reliability (HCR) model (26). This model is the most sophisticated model presently available and is designed to take into account the time available for action, the time required to make a diagnosis and decide on a course of action, the stress level of the situation, the quality of the control room interface, the level of training of the crew, and the type of behavior expected. A description of each of these parameters is given in Table 7.4. The problem with using this model is that in many cases there is insufficient data available to assess the median response time (the time required to make a diagnosis and decide on a course of action) and the model is extremely sensitive to the selection of this parameter. Another problem is that the model is new and has not been sufficiently validated, especially at the low HEP end of the model. In order to deal with this, three other models were also utilized. One was the Wreathall time reliability correlation (TRC) from NUREG/CR-3010 (27). Another was the Swain TRC from NUREG/CR-1278 (25). These correlations take into account only the thinking time available to decide on a course of action, and thus are less sophisticated. However, that parameter is much easier to assess than the series of parameters required for HCR. The fourth model is the behavioral screening model from Appendix A of SHARP (24), which assigns an HEP based solely on the behavior type and stress level.

TABLE 7.4 Description of HCR Model Parameters (Ref. 26)

TIME AVAILABLE:

The amount of time available to the crew from the beginning of a stimulus which would solicit a response to the time by which the crew must begin the required manipulative actions.

MEDIAN RESPONSE TIME:

The median time taken by a crew (from the beginning of the stimulus) to diagnose the situation and decide upon a course of action.

BEHAVIOR TYPE:

1. The behavior can be classed as skill-based if the operator is well trained, is motivated to perform the task, and has experience in performing the task with no ambiguity, OR

2. The behavior can be classed as rule-based if the operator has a clearly understood set of rules to follow in responding to a well understood transient of situation, OR

3. The behavior can be classed as knowledge-based if the above do not apply or the operator must understand the condition of the plant, interpret some of the instrument readings, or make a difficult diagnosis.

OPERATOR EXPERIENCE LEVEL:

1. Expert, well trained, OR
2. Average knowledge and training, OR
3. Novice, minimum training.

STRESS LEVEL:

1. Situation of grave emergency, OR
2. Situation of potential emergency, OR
3. Active, no emergency, OR
4. Low activity, low vigilance.

QUALITY OF OPERATOR/PLANT INTERFACE

1. Excellent, OR
2. Good, OR
3. Fair, OR
4. Poor, OR
5 Extremely poor.

For the screening analysis, the PSS analysts developed an HEP for each cognitive decision using each of the four methods mentioned above, except that a cutoff of 0.001 was used. That is, if a model resulted in a calculated value less than 0.001, the cutoff value was used instead. The screening value used for each decision was a combination of the values from each model, although the particular combination varied for each given decision. For example, in some cases all four values were averaged. In other cases, one value may have been an outlier and was discarded. In other cases, the high and low values were discarded. In still other cases, HCR was used alone. For the final quantifications of the important decisions, the models were reviewed and, where possible, the parameters were refined. If necessary, distributions were applied to upper and lower bound HEP estimates and mean HEPs were calculated. Also, values lower than 0.001 were permitted if it was felt the case warranted it. The reasons for each approach are not discussed in the PSS. In fact, there is insufficient information included in the PSS to determine how any of the cognitive decisions were actually quantified. That information is contained only in the utility calculation file in the utility offices. This is an important deficiency in the documentation in the PSS, and is particularly important given the nature and importance of the HRA. The review team was given access to this file at the utility's offices and the review of the quantification is based on this limited access. Insofar as possible, the reasons for a particular approach being used were reviewed for each cognitive action and it was determined that, by and large, they were reasonable.

The review team offers no criticism of the overall method used to quantify these cognitive decisions and recognizes that HRA (especially in the cognitive arena) is still very much an art requiring the extensive use of judgment. In keeping with that, our specific comments (Section 7.2.1 and 7.2.2) are limited to those that may have an effect on the results and that pertain to judgments that might be inappropriate. However, as noted before, the documentation in the PSS is inadequate for an area of such extreme importance; the limited time available for access to the utility files made the review process very difficult.

One other general area that warrants discussion is the manner in which the PSS handled dependent (or conditional) cognitive actions. This was done in a straightforward manner. If two decisions occur in the same

thought path, the conditional error probability (HEP) of the second decision, given that the first decision is incorrect, is given by the following equation:

$$P(B|A) = P(B)/P(A)$$

For example, if A is OA-9 (HEP = 0.05) and B is OA-8 (HEP = 0.01), then

$$P(OA\text{-}8|OA\text{-}9) = 0.05/0.01 = 0.2$$

In some cases, common sense judgment required that the calculated values be modified. Further, the conditional HEPs were limited to a maximum value of 0.5. That is, the assumption was made that there were no cases where complete dependence between two cognitive errors existed. Again, this is part of the judgment required by the "art" of HRA. Overall, this method of determining conditional probabilities is reasonable. However, there are errors in the application of these conditional HEPs to some support states. As discussed in Section 7.1.2, adjustment factors were applied to HEPs under certain support states to account for the effects of lost instrumentation. These factors ranged from 2 to 5, with an HEP ceiling of 0.5. The error made in the PSS results from applying these factors not only to the individual HEPs but also to the conditional HEPs discussed above. The adjustment factors should be applied to each individual HEP and then those new HEPs should be used to determine conditional HEPs. Thus, as in the example above, if the support state requires multiplying the HEPs by 2, the HEPs for both OA-8 and OA-9 would be multiplied by 2. The conditional HEP, therefore, does not change when the conditional equation is applied. The PSS, on the other hand, when quantifying sequences in this support state, multiplied the HEPs for OA-8, OA-9, and OA-8|OA-9 by 2. In the requantification, we have reassessed the conditional HEPs for each support state and determined if this has any effect on the results of the analysis.

7.2.1 Cognitive Human Actions Important to the PSS Results

Four of the cognitive human actions listed in Table 7.3 appear, based on the requantification discussed in Chapter 9, to be important to the PSS results.

a. Cognitive Action OA-1

In this action the operator determines the need to initiate low-pressure recirculation during a large LOCA. The review has determined that the final HEP estimate was derived in a reasonable manner.

b. Cognitive Action OA-2

In this action the operator determines the need to initiate high-pressure recirculation during all other LOCA sizes. The review has determined that the final HEP estimate for the medium-break LOCA event was derived in a reasonable manner, but that further refinement of the analysis for small break LOCAs is desirable.

The problem with the small break analysis is that the HEP is determined using the least amount of time available for that break range (54 min., based on a 2 in. diameter break). This yields a conservative estimate of the HEP. The analysis should have considered the range of times available across the break size range. The review team reevaluated the HEP in this manner and developed HEPs for the two small LOCAs (small and small-small) which resulted from breaking up the PSS small LOCA as discussed in Section 3.1.1.

For the small LOCA (3/4 in. to 2 in.) the large end of the break size range was adequately handled in the PSS and an HEP of 1E-2 was determined. For the lower end of the break size range, it was estimated (based on very simplified and conservative calculations) that recirculation can be initiated after about 2.5 hours and that the operator will have about 3.5 hours in which to perform the action. Using the models utilized in the PSS, an HEP estimate of 1E-4 is determined for this end of the range. This value results because it is felt that a cutoff of 1E-4, as recommended in NUREG/CR-3010 (27), is reasonable for decisions made under moderate stress that can be performed over a long time frame. Assuming a lognormal distribution for the HEP over the break size range, with the two values above representing symmetrical confidence bounds, the estimate of the HEP for recirculation during a small LOCA is 1E-3.

For the small-small LOCA (3/8 in. to 3/4 in.) the large end of the break size range corresponds to the lower end of the range discussed above, or an HEP of 1E-4. At the lower end of the range, the simplified calculations indicate that recirculation can begin at about 10 hours or so and that the operator will have on the order of 13 hours to initiate recirculation. As expected, the calculated HEP is 1E-4, due to the cutoff. Thus, the revised estimate of the HEP for recirculation during a small-small LOCA is 1E-4.

It should be noted that, as explained in Section 3.1.1, in some cases the decision to initiate recirculation involves determining that high-pressure recirculation is unavailable and that it is necessary to depressurize the primary system to utilize low pressure recirculation. However, even if the median response time for the crew in this situation were doubled, it would have no effect on the results due to the exceedingly long available time. Thus, the values given above can be used for all cases of OA-2 for the given break size range.

There is also a special case of OA-2 that includes recovery of MCC-5 (see Section 3.2.13). This is used in the event trees where loss of MCC-5 is the initiating event (or part of the initiating event) and core melt has been delayed by successful operator response despite the fact that MCC-5 was not recovered early in the sequence. Long-term recovery is considered because it is required that MCC-5 operate in order to establish long-term (recirculation) cooling. It is reasonable to consider this to be a single diagnostic step because the recovery of MCC-5 in the long term is directly linked to the need to recover recirculation. That is, the operator must diagnose the need to establish recirculation and as part of that he must determine the availability of MCC-5. The parameters for this would be the same as for OA-2 for a small-small LOCA (RCP seal LOCA) and thus the HEP value would be unchanged, although the final value used would still be adjusted for the support state.

c. Cognitive Action OA-8

In this action the operator determines the need to initiate bleed-and-feed cooling in situations where steam generator cooling is required but is not available. The review has determined that the final HEP estimates

used for this event are reasonable, although one particular parameter used in the HCR model may be questionable.

The parameter in question is the median crew response time, the time required for the crew to determine that bleed-and-feed cooling is necessary. The value used is 5 minutes, which is reasonable based on a task analysis stepping through the procedures and accepting that a system is failed if so indicated in the control room. What is not taken into consideration, however, is that the procedure calling for bleed-and-feed cooling instructs the control room crew to dispatch an auxiliary operator to attempt local manual recovery of auxiliary feedwater prior to implementing bleed-and-feed. It is felt that the decision to implement bleed-and-feed would not be made until that operator reported back that auxiliary feedwater was inoperable. This would take somewhat longer than a simple procedure walk-through would indicate, probably making the total median response time closer to 10 minutes. This has a significant effect on the quantification of the HCR model, but not on the overall assessment of the HEP for OA-8 since the HCR model was not the primary model used for the selection of an HEP. The other time-dependent models indicated an HEP of 0.01, which was the figure used in the PSS. The HCR model revised as indicated above would also yield an HEP of about 0.01; thus, the review team is comfortable with the final PSS number used.

It should be pointed out that the review team expanded OA-8 to include the decision to utilize steam generator blowdown and low-pressure injection cooling for certain scenarios (see Section 3.2.3). Since this action is more directly called for in the procedures and is less "traumatic" for the operator, it is felt that the lower bound HEP of 0.005 (used in the PSS for OA-8 in simple scenarios) should be used for this case.

d. Cognitive Action OA-18

In this action the operator determines the need to attempt to recover MCC-5 when its failure is the initiating event in a sequence. The review has determined that the final HEP estimate was derived in a reasonable manner.

7.2.2 Cognitive Human Actions Not Important to the PSS Results

The review of these actions was intended only to assure that the HEP estimates used for these actions were derived in a manner which is not optimistic (i.e., that techniques appropriate to a screening assessment were used). The review has determined that this is the case, and that there is no reason to believe that further detailed analysis would yield HEPs for these actions that are greater than the values used.

7.2.3 Additional Cognitive Human Actions Required in the HRA

This section deals with the quantification of two cognitive action nodes newly defined by the review team which should be included in the PSS. Only the quantification is discussed here; the reasons for adding these actions are discussed in other sections.

a. Cognitive Action OA-2 (see Section 3.2.16)

In this action the operator determines the need to restore sufficient service water flow to establish long-term cooling (RHR or HPR) for loss of service water initiators where bleed-and-feed operation is utilized to delay core damage. This action is not required for an extended period of time, similar to the amount of time available for event LTC or OA-2 for a small-small LOCA. The HCR parameters for these events would be similar and the expected HEP estimate would be of the same order (see Sections 7.2.1b. and 7.3.1a.). Thus, our estimate of the HEP for this event is about 2E-4.

b. Cognitive Action OA-21 (see Section 7.3.1b.)

In this action the operator determines the need to dispatch an auxiliary operator to take local manual control of the auxiliary feedwater system in order to restore feedwater flow to the steam generators. It is used for certain initiating events where control room actuation and control of auxiliary feedwater is lost but local manual actuation and control is possible (no equipment failures). The actions OA-17 and OA-8 are dependent on this action.

The time frame for each of these actions is about 40 minutes, and the effect of OA-21 on the other two can vary greatly. It all hinges on how long it actually takes for the operator to either make or fail to make the correct decision, since that determines how much time is available to him to make a correct decision on a subsequent action. Further, OA-8 is also dependent on OA-17, which is already dealt with in the PSS. In any case, the total amount of time available to make any decision regarding one of these actions is 40 minutes.

In order to perform the analysis, the review team made the simplifying assumption that, in reality, the operator only has 20 minutes to implement OA-21 and that, failing to act within this time frame, he must proceed to the other actions in order to be successful. We will assume the HCR model parameters to be as follows:

1. The time available is 20 minutes.

2. The median crew response time is 5 minutes. This is consistent with similar actions in the PSS, and is reasonable based on a step-by-step walk-through of the procedures.

3. The behavior is rule-based. This is consistent with similar actions in the PSS and with the definition of rule-based behavior.

4. The stress level is, obviously, grave.

5. Other parameters are nominal.

Incorporating these assumptions into the four models used in the PSS yields the following HEPs:

HCR	4E-2	(Reference 26)
TRC	1E-2	(Reference 27)
NUREG/CR-1278	3E-2	(Reference 25)
Behavioral	1E-2	(Reference 24)

The overall best estimate, giving somewhat more weight to the HCR model than to the others, is 3E-2, which is used as the HEP for this event in the requantification of the PSS.

It is also necessary to develop conditional HEPs for OA-17 and OA-8 for use in sequences when OA-21 fails. Both OA-17 and OA-8 have nominal HEPs (not accounting for stress or other factors) of 1E-2. Using the technique applied in the PSS to conditional HEPs as described in Section 7.2, the following conditional HEPs are calculated:

$$P(\text{OA-17}|\text{OA-21}) = 0.33$$
$$P(\text{OA-8}|\text{OA-21}) = 0.33$$

In addition, it is necessary to determine a conditional HEP for OA-8 for the case where both OA-21 and OA-17 fail. In our judgment, this is a case where the limit of 0.5 for conditional HEPs is not applicable since a triple dependency exists, and it should be assumed that OA-8 will definitely fail if the operator has not recognized the need for cooling at nodes OA-21 and OA-17. Thus:

$$P(\text{OA-8}|\text{OA-21}*\text{OA-17}) = 1.0$$

7.2.4 Summary of the Results of the Review of Cognitive Human Errors

The results of the review are summarized in Table 7.5. The HEP values used in the PSS are given in the second column. Values we have developed that differ with those in the PSS appear in the third column.

7.3 Review of the Analysis of Manipulative Human Error

The PSS has identified a series of manipulative human errors that correspond to each of the manual actions that may be required of the operator in response to the initiators (and subsequent automatic system failures) modeled in the PSS. The list of manipulative errors evaluated is shown in Table 7.6, and the review indicates that this list adequately identifies the actions which are (a) desirable in one or more event sequences and (b) clearly called for in the plant emergency operating procedures. No credit is given for actions that are not included in the

TABLE 7.5 Results of Review of Cognitive Human Errors

ACTION	PSS HUMAN ERROR PROBABILITY (HEP)	SUGGESTED HUMAN ERROR PROBABILITY (HEP)	COMMENTS
OA-1	1.8E-2		
OA-2	1.9E-2		Medium LOCA
	1.0E-2	1.0E-3	Small LOCA (Section 7.2.1b.)
	------	1.0E-4	Small-small LOCA (Section 7.2.1b.)
OA-3	1.2E-2		
OA-5	5.0E-3		
OA-6	1.0E-3		
	1.0E-1		Conditional - Given RTI Failure
	5.0E-2		Consequential SGTR Case
OA-7	1.0E-1		SLB Upstream of NRV
	1.0E-2		SLB Downstream of NRV
OA-8	1.0E-2		
	5.0E-2		Loss of MCC-5, SS-12 only
	1.0E-1		Conditional - OA8|OA7
	2.0E-1		Conditional - OA8|OA9
	5.0E-1		Conditional - OA8|OA17
	------	3.3E-1	Conditional - OA8|OA21 (Section 7.2.3b.)
	------	1.0	Conditional - OA8|OA21*OA17 (Section 7.2.3b.)
	5.0E-3	1.0E-2	Simple Scenarios (Section 7.2.1c.)
	------	5.0E-3	Secondary Blowdown/LPI only (Section 7.2.1c.)
OA-9	5.0E-2		
OA-12	3.0E-3		Loss of Service Water
	1.0E-3		ATWS
OA-13	1.0E-1		
OA-14	1.0		
OA-15	1.0E-1		
OA-16	1.0E-2		

TABLE 7.5 Results of Review of Cognitive Human Errors (Continued)

ACTION	PSS HUMAN ERROR PROBABILITY (HEP)	SUGGESTED HUMAN ERROR PROBABILITY (HEP)	COMMENTS
OA-17	1.0E-2 5.0E-2 ------	3.3E-1	LOSP only Conditional - OA17|OA21 (Section 7.2.3b.)
OA-18	5.3E-2		
OA-19	1.0		
OA-20	------	2.0E-4	(Section 7.2.3a.)
OA-21	------	3.0E-2	(Section 7.2.3b.)

TABLE 7.6 Manipulative Operator Actions Evaluated in the PSS

Operator Action	Description
LPR	Operator Fails to Perform Actions Necessary to Initiate Low-Pressure Recirculation
TPR	Operator Fails to Perform Actions Necessary to Initiate Two-Path Recirculation
CHR	Operator Fails to Perform Actions Necessary to Initiate Containment Heat Removal Function
HPR	Operator Fails to Perform Actions Necessary to Initiate High-Pressure Recirculation
CHG	Operator Fails to Perform Actions Necessary to Assure Charging Function
MSI	Operator Fails to Perform Actions Necessary to Isolate the Affected Steam Generator Given an SGTR
DEP	Operator Fails to Perform Actions Necessary to Initiate Primary System Depressurization
LIV	Operator Fails to Perform Actions Necessary to Initiate Closure of the Loop Isolation Valves
LTC	Operator Fails to Perform Actions Necessary to Initiate Long-Term Cooling of the Primary System
BAF	Operator Fails to Perform Actions Necessary to Initiate Bleed-and-Feed Cooling of the Primary System
AF3	Operator Fails to Perform Actions Necessary to Assure Auxiliary Feedwater Function Given Adverse Break Location of Feedline Break
MFI	Operator Fails to Perform Actions Necessary to Isolate Main Feedline Break (downstream of MFW isolation MOV)
MFIa	Same as for MFI but for break upstream of MFW isolation MOV

TABLE 7.6 Manipulative Operator Actions Evaluated in the PSS (Continued)

Operator Action	Description
MS2	Operator Fails to Perform Actions Necessary to Isolate Main Steamline Break for Break Upstream of NRV
AF4	Operator Fails to Perform Actions Necessary to Initiate Local Manual Control of Steam Generator Level Using Auxiliary Feedwater
RMF	Operator Fails to Perform Actions Necessary to Initiate Recovery of Main Feedwater
RMC	Operator Fails to Perform Actions Necessary to Initiate Recovery of MCC-5 Power
RSV	Operator Fails to Perform Actions Necessary to Initiate Recovery of Semi-Vital A.C. Power
RT2	Operator Fails to Perform Actions Necessary to Initiate Manual Reactor Trip
TT	Operator Fails to Perform Actions Necessary to Initiate Manual Turbine Trip
EB	Operator Fails to Perform Actions Necessary to Initiate Emergency Boration
AIR	Operator Fails to Perform Actions Necessary to Assure Cooling Water Flow to Air Compressors
MS4	Operator Fails to Perform Actions Necessary to Isolate Main Steamline Break for Break Downstream of NRV

procedures. With the exception of a minor addition to the definition of event HPR under certain conditions (discussed later in this section), there appears to be no problem with the manipulative actions selected for inclusion in the PSS.

