

INDIVIDUAL PLANT EXAMINATION REPORT
FOR
SAN ONOFRE NUCLEAR GENERATING STATION
UNITS 2 AND 3
IN RESPONSE TO
GENERIC LETTER 88-20

Submittal Document

Southern California Edison

April 1993

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
LIST OF TABLES	iv
LIST OF FIGURES	viii
TABLE OF ACRONYMS	xiii
1.0 EXECUTIVE SUMMARY	1-1
1.1 Background and Objectives	1-1
1.2 Plant Familiarization	1-1
1.3 Overall Methodology	1-6
1.4 Summary of Major Findings	1-6
1.4.1 Level I Results	1-6
1.4.2 Level II Results	1-11
1.4.3 Conclusion	1-13
1.5 References	1-15
2.0 EXAMINATION DESCRIPTION	2-1
2.1 Introduction	2-1
2.2 Conformance with Generic Letter 88-20 and Supporting Material	2-1
2.3 General Methodology	2-1
2.3.1 Applicability of Results to Both Units	2-4
2.4 Information Assembly	2-5
2.5 References	2-7
3.0 FRONT-END ANALYSIS	3-1
3.1 Initiating Event and Plant Response Analysis	3-1
3.1.1 Initiating Events	3-1
3.1.2 Event Trees	3-12
3.2 System Analysis	3-112
3.2.1 Auxiliary Feedwater	3-113
3.2.2 Main Feedwater and Condensate System	3-115
3.2.3 Main Steam System	3-121
3.2.4 Safety Injection Tanks	3-123
3.2.5 High Pressure Safety Injection	3-125
3.2.6 Low Pressure Safety Injection	3-127
3.2.7 Chemical Volume and Control System	3-129
3.2.8 Containment Spray and Containment Emergency Fan Coolers	3-132
3.2.9 Reactor Coolant System Pressure Control	3-135
3.2.10 Component Cooling Water	3-138
3.2.11 Saltwater Cooling	3-142
3.2.12 Instrument Air	3-145
3.2.13 Heating Ventilation and Air Conditioning	3-146

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
	3.2.14 Electric Power	3-152
	3.2.15 Plant Protection	3-156
	3.2.16 Containment Isolation	3-171
3.3	Sequence Quantification	3-179
	3.3.1 Generic Data Analysis	3-179
	3.3.2 Plant Specific Data and Analysis	3-180
	3.3.3 Human Failure Data	3-206
	3.3.4 Common Cause Failure Data	3-232
	3.3.5 Quantification of Unavailability of Systems and Functions	3-249
	3.3.6 Generation of Support System States and Quantification of Their Probabilities	3-251
	3.3.7 Quantification of System Frequencies	3-251
	3.3.8 Internal Flooding Analysis	3-253
	3.3.9 Interfacing System LOCA (ISLOCA) Analysis	3-277
	3.3.10 Level I Quantification Results	3-292
3.4	Results and Screening Process	3-315
	3.4.1 Application of Generic Letter Screening Criteria	3-315
	3.4.2 Vulnerability Screening	3-321
	3.4.3 Decay Heat Removal (DHR) Evaluation	3-321
	3.4.4 Steam Generator Overfill Evaluation	3-326
3.5	References	3-334
4.0	BACK-END ANALYSIS	4-1
4.1	Plant Data and Plant Description	4-1
	4.1.1 Containment Structure	4-1
	4.1.2 Containment Systems	4-9
	4.1.3 Containment Data	4-13
4.2	Plant Models and Methods for Physical Processes	4-13
4.3	Bins and Plant Damage States	4-15
	4.3.1 Level II Event Trees	4-15
	4.3.2 Plant Damage State Characterization	4-40
	4.3.3 Binning and Screening of Level II Sequences	4-45
4.4	CONTAINMENT FAILURE CHARACTERIZATION	4-46
	4.4.1 Containment Ultimate Strength	4-46
	4.4.2 Unlikely Failure Modes	4-63
	4.4.3 Failure Modes Considered	4-69
	4.4.4 Summary of Containment Failure Characterization	4-73