The manipulative human errors are incorporated into the PSS at the system fault tree level. That is, since each error identified only affects a single system (top event on an event tree), the associated HEP for each system is added to the mechanical unavailability for that system in order to arrive at the total system unavailability. This method is acceptable since there are no direct dependencies between the various manipulative errors, only between manipulative actions and the cognitive actions which are the basis for deciding to perform them. Since the cognitive actions are incorporated separately (see below for exceptions) the resultant manipulative actions are independent.

The approach used in the SHARP process (discussed in Section 7.1) calls for using a screening analysis to determine which actions are important and then refining the analysis of the important actions by performing a detailed analysis of those actions. This is what was generally done in the PSS for the manipulative actions considered. Our review is structured in the same manner. A detailed review has been performed of the actions which were found to be important in the PSS (LTC, AF4, CHG, RMC, BAF) in order to assure that the best possible estimate of the HEP was used in the final sequence quantification. For the other actions, our review was simply intended to assure that the HEP values used were based on models that did not yield overly optimistic HEPs. Section 7.3.1 discusses the important manipulative actions and Section 7.3.2 the manipulative actions which did not impact the results.

The HEPs for the manipulative actions are determined by using the Technique for Human Error Rate Prediction (THERP) as developed by Swain (25). However, rather than using the THERP event tree style model, human error fault trees were developed to represent each action modeled. Both models are Boolean logic representations and, properly applied, either model will adequately represent the ways in which errors can be made in performing the manipulative tasks required to perform each action. The failure probability assigned to each task on the fault trees is taken directly from the

THERP handbook. Included in some of the models was credit for recovery/correction by the shift supervisor (SS) and senior reactor operator (SRO). Generally, this was done only for those actions which were found to be important during the screening analysis.

The applicability of recovery credit was considered and applied during the conversion of the HEPs for these actions from screening values to final values, as per the SHARP process. By assuming a high dependence for the SRO and a low dependence for the SS, and using the appropriate values from the THERP handbook, a recovery factor of 0.075 was obtained. This is felt to be reasonable if properly applied. However, it should probably not be applied to manipulative actions performed early in a sequence. In discussions with a shift supervisor during the review, the team was told that the duties of the SS require that he implement the plant's emergency notification procedure (which could take on the order of 15 minutes) and, upon completion of this, monitor the plant's critical safety functions (apparently until such time as the plant has been stabilized). During this time frame, it is very unlikely that he would be able to monitor the manipulative actions performed by the operators. The time at which he could stop monitoring the critical safety functions is quite event dependent, but we feel in general that it would be reasonable to assume that no SS recovery credit should be applied to actions in the first 60 minutes of an event (unless there is a compelling reason to assume a shorter or longer time for specific events). We have reviewed each application of SS recovery in the PSS and, where necessary, adjusted the HEP values to reflect this conclusion. The effect of these changes are assessed through our requantification process to determine whether they are of any significance.

In any case, we agree that the recovery value of 0.075 is reasonable and that it can be applied to all manipulative actions that take place in the control room after 60 minutes into the event. Prior to 60 minutes, a recovery factor of 0.5 for the SRO (high dependence) is reasonable. These recovery factors should not under any circumstances, however, be applied to cognitive errors since the quantification models for cognitive errors already apply to a control room team rather than to an individual operator.

7.3.1 Manipulative Human Actions Important to the PSS Results

a. Manipulative Action LTC

The first of the important actions is LTC, in which the operator performs the necessary manipulations to establish normal long-term (RHR) cooling or an appropriate alternative. This is one of the actions which combines the cognitive decision with the manipulative action instead of including it separately on the event tree. This is done to simplify the event tree. While it would be clearer and more consistent if the actions were separated, in this case there is not likely to be a problem. First, the cognitive action associated with LTC, unlike most other actions, only affects a single system and is independent of other cognitive actions that may occur before it. That is, the HEP for LTC is not affected by the success or failure of actions appearing earlier in the sequence, nor does it affect actions appearing later in the sequence. Rather, it is only dependent on whether conditions conducive to establishing LTC are reached (if those conditions are not reached, LTC is not considered). Further, the decision to implement LTC is a common one (taken at every shutdown) and there is a long time period over which it can be performed, which should result in a low HEP and not be a major factor in the quantification.

The PSS used a screening value for the cognitive part of this action (0.013, taken from Appendix A of the SHARP document for rule-based behavior and modified to .026 because of a poor panel interface). Even after determining that this was an important operator error, the value was not improved by using a more detailed analysis. This appears to be much too conservative. A final value should have been developed using the techniques applied to the other cognitive errors evaluated in the PSS.

The assumptions used by the reviewers in estimating a final HEP value for the cognitive part of LTC are as follows:

1. The time available to make the decision is about 75 minutes. This is based on the analysis of bleed-and-feed given in Reference 7-5, which carries out the bleed-and-feed scenario to 10,000 seconds. For the case where two PORVs and one HPSI pump are used for cooling, RHR conditions (required for LTC) can be reached at any

time after 5,500 seconds into the event, leaving at least 4,500 seconds (75 minutes) for the operator to make his decision. This estimate is probably conservative, but this cannot be determined from the information provided. For the one PORV and one charging pump case, the analysis is not carried out far enough to determine when RHR conditions can be reached, but it is assumed that when that occurs, the operator will still have at least 75 minutes to respond.

2. The procedure for transition from bleed-and-feed to RHR is not well written, but plant operators have an understanding and appreciation of the need to depressurize and reach RHR conditions. Thus, rule-based behavior is assumed.

3. The stress level is considered to be "potential grave" since core damage is not imminent.

4. The median task time is 5 minutes. This is based on the task time for recirculation, which ranges from 5 to 10 minutes. Establishing RHR is a more familiar action than going to recirculation, and thus the time needed for the operators to recognize the need for RHR should be at the shorter end of the time range for recirculation.

5. The control room interface is fair and the crew training is nominal (from PSS).

Incorporating these assumptions into the four models used in the PSS yields the following HEPs:

HCR	1E-4	(3E-5 calculated, 1E-4 cutoff applied)
TRC	3E-4	
NUREG/CR-1278	1E-4	
Behavioral	1E-2	

The value derived from the behavioral model is discarded because this model is not time dependent, does not apply to events with long time frame, and is strictly a screening method, whereas this is a detailed

analysis. The other results indicate that a value on the order of 2E-4 is a reasonable best estimate (based on the available information) for the cognitive part of LTC.

A final comment regards an arbitrary recovery factor (probability of failing to recover) of 0.1 which was applied to the overall LTC action (both the manipulative and cognitive parts). No explanation was given for this value. The 0.075 value discussed previously, and adequately justified in the PSS, should have been applied. However, the recovery factor should not be applied to the cognitive part of the human error, as previously mentioned. In general, it is concluded that the analysis of event LTC was not properly converted from a screening analysis to a detailed analysis as called for in the SHARP process. The review team has suggested corrections to these errors as they apply to the cognitive and manipulative recovery parts of the analysis to arrive at a final value for this error probability. The revised human error fault tree and data worksheet are shown in Figures 7-1 and 7-2. The revised HEP suggested for this action is 1.7E-3.

b. Manipulative Action AF4

This important operator action represents the performance of the necessary manipulations to establish auxiliary feedwater cooling locally in the auxiliary feedwater pump room. It is used for sequences where support system failures render remote (from the control room) automatic and manual control of the system inoperable. This is another of the actions which includes the cognitive decision in the manipulative action.

The fault tree and quantification of the manipulative portion of this action is reasonable. It should be noted that no credit is given for recovery by the SS or SRO. This is reasonable since the actions are performed outside of the control room and cannot be monitored by the SS or SRO.

There does appear to be a problem, however, with the handling of the cognitive error as part of this manipulative action. Unlike the previous action (LTC), this cognitive decision does have a dependence relationship with other cognitive decisions in certain sequences. The recognition of the need to provide secondary cooling by taking local manual control

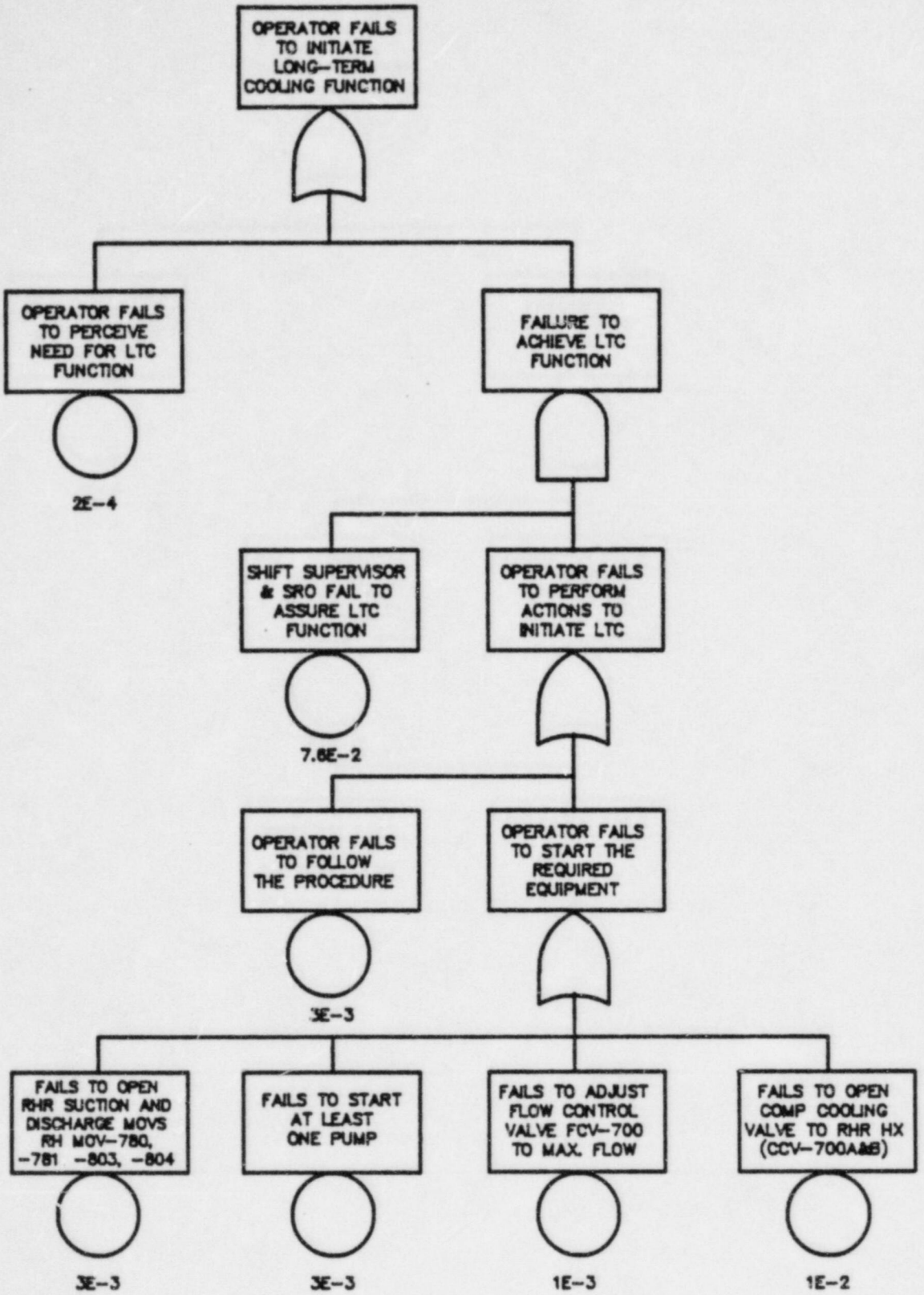


FIGURE 7.1. Human Error Fault Tree for Node LTC.

HI DATA WORKSHEET: LTC

PERFORMANCE SHAPING FACTORS

CONTROL ROOM	STRESS STATE	OTHER
Good _____	Grave _____	
Fair __x__	Potential x	
Poor _____	Normal _____	
	Low _____	

Written Procedure Step No. or Task Description	Potential Error	NUREG/CR-1278 Table No./ Item No.	Tabled HEP	Performance Shaping Factors	Adjusted HEP	Comments
ES-3.2, Step 6d	Cognitive Error (Failure to Select NOP 2.9-1	-----	.0006			Mix of time-dependent cognitive models
	SS/SRO Fails to Assure HPR Function:					
	SRO (High Depend)	20-24/4	.5		.075	P = (.5x.15)
	SS (Low Depend)	20-24/4	.15			= .075
NOP 2.9-1	Fails to Follow NOP	20-7/3	.003			
	Fails to Open RHR MOVs	20-13/2	.003			
	Fails to Start RHR Pumps	20-13/2	.003			
	Fails to Open CCVs	20-13/5	.01			
	Fails to Adjust FCVs	20-12/3	.001			

Figure 7-2. Data Worksheet Associated With Human Error Fault Tree for Node LTC.

of auxiliary feedwater is part of the recognition that all secondary cooling has failed. This guides the operator to a procedure which instructs him to attempt local manual recovery of auxiliary feedwater; failing that he is instructed to attempt to recover main feedwater; and failing that he is instructed to initiate bleed-and-feed cooling. Thus, the failure of the cognitive part of AF4 would affect the HEP for cognitive actions OA-17 (recognize need to recover main feedwater) and OA-8 (recognize need to initiate bleed-and-feed). If the failure of AF4 were due to a manipulative failure, there would be no effect on OA-17 and OA-8. Since no dependency is modeled between AF4 and these OAs, the treatment of the dependency between them is optimistic.

In order to rectify this and assess the significance of the dependency, it is necessary to separate the cognitive and manipulative parts of AF4. The manipulative part will remain as AF4, with an HEP of 1.5E-3 (taken from the model in the PSS). A new cognitive action, OA-21, is defined and added to the event tree models. The quantification of this new action and its effect on conditional HEPs for OA-17 and OA-8 was given previously in Section 7.2.3b.

c. Manipulative Action CHG

This important operator action involves the performance of the necessary manipulations to establish the charging function in those situations in which manual alignment in required. The model used is reasonable with the exception that credit should have been allowed for recovery by the senior reactor operator (see Section 7.2). This credit reduces the HEP estimate to 3E-3.

d. Manipulative Action RMC

This important operator action involves the performance of the necessary manipulations to recover power to bus MCC-5. The model used and the resultant HEP are reasonable.

e. Manipulative Action BAF

This important operator action involves the performance of the necessary manipulations to establish bleed-and-feed cooling in those situations in which steam generator cooling is unavailable. The model used is reasonable with the exception that credit should have been allowed for recovery by the senior reactor operator (see Section 7.2). This credit reduces the HEP estimate to 6E-3. It should be noted that this value also reflects a minor change in the PSS HEP estimate which resulted from modifications to the model but which was not incorporated in the PSS quantification.

7.3.2 Manipulative Human Actions Not Important to the PSS Result

As previously discussed, the review of these actions is limited to assuring that the HEP values used in the PSS are not optimistic, i.e., further detailed analysis would not result in HEP estimates greater than those used. In general, the HEP values used are reasonable for a screening analysis, and meet the above criterion. There are, however, two exceptions, discussed below.

a. Manipulative Action LPR

This action represents the performance of the necessary manipulations to establish low-pressure recirculation in the event of a large LOCA. In the PSS, credit was given for recovery of errors by the shift supervisor. This action must be performed early in the event sequence (within 20 minutes or so) and it is felt that the shift supervisor would not be able to offer such support at that time (see Section 7.3). Thus, this credit should be removed from the model, which results in a revised HEP estimate of 9.3E-3 for this action.

b. Manipulative Action HPR

This action represents the performance of the necessary manipulations to establish recirculation in the event of LOCAs other than a large LOCA. Again, in the PSS, credit was given for recovery of errors by the shift supervisor. For the reason mentioned above, the reviewers feel that

it is not proper to give credit for the medium LOCA case, but that credit is warranted for the small and small-small LOCA cases (see Section 7.2.1b regarding timing of recirculation). Thus, this credit should be removed for the medium LOCA case only, which results in a revised HEP estimate of 1.7E-2 for this action during medium LOCAs. For small and small-small LOCAs, the HEP estimate remains 2.5E-3.

There is also a special case of HPR which includes recovery of MCC-5 (See Section 3.2.13) for cases where MCC-5 is lost as an initiating event and not recovered initially. In these cases, additional manipulative actions are required locally to clear the fault on the bus and re-energize at least some of the equipment on the bus. The specific actions required would depend on the specific fault to be cleared, but as a general estimate it is reasonable to assume that the HEP for HPR would double for these cases. Thus, the HEP value will be 5.0E-3. This value would have no additional adjustment for stress since it is in the long term, the MCC-5 recovery part is outside the control room and is not further affected by the loss of MCC-5, and the original HPR part (inside the control room) would actually take place only after the recovery of MCC-5.

In a similar manner, is is also assumed that long-term recovery of service water (RSW), which is not combined with any other event but is also needed for HPR on long-term cooling (see Section 3.2.16), also has an HEP about that of regular HPR (2.5E-3) for evaluation purposes.

7.3.3 Summary of the Results of the Review of Manipulative Human Actions

The results of the review are summarized in Table 7.7. The HEP values used in the PSS are given in the second column. Values developed during the review that differ from those in the PSS appear in the third column.

TABLE 7.7 Results of Review of Manipulative Human Errors

ACTION	PSS HUMAN ERROR PROBABILITY (HEP)	SUGGESTED HUMAN ERROR PROBABILITY (HEP)	COMMENTS
HPR	2.5E-3	1.7E-2	Medium LOCA (Section 7.3.2b.)
	2.5E-3		Small & Small-small LOCAs
	------	5.0E-3	ET-13,-18 cases, Failure at OA-18 or RMC
	------	1.4E-3	Conditional HPR given SBD is successful Actions same as LPR (Section 4.2.3)
LPR	1.4E-3	9.3E-3	(Section 7.3.2a.)
TPR	5.3E-4		
CHR	1.7E-2		
CHG	6.0E-3	3.0E-3	(Section 7.3.1c.)
MS1	2.0E-3		
MS2	2.0E-4		
DEP	3.0E-3		
LIV	2.0E-3		
LTC	5.2E-3	1.7E-3	(Section 7.3.1a.)
BAF	1.0E-2	6.0E-3	(Section 7.3.1e.)
AF3	9.0E-3		
MFI	4.5E-3		
MFIa	6.5E-3		
MSF	1.0E-2		
AF4	2.6E-3	1.5E-3	(Section 7.3.1b.)
RMF	1.0E-1		ET-12 case, Failure at OA-17
	2.0E-3		
RMC	4.0E-3		
RSW	------	2.5E-3	(Section 7.3.2b)

TABLE 7.7 Results of Review of Manipulative Human Errors (Continued)

ACTION	PSS HUMAN ERROR PROBABILITY (HEP)	SUGGESTED HUMAN ERROR PROBABILITY (HEP)	COMMENTS
RSV	4.0E-3		
RT2	6.0E-3		
TT	3.0E-3		
EB	4.0E-3 3.0E-3		ET-22 case, Requires add. actions
AIR	1.2E-2		
BLED	------	3.0E-3	From "Bleed" part of PSS BAF tree w/SRO recovery credit
SBD	------	3.0E-3	Action similar to BLED

8.0 OPERATING EXPERIENCE ANALYSIS

A review of the Haddam Neck operating experience using Licensee Event Reports (LERs) was performed to identify any events or trends that might point to an inherent weakness in the design or operation of this plant. In particular, it is desirable to determine if the actual plant operating experience indicates that any of the data/models in the PSS seriously underestimated the frequency or importance of any initiating events or system failures. The review focused on the risk relevant aspects of Haddam Neck's performance such as failures that could initiate core damage sequences or impact the response of transient mitigating systems and determined if they were adequately reflected in the PSS. The review involved an examination of the facility operation during the period January 1975 through July 1986.

8.1 Approach

The approach used in the review process was to first identify systems which are pertinent from a core melt perspective. Systems which are important to core melt are those which perform a mitigation function to reduce the impact of transient or accident conditions on plant operations. Some important mitigating systems include: Auxiliary Feedwater System (AFWS), High Pressure Injection System (HPIS), Low Pressure Injection System (LPIS), Residual Heat Removal System (RHRS), Charging System (CS), and emergency power.

In addition, a review of plant-specific transient information was undertaken. The purpose of the transient review was to determine if plant-specific data for transient frequency was consistent with the initiating events and frequencies used in the PSS.

An initial review of all the LERs was then completed. The initial review sorted the events according to the system or equipment they impacted. A detailed review of all the events involving a particular system or component was then undertaken to determine the significance of the events. Events which would mildly degrade system performance were classified as minor events. For example, the four events impacting the high pressure injection system were classified as minor because they would not have

disabled pump operation had it been required. Events which would prevent a component from changing state when demanded or from operating continuously under accident conditions were classified as potentially serious events. Finally, the frequency of these events was compared with the system failure data in the PSS to determine if the PSS models adequately reflected these historical failures.

8.2 Sources of Information

The primary source of information used in the Haddam Neck review was the Licensee Event Reports (LERs) for the period January 1976 through July 1986 and the Abnormal Occurrence Reports for 1975. Approximately 297 LERs were examined during the course of this review.

Events at the Haddam Neck Plant identified in the Accident Sequence Precursor (ASP) program were also reviewed. The events selected in the ASP program are documented in ASP reports for the 1969-1979, 1980-1981, and 1985 periods (References 28 to 31).

Transient event data was reviewed to compare the frequency of transients observed at Haddam Neck with those expected based on an industry average. The source of this data was "Development of Transient Event Frequencies for Use in Probabilistic Risk Assessments (DRAFT)," NUREG/CR-3862 (32).

In addition to these documents, plant specific information regarding plant configuration and the criteria for successful system operation were obtained from the Haddam Neck Facility Description and Safety Analysis (FDSA) Report (33) and the Probabilistic Safety Study (1). Haddam Neck events identified in the Abnormal Occurrence Reports to Congress (NUREG-0090 series documents) were also included in this review.

8.3 Event Selection

The primary purpose of any selection criterion is to extract from a large data base a manageable set of potentially significant items to be analyzed in more detail. The initial LER review was a bounding review, meant to select events that in any way appeared to deserve detailed review

but to eliminate events that did not appear important. The detailed review examined the risk relevance of each event to determine its impact on systems to mitigate off-normal events and accidents. After the detailed review was completed, the events which were eliminated in the earlier reviews were re-examined to ensure that no important events were inadvertently discarded.

The events were categorized as important in the initial review if they impacted:

- Systems that provide emergency core cooling (including recirculation), e.g., HPI, LPI;
- Systems that provide reactor heat removal, e.g., steam generators, MFW, AFW;
- Systems that provide reactor inventory and pressure control, e.g., pressurizer, chemical and volume control system (CVCS);
- Containment systems, e.g., containment spray system, containment air recirculation fans;
- Reactor shutdown system, e.g., reactor protection system, CRDMs;
- Vital power systems, e.g., batteries, diesels;
- Actuation of engineered safeguards systems.

Also selected for further review were those events previously identified as accident sequence precursors and in Abnormal Occurrences Reports to Congress.

As a result of this review, events which were considered to contribute little to the overall plant risk were eliminated from further consideration. Types of events in this group include:

- Fish kills resulting from impingement on the intake screens, and

- Minor releases of radioactivity both liquid and gaseous.

The detailed review examined the events selected to determine if they were a potentially serious event, if they recurred for a particular component, recurred in a particular system, or impacted two or more trains in one system. Those events which appeared to be isolated single failures of equipment due to random failure were considered to have been included in the component failure rate used in the PSS. In addition, events involving components out of service for maintenance were considered minor since they are reflected in the maintenance unavailabilities used in the PSS. In those cases in which the level of detail of the LER permitted, common-cause failures of equipment were identified.

Recurring failures were examined to determine if the failure was complete or just a minor degradation of system performance. In some cases, equipment was declared inoperable because of a minor problem, which would most likely not impact its operation under transient conditions. Events of this nature were considered of minor importance. Numerous minor events, e.g., recurring maintenance outages, in critical systems can be indicative of problems in design, operation, or maintenance and were investigated further.

The systems for which recurring potentially serious events were found are discussed in Section 8.4. In addition to describing the specific events which occurred for each system, the conditions under which performance of the system becomes critical to plant safety are described.

8.4 Potentially Serious Events

Events identified as potentially serious are grouped according to the systems or equipment they impacted. Most of the events identified in this review were recurring events which impacted the important systems discussed in the previous section.

8.4.1 Chemical and Volume Control System

For the Chemical and Volume Control System, numerous problems appear to be centered in and around the charging pumps. Fifteen events were

TABLE 8.1. Chemical and Volume Control System

Potential Impact	LER No.	Description
Minor	76-05	Seal leakage around an O ring
Minor	77-05	1A decrease in pump pressure discharge due to shaft cracks
Minor	77-06	1A seal housing minor leakage
Serious	77-07	A Pump runs hot; bearings replaced
Minor	77-16	B Pump isolation valve pinhole leak
Minor	78-07	Pinhole leak in B recirculation orifice bypass valve
Minor	78-08	B Pump recirculation orifice bypass valve leak
Minor	78-12	B pressure gauge isolation valve leak
Serious	78-20	Controller failure caused flow control valve to close
Serious	81-10	Oil leak B Pump
Serious	81-19	Excess vibration on charging pump
Minor	82-09	Pinhole leak B Pump throttle valve
Serious	83-09	Unable to turn pump due to solidified boric acid
Minor	83-16	Pump declared inoperable due to broken thermocouple
Minor	83-18	Pump B out of service due to pump seal leak

identified in Table 8.1 for the period January 1975 through July 1986; five of those events were considered serious enough that they would impact long-term pump operation under emergency conditions. Both the potentially serious and minor events are fairly evenly distributed in the first eight years of the 1975-1986 period.

The first event identified as potentially serious occurred in April of 1977 and is documented in LER 77-7/3L. Following pump maintenance, 1A charging pump was returned to service. After approximately 20 minutes of operation, the inboard motor bearing temperature increased to 196^{o}F and the pump was shut down. Motor bearings were replaced and the axial alignment between pump and motor corrected. The pump would probably have failed had continuous operation been required. It is important to note that the charging pump was returned to operation without post-maintenance testing. This is not a sound operations practice because it risks placing a degraded pump on line and a failure to restart the previously operating pump.

In October of 1978 (LER 78-20/3L), the selector switch on the charging flow recorder/controller failed. This failure caused the recorder/controller to go full scale and the charging flow control valve to close. The pressurizer level decreased by 5% and the pressurizer pressure decreased to 1990 psig.

Two events occurred in 1981 which could have seriously impacted continuous charging pump operation. In July of 1981 (LER 81-10/3L), 1B charging pump was found to have an oil leak which required that it be removed from service. Vibration had caused cracking of pipe thread sealing material. The charging pump oil lubricating system is not isolable so that once a leak occurs the lubrication of the pump is jeopardized. Continued operation of the pump without lubricating oil is expected to result in pump failure.

In November of 1981 (LER 81-19/3L), routine vibration monitoring under the inservice inspection (ISI) program showed radial vibration on a charging pump had increased above reference level. Pump vibration was found to be caused by a worn key and worn parts of thrust bearing elements. Pump vibration may result in pump failure with continued operation.

In May of 1983 (LER 83-09) during normal surveillance testing, 1A charging pump shaft was found to be bound such that it could not be turned by hand. The pump was uncoupled from the motor so that additional force could be applied. The shaft eventually broke free permitting continuation of the test. The source of the binding is thought to be solidified boric acid. It is considered unlikely that the pump would have started upon demand.

Minor events in the charging system included eight small leaks, one decrease in pump discharge pressure, and one event in which the pump was declared inoperable due to a broken thermocouple. Most of the leaks involved the charging pump seals.

Of the five serious events identified, the first four represent random failures of a single pump. The occurrence of four events of this type over the review period is not indicative of a failure rate higher than that used in the PSS. The fifth event appears, at first glance, to be a potential common mode failure since boron precipitation could be equally likely to occur in both pumps at the same time. However, it must be kept in mind that one pump is always running. Only the standby pump would be susceptible to this type of boron precipitation and shaft binding. Thus, the operating experience does not indicate any deficiencies in the PSS analysis of this system.

8.4.2 Pressurizer and Associated Equipment

The pressurizer and associated equipment considered in this review encompasses the pressurizer, spray valves, heaters, instrumentation and pilot operated relief valve. Twelve events were identified in Table 8.2 during the period January 1975 through July 1986; five of these events are considered potentially serious from a safety perspective. The events appear fairly evenly distributed in the 1975-1986 period.

The first significant event identified occurred in August of 1979 (LER 79-10/3L). While operating at steady state full power, the pressurizer pilot operated relief valve and its isolation valve spuriously opened on a light source failure in the bistable of the pressure controller. The failure led to the pressure controller signaling the valve to open. The

TABLE 8.2. Pressurizer and Associated Equipment

Potential Impact	LER No.	Description
Minor	77-12	Level on channel 3 different from 1 and 2; could actuate low core cooling
Minor	77-28	Leaking pressure transmitter
Minor	78-09	Pinhole leak in spray isolation valve
Minor	78-12	Trip occurred due to testing of pressurizer level
Minor	78-17	Spray valve failed open due to transister failure
Minor	79-04	Leak in primary drain cooler discharge line
Serious	79-10	Pilot operated relief valve and isolation valve opened
Serious	80-04	Pilot operated relief valve and isolation valve opened due to spurious signal
Serious	81-03	Pilot operated relief valve and blocking valve opened due to a loose electrical connection
Serious	83-20	Loss of air caused loss of control to spray valves and pilot operated relief valve
Serious	83-21	Loss of air caused loss of control to spray valves and pilot operated relief valve
Minor	85-26	Inadequate trip circuitry for low pressurizer pressure

opening of these valves allowed the pressurizer pressure to drop from its normal steady state pressure of 2000 psig to 1950 psig before the PORV could be shut.

In February of 1980 (LER 80-04/3L), a similar event occurred. Reactor coolant system pressure was reduced to 1992 psig from 2016 psig before manual isolation terminated the transient. The cause of the valve actuation appeared to be a spurious signal from the pressurizer pressure control.

Again in April of 1981 (LER 81-03/3L), the PORV and its isolation valve spuriously opened causing a momentary decrease in RCS pressure from 2000 psig to 1980 psig. The source of the problem was a loose electrical connection in the pressurizer pressure controller.

The PORV events described above were identified as accident sequence precursors in previous NRC studies. Subsequent to the April 1981 event, the PORV actuation logic was changed from a one channel pressure signal to 2 out of 3 channels to prevent spurious actuations. Since the actuation logic change, there have been no spurious PORV opening events.

In November of 1983, two events (LERs 83-20 and 83-21) occurred which resulted in the loss of control air to the PORV. Loss of control air to the PORV prevents opening of the valve. The ability to open and close the valve becomes critical should it be necessary to perform a "bleed and feed" operation. Given a safety injection signal, it is not known whether containment air is isolated. Both of the loss of control air events were the result of a broken air filter.

The nine minor failures identified by the review included:

- 3 minor leaks,
- One event in which a spray valve failed open,
- One trip due to pressurizer level testing,
- One maintenance error,
- One event in which a pressurizer level instrument drifted from calibration.

The three occurrences of inadvertant opening of a PORV were responded to by the utility by a modification to the PORV actuation logic. The possibility of additional occurrences of this type of event given the present plant design is explicitly and adequately modeled in the PSS. With regard to the last two occurrences, loss of control air to the PORVs is explicitly modeled in the PSS. The overall failure probability of bleed-and-feed calculated in the PSS is not affected by these occurrences.

8.4.3 Emergency AC Power

Seventeen events involving the emergency AC power system were identified in Table 8.3 during the January 1975 through July 1986 period. Nine of these events were considered serious in that they would have impacted safe plant operation had offsite power been lost. The events are evenly distributed within the study period. Loss of offsite power (LOSP) is discussed in this section because it provides the challenge to the emergency AC power system.

The first serious event identified occurred in February of 1976 (LER 76-6/3L). During monthly testing emergency diesel 2B tripped on overspeed. A calibration tool left in the injector rack following governor replacement caused the rack to be held open and the diesel to trip on overspeed.

In early May of 1978 (LER 78-06), calculations were performed which showed that emergency diesels 2A and 2B had a potential for overload under certain loss of coolant accident conditions. It was determined that the original loading analysis of the diesel generators had used incorrect assumptions. Reanalysis showed the diesel loading calculations to be higher than the diesels highest rated loading. In late May of that year, a plant design change was implemented to block automatic charging pump loading on signals indicating a LOCA or MSLB coincident with a loss of offsite power. According to the design change, charging pump operation would be blocked or tripped, if operating, upon initiation of a diesel start signal.

In January of 1980 (LER 80-003/3T), the emergency diesel generator loads were reviewed again in light of TMI. It was determined that an overload could still exist in the situation where the plant had experienced

TABLE 8.3. Emergency AC Power

Potential Impact	LER No.	Description
Serious	76-06	Diesel Generator tripped on overspeed
Serious	78-06	Calculations determine diesel generators have potential for overload
Minor	79-09	Thrust bearing lubrication may be impacted
Minor	80-01	Timers on diesel generator failed to sequence in loads correctly
Minor	80-02	Electrical leads to transformer were cut
Serious	80-03	Review showed potential overload for diesel
Minor	81-07	B Diesel load sequencing did not satisfy tests
Serious	81-11	Diesel generator overloaded itself
Serious	81-14	Cooling leak on Diesel Generator B
Serious	82-01	Both A & B battery chargers powered by Diesel Generator B
Minor	83-02	Air compressor failure
Minor	83-12	2A governor voltage setting drifted
Minor	83-13	2A failed to attain proper speed during test
Minor	83-19	Setpoint drift in B diesel timer
Serious	83-23	Diesel Generator B assumed load greater than governor setting
Serious	84-14	Circuit Breaker on diesel failed to close in for 20 minutes
Serious	85-29	Interdependency could prevent the flow of service water to both diesel generators

a trip with loss of offsite power, followed by an accident. Procedures were changed so that a charging pump could not be loaded and no more than 500 kw of load could be added to the diesel. Seal injection would be accomplished via the metering charging pump which was included in the 500 kw load allowed on each diesel.

At this point in the operating history, it would appear that the diesel generator overload problem had been corrected. However, on August 3, 1981 (LER 81-11/1P), the diesel generator overloaded itself. Following repairs for inability to phase on the emergency diesel generator during a surveillance test, the diesel was being run for two hours when it was observed to have overloaded. The load was manually reduced. The motor-operated potentiometer in the governor control circuit was replaced.

In September 1981 (LER 81-14/3L), cooling system tube leaks on emergency generator 2B necessitated taking it out of service for repair. The extent of leakage is not known. Total loss of cooling to the diesel would seriously impact its emergency operation.

During an engineering evaluation in January of 1982 (LER 82-01), it was observed that both A and B battery chargers were powered by emergency diesel generator 2B. If this diesel failed following a loss of offsite power, both chargers would be unavailable until a realignment of circuit breakers could be accomplished. Loss of both battery chargers for more than four hours would result in loss of both batteries and loss of control power to vital safety equipment, including the 2A diesel generator. A failure of this sort could go undetected until the batteries were depleted. Realignment of the circuit breaker in time to start the backup diesel may be jeopardized. A plant design change was completed to separate the battery charger emergency power supplies.

In December of 1983 during a monthly surveillance test (LER 83-23), diesel generator 2B assumed a load greater than the governor setting. The suspected cause of the event was a diesel generator governor assembly out of adjustment. Subsequent to this event, load was adjusted manually during testing until the governor assembly could be repaired during the next refueling outage.

During the refueling in August of 1984 (LER 84-014), a shutdown-related loss of offsite power was initiated by the start of a large pump. One of the offsite grid lines was undergoing maintenance at the time of the event. The other offsite grid line was lost when the pump was started. Both diesel generators started and unnecessary loads were shed. The automatic closure of one diesel generator output circuit breaker was delayed 20 minutes. The cause of the diesel malfunction was reported to be a diesel voltage regulator which was left slightly below the breaker voltage permissive relay setpoint. Operating procedures were changed so that the diesel voltage regulator is adjusted well above the permissive setpoint prior to shutdown. Later in 1984 (LER 84-23), it was determined that the failure was caused by a failed "X-Relay." Failures in "X-Relays" were determined to be a generic problem because Westinghouse did not provide instructions for maintenance of the "X-Relays" in their maintenance procedures. All Westinghouse DB and DHB breakers were subsequently inspected and cleaned.

During efforts to complete a Probabilistic Safety Study in November of 1985 (LER 85-29), a serious interdependency involving cooling water to the diesel generator was discovered. The normally closed air-operated valves (AOV) which allow cooling water to the emergency diesel generators are operated by solenoid-operated valves (SOV). Upon loss of air, the air-operated valves will open permitting flow of cooling water to the diesel generator. However, AC power is required to energize the SOV and open the AOV. A loss of offsite power coincident with an interruption of power to a single motor control center (MCC-5) could prevent opening of the AOV and cause both emergency diesel generators to overheat in a short period of time. In order to assure diesel generator cooling, the impact of maintaining the AOVs in the open position was evaluated. It was determined that continuous water flow to the jacket water heat exchangers would not adversely affect operation as long as lube oil exiting the lube oil cooler did not decrease below 85 degrees F. Testing showed the lube oil temperature would drop no lower than 120 degrees F, and the cooling water AOVs were subsequently configured to stay in the open position at all times.

The above event, in combination with the charger dependency discussed earlier resulted in an emergency power system with multiple points of non-redundancy. If the 2A diesel failed to start and load, MCC-5 would be without power until transferred to the opposite bus. Emergency diesel 2B

would be without cooling water during the bus transfer time. This review assumed that this transfer would have taken place in a timely manner to prevent overheating of diesel 2B.

Loss of offsite power which initiates a diesel start has been identified as an accident sequence precursor for the Haddam Neck Plant. The two losses of offsite power identified in the ASP studies happened in 1969 and 1974. Two additional losses of offsite power were reported in the LERs for the review period 1975-1985; one in 1976 (LER 76-14) and one in 1984 (LER 84-14). The 1976 loss of offsite power event was the result of poor design in the protective relays. The 1984 loss of offsite power event was due to improper maintenance on a differential relay current transformer.

Most of the eight minor events involved failure of the diesel load sequencer to satisfy test. In these cases the sequencer failed to meet the requirements by only a few tenths of a second. Other minor events included an air compressor failure, minor cuts in the electrical leads to the transformer, and failure to attain proper speed during testing.

Loss of offsite power with emergency AC power failures was found in the PSS to be a significant contributor to core melt frequency. In reviewing the events above, it can be noted that some of them (for example, diesel overload) have common mode failure potential. Both the overall number of diesel failures and the common mode failure potential are adequately modeled in the PSS. The service water interdependency and the effect of bus MCC-5 were discovered by the PSS process and were explicitly treated therein.

8.4.4 Auxiliary Feedwater System

Ten events in the auxiliary feedwater system were identified in Table 8.4 for detailed review. Four of the ten events were identified as having a potentially serious impact on the performance of the auxiliary feedwater system under emergency conditions. The impact of two other events was difficult to ascertain because the LERs were somewhat vague. These LERs describe events in which the AFW pumps failed to satisfy test requirements. However, the margin by which the pumps failed was not reported. One event (LER 77-15) involved a failure of an AFW pump. During this event, the pump

TABLE 8.4. Auxiliary Feedwater System

Potential Impact	LER No.	Description
Minor	76-11	Pump B failed test due to relief valve opened
Serious	76-16	Both pumps fail to develop proper pressure - vapor bound
Serious	77-15	Pump B failed to meet test by 200 psig
Minor	79-06	Feed pump did not discharge at rated power
Minor	81-04	Valve problem on motor operated isolation valve for backup auxiliary feedwater system
Minor	81-06	B Pump started due to failed control valve
Serious	81-08	B Pump down due to leak; A Pump recirculation valve closed
Minor	83-03	Pump fails test due to open relief valve on steam supply
Serious	85-05	Valve problem required operator action to get feed into Loops 1 and 4
Minor	85-24	1 of 4 valves did not change state

discharge pressure was 75% of the minimum required for a successful test. This failure was determined to be serious because of the failure margin (25%). Failures by less than 10% were considered to be less serious in this study.

Other serious events identified in the detailed review involved failures of the auxiliary feedwater pumps and loss of feedwater flow path due to valve problems. In July of 1976 while plant was in the startup mode (LER 76-16), the operator attempted to start an auxiliary feedwater pump to raise levels in the steam generators. After the pump failed to start, the operator attempted to start the second auxiliary feed pump with the same results. After shutdown, the pumps were checked and found to be vapor bound. Probable cause of the event was thought to be back-leakage from number three steam generator through the check valve in the feed line. This event appears to be a precursor to a vapor binding problem which occurred more recently at Robinson and which is a current NRC concern.

In June of 1981 (LER 81-08), the "B" turbine-driven auxiliary feed pump developed a leak on a turbine oil gland. Before taking the pump out of service, the "A" turbine driven auxiliary feed pump was test run to verify operability in accordance with the surveillance procedure. The "B" pump was subsequently taken out of service and vented. During a second check of the valve lineup, it was found that the "A" pump recirculation valve had been closed rather than the "B" pump recirculation valve. For a period of two hours, the "A" pump would not have had recirculation flow. Under emergency conditions, the flow of feedwater from the pump to the steam generators would have removed pump heat (provided this flow was not substantially reduced, as it could be later in time following a loss of feedwater). This event was significant because both auxiliary feed pumps were impacted. The event occurred because the valve number in the procedure was incorrectly identified. The procedure was later corrected.

In November of 1984 (LER 85-05), a test of the automatic initiation of the auxiliary feedwater system was performed during refueling. During the test, it was discovered that the air-operated SG feedwater bypass valves in Loops 1 and 4 did not open automatically. As a result, auxiliary feedwater could not flow to SGs in Loops 1 and 4 without operator action. The cause of the failures appeared to be the solenoids on the air-operated

valves. The valves were retested successfully and declared operational for continued use.

Minor events identified in the auxiliary feedwater system included:

- Spurious start of an auxiliary feedwater pump
- Motor operated isolation valve problem on a backup line
- One of four valve failure in auxiliary feedwater lines
- Feedwater pump did not discharge at rated power.

Again, with the exception of the vapor binding occurrence, which has common mode connotations, the other major events are in keeping with the AFW pump failure rate used in the PSS. The vapor binding problem was identified and discussed in the PSS. A plant modification made specifically to detect potential vapor binding conditions was implemented and its benefits were specifically addressed in the PSS. Therefore, the occurrences identified are adequately treated in the PSS.

8.4.5 Containment Air Recirculation (CAR) System

Twelve events (Table 8.5) in the containment air recirculation system were selected for detailed review. The containment air recirculation system includes four motor driven fans with their associated coolers and dampers. The fan dampers are provided to prevent back flow through a non-operating fan which could degrade the performance of the operating fans. The containment air recirculation system removes heat from the reactor containment atmosphere during normal operation and after an accident which causes containment pressurization such as a loss of coolant accident (LOCA).

Only one of the events selected for detailed review was determined to be a potentially serious event. In November of 1975 (AO·75-14), service water to all four containment recirculation fan coolers was lost. The filter in the "A" service water train had not been operating correctly. When the operator removed the "A" filter from service, he assumed the "B" filter was in parallel operation because it was turning. After containment high temperature and cooler low flow alarms were received, it was determined that the "B" filter had been on backwash. The service water was interrupted

TABLE 8.5. Containment Air Recirculation System

Potential Impact	LER No.	Description
Serious	75-04	Service water to all four containment recirculation fan coolers was lost
Minor	77-08	#2 fan vibrating
Minor	78-13	Hole in cable sheath
Minor	80-06	Fans inoperable dampers remain open
Minor	81-01	Fan damper did not close
Minor	82-05	Fan damper fails test
Minor	82-10	Damper linkage failure
Minor	83-01	Leak in coil of fan cooler
Minor	83-05	Fan damper linkage failure
Minor	83-10	Loss of service water to fan cooler due to clogged filter
Minor	83-24	Service water flow requirements insufficient for fan cooler; needs 2 pumps
Minor	85-02	Fans 2, 3, 4 did not meet test

to all four containment recirculation fan coolers for a period of approximately 45 minutes. The containment recirculation fan coolers were rendered inoperable for containment temperature control during this period. During this 45 minute period, containment average temperature increased by 13°F.

The Haddam Neck PSS assumed proper operation of the dampers was not necessary for the CAR fans to perform their cooling function. Five of the events selected for detailed review were damper failures. The other LERs identified failures which resulted in mildly degraded operation of the CAR system. Hence, only one of the events selected for detailed review was determined to be a serious failure of the CAR system. The dependency of the fan coolers on service water cooling was explicitly and adequately modeled in the PSS. The single event identified does not warrant any change to the PSS model regarding availability of CAR fans during an accident.

8.4.6 Reactor Protection System (RPS)

Eighteen events (see Table 8.6) in the reactor protection system were selected for detailed study by the initial LER review. All of these events were determined to be minor by the detailed review. Six of the events involved drift of the overpower setpoint. The margin above setpoint reached as high as 3% above the Technical Specification limit of 109% of rated power. Two setpoint drift events were identified for the dropped rod load runback. In two cases, a reactor trip relay did not operate; one involved the high pressurizer level and the other, the low flow trip. Two events selected involved failures of a potentiometer which caused spurious power signals and initiated dropped rod runbacks. Four events selected for spurious dropped rod indication were not readily attributed to a specific cause. The other events involved degraded RPS cabling and erratic current indications.

Although the events were minor in nature, the large number of events in such an important system may be a basis for further investigation. The overpower trip setpoint drift appears to be a chronic problem. Problems involving drift were primarily observed for the overpower trip setpoint. It would be expected that drift would impact all instrumentation to some extent. However, the evidence from the LER review does not support this. Overall, the substantial redundancy in the RPS is not significantly

TABLE 8.6. Reactor Protection System

Potential Impact	LER No.	Description
Minor	76-03	Channel 33 overpower trip setpoint 1/2% above setpoint
Minor	76-07	Channel 34 overpower trip setpoint 2% above setpoint
Minor	77-11	Channel 32 current became erratic
Minor	77-18	Low flow trip matrix did not operate
Minor	77-22	Bimonthly test overpower trip setpoint 110% instead of 109%
Minor	83-15	No high pressurizer trip function
Minor	84-17	Degraded reactor protection system cables
Minor	84-27	Overpower trip setpoint high for 2 of 4 channels
Minor	84-29	Erroneous dropped rod alarm
Minor	85-04	Overpower trip setpoint high for 2 of 4 channels
Minor	85-15	Bad potentiometer caused power spiking
Minor	85-16	Power decrease setpoint was in error
Minor	85-19	Bad potentiometer caused power spiking
Minor	86-21	Channel 34 dropped rod runback setpoint drift
Minor	86-22	Spurious dropped rod indication
Minor	86-23	Spurious dropped rod indication
Minor	86-24	Spurious dropped rod indication
Minor	86-30	Spurious dropped rod indication

compromised by any of the events listed, and there is no reason to believe based on these events that the Haddam Neck RPS is any less reliable than other Westinghouse plants.

8.4.7 Main Steam Line Valves and Instrumentation

Ten events (see Table 8.7) involving the main steam line valves and instrumentation were selected for detailed study by the initial review. Subsequent study identified two of these events as potentially serious from a plant risk perspective.

The first potentially serious event occurred in January of 1976 (LER 76-02). During surveillance testing of #2 MSIV, a limit switch malfunctioned which might have prevented the reactor protection system from receiving a trip signal in case of accidental trip valve closure. No redundant systems were available, although trip signals from other RPS sensors would have provided ample backup to this signal. Overall, the reliability of the RPS would not have been degraded and MSIV closure would not have been prevented. The cause of the problem was attributed to a frozen solenoid.

The other potentially serious event occurred in November of 1984 (LER 84-24). At 25% of full power, one portion of the reactor protection system was found to be inoperable. This portion was the steam/feedwater flow mismatch coincident with low steam generator level reactor trip logic. The problem involved instrumentation which indicated less than normal steam flow. Because the trip signal is based on a steam/feedwater mismatch, the trip signal at low power conditions (25%) would not actuate even if there were no feedwater flow. The problem is only judged to be only potentially serious because at higher power levels (100%), the trip function is not compromised. Further, as above, ample backup to this signal is provided by the RPS. The event was caused by an operator error which left the steam pressure density compensation lines to the four flow transmitters valved out. Corrective action was taken to develop a procedure to check the functional operability of all reactor protection inputs after an extended outage prior to startup.

Overall, none of the events observed would call into question the results of the PSS analysis of this system.

TABLE 8.7. Main Steam Line Valves and Instrumentation

Potential Impact	LER No.	Description
Serious	76-02	Limit switch malfunction might prevent reactor protection system from receiving trip
Minor	76-09	Spurious low flow alarm
Minor	77-20	Repeated attempts necessary to cycle main steam isolation valve
Minor	77-26	Wiring problems in main steam isolation valve circuitry
Minor	78-15	Spurious steam line break alarm
Minor	78-19	Spurious steam line break alarm
Minor	82-03	Valve movement did not meet acceptance criteria
Minor	82-04	Main steam isolation valve disc misaligned
Serious	84-24	Less than actual steam line flow indicated as a result of operator error
Minor	86-29	Main steam isolation valve did not meet acceptance criteria

8.5 Transient Frequency at Haddam Neck

Transient frequencies were reviewed to compare Haddam Neck's performance with the average of all PWRs based on data for the period 1975-1982 (32). Table 8.8 shows the observed frequency and the expected frequency of each transient analyzed in Reference 32 for the period. The expected number of Haddam Neck transients was calculated using the industry mean frequency for PWR operation through 1982.

Haddam Neck's performance appears to be somewhat better than the industry average for the following individual transients:

- Control Rod Drive Mechanism Problems
- Loss or Reduction in Feedwater Flow (1 Loop)
- Feedwater Flow Instability - Operator Error
- Feedwater Flow Instability - Miscellaneous Causes
- Manual Trip - No Transient.

For one transient, loss of RCS flow in one loop, Haddam Neck's performance is somewhat less than the industry average. However, from an overall transient frequency perspective, Haddam Neck's performance is superior to the industry, with less than one-half the total expected number of transients. Part of this better than average performance can be attributed to plant maturation.

It should be noted that the data presented in Table 8.8 does not exactly correspond to the information in the LERs. Reference 32 used existing data published by the Electric Power Research Institute (EPRI) and information from the Nuclear Regulatory Commission's Operating Unit Status Reports. As an example, the three PORV events identified in LERs were not identified as leakage in the primary system in Table 8.8. Also, the pressurizer spray valve failure identified in the LERs was not included in Reference 32.

The actual plant experience data for initiating events was identified and reflected in the PSS. Further discussion of this appears in Section 3.0 of this review.

TABLE 8.8. Haddam Neck Transient Experience Versus Industry Average

		Industry Mean (/Yr)	1975-1982 Expected Haddam Neck	1975-1982 Observed Haddam Neck
1.	Loss of RCS Flow (1 Loop)	0.30	2.4	4
2.	Uncontrolled Rod Withdrawal	0.01	0.08	0
3.	CRDM Problems	0.53	4.2	2
4.	Leakage From Control Rods	0.02	0.16	0
5.	Leakage in Primary System	0.05	0.40	0
6.	Low Pressurizer Pressure	0.03	0.24	0
7.	Pressurizer Leakage	0.01	0.08	0
8.	High Pressurizer Pressure	0.03	0.24	0
9.	Inadvertent Safety Injection	0.06	0.48	0
10.	Containment Pressure Problems	0.01	0.08	0
11.	CVCS Malfunction	0.03	0.24	0
12.	Pressure/Temperature/Power Imbalance	0.12	0.96	0
13.	Startup of Inactive Coolant Pump	0.0	0.0	0
14.	Total Loss of RCS Flow	0.03	0.24	0
15.	Loss or Reduction in Feedwater Flow (1 Loop)	1.57	12.6	3
16.	Total Loss of Feedwater (All Loops)	0.17	1.36	0
17.	Full or Partial Closure of MSIV (1 Loop)	0.17	1.36	1
18.	Closure of All MSIV	0.04	0.32	0
19.	Increase in Feedwater Flow (1 Loop)	0.46	3.68	2

TABLE 8.8. Haddam Neck Transient Experience Versus Industry Average (Continued)

		Industry Mean (/Yr)	1975-1982 Expected Haddam Neck	1975-1982 Observed Haddam Neck
20.	Increase in Feedwater Flow (All Loops)	0.02	0.16	0
21.	Feedwater Flow Instability - Operator Error	0.30	2.40	0
22.	Feedwater Flow Instability - Miscellaneous Causes	0.35	2.8	0
23.	Loss of Condensate Pumps (1 Loop)	0.07	0.56	0
24.	Loss of Condensate Pumps (All Loops)	0.01	0.08	0
25.	Loss of Condenser Vacuum	0.15	1.20	0
26.	Steam Generator Leakage	0.03	0.24	0
27.	Condenser Leakage	0.04	0.32	0
28.	Miscellaneous Leakage in Secondary System	0.09	0.72	2
29.	Sudden Operation of Steam Relief Valves	0.02	0.16	0
30.	Loss of Circulating Water	0.06	0.48	0
31.	Loss of Component Cooling Water	0.02	0.16	0
32.	Loss of Service Water System	0.01	0.08	0
33.	Turbine Trip, Throttle Valve Closure, EMC Prob.	1.24	9.92	7
34.	Generator Trip or Faults	0.46	3.68	4
35.	Total Loss of Offsite Power	0.16	1.28	1
36.	Pressurizer Spray Failure	0.03	0.24	0

TABLE 8.8. Haddam Neck Transient Experience Versus Industry Average (Continued)

	Industry Mean (/Yr)	1975-1982 Expected Haddam Neck	1975-1982 Observed Haddam Neck
37. Loss of Power to Necessary Plant System	0.10	0.8	0
38. Spurious Trips Cause Unknown	0.09	0.72	0
39. Auto Trip - No Transient	1.47	11.76	8
40. Manual Trip - No Transient	0.47	3.76	1
41. Fire Within Plant	0.02	0.16	0
TOTAL ALL TRANSIENTS	8.84	71	35

8.6 Potential Impact of Events Observed at Other Plants on Haddam Neck

PWR events identified in the Accident Sequence Precursor program were reviewed for applicability to Haddam Neck. These events include core damage initiators, total system failures (even if potentially recoverable) and multiple system degradations. For many events, the actual failure mechanisms are quite plant specific and cannot be "mapped" directly to another plant except at a general train or higher level. This is all the more true at Haddam Neck, since the detailed system designs date from early stages of the commercial nuclear power program.

For the time period applicable to this study, thirty-five precursors were identified from References 28 to 31 as having potential applicability to Haddam Neck. These are shown in Table 8.9. For this identification, events involving failure modes believed applicable to Haddam Neck were selected. Precursors which involved unique electric bus arrangements and control systems (such as the ICS in B&W plants) and precursors of a type already observed in the LER data base for Haddam Neck (such as losses of offsite power and spurious PORV openings) were not included in Table 8.9.

Because of the relatively long operating history of Haddam Neck, observed performance is considered a better indicator of future performance than events observed at other plants, except in cases where the expected number of events of a particular type is low. Such events include total system failures and unusual initiators. Other events listed in Table 8.9 include RCP seal failures, inadvertent safety-related bus load shedding and a partial loss of DC power. Several AFW system failures are listed for Davis-Besse and Turkey Point. These are of interest since these two plants also utilize AFW systems with only turbine-driven pumps.

The events listed in Table 8.9 formed a basis for a completeness check of procedures and reliability/risk models for Haddam Neck. While hardly any event will directly correspond in all details to a failure possibility at Haddam Neck, the application of reasonable extrapolation from the events listed to the plant was beneficial. Without exception, the review found no events on the list which would necessitate a modification to the Haddam Neck plant models.

TABLE 8.9. Accident Sequence Precursors With Potential Applicability to Haddam Neck

NSIC Accession Number	Description
NUREG/CR-2497 (Reference 1):	
103077	RCP Seal Failure at Robinson.
104087	Safety Injection Tank Valves Closed at Maine Yankee. Valves were assumed locked open when in fact they were locked closed.
116212	Inadvertent Load Shedding on Safety-Related Buses at Millstone 2. This was due to incorrect set undervoltage relays.
120207	Failure of Charging Pump Supply Valves from RWST to Open at Trojan. Both valves had been manually closed using excessive force.
120995	Suction (Sump Isolation) Valves to Decay Heat Pumps Fail to Open at Rancho Seco. The torque switch bypass switch setpoints required adjustment.
123118	Both AFW Pumps Unavailable at Rancho Seco. This was caused by improper manual/overspeed trip reset on one pump when the other was unavailable due to maintenance.
127384	Dummy Loads Installed in All Safety Systems at Zion 2. This resulted in total draining of the pressurizer while in hot shutdown.
130788	Half-trip of SFRCS Causes RCS Pressure Rise at Davis-Besse 1. PORV failure resulted from incorrectly-assembled control circuit. Pressurizer level went to maximum and HPI was run back. U Tube SG capacity would increase the response time for this transient at Haddam Neck.
132979	Both Diesel Generator Fuel Supply Valves Found Shut at Millstone 2.
133706	Control of Both Auxiliary Feed Pump Turbines Lost at Davis-Besse 1. Control of one pump was lost due to mechanical binding; the other due to a blown fuse.

TABLE 8.9. Accident Sequence Precursors With Potential Applicability to Haddam Neck (Continued)

NSIC Accession Number	Description
137305	Auxiliary Feedwater System Failure at Farley 1. This was due to failure of turbine AFW pump to start and open recirculation valves on all three pumps.
137384	Two Makeup Pumps Trip During Testing at Three Mile Island 2. In one case a lube oil pressure timer failed to close, in the other a relay failed to disengage.
139573	Both Diesel Generators Inoperable at Cook 2. The second diesel was incorrectly removed from service because the operator entered the wrong DG room after the first DG had been removed from service in the control room.
143296	Both RWST Outlet Valves Inadvertently Closed at Maine Yankee During Surveillance Testing. During later LPSI pump operability checks, the pumps failed to develop adequate discharge head.
146540	Both Diesel Generators Out of Service at Kewaunee. One diesel was removed from service for maintenance. The second diesel (operability had been initially confirmed) subsequently failed due to a blown fuse.
147399	Both Diesel Generators Unavailable at Kewaunee. One diesel was unavailable because of maintenance. The second failed due to improper gear alignment and failure of a limit switch.
147400	Both Main Steam Isolation Valves Fail to Close at Point Beach 2. This was due to deposits on valve shaft or packing gland hardening.
148764	Steam Dump Valves Fail to Close Following Load Rejection at Beaver Valley 1. The valves failed because their operators were exposed to cold temperatures due to improperly adjusted dampers.
149250	Two Main Steam Isolation Valves Fail to Close at Trojan. This was due to binding between the stems and packing.
152563	Tube Break Occurs in Steam Generator at Prairie Island 1.

TABLE 8.9. Accident Sequence Precursors With Potential Applicability to Haddam Neck (Continued)

NSIC Accession Number	Description
153003	LPR Service Water Valves Left Closed Following Testing at Oconee 2. This was caused by personnel error and failure to include the valves in a revised checklist.
153164	Core Damage and Radioactivity Release Occurs at Three Mile Island 2. This was due to loss of feedwater, AFW inoperability, stuck open PORV and reactor isolation of HPI on high pressurizer level. U tube steam generator capacity would have increased the response time in this transient at Haddam Neck.
154286	Safety Injection Pumps Fail at Salem 1. This was due to loose impeller locknuts resulting in worn spacer sleeves and a bent impeller.
154639	Both Diesel Generators Inoperable at Davis-Besse 1. One diesel was removed from service for maintenance. The second DG was inadvertently removed from service when a technician opened its output breaker in lieu of the first DG's output breaker.
NUREG/CR-3591 (Reference 2):	
156204	Failure of MSIVs to Close on Demand at Trojan. Three of four valves failed to close due to sticking valve stems.
158650	Failure of Service Water System at Calvert Cliffs 1. Both service water trains were rendered inoperable when a non-safety portion of the system was returned to service following maintenance. Air had leaked into that portion of the system due to leaks in a compressor aftercooler. When the non-safety portion was returned to service, the air travelled to both safety-related portions of the system, resulting in loss of pump suction in both trains. After the plant was shutdown, both condensate tanks were inadvertently isolated from the AFW system.
163356	Output Breakers for Both Station Batteries Inadvertently Opened at Palisades.
163499	Reactor Coolant Pump Seal Failure at Arkansas Nuclear 1.

TABLE 8.9. Accident Sequence Precursors With Potential Applicability to Haddam Neck (Continued)

NSIC Accession Number	Description
164617	Partial Loss of DC Power and Diesel Generator Trip at Millstone 2. The loss of one DC bus was caused by personnel error. This was a complicated transient, the details of which were most likely plant specific. However, it pointed to the need for DC power failure analysis on all plants.
166650	Safety Injection Supply Valve Found Unlocked and Closed at Beaver Valley. This rendered the safety injection system unavailable. This event was associated with an earlier event, involving tampering with the EFW locking chains.
171733	Unavailability of Three Auxiliary Feedwater Pumps at Zion 2. The turbine driven pump was unavailable because of maintenance. The two motor driven pumps failed to start due to inproperly sensed low suction pressure caused by reverse flow in the pressure switch sensing lines.
NUREG/CR-4674 (draft) (Reference 4):	
LER 250/85-019, 021	Multiple AFW Train Failures Following LOFW from Hot Standby at Turkey Point. Multiple AFW pump and associated valve failures occurred in conjunction with recovery from a trip.
LER 309/85-009	No Trip Signals would have existed for SG Isolation in Event of a SLB at Maine Yankee. This was due to a procedure error which resulted in nine of 12 steam flow transmitter root valves not being opened following testing.
LER 318/85-006	Unavailability of Emergency Power at Calvert Cliffs 2. Both DGs had been damaged due to interphase connecting bus on one DG rotor breaking free and damaging its stator and associated cracks on the second DG.

TABLE 8.9. Accident Sequence Precursors With Potential Applicability to Haddam Neck (Continued)

NSIC Accession Number	Description
LER 346/85-013	LOFW and AFW failure at Davis-Besse due to pump and valve problems. While the initial AFW trip associated with this event is plant specific, subsequent AFW inoperability may not be.

Note: Prior to 1984, losses of feedwater were typically non-reportable and hence not documented in the ASP program unless an additional system failure or multiple degraded systems also occurred during the event. The 1985 precursor reviews include such events and document losses of feedwater with simple AFW train unavailabilities as well. These events may also be applicable to Haddam Neck.

8.7 Summary

Approximately 297 Licensee Event Reports (LERs) for the Haddam Neck Plant were reviewed to identify events or trends which might indicate an inherent weakness in the design or operation of the plant. The review focused on accident mitigating systems and priority was given to those systems necessary for mitigation of Haddam Neck's most frequent transients. Events which would marginally degrade the operation of an important system were categorized as minor events. Events which would jeopardize the successful response of a system to a transient were categorized as potentially serious events. The twenty-seven potentially serious events identified in this review are listed in Table 8.10. Although Haddam Neck has experienced a lower transient frequency than the industry average, potentially serious events appear to recur in a few important systems. However, the operating experience review has not identified any events which were omitted from the PSS in such a way as to have a material effect on the results or which would require any modification to the models or data used in the PSS.

TABLE 8.10. Potentially Serious Events Identified

LER No.	Description
75-04	Service water to all four containment recirculation fan coolers was lost
76-02	Main steam limit switch malfunction might prevent reactor protection system from receiving trip signal
76-06	Diesel generator tripped on overspeed
76-16	Both auxiliary feed pumps vapor bound
77-07	Charging Pump A runs hot; bearings replaced
77-15	Auxiliary feed pump B fails to meet test by 200 psig
78-06	Calculations determine diesel generators have potential for overload
78-20	Controller failure caused charging flow control valve to close
79-10	Pilot operated relief valve and isolation valve opened
80-03	Review showed potential overload for diesel generator
80-04	Pilot operated relief valve and isolation valve opened
81-03	Pilot operated relief valve and isolation valve opened
81-08	Auxiliary feed pump B down due to leak; A pump recirculation valve closed
81-10	Charging Pump B oil leak
81-11	Diesel generator overloaded itself
81-14	Cooling leak on diesel generator B
81-19	Excessive vibration on charging pump
82-01	Both A and B battery chargers powered by diesel generator B
83-09	Unable to turn charging pump due to solidified boric acid
83-20	Loss of control to pilot operated relief valve

TABLE 8.10. Potentially Serious Events Identified (Continued)

LER No.	Description
83-21	Loss of control to pilot operated relief valve
83-23	Diesel generator B assumed load greater than governor setting
84-14	Circuit breaker on diesel generator failed to close in for 20 min
84-24	Less than actual steam line flow indicated due to operator error
85-05	Valve problem required operator action to get feedwater into Loops 1 and 4
85-29	Interdependency could prevent flow of service water to both diesels
86-18	Instrument uncertainties could cause no recirculation flow and inadequate core cooling

9.0 REVIEW OF THE HADDAM NECK PSS EVENT TREE QUANTIFICATION

In the Haddam Neck PSS, a support state methodology was used for the development and quantification of the core melt model. (This methodology is described in Chapter 7 of Reference 34.) As described in Section 5, system fault trees were developed and quantified for several different combinations of support system failures, or support states. The support states are themselves delineated by means of a support state event tree. The event trees for each initiator were quantified in each support state. (The support states used in the Haddam Neck PSS are listed in Table 5.1.) By using the support state methodology, the effects of system interactions between front line and support systems are removed from the fault trees and handled in the quantification of the event trees. Each event tree node is treated as an independent event in relation to the other event tree nodes in each sequence.

This section is limited to a review of the quantification procedure used in the PSS and is intended to verify the proper use of the information used in the event tree quantification. This information includes the results of the system reliability analysis, the human reliability analysis, the event tree development, and the initiating event frequency analysis. The review also is intended to assess the impact of assumptions used by the PSS analysts to simplify the quantification procedure. The impact of changes in the plant model recommended on the basis of the review is examined in Section 10, which describes the requantification effort.

9.1 Haddam Neck PSS Quantification Procedure

The event tree quantification procedure used in the Haddam Neck PSS consists of two steps. The first quantifies the probability of each combination of support system failures (support states) occurring after an initiating event. The probability of the support system failures is referred to as the "support state split fraction." The second step quantifies the event trees generated for each initiating event for each support state. The results of the event tree quantifications are then summed to determine each plant damage state frequency and the total core melt frequency.

A matrix multiplication methodology is used to generate the plant damage state frequencies from which the total core melt frequency is calculated. Both the support state event tree and the event trees for each initiating event are quantified using a computer code "ARBRE" (1) which multiplies the appropriate system failure and success probabilities to quantify each sequence probability. For the support state event tree, the sequence probability, and in some cases the combination of sequence probabilities, represents the support state split fraction. In the definition of the support states, support system failures deemed to have similar impacts on the front line systems were grouped together as a single support state.

The event trees are quantified using the initiating event frequencies, the results of the system reliability analysis, human reliability analysis, and the additional quantification of special events (such as bleed-and-feed, consequential LOCAs, recovery of offsite power). Each of the headings on the event tree is treated as an independent event by the computer code that performs the quantification. While in most cases these events are independent, in some cases conditional failure probabilities for the events were used to account for dependencies. For example, the containment heat removal node on each event tree is dependent on the success or failure of long-term cooling following bleed-and-feed. The probability of this node was calculated for the two cases where long-term cooling succeeded and where it failed and the appropriate conditional probability was used for different sequences in the same event tree.

Two types of human errors are incorporated in the event tree quantification. Cognitive human errors are treated as individual events on the event trees and are treated in much the same way as system failures. The manipulative operator errors that were removed from the system fault tree analysis are included as part of the quantification of the event tree nodes along with the mechanical system failures. Each system failure probability used in the quantification of the event tree nodes is a combination of manipulative human error probabilities and mechanical system failure probabilities.

Once the event trees have been quantified for each support state, a single sequence probability is generated to account for the contributions from all sixteen support states. This is done by multiplying the support

state-dependent sequence probability by the support state split fraction and summing the products. The probabilities of all sequences resulting in the same plant damage state (The definition of the plant damage state is provided in Section 4.) are summed, and the resulting probability becomes an element in the "M matrix." Thus, the M matrix element M_{IP} is the conditional probability of plant damage state P for the I^{th} initiator. A row of elements represents the probabilities of all plant damage states given an initiator. A column of elements represents the probability of a particular plant damage state for each initiator.

Using the code "PHIM" (1), the M matrix is multiplied by the Φ matrix, a vector matrix of initiator frequencies. The elements of the resulting one-dimensional matrix are the frequencies of each plant damage state, which are summed to yield the total core melt frequency.

Uncertainties, in the form of variances, were calculated for component failure probabilities, initiator frequencies, and most system failure probabilities. However, no uncertainty analysis was performed in the PSS at the event sequence or core melt frequency level.

9.2 Review of the Haddam Neck PSS Quantification Procedure

The review of the PSS event tree quantification was undertaken for two reasons. The first was to confirm our understanding of the procedure used to quantify the event trees and the second was to verify the accuracy of the results of the event tree quantification. In no PRA is the quantification procedure as simple as a description of the process would imply. Subtle modifications of the procedure are made primarily to eliminate the cumulative impact of conservatisms within the analysis. It was necessary to identify these modifications to the basic quantification procedure (some of which were not described in the PSS documentation) so that we would have more confidence in the results of the PSS and our requantification effort. Differences between the PSS results and the requantified results based on the changes recommended from the reviews of the system, human error, data, initiator, and event tree analyses reviews can be attributed to those changes with a great deal more confidence than if this quantification review had not been performed.

Modifications to the Haddam Neck PSS event tree quantification procedure made by the PSS analysts themselves range from considering special case system dependencies to revising the loss of offsite power (LOSP) recovery model for station blackout sequences. The more significant of these modifications are described in the next three paragraphs. All are appropriate and result in a better model of the Haddam Neck Plant.

In the Haddam Neck PSS, a time-dependent LOSP and diesel generator failure model was used to model the station blackout sequences involving the failure of the diesel generators. The model accounted for the longer recovery periods available for a LOSP if one diesel generator initially operated properly but subsequently failed. The lower probability associated with the longer periods of unavailability of offsite power resulted in a reduced frequency for this type of event. Also related to a LOSP, the treatment of system failure probabilities after a recovery of offsite power was dependent on the type of system (normally operating or standby) and the support state in which the event tree was being evaluated. The loss of offsite power affects the failure probability of a running system even if power is ultimately restored (normally running equipment must be restarted) while it has little effect on standby equipment, provided emergency power is available. Comments on how the effect of various support states were handled are contained in Section 9.3.

Two modifications to the event tree quantification procedure involved the treatment of the primary integrity (PIT) or consequential LOCA (S2) event. In the loss of DC 1 event tree the event tree node for charging was modified to take credit for those system failures that resulted in PIT failure but did not fail the charging system when used for vessel injection. Normally, a PIT failure is assumed to result from a charging system failure (due to a loss of RCP seal cooling). However, for this initiating event, component failures that fail the charging systems RCP seal cooling capability but not the injection capability are significant contributors to PIT failure probability. This dependency is treated in the event tree quantification. In the general plant transient analysis, a transfer is made to the consequential LOCA tree. For support states where MCC-5 has failed, the PIT analysis is substituted for the S2 consequential analysis LOCA. (For more details, see Section 9.3.)

Human error probabilities were often modified within one event tree to account for different stress levels, time available to perform actions, etc. Not all such modifications were adequately documented in the event tree quantification. For example, OA6, the cognitive decision to isolate a failed steam generator, is modified for cases where less time is available to isolate the steam generator. This modification is modeled in the human reliability analysis but the event sequences for which it was applicable were not defined in the event tree quantification. As part of the review it was determined that this modified value was used for sequences where reactor pressure was not reduced.

The review was performed using two SAIC proprietary computer codes, Event Tree Analysis (ETA) (35), and the Risk Management Query System (RMQS) (3). ETA is a PC-based code that can be used to draw and quantify event trees. Quantification is performed by assigning point estimates to event tree nodes, which are treated as independent events. ETA was used primarily on event trees which were quantified in relatively few support states, such as the Station Blackout event tree, which was evaluated in only three support states. This code will evaluate the sequence frequencies for each accident sequence taking into consideration both system successes and system failures. As with the code used in the Haddam Neck PSS, all event tree nodes are treated as independent events. All of the event trees were quantified using the code RMQS, including those originally screened using the ETA code. The PC-based RMQS code is designed to accept as input the sequence cut sets, data for each element of the cut sets and the plant damage state for each cut set. This data is then used to calculate several risk measures, including core melt frequency, and the code can sort the dominant sequences using several parameters, including sequence frequency and failed systems. In this review, the event tree sequences were input into RMQS in the form of the cut sets, systems were used as elements of the cut sets rather than components. This was possible since the PSS provided independent failure probabilities for each system in all the necessary support states. By making this change to the RMQS input, RMQS could be used in the same way in which the event tree analysis code in the PSS was used.

In our review, we quantified all the PSS event trees using the PSS assumptions and data. In many cases, the information presented in the PSS was not sufficient to reproduce the intermediate PSS steps. In these cases,

discussions with the utility analysts were necessary to clarify these points. Also, in some cases, after quantification of an event and generation of the dominant accident sequencies, the results were substantially different from the PSS results. It was obvious that some other modeling techniques beyond those presented in the PSS documentation were used for the quantification of these particular trees. Many of these differences were the result of the modifications made to the models during quantification which have been discussed in the preceding paragraphs. In these cases also, the discrepancies in the results were discussed with utility analysts and resolved.

The result of quantification of the PSS event trees was the generation of all the dominant core melt sequences and their frequencies. The review of these results is discussed in the next section.

9.3 Results of the PSS Quantification Procedure Review

Our review of the PSS quantification resulted in two types of comments. The first set deals with the impact of some assumptions made during the PSS quantification on the study results. The second set deals with errors made in quantifying the PSS event trees. The errors found were all relatively minor, having a total numerical impact of less than 2% of the core melt frequency, and do not change perceptions of the areas of plant vulnerability.

9.3.1 Assumptions

Multiple support system failure combinations treated as one support state

The assumption in the event tree quantification that was found to have the largest impact on the results of the PSS dealt with the combination of support system failures with similar effects on front-line systems into a single support state. The one support state of interest is support state 6, which is listed as being the failure of both DC power trains and MCC-5. This support state is comprised of three support system failure combinations: the loss of DC bus 1 and MCC-5, the loss of DC bus 2 and MCC-5, and the loss of both DC buses and MCC-5. The most conservative support system failure combination was used in the quantification of system failures in

this support state. However, the support state split fraction is dominated by the failure of either DC bus and MCC-5. (The probability of both DC buses and MCC-5 failing is more than three orders of magnitude less than that for the failure of a single DC bus and MCC-5.) The importance of this difference can be seen by evaluating the MCC-5 event tree in support state 6 under the assumptions that one DC bus is unavailable or that both DC buses are unavailable.

As quantified in the Haddam Neck PSS (assuming both DC buses are unavailable), the dominant sequences for a loss of MCC-5 with the failure of both DC buses contribute 1.3E-5/yr to the core melt frequency. This is more than one third of the core melt frequency associated with a loss of MCC-5 initiator (total of 3.36E-5/yr) and almost all of the core melt frequency associated with support state 6 (total of 1.65E-5/yr). These sequences are primarily the result of the failure, with a probability of 1.0, of primary integrity and bleed-and-feed given that MCC-5 is originally unavailable and both DC buses fail. (The loss of MCC-5 causes the running charging pumps to trip and without DC power the HPSI and charging pumps cannot start. These pumps are required for bleed-and-feed operations and the charging pumps are needed to maintain primary integrity.)

If the loss of MCC-5 event tree is requantified assuming that only one DC bus was originally unavailable, the charging and HPSI systems no longer fail with a probability of 1.0. Additionally, the values for several other system failure probabilities drop substantially. For instance, local manual control of the auxiliary feedwater system is no longer needed if one DC bus is available and MCC-5 is recovered. This results in a much smaller failure probability because the human actions which dominate auxiliary feedwater failure when both DC buses are unavailable are no longer required. The result of the requantification, using the system and human error data in the PSS, is a core melt frequency contribution of approximately 4E-6/yr, a reduction of almost 9E-6/yr from the contribution calculated in the PSS.

Impact of Offsite Power Recovery

A second assumption made in the Haddam Neck PSS was that for some support states, a recovery of offsite power would not result in the recovery of AC power to the emergency buses. The support states affected are those

in which there is a loss of offsite power and either a DC or AC bus failure. If the bus failure is due to a DC bus failure, which will fail the AC power supply, motive and control power for the AC breakers is not available. Therefore, even with a recovery of offsite power, the AC breakers needed to restore AC power would not be able to close. In the PSS it was conservatively assumed that for these support states a DC bus was always unavailable, even though the split fraction for each of these support states is dominated by a failure other than a DC bus failure, either an AC bus failure or service water failure.

This assumption had virtually no effect on the results of the PSS. In the course of this review, those sequences affected by this assumption were identified and requantified assuming that AC power was recoverable. The total change in the calculated core melt frequency was on the order of 10^{-7} per year. There were some minor changes to the dominant sequences. Specifically, for Station Blackout support state 11 (all support systems failed), the sequences that involve failure of bleed-and-feed are less dominant than listed in the PSS. However, this is offset by the increased frequency of sequences resulting from the failure of long term cooling.

Consequential LOCAs

The PSS defines two events which are both consequential LOCAs, S2 and primary integrity (PIT). The analysis performed to quantify the S2 event is generally less detailed and more conservative than the analysis for PIT. This is particularly true for support states other than support state 1, where no support systems are failed. However, during the review it was found that for sequences involving the S2 event and a support state other than support state 1, the analysis was requantified using the more complete PIT analysis instead of the S2 analysis.

For example, quantifying the general plant transient followed by an S2 consequential LOCA in support state 12 (MCC-5 unavailable) results in some high frequency core melt sequences. Reevaluating these sequences using the assumptions of the PIT analysis (essentially, reevaluating this sequence of events as a loss of MCC-5 initiator using the product of the general plant transient frequency and the split fraction for support state 12 as the

initiating event frequency) effectively eliminates any significant contribution of this combination of events to the core melt frequency. The underlying assumption is that the general transient followed by a loss of MCC-5 is not different from the loss of MCC-5 as an initiating event.

In all cases where we were able to identify differences in the S2 and PIT analyses (and these differences could significantly affect the quantification results), the more detailed PIT analysis appears to have been used in the PSS. The differences in the S2 and PIT analysis therefore did not conservatively bias the results of the PSS when the S2 consequential LOCA analysis was used.

9.3.2 Quantification Errors

Some errors were made during the quantification of the Haddam Neck PSS. The largest effect any of these individual errors had on the core melt frequency was of the order of 5E-6/yr, approximately 1% of the total core melt frequency, and collectively the total effect on the core melt frequency is less than 1E-5/yr, approximately 2% of the total core melt frequency.

S2: Consequential LOCAs

The two errors that led to the largest difference appear in the quantification of the S2 consequential LOCA. The first error appears to be the misuse of the numerical value for the fraction of consequential LOCAs that are due to RCP seal failures versus relief valve (SRV or PORV) failures for the accident sequences following an LOSP and a failure of one AC or DC bus. (The second error is discussed in the next subsection.) According to data in the PSS, 34% of these consequential LOCAs are the result of seal failures. It appears that in quantifying this event tree, 34% of the consequential LOCAs were attributed to relief valve failures. The significant impact of this reversal of data is that the frequency of the dominant sequence of an LOSP followed by a seal failure and high pressure injection failure is a factor of 2 higher in the PSS than it should be, 1E-5/yr instead of approximately 5E-6/yr.

Human Reliability Analysis Probabilities

Several human error probabilities used in the PSS event tree quantification are not in agreement with the values recommended in the human reliability analysis performed in the PSS. These operator actions are:

- OA2 and OA3 in the Consequential LOCA event tree - OA2 is the cognitive error to go to recirculation and OA3 is the cognitive error to fail to depressurize. The human reliability analysis suggests values of 1.0E-3 and 1.2E-2 respectively.

- OA8 (the cognitive error to initiate feed and bleed) is not modified for the support state 10 in the loss of offsite power and one emergency bus event tree when offsite power is not recovered.

- In the steam generator tube rupture event tree the recommended value of 1.7E-2 does not appear to have been used for OA6, the cognitive error to isolate the faulted steam generator.

- In the event tree for an LOSP with one diesel generator unavailable, a value of 5.0E-2 was recommended for O17 (the cognitive error to restore main feedwater) but apparently not used.

The values stated above for each operator action are derived from the review of the human reliability analysis of the PSS (see Section 7). Collectively, these discrepancies result in an increase of less than 5.0E-6/yr in the core melt frequency for the Haddam Neck plant. More importantly, there are no significant changes in the list of dominant accident sequences or to perceived areas of plant vulnerabilities.

Loss of DC Power Initiators

In the PSS there is an inconsistency in the treatment of the total loss of DC power that results in a double counting of the contribution of this initiator to the core melt frequency. The total loss of DC power initiator is defined as the loss of one DC bus followed by the random

failure of the second DC bus. This is the same definition used for the loss of a single DC bus initiator in the loss of both DC buses support state. To avoid the double counting of the total loss of DC power from the total loss of DC power initiator and the total loss of DC power support state following the loss of a single DC bus initiator, the split fraction for the total loss of DC support state for the loss of DC bus 1 or 2 initiator should be set to 0.0 instead of the 4.6E-4 value used in the PSS. The estimated impact of this correction is a reduction in the core melt frequency of approximately 2.5 E-6 per year. This reduction was estimated by subtracting from the total core melt frequency attributed to the total loss of DC support state (7.3E-6/yr) the contribution from the total loss of DC initiator (4.4E-6/yr) and an estimate of the contribution from all other initiators in the total loss of DC support state (approximately 3.0E-7).

Recovery of Offsite Power

Finally, in the quantification of the loss of offsite power event tree, the absolute value for ER3, the failure to recover offsite power given an earlier failure to recover power, was used instead of the conditional probability for ER3. The conditional value varied from 0.72 to 0.12 depending on the sequence being analyzed; the absolute value is 0.06. Although this error appears in the Station Blackout event tree for each support state analyzed, only in support state 14 (loss of both diesel generators) does it have a noteworthy impact. Specifically, the frequency of the sequence that involves a failure to recover offsite power and the failure of auxiliary feedwater is an order of magnitude smaller than it should be. Using the Station Blackout analysis of the PSS for a period of 100 minutes (the time to core uncovery with no steam generator cooling), this sequence has a probability of approximately 2E-6/yr compared to approximately 1 0E-7/yr given in the PSS. The expression used is

$$FSB(100\ min) \cdot P(AF4) \qquad (9.1)$$

where FSB(100 min) is the frequency of 100 min station blackout due to a loss of offsite power and both diesel generators failing = 1.79E-4/yr * exp (-0.274 * 100/60)

P(AF4) is the auxiliary feedwater failure probability with local control required = 0.017

The expression used to calculate FSB(100 min) takes into account the recovery of offsite power during the 100 minutes after a total loss of power and before the core becomes uncovered. This expression was used for the dominant accident sequence for a station blackout with both diesel generators failed and offsite power not recovered within eight hours and is a more detailed analysis than the more conventional analysis, which just multiplied the frequency of the LOSP and failure of both diesel generators by recovery factors.

9.3.3 Summary

In summary, the quantification process used in the Haddam Neck PSS contained a few errors and conservative assumptions that had a small effect on the outcome of the study. Numerically, the effect of these errors on the total core melt frequency was on the order of 2%. More importantly, these errors had almost no effect on the selection of dominant accident sequences and the perceived areas of plant vulnerability.

10.0 MODEL REQUANTIFICATION, RESULTS AND INSIGHTS

The core melt model for the Haddam Neck Plant was revised based on changes to the event trees discussed in Section 4.0. The revised event tree model was requantified using changes in the initiating event frequencies, system models, component data, and human error probabilities produced in this review. The results derived from the revised model are discussed in this section.

10.1 Requantification Process

The requantification process was begun with preparation of the revised event trees for the RMQS code (3). Table 10.1 shows the list of fourteen revised event trees based on the review presented in Section 4.0 of this report. In addition, as was discussed in Section 4.0, a new initiator (small-small LOCA) was created from the lower end of the small LOCA range, which required the development of an additional tree. Thus, a total of fifteen event trees were modified in the requantification process.

The changes to the fifteen event trees mentioned above fall into two categories. The first consists of changes due to disagreements with the assumptions used in modeling of the sequences of events in the Haddam Neck PSS. An example of this category is treatment of consequential Reactor Coolant Pump (RCP) seal failure, which can occur due to loss of cooling to all four RCP seals. In the PSS, this event was assumed to lead to a total leak rate of 200 gpm based on the assumption of a maximum leak rate of 50 gpm per RCP seal. This led to the PSS assumption that normal plant makeup capability is sufficient to compensate for this leak rate. In our review, this leak rate was not accepted and a higher leak rate, on the order of 100 gpm average flow rate per RCP seal, was suggested. This resulted in major changes to a series of event trees since at the higher leak rate the event becomes similar to a small-small break LOCA with the requirements of high pressure injection for keeping the core covered in the short term and high pressure recirculation for long-term heat removal.

The second category of changes to the event trees consists of those changes necessary to check the validity of simplifying assumptions made in the PSS. The objective of these simplifying assumptions in the PSS

Table 10.1 List of Event Trees That Were Modified in this Review

1.	Small-Break LOCA (New "small-small break" and "small-break" LOCA event trees were generated in this review)
2.	Steam Generator Tube Rupture
3.	Unisolated RCP Seal Leak
4.	Loss of DC Bus 2
5.	Loss of Offsite Power and MCC-5
6.	Station Blackout
7.	Insufficient Flow of Service Water
8.	Loss of Control Air
9.	Loss of MCC-5
10.	Total Loss of DC Power
11.	Loss of DC Bus 1
12.	Loss of Semi-Vital AC
13.	Consequential Small LOCA
14.	Consequential Steam Generator Tube Rupture

was to reduce the size of the event trees, as discussed in Section 4. For example, in some event trees the tree headings are placed in non-chronological order for the sake of simplifying the event tree and reducing the number of sequences. In other cases headings or event trees are combined based on the judgment that the results would not be significantly affected. Even though there is no fundamental question about the way the plant's response is modeled, there is a need to confirm that the simplifying assumptions used in the PSS do not result in incorrect accident sequences.

Following these revisions to the event trees, the entire model, consisting of the revised and unrevised trees, was requantified incorporating changes to initiating event frequencies, component data, system unavailabilities, and human error probabilities. Table 10.2, reproduced from Table 3.5, shows the changes to the initiating event frequencies used in the requantification process. Table 10.3, reproduced from Tables 7.5 and 7.7, shows changes or additions to the cognitive and manipulative human error probabilities used in the quantification. Finally, some changes to the system unavailabilities were made due to changes in the system models discussed in Section 5.0 and changes to the component data discussed in Section 6.0. The results of these system unavailability changes for different support states and event trees are shown in Table 10.4.

10.2 Results of the Requantification

The change in core melt frequency for each initiator category is shown in Table 10.5. In the table the PSS results are arranged by decreasing contribution of each initiator category to the core melt frequency. The review results shown are the revised core melt contributions for each of these categories developed from our revised model. The total core melt frequency as a result of the requantification increased from 5.4E-4 per year to 8.1E-4 per year, i.e., by about 50%. This change in core melt frequency by itself is not very significant. What is significant are changes in the contribution of different initiators to the core melt frequency, the creation of new dominant accident sequences, and the rearrangement of the PSS dominant core melt sequences as a result of our review and requantification. Figure 10.1 compares the relative contribution of each initiator from the PSS with the contribution from the review requantification. The remainder of Section 10.2 discusses the specific

Table 10.2 Changes in Accident Initiator Frequencies Used in the Requantification Process

Initiator	Frequency (Per Year) PSS	Suggested
Large-Break LOCA	3.9E-4	2.6E-4
Medium-Break LOCA	6.1E-4	7.9E-4
New Small-Break LOCA	-	2.0E-3
New Small-Small Break LOCA	-	6.2E-4
Interfacing System LOCA in CVCS Letdown Line	4.9E-6	9.6E-6
Steamline Break Downstream of Nonreturn Valve	8.0E-3	2.2E-3
Loss of Instrument Air	1.1E-2	7.0E-4
Loss of MCC-5	1.4E-2	2.1E-3

Table 10.3 Human Error Probabilities Changed or Added in the Review

Human Error		Human Error Probability PSS	Suggested
Cognitive			
OA-2	(Initiate Recirculation) For Small LOCA	1.0E-2	1.0E-3
OA-2	For Small-small LOCA	N/A	1.0E-4
OA-8	(Initiate Bleed-and-Feed) Given Failure at OA-21	N/A	3.3E-1
OA-8	Given Failure at OA-17 and OA-21	N/A	1.0
OA-8	For simple scenarios	5.0E-3	1.0E-2
OA-8	Secondary Blowdown and LPI mode	N/A	5.0E-3
OA-17	(Initiate Main Feedwater Recovery) Given Failure at OA-21	N/A	3.3E-1
OA-20	(Initiate Recovery of Service Water)	N/A	2.0E-4
OA-21	(Initiate Local Control of AFW)	N/A	3.0E-2
Manipulative			
HPR	(High Pressure Recirulation) For Medium LOCA	2.5E-3	1.7E-2
HPR	Given Failure at OA-18 or RMC	N/A	5.0E-3
HPR	Given Secondary Blowdown Successful	N/A	1.4E-3
LPR	(Low Pressure Recirculation)	1.4E-3	9.3E-3
CHG	(Manual Charging Initiation)	6.0E-3	3.0E-3
LTC	(Long Term Cooling)	5.2E-3	1.7E-3
BAF	(Bleed-and-Feed)	1.0E-2	6.0E-3
AF4	(Local Manual Control of AFW)	2.6E-3	1.5E-3
RSW	(Service Water Recovery, Long Term)	N/A	2.5E-3
BLED	(Primary Bleed Using PORVs)	N/A	3.0E-3
SBD	(Secondary Blowdown Using S/G Atmos. Dump Valves)	N/A	3.0E-3

Table 10.4 Results of the Review of the Haddam Neck PSS System Unavailabilities

System	Failed Support State	Unavailability		Major Reason(s) for the change in System Unavailability
		PSS	Suggested	
AC Power		3.9E-3	2.9E-3	Lower common-cause failures for both diesels in our review
MCC-5	None	4.3E-5	6.7E-6	Lower circuit breaker failure to remain closed failure probability
	DC 1 or DC 2 or Both DC	1.8E-4	4.4E-5	Lower circuit breaker failure to remain closed failure probability
	Offsite power and EAC 8	1.2E-2	1.7E-2	Increase in relay failure to energize probability
	Offsite power	9.7E-2	1.2E-2	Increase in relay failure to energize probability
Main Feedwater Break Isolation				
a. Feedstation to containment	None	3.3E-2	5.5E-2	Increase in main feedwater isolation valve failure to close probability
b. Feed pumps to feedstation	None	1.1E-2	2.0E-1	Increase in main feedwater isolation valve failure to close probability
Steam Generator Tube Rupture Isolation	None	9.3E-5	1.6E-4	Increase in MOV and air-operated valve failure probabilities
Steamline Break Isolation				
a. Upstream of NRVs	None	3.0E-4	3.4E-4	Increase in air-operated valve failure probability
b. Downstream of NRVs	None	1.6E-2	3.0E-2	Increase in MOV and air-operated valve failure probability
	DC Bus 1	9.1E-2	1.3E-1	Increase in MOV and air-operated valve failure probability
	DC Bus 2	1.8E-1	2.0E-1	Increase in MOV and air-operated valve failure probability
High Pressure Safety Injection	None	4.1E-3	1.0E-2	Increase in MOV, pump common-cause failures, and maintenance unavailabilities

Table 10.4 Results of the Review of the Haddam Neck PSS System Unavailabilities (continued)

System	Failed Support State	Unavailability PSS	Unavailability Suggested	Major Reason(s) for the change in System Unavailability
High Pressure Safety Injection	Loss of DC 1 or DC 2	9.1E-2	1.6E-1	Increase in MOV and SIAS failures
Low Pressure Safety Injection	None	7.9E-3	9.4E-3	Increase in MOV and pump common cause failures
Low Pressure Safety Injection	DC 1 or DC 2	2.9E-2	3.2E-2	Increase in SIAS failure probabi ity
Residual Heat Removal				
a. Low Pressure Recirculation Mode	None	1.5E-3	3.1E-3	Increase in MOV failure probability
	DC 1 or DC 2	4.0E-3	5.3E-3	Increase in MOV failure probability
	LOSP + DC 1 or DC 2	5.1E-3	6.4E-3	Increase in MOV failure probability
b. High Pressure Recirculation Mode	None	4.9E-3	6.3E-3	Increase in MOV failure probability
	DC 1 or DC 2	7.4E-3	8.7E-3	Increase in MOV failure probability
	LOSP + DC 1 or DC 2	8.5E-3	9.9E-3	Increase in MOV failure probability
c. Long term cooling after bleed-and-feed	None	1.3E-3	5.8E-3	Increase in air-operated valve failure probability
	LOSP + DC 1 or DC 2	4.9E-4	9.7E-3	Increase in air-operated valve and pump train failure probability
after SGTR	None	9.1E-4	5.4E-3	Increase in air-operated valve failure probability
	LOSP + DC 1 or DC 2	4.7E-3	9.5E-3	Increase in air-operated valve and pump train failure probability

Table 10.4 Results of the Review of the Haddam Neck PSS System Unavailabilities (continued)

System	Failed Support State	Unavailability PSS	Unavailability Suggested	Major Reason(s) for the change in System Unavailability
Charging System				
a. RCP seal cooling after a general plant transient	None	2.3E-5	2.2E-5	Decrease in CCW failure probability
	DC 2	4.5E-5	4.2E-5	Decrease in CCW failure probability
	LOSP + DC 1	5.7E-2	5.5E-2	Decrease in CCW failure probability
	DC 1	1.1E-2	1.7E-2	Higher MOV failure probability
	SWS	3.4E-2	5.6E-2	Higher MOV failure probability
	DC 1 + DC 2	1.5E-2	2.0E-2	Higher MOV failure probability
b. Vessel makeup after Loss of MCC-5, control air, or semi-vital AC	None	5.3E-3	6.7E-3	Increase due to addition of check valve failure
	LOSP	6.5E-3	7.4E-3	Increase due to addition of check valve failure
	LOSP + MCC-5	5.0E-3	6.4E-3	Increase due to addition of check valve failure
	DC 1 + DC 2	2.6E-2	4.0E-2	Increase in charging pump failure probability
c. High pressure injection after small LOCA	None	2.3E-2	3.8E-2	Increase in MOV failure probability
	DC 1 or DC 2	2.4E-2	3.9E-2	Increase in MOV failure probability
	LOSP	2.9E-2	4.3E-2	Increase in MOV failure probability
	LOSP + DC 1 or DC 2	7.1E-2	8.0E-2	Increase in MOV failure probability
d. Two path recirculation		2.2E-3	3.5E-3	Increase in MOV failure probability
Component Cooling Water System				
Normal mode	None	6.8E-4	4.5E-4	Decrease in transformer and pump common-cause failure probabilities
	LOSP	1.9E-3	1.3E-3	
	LOSP + MCC-5	4.2E-4	2.5E-4	
	LOSP + DC 1	1.9E-2	1.7E-2	
Thermal barrier cooling	LOSP	1.2E-2	4.9E-2	Increase in air operated valve failure probability

Table 10.4 Results of the Review of the Haddam Neck PSS System Unavailabilities (continued)

System	Failed Support State	Unavailability PSS	Unavailability Suggested	Major Reason(s) for the change in System Unavailability
Service Water System	LOSP	5.1E-5	9.5E-5	Increase in pump common-cause failure
	LOSP + EAC	1.5E-3	3.0E-3	Increase in MOV failure probability
	LOSP + MCC-5	6.0E-4	4.0E-4	Decrease in transformer and circuit breaker failure probability
Instrument Air	SWS	2.3E-2	4.7E-2	Increase in air operated valve failure probability
	MCC-5	2.5E-2	4.9E-2	
Feedwater				
All four SGs available	None	5.0E-5	8.0E-5	Increase in MOV and relay failure probability
Three SGs available	None	5.6E-5	9.0E-5	Increase in MOV and relay failure probability
	DC 2	6.3E-5	8.0E-5	Increase in MOV and relay failure probability
Following ATWS		1.7E-4	1.4E-4	Increase in MOV and relay failure probability
Safety Injection Actuation System	None	1.1E-5	2.5E-5	Increase in relay failure probability
(no high containment pressure)	DC 1 or DC 2	7.3E-3	9.5E-3	Increase in relay failure probability
Integrated Safety Injection for SGTR	SW or LOSP	7.6E-3	1.2E-2	Increase in MOV and HPSI pump failure probabilities
	DC 1 or DC 2	7.0E-3	1.3E-2	Increase in MOV and relay failure probabilities
	SW + DC 1 or DC 2	9.3E-2	1.5E-1	Increase in MOV failure probability
Emergency Boration	None	3.0E-2	5.2E-2	Increase in MOV failure probability
	Offsite Power and 1 AC Bus	3.6E-2	5.8E-2	Increase in MOV failure probability
Loop Isolation Valves	-	5.0E-2	9.0E-2	Increase in MOV failure probability

Table 10.4 Results of the Review of the Haddam Neck PSS System Unavailabilities (continued)

System	Failed Support State	Unavailability PSS	Unavailability Suggested	Major Reason(s) for the change in System Unavailability
Bleed-and-Feed	None	1.8E-2	2.9E-2	Increase in air-operated valve failure probability
	Service Water (SW)	1.3E-1	2.5E-2	Increase in air-operated valve failure probability
	1 DC Bus	3.0E-2	4.4E-2	Increase in air-operated valve failure probability
	1 DC Bus and SW	2.1E-1	4.0E-1	Increase in air-operated valve failure probability
	Offsite power	1.8E-2	3.5E-2	Increase in air-operated valve failure probability
	Offsite power and 1 AC Bus	6.8E-2	9.2E-2	Increase in air-operated valve failure probability
Primary Integrity				
1. Loss of DC Initiator	Offsite power and 1 AC Bus	8.1E-4	3.4E-3	Increase in air-operated valve failure probability
2. Loss of Control Air Initiator	None	6.6E-3	9.5E-3	Increase in charging system unavailability and relay failure probability
Consequential LOCA				
1. General Plant Transient	None	2.9E-4	6.0E-4	Increase in relay failure probability
	Offsite power	1.0E-3	1.3E-3	Increase in relay failure probability
	SW	3.4E-2	5.6E-2	Increase in charging system unavailability due to higher MOV failure probability
2. Loss of Main Feedwater	None	3.5E-4	7.2E-4	Increase in relay failure probability
	Offsite power	1.1E-3	1.5E-3	Increase in relay failure probability
	SW	3.4E-2	5.7E-2	Increase in relay failure probability
3. Loss of Offsite Power	Offsite power	8.8E-4	1.0E-3	Increase in relay failure probability

Table 10.5 Results of the Core Melt Frequency By Initiators

Accident Initiator	Core Melt Frequency (Percent Contribution) PSS	Review Results
1. Small-Break LOCA	1.3E-4 (24%)	1.2E-4 (15%)
2. New Small-Small Break LOCA	-	5.4E-6 (0.6%)
3. Loss of Offsite Power	1.2E-4 (22%)	2.0E-4 (25%)
4. Medium-Break LOCA	8.1E-5 (15%)	1.4E-4 (17%)
5. General Plant Transient	5.3E-5 (10%)	1.1E-4 (14%)
6. Loss of MCC-5	3.3E-5 (6%)	6.8E-5 (8%)
7. Loss of DC Bus 1	2.9E-5 (5%)	1.1E-5 (1%)
8. Total Loss of Main Feedwater	1.3E-5 (2%)	2.2E-5 (2.7%)
9. Large-Break LOCA	1.2E-5 (2%)	1.1E-5 (1%)
10. Steamline Break Downstream of NRV	1.1E-5 (2%)	4.9E-6 (0.6%)
11. Steam Generator Tube Rupture	1.0E-5 (2%)	4.8E-5 (6%)
12. Unisolated RCP Seal Leakage	8.4E-6 (2%)	8.2E-6 (1%)
13. Main Feedline Break	7.4E-6 (1%)	8.7E-6 (1%)
14. Steamline Break Upstream of NRV	7.0E-6 (1%)	7.6E-6 (1%)
15. Insufficient Flow of Service Water	5.9E-6 (1%)	3.2E-6 (0.4%)
16. LOCA Outside Containment	5.4E-6 (1%)	1.0E-5 (1%)
17. Total Loss of DC Power	4.4E-6 (0.8%)	4.4E-6 (0.5%)
18. Loss of Control Air	3.4E-6 (0.1%)	1.4E-5 (2%)
19. Loss of DC Bus 2	2.6E-6 (0.4%)	8.4E-7 (0.1%)
20. Loss of Semi-Vital AC	1.3E-6 (0.2%)	1.6E-5 (2%)
Total	5.4E-4	8.1E-4

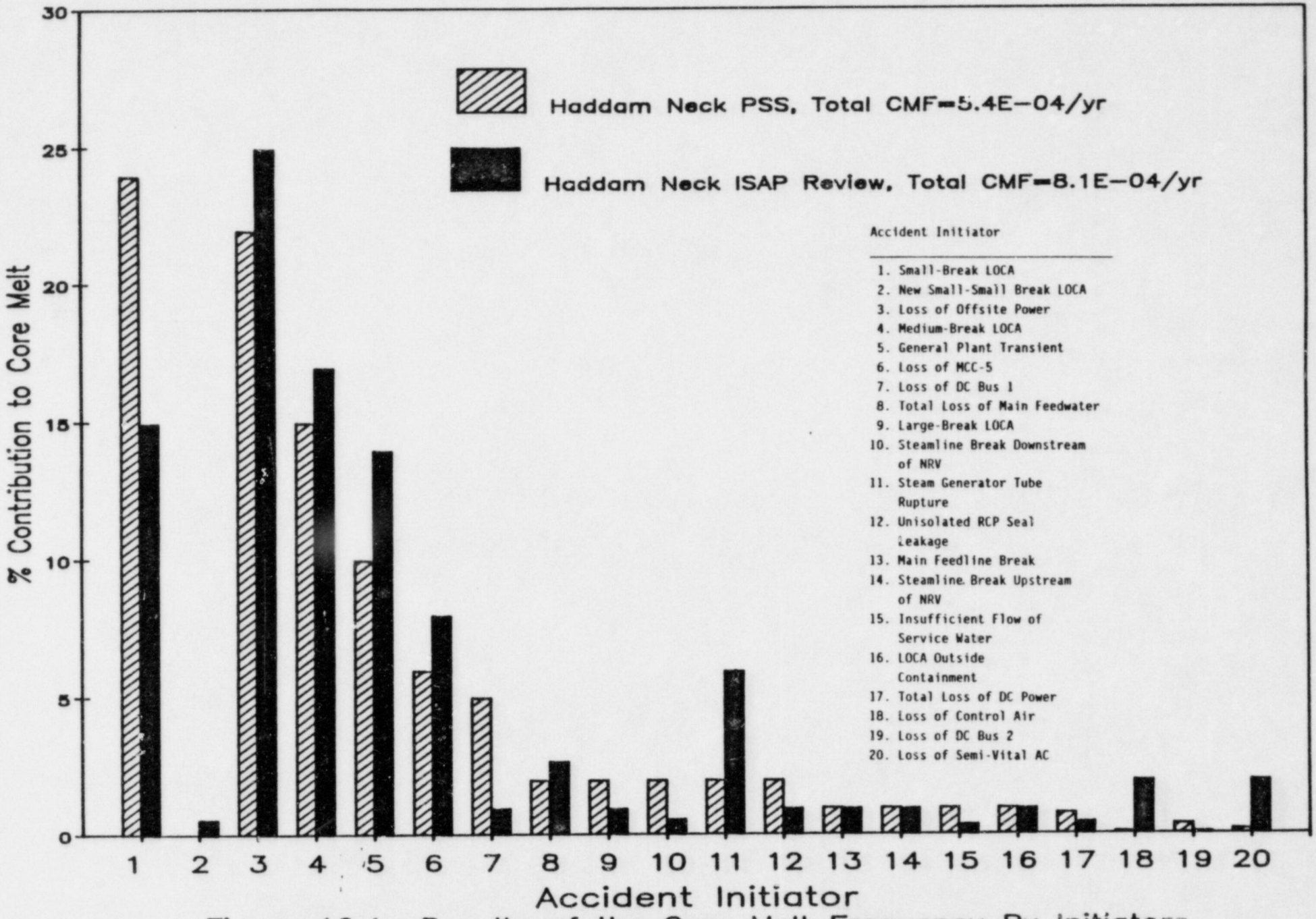


Figure 10.1 Results of the Core Melt Frequency By Initiators

results for each initiating event and identifies the reasons for any differences between the PSS and the review quantification results.

From Table 10.5, the core melt frequency from our new small and small-small break LOCAs is 1.25E-4 compared to 1.3E-4 in the PSS. This minor difference is principally due to small changes in the component data.

For the loss of offsite power initiator in the revised model, core melt frequency increased by about 50% compared to the PSS. In fact, the loss of offsite power became the most dominant contributor to the core melt frequency. In the PSS, small-break LOCA is the most dominant and loss of offsite power is the second most dominant. This order was reversed in our model. Several competing factors contribute to this increase. The most important was in the Station Blackout event tree where, due to changes in the RCP seal failure leakage rate discussed before, the amount of time available for recovery of power before the core becomes uncovered was reduced by about one-half. Another contributor to the increase was the addition of a cognitive operator error in manually controlling the AFWS in all event trees where the ability to actuate and control this system from the control room is lost. Finally, changes in component failure data also contributed to the increase.

For the medium-break LOCA in the revised model the core melt frequency increased by 70% compared to the PSS. This increase is partially due to an increase in the initiator frequency and partially due to changes in component failure data.

For the general plant transient, the core melt frequency in the revised model is a factor of two higher than in the PSS. This is due mostly to the sequences where the transient leads to a consequential small-small LOCA resulting from a stuck open PORV. The frequency of a stuck open PORV more than doubled in the revised model due to an increase in the relay failure probability. Also, the charging system unavailability in both injection and recirculation modes increased due to component data changes.

For the Loss of MCC-5 initiator, the core melt frequency in the revised model doubled compared to the PSS. Several competing factors contributed to this change. In our review the initiator frequency was

reduced by a factor of two compared to the PSS. The major contributor to the increase in the core melt frequency as a result of this initiator was the addition of a cognitive operator error in manually controlling the AFWS when actuation and control from the control room is not available. Another contributor to the increase was the treatment of consequential RCP seal LOCA as a small-small break LOCA in the revised model. This resulted in the requirement of high pressure injection and recirculation systems for mitigation of this initiator. The impact of the requirement of high pressure recirculation is limited due to the addition of credit for long-term MCC-5 recovery and manual manipulation of the valves powered through MCC-5 in the RHR system.

For the Loss of DC Bus 1, the core melt frequency in our model is lower than in the PSS by a factor of 2.6. This reduction was primarily due to a modeling change in the revised model which gave credit for secondary blowdown as an alternative means for providing emergency coolant injection and recirculation. Secondary blowdown was not modeled in the PSS analysis.

For total loss of main feedwater, in the revised model the core melt frequency increased by about 70% over the PSS. As in the general plant transient category, this increase arises mostly from the sequences where the transient leads to a consequential small-small LOCA due to a stuck open PORV. The frequency of a stuck open PORV more than doubled in the revised model due to an increase in the relay failure probability. Also, the charging system unavailability in both injection and recirculation modes increased due to component data changes.

For the large-break LOCA, the core melt frequency in the revised model is about 10% less than in the PSS. This is the net result of two competing effects. The revised initiator frequency was lower but the revised system unavailabilities were higher due to changes in the component data.

For steamline break downstream of the nonreturn valve (NRV), the core melt frequency in the revised model was 50% of that in the PSS. This is again due to two competing effects. The initiator frequency in the revised model was reduced but the system unavailabilities were somewhat higher due to changes in the component data.

The steam generator tube rupture core melt frequency in the revised model increased by almost a factor of 5 compared to the PSS. The major reason for this increase was a modeling change. In the PSS it was assumed that if the secondary steam relief valves are stuck open, depressurization of the primary system along with long-term decay heat removal results in a safe condition. In our analysis, it was assumed that if the secondary steam relief valves are stuck open and the steam generator is not isolated, the coolant will be lost to the atmosphere and core melt will result. This modeling change created one major new dominant core melt sequence that resulted in the increase.

The next two initiators are the unisolated RCP seal leakage and the main feedline break. The core melt frequency from these initiators in the revised model and in the PSS is fairly close. Minor differences are due to changes in component failure data.

For the steamline break upstream of the nonreturn valve (NRV), the core melt frequency in the revised model increased by a negligible amount because of increases in the system unavailabilities due to changes in component data.

The insufficient flow of service water system core melt frequency in the revised model decreased by 50% primarily due to giving credit for long-term recovery of the service water system in the modeling of the event tree. The contribution of this initiator to the total core melt frequency is very small.

The LOCA outside containment core melt frequency in the revised model increased by 80% due to a change in the initiator frequency.

The total loss of DC power core melt frequency did not change between the revised model and the PSS. Also, the change in loss of DC 2 core melt frequency was quite small and mainly due to changes in component data.

For the loss of control air, in the revised model the core melt frequency increased by a factor of 4. This was due to several competing effects. The initiator frequency decreased by almost two orders of

magnitude in the revised model. The frequency of several sequences in this initiator category increased due to modeling changes and the addition of a cognitive operator error for manual operation of AFWS, as discussed before. In addition, in one particular dominant sequence in our model, this cognitive operator error was coupled with operator errors in recovering, main feedwater and initiating bleed-and-feed, which increased the sequence frequency. Finally, in the revised model, failure of RCP seals was assumed to be a small-small LOCA requiring high pressure injection and recirculation. One sequence involving consequential small-small LOCA and failure of high pressure recirculation also contributed to this increase.

The final initiator is the loss of semi-vital AC, for which the core melt frequency increased by a factor of 12 compared to the PSS. This was primarily due to a modeling change where, in those sequences that led to a consequential small-small LOCA due to RCP seal failure, high pressure injection and recirculation were required in our model.

Table 10.6 shows all the revised dominant accident sequences for each of the initiator categories.

10.3 Insights

Several insights about the Haddam Neck Plant design and the PSS methodology were gained from this review. These insights are discussed in this section.

The first series of insights pertain to areas of plant vulnerability. In the PSS model, approximately 55% of the total core melt frequency, 3.0E-4/yr, can be attributed to sequences that include the failure of the high pressure recirculation (HPR) function. The HPR function failure can occur due to one of three separate events: (1) cognitive operator error in initiating the recirculation, (2) manipulative operator error in initiating recirculation, and (3) mechanical failure of the charging or residual heat removal systems. The high failure probability of this function is due to two basic reasons. The first is that the charging system in this plant can only inject into loop 2. Thus, if the LOCA is due to a break in loop 2, the recirculation function is lost. The second reason is that the switchover from high pressure injection to recirculation in this

Table 10.6 List of Dominant Core Melt Sequences Generated As a Result of the Review

Initiator	Failed Support Systems	Sequence Description	Frequency (per year)	Percent of Total Core Melt Frequency
Loss of Offsite Power	Offsite power	o AFW fails, fail to recover offsite power, bleed-and-feed fails	1.0E-5	1.2
		o AFW fails, offsite power recovered, operator fails to initiate main feedwater recovery, operator fails to initiate bleed-and-feed	3.2E-6	0.4
		o AFW fails, fail to recover offsite power, operator fails to initiate bleed-and-feed	2.9E-6	0.4
		o AFW fails, fail to recover offsite power, bleed-and-feed available, long term cooling fails	2.0E-6	0.2
		o Consequential S/RV LOCA, high pressure injection available, charging fails (no recirculation	1.6E-6	0.2
	Offsite power * MCC-5	o MCC-5 recovered, fail to recover offsite power, operator fails to initiate AFW control, operator fails to initiate bleed-and-feed	6.5E-6	0.8
		o MCC-5 recovered, AFW available, charging available, high pressure recirculation fails	5.9E-6	0.7
		o operator fails to initiate recovery of MCC-5, operator fails to initiate AFW control	5.9E-6	0.7
	Offsite power * MCC-5 * (DC1 + EAC8 + DC2 + EAC9)	o MCC-5 recovered, AFW available, high pressure injection available, charging fails, high pressure recirculation (SBD & LPR mode) fails	6.1E-6	0.7
		o MCC-5 recovered, fail to recover offsite power, operator fails to initiate AFW control, operator fails to initiate bleed-and-feed	2.9E-6	0.4

Table 10.6 List of Dominant Core Melt Sequences Generated As a Result of the Review (continued)

Initiator	Failed Support Systems	Sequence Description	Frequency (per year)	Percent of Total Core Melt Frequency
		o MCC-5 recovered, AFW available, charging available, high pressure recirculation fails	2.0E-6	0.2
		o Operator fails to initiate recovery of MCC-5, operator fails to initiate AFW control	1.4E-6	0.2
	Offsite power * (DC1 + EAC8 + DC2 + EAC9)	o Consequential RCP seal LOCA, AFW available, high pressure injection available, high pressure recirculation (SBD & LPR mode) fails	2.9E-5	3.6
		o Consequential S/RV LOCA, high pressure injection available, charging fails (no recirculation)	9.2E-6	1.1
		o Consequential S/RV LOCA, charging available, high pressure recirculation fails	7.6E-6	0.9
		o AFW fails, no recovery of offsite power, bleed-and-feed fails	2.9E-6	0.4
		o AFW fails, no recovery of offsite power, operator fails to initiate bleed-and-feed	1.6E-6	0.2
	All support systems	o No recovery of offsite power	3.3E-5	4.1
	EAC8 * EAC9	o AFW available, fail to recover offsite power in 4 hours	5.0E-5	6.2
		o Operator fails to initiate AFW control, fail to recover offsite power in 50 minutes	2.0E-5	2.5
		o Operator fails to initiate AFW control, offsite power recovered in 50 minutes, operator fails to initiate bleed-and-feed	4.3E-6	0.5
		o AFW available, offsite power recovered in 4 hours, charging available, high pressure recirculation fails	2.2E-6	0.3

Table 10.6 List of Dominant Core Melt Sequences Generated As a Result of the Review (continued)

Initiator	Failed Support Systems	Sequence Description	Frequency (per year)	Percent of Total Core Melt Frequency
Medium-Break LOCA	None	o High pressure injection available, adverse break size and location	7.0E-5	8.6
		o High pressure injection available, charging fails (no recirculation)	2.6E-5	3.2
		o High pressure injection available, high pressure recirculation fails	1.7E-5	2.1
		o High pressure injection available, operator fails to initiate high pressure recirculation	1.4E-5	1.7
Small-Break LOCA	None	o High pressure injection available, charging fails (no recirculation)	7.8E-5	9.6
		o High pressure injection available, adverse break size and location	2.4E-5	3.0
		o High pressure injection available, high pressure recirculation fails	1.7E-5	2.1
General Plant Transient	None	o Consequential PORV LOCA, high pressure injection available, charging fails (no recirculation)	6.8E-5	8.4
		o Consequential PORV LOCA, high pressure injection available, high pressure recirculation fails	1.5E-5	1.9
		o Anticipated transient without scram, pressure relief valves fail to reseat	1.1E-5	1.4
Loss of MCC-5	MCC-5	o MCC-5 not recovered, operator fails to initiate control air recovery, operator fails to initiate AFW control	3.4E-5	4.2
		o MCC-5 recovered, AFW available, charging available, high pressure recirculation fails	1.3E-5	1.6
		o Operator fails to initiate recovery of MCC-5, operator fails to initiate control air recovery, operator fails to initiate AFW control	8.3E-6	1.0

Table 10.6 List of Dominant Core Melt Sequences Generated As a Result of the Review (continued)

Initiator	Failed Support Systems	Sequence Description	Frequency (per year)	Percent of Total Core Melt Frequency
Steam Generator Tube Rupture	None	o SGC available, high pressure injection available, S/G isolation successful, secondary S/RV fails to reseat, loop isolation fails	3.9E-5	4.8
		o SGC available, high pressure injection available, S/G isolation successful, primary depressurization fails, loop isolation fails	4.5E-6	0.6
		o SGC available, high pressure injection available, operator fails to initiate S/G isolation, secondary S/RV fails to reseat	2.1E-6	0.3
Total Loss of Main Feedwater	None	o Consequential S/RV LOCA, high pressure injection available, charging fails (no recirculation)	7.8E-6	1.0
		o AFW fails, main feedwater not recovered, bleed-and-feed fails	6.4E-6	0.8
		o AFW fails, main feedwater not recovered, operator fails to initiate bleed-and-feed	2.3E-6	0.3
		o Consequential S/RV LOCA, high pressure injection available, high pressure recirculation fails	1.8E-6	0.2
		o AFW fails, main feedwater not recovered, bleed-and-feed available, long term cooling fails	1.6E-6	0.2
		o Anticipated transient without scram, pressure relief valves fail to reseat	1.2E-6	0.1
Loss of Semi-Vital AC	None	o Semi-vital AC recovered, AFW available, charging available, high pressure recirculation fails	1.3E-5	1.6
		o Operator fails to initiate recovery of semi-vital AC, AFW available, charging available, high pressure recirculation fails	3.8E-6	0.5

Table 10.6 List of Dominant Core Melt Sequences Generated As a Result of the Review (continued)

Initiator	Failed Support Systems	Sequence Description	Frequency (per year)	Percent of Total Core Melt Frequency
Loss of Control Air	None	o Operator fails to initiate AFW control, operator fails to initiate recovery of main feedwater, operator fails to initiate bleed-and-feed	6.9E-6	0.9
		o Primary integrity fails, AFW available, high pressure injection available, charging fails (no recirculation)	5.1E-6	0.6
		o Operator fails to initiate AFW control, main feedwater recovery fails, operator fails to initiate bleed-and-feed	2.5E-7	
Large-Break LOCA	None	o Low pressure injection available, operator fails to initiate low pressure recirculation	4.7E-6	0.6
		o Low pressure injection available, low pressure recirculation fails	3.2E-6	0.4
		o Low pressure injection fails	2.4E-6	0.3
Loss of DC 1	DC 1	o Primary integrity fails, SGC available, charging available, high pressure recirculation fails	4.1E-6	0.5
	DC 1 * LOSP * MCC-5	o Primary integrity fails, semi-vital AC fails, SGC available, charging & high pressure injection fail, secondary blowdown and LPI fails.	3.6E-6	0.4
		o Primary integrity fails, SGC available, charging fails, high pressure injection available, high pressure recirculation (SBD and LPR mode) fails	9.7E-7	0.1
Steamline Break Upstream of NRV	None	o Operator fails to isolate break, bleed-and-feed fails	6.0E-6	0.7
		o Operator fails to isolate break, operator fails to initiate bleed-and-feed	1.6E-6	0.2
		o Consequential SGTR, loop isolation valves fail	1.1E-6	0.1
		o Consequential SGTR, operator fails to initiate loop isolation	6.1E-7	0.1

Table 10.6 List of Dominant Core Melt Sequences Generated As a Result of the Review (continued)

Initiator	Failed Support Systems	Sequence Description	Frequency (per year)	Percent of Total Core Melt Frequency
Main Feedline Break	None	o Operator fails to initiate break isolation, operator fails to initiate bleed-and-feed	5.1E-6	0.8
		o Feedwater isolation fails, bleed-and-feed fails	8.7E-7	0.1
		o Adverse break location, bleed-and-feed fails	8.6E-7	0.1
		o Operator fails to initiate break isolation, bleed-and-feed fails	5.9E-7	0.1
Unisolated RCP Seal Leak	None	o SGC available, charging fails, bleed-and-feed fails	4.9E-6	0.6
		o SGC available, charging fails, operator fails to initiate bleed-and-feed		
Small-small Break LOCA	None	o High pressure injection available, SGC available, high pressure recirculation fails	5.3E-6	0.7
Steamline Break Downstream of NRV	None	o Main steam isolation fails, bleed-and-feed fails	1.6E-6	0.2
		o Consequential SGTR, loop isolation valves fail	7.3E-7	0.1
		o Main steam isolation fails, operator fails to initiate bleed-and-feed	5.7E-4	0.1
		o Consequential SGTR, operator fails to initiate loop isolation	4.2E-7	0.1
		o Main steam isolation fails, bleed-and-feed available, long term cooling fails	4.1E-7	0.1
		o Automatic main steam isolation fails, operator fails to initiate isolation, operator fails to initiate bleed-and-feed	4.1E-7	0.1
Total Loss of DC	DC1 * DC2	o Operator fails to control charging flow, primary integrity successful, auxiliary feedwater fails	3.4E-6	0.4
		o Operator fails to control charging flow, primary integrity fails	1.0E-6	0.1

Table 10.6 List of Dominant Core Melt Sequences Generated As a Result of the Review (continued)

Initiator	Failed Support Systems	Sequence Description	Frequency (per year)	Percent of Total Core Melt Frequency
Loss of Service Water	SW	o Charging metering pump fails, control air recovered, AFW available, secondary blowdown and LPI available, failure of long term recovery of service water	1.9E-6	0.2
		o Charging metering pump fails, operator fails to initiate recovery of control air	5.7E-7	0.1
Loss of DC 2	DC 2	o AFW fails, main feedwater fails, operator fails to initiate bleed-and-feed	7.0E-7	0.1
		o Main feedwater available, primary integrity fails, high pressure injection available, charging fails (no recirculation)	1.5E-7	

plant is a manual operation. This introduces two additional failure mechanisms for this function compared to automatic switchover systems, namely the cognitive and manipulative operator errors.

In the revised model, the contribution to the total core melt frequency from sequences containing failure of the HPR function increased from 3.0E-4/yr in the PSS model to 5.5E-4/yr. This corresponds to 68% of the total core melt frequency in the revised model. This increase was primarily due to the treatment of reactor coolant pump (RCP) seal failure as a small-small LOCA in our model. As was discussed in detail in Section 4.0, the PSS assumption of 50 gpm leakage per RCP if the RCP seal cooling is failed was not accepted. As discussed earlier in the report, in our model it was assumed instead that the leak rate is closer to about 100 gpm per pump. This implies that failure of all the RCP seals due to loss of cooling to the seals is equivalent to a small-small LOCA, requiring both high pressure injection and recirculation. Thus, a number of event trees were modified to reflect this change.

This change had the potential of resulting in a much larger increase in core melt frequency in our model, but was mitigated somewhat by credit given by the reviewers to several alternatives for recovery of the HPR function. The first alternative is credit for an alternate mode of recirculation through the use of secondary blowdown to lower the primary pressure and use of the low pressure recirculation system. The second alternative is credit for long-term recovery of the service water system and MCC-5 in order to establish high pressure recirculation in sequences involving failure of these systems. The third alternative is credit for local manual alignment of recirculation valves when remote control power is lost. These alternatives were not considered in the PSS model.

In one of the Haddam Neck ISAP topics (topic 1.27), "Compliance With 50.46 (ECCS)," addition of an alternative HPR path through the use of the high pressure safety injection (HPSI) pump as a backup to the charging pumps is discussed (36). This modification, which is intended to add some redundancy to the HPR, will result in approximately a 3.0E-4/yr reduction in the contribution of the sequences involving HPR to the total core melt frequency in the revised model. This corresponds to a 37% reduction in the total revised core melt frequency.

The second area of plant vulnerability is the loss of motor control center 5 (MCC-5). In the PSS model, the contribution of failure of MCC-5 to the total core melt frequency is approximmately 4.5E-5/yr, or approximately 9% of the core melt frequency. This contribution in our model increased to about 1.0E-4/yr, corresponding to 12% of the core melt frequency, due to several competing factors which were discussed in Section 10.2. The reason for this large contribution to core melt frequency in both models is that MCC-5 provides the only non-redundant power source to a number of key safety system valves and instruments. This contribution to the core melt frequency can be greatly reduced by the addition of a redundant bus to MCC-5.

The third area of plant vulnerability is the dependence of the auxiliary feedwater system (AFWS) on control air. If air is not available to several AFWS air-operated valves, operator action must be taken to control AFW locally in the pump room. In the PSS, the contribution to the total core melt frequency of sequences including this dependency is 3.0E-5/yr, i.e., 6%. In the revised model, this contribution was increased to 1.0E-4/yr, or about 12% of the total core melt frequency. This increase is due to the correction of an inconsistency in the analysis of cognitive error with regard to the operator response to loss of auxiliary feedwater and the subsequent operator decisions, as discussed in detail in Sections 7.2.3b and 7.3.1b. One potential fix for this problem would be the installation of backup compressed air bottles for the auxiliary feedwater system, which would eliminate the total dependency of the system on control air. This would also result in the elimination of most of the contribution of this system failure to the total core melt frequency.

The rest of the insights are related to the methodology and assumptions used in probabilistic analyses in general and the Haddam Neck PSS specifically.

In the Haddam Neck PSS, about 22% of the total core melt frequency (1.2E-4/yr) is due to loss of offsite power. Of this, approximately 50% is due to station blackout sequences. The revised contribution to the core melt frequency increased to 2.0E-4/yr, corresponding to 25% of the total core melt frequency, making loss of offsite power the most dominant core

melt contributor. These percentage contributions are in agreement with the results of other PSAs.

Since loss of offsite power is shown to be the major contributor to the core melt frequency in most recent PSAs, it is important to realize that several key assumptions have major impacts on this contribution at each nuclear power plant. These assumptions include the loss of offsite power frequency, the time dependent offsite or onsite power recovery curves, the assumed time beyond which RCP seals are assumed to fail due to lack of cooling, and the assumed time for core uncovery given no recovery of offsite power and operation or failure of AFWS. This last assumption regarding core uncovery time is also dependent on the assumed rate of RCP seal leakage. One potential solution for a prolonged station blackout (beyond the point of RCP seal failure) is addition of a steam or direct diesel-driven injection pump. Addition of such a pump would help to keep the core covered for an extended period of time (depending on the rate of RCP seal leakage), allowing more time for the recovery of the offsite or onsite power.

Another interesting insight is related to the modeling of cognitive operator errors. In the Haddam Neck PSS, the cognitive operator error of failing to realize various plant conditions was explicitly modeled on event trees. The contribution to the total core melt frequency in the PSS of the sequences which include cognitive operator error is approximately 7.0E-5/yr, or about 13% of the total core melt frequency. This contribution in the revised model increased to 2.0E-4/yr, or 25% of the total core melt frequency, due to several changes discussed in Section 7.0. The most important change is the addition of a cognitive error for local manual control of AFWS and the consideration of its interdependency with other operator actions to establish early core cooling (as previously discussed). Inclusion of cognitive operator errors on the event trees, which has been done in the most recent PSAs, is an advancement in accident sequence modeling. The accident sequences produced as a result of these event trees more correctly represent the actual sequence of events that could occur at a given plant. But, it is important to realize that despite major advancements in the area of human reliability analysis in general and cognitive operator errors specifically, the uncertainty in these cognitive operator error probabilities is still very large. Thus, the significant contributions of these types of cognitive operator errors to the core melt frequency

should be accompanied by the realization that there are relatively large uncertainties associated with these sequences compared to sequences which are primarily due to system hardware failures.

Finally, in the revised model, the PSS small-break LOCA range was divided into two break ranges. The first break range was called small-small break LOCA, where in addition to injection, decay heat removal via steam generator cooling is also required. The second break range was called small-break LOCA, which is similar to the traditional small-break LOCA, i.e., only high pressure injection and recirculation are sufficient to keep the core covered and remove decay heat. This division had virtually no effect on the dominant core melt sequences and the contribution to total core melt frequency from random LOCAs in this size range. However, this division did have a significant effect on the modeling of the RCP seal failures, which lie in the small-small break LOCA range rather than small-break LOCA range. The small-small break LOCA success criteria offer more options for mitigation of these consequential LOCAs (e.g., secondary blow-down) compared to the PSS small-break LOCA success criteria. Thus, without this division the contribution to the total core melt frequency of consequential small-break LOCA due to RCP seal failure would have been substantially higher than what is shown in our model.

In summary, the relative importance of the dominant contributors to the PSS core melt frequency was revised by the review principally due to five major factors. The first is the assumption of higher RCP seal leakage rate and treatment of this event as a small-small break LOCA requiring both high pressure injection and recirculation. The second factor, which again is due to the RCP seal leakage rate, is in the station blackout sequences, where the offsite power recovery times before core uncovery for different scenarios were essentially cut in half because of higher assumed RCP seal leakage rate. The third factor that had a significant impact on the results was the addition of a cognitive operator error in manually controlling the AFWS in all event trees in which actuation and control of this system is lost from the control room. The fourth factor is breaking up of the small LOCA range into two break sizes, which credited alternative cooling methods for RCP seal LOCAs, thus limiting the adverse effects of the first change. The final factor is a more realistic treatment of the initiating event frequencies and recovery potential for "Loss of MCC-5" and "Loss of Control

Air" initiating events, which prevented the contribution from these initiators from becoming very dominant due to the effects of the first and third changes discussed above. Except for these changes, the review indicates that for all practical purposes the model developed in the Haddam Neck PSS was sufficient (in a quantitative sense) to estimate the core melt profile associated with the operation of this plant.

11.0 REFERENCES

1. "Connecticut Yankee Probabilistic Safety Study," Northeast Utilities Service Company, NUSCO 149, February 1986.

2. Atefi, B., Gallagher, D.W., Le, P.T., Drouin, M.T., and P.J. Amico, "A Review of the Connecticut Yankee (Haddam Neck) Nuclear Power Plant Probabilistic Safety Study," Interim Report, July 15, 1986.

3. Riley, J.E. and B.F. Putney, "The Risk Management Query System (RMQS)," Proceedings of the Annual Reliability and Maintainability Symposium, p. 358, January 1986.

4. "Millstone Unit 3 Probabilistic Safety Study," Northeast Utilities Service Company, August 1983.

5. "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

6. Kelly, Glenn, USNRC, Private Communication, 1986.

7. Memorandum for D.G. Eisenhut, NRC, from T.E. Murley, NRC, Subject: Reactor Coolant Pump Seal Failure, nd.

8. "NRC Integrated Program for the Resolution of Unresolved Safety Issues A-3, A-4 and A-5 Regarding Steam Generator Tube Integrity," April 1985.

9. ATWS: A Reappraisal, Part III: Frequency of Anticipated Transients, EPRI NP-2230, January 1982.

10. "Seabrook Station Probabilistic Safety Assessment," Public Service Company of New Hampshire, PLG-0300, December 1983.

11. "Interim Reliability Program Procedures Guide," NUREG/CR-2728, SAND82-1100, January 1983.

12. Stevenson, J.A. and C.L. Atwood,"Common Cause Fault Rates for Valves," NUREG/CR-2770, EGG-EA-5485, February 1983.

13. "Millstone Unit 1 Probabilistic Safety Study," Northeast Utilities Service Company, NUSCO 147, July 1985.

14. "IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear-Power Generating Station," IEEE Std. 500-1984.

15. Fleming, K.N. and A. Mosleh, "Classification and Analysis of Reactor Operating Experience Involving Dependent Event," EPRI NP-3967, June 1985.

16. "Best Estimate LOCA Analysis," Northeast Utilities Service Company, NUSCO 150, February 1986.

17. Letter from J.F. Opeka, Northeast Utilities to C.I. Grimmes, USNRC, Subject: Haddam Neck Plant Comments on Draft NRC Review of the Haddam Neck Probabilistic Safety Study, September 8, 1986.

18. Mosleh, A. Apostolakis, G., "Some Properties of Distributions Useful in the Study of Rare Events," IEEE Transactions on Reliability, Vol. R.31, No. 1, TR-80-116, April 1982.

19. PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, January 1983.

20. Welker, E.L. and M. Lipow, "Estimating the Exponential Failure Rate from Data with No Failure Events," Proceedings of 1974 Annual Reliability and Maintainability Symposium, January 1974.

21. Atwood, C.L., "Common Cause Fault Rates for Pumps," NUREG/CR-2098, EGG-EA-5298, February 1983.

22. Atwood, C.L., and J.A. Stevenson, "Common Cause Fault Rates for Diesel Generators," NUREG/CR-2099, June 1982.

23. Atwood, C.L., "Common Cause Fault Rates for Instrumentation and Control Assemblies," NUREG/CR-2771, EGG-EA-5623, February 1983.

24. Hannaman, G.W. and A.J. Spurgin, "Systematic Human Action Reliability Procedure (SHARP)," EPRI NP-3583, June 1984.

25. Swain, A.D., and H.C. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG/CR-1278, 1983.

26. Hannaman, G.W., Spurgin, A.J., and Y.D. Yukic, "Human Cognitive Reliability Model for PRA Analysis," NUS-4531 (Draft), December 1984.

27. Hall, R.E., Fragola, J.R., and J. Wreathall, "Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation," NUREG/CR-3010, 1982.

28. Minarick, J.W. and Kukielka, C.A., "Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report," NUREG/CR-2497, Oak Ridge National Laboratory, Oak Ridge, TN, June 1982.

29. Minarick, J.W., Cottrell, W.B., Austin, P.N., Hagen, E.W., and Harris, J.D., "Precursors to Potential Severe Core Damage Accidents: 1980-1981, A Status Report," NUREG/CR-3591, Oak Ridge National Laboratory, Oak Ridge, TN, February 1984.

30. Phung, D L., Minarick, J.W., and Harris, J.D., "A Review of Comments on the 1969-1979 Accident Sequence Precursor Program Status Report: NUREG/CR-2497," ORNL/NRC/LTR-85-14, Oak Ridge National Laboratory, Oak Ridge, TN, June. 1985.

31. Minarick, J.W., Harris, J.D., Austin, P.N., Cletcher, J., and Hagen, E.W., "Precursors to Potential Severe Core Damage Accidents: 1985," NUREG/CR-4674 (Draft), Oak Ridge National Laboratory, Oak Ridge, TN.

32. Mackowiak, D.P., Gentillon, C.D., Smith, K.L., and Weber, D.A., "Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments (Draft)," NUREG/CR-3862, EG&G Idaho, Inc., Idaho Falls, Idaho, June 1984.

33. Connecticut Yankee Atomic Power Company, "Facility Description and Safety Analysis Report," Topical Report 3250-5, Haddam Neck Plant, Haddam, Connecticut.

34. "Methodology for Probabilistic Risk Assessment of Nuclear Power Plants," PLG-0209, Pickard, Lowe and Garrik, Inc., June 1981.

35. ETA, An Interactive Event Tree Development Program, Science Applications International Corporation, 1984.

36. Letter from J.F. Opeka, Northeast Utilities to C.I. Grimes, USNRC, Subject: ISAP Topic No. 1.27-"Compliance with 50.46(ECCS)," September 17, 1986.