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
4.5 Containment Event Tree (CET)	4-73
4.5.1 Overview of CET Structure	4-76
4.5.2 CET Top Events and Success Criteria	4-79
4.5.3 CET Structure and End-States	4-83
4.6 Accident Progression and CET Quantification	4-85
4.7 Radionuclide Release Characterization	4-86
4.7.1 Overview	4-86
4.7.2 Source Term Sequence Selection	4-88
4.7.3 Source Term Analysis	4-92
4.7.4 Sensitivity Analysis	4-111
4.8 Summary of Back-End Results	4-128
4.9 References	4-132
5.0 UTILITY PARTICIPATION AND INTERNAL REVIEW TEAM	5-1
5.1 IPE Program Organization	5-1
5.2 Composition of Independent Review Team	5-2
6.0 SAFETY FEATURES AND POTENTIAL PLANT IMPROVEMENTS	6-1
6.1 Safety Features	6-1
6.2 Potential Plant Improvements	6-2
7.0 SUMMARY AND CONCLUSIONS	7-1
Appendix A Additional Plant Drawings	A-1

	<u>LIST OF TABLES</u>	<u>PAGE</u>
Table 1.2-1	Summary of SONGS 2/3 Design Features	1-4
Table 1.4-1	SONGS 2/3 Level I IPE Results Contribution of Initiating Events to CDF	1-8
Table 1.4-2	SONGS 2/3 Level I IPE Results Contribution of Functional Accident Classes to CDF	1-9
Table 1.4-3	SONGS Units 2/3 Level II IPE Results Airborne Release Category and Probability	1-12
Table 3.1-1	Transient Initiating Events	3-4
Table 3.1-2	SONGS 2/3 Transient Initiating Event Frequencies	3-6
Table 3.1-3	Summary of Support System Initiators	3-13
Table 3.1-4	SONGS 2/3 Initiating Event Summary and Basis	3-14
Table 3.1-5	Safety Function Requirement vs. Initiating Event Category	3-15
Table 3.1-6	Functional Accident Sequence Definition	3-20
Table 3.1-7	TT Event Tree Success Criteria	3-29
Table 3.1-8	PCS Event Tree Success Criteria	3-37
Table 3.1-9	TWS Event Tree Success Criteria	3-45
Table 3.1-10	LOP Event Tree Success Criteria	3-54
Table 3.1-11	SBO Event Tree Success Criteria	3-63
Table 3.1-12	SLB Event Tree Success Criteria	3-69
Table 3.1-13	LL Event Tree Success Criteria	3-75
Table 3.1-14	ML Event Tree Success Criteria	3-81
Table 3.1-15	SL Event Tree Success Criteria	3-87
Table 3.1-16	SSL Event Tree Success Criteria	3-94

<u>LIST OF TABLES</u> (continued)		<u>PAGE</u>
Table 3.1-17	SGR Event Tree Success Criteria	3-100
Table 3.1-18	SS Event Tree Success Criteria	3-107
Table 3.1-19	CCW Event Tree Success Criteria	3-110
Table 3.2-1	System Dependency Table	3-117
Table 3.2-2	Containment Isolation Valves that Close on CIAS	3-173
Table 3.3-1	SONGS 2/3 Generic Data List	3-181
Table 3.3-2	Components Identified for SONGS 2/3 Plant Specific Evaluation	3-190
Table 3.3-3	Nuclear Plant Reliability Data System Summary	3-195
Table 3.3-4	Plant-Specific Data Summary	3-203
Table 3.3-5	Plant-Specific Component Unavailabilities	3-205
Table 3.3-6	Quantification of Pre-Initiator Human Actions	3-209
Table 3.3-7	Results of Pre-initiator Analysis	3-211
Table 3.3-8	Post-Initiator Human Error Probability Summary Table	3-223
Table 3.3-9	Post-Initiator Human Actions	3-224
Table 3.3-10	Common Cause Beta Factors	3-249
Table 3.3-11	Main Characteristics of Total Flood Frequency Distributions	3-258
Table 3.3-12	SONGS 2/3 Flood Zones	3-266
Table 3.3-13	SONGS 2/3 IPE Internal Flood Analysis Summary Results	3-277
Table 3.3-14	Candidate ISLOCA Pathways	3-283

	<u>LIST OF TABLES</u> (continued)	<u>PAGE</u>
Table 3.3-15	LPSI Line(s) Valves	3-290
Table 3.3-16	ISLOCA Frequency Contributors	3-292
Table 3.3-17	Dominant Sequences from Level I PRA	3-293
Table 3.3-18	Functional Accident Sequence Contribution to Core Damage	3-299
Table 3.3-19	Dominant Cutsets from Level I PRA Model	3-300
Table 3.3-20	Fussell-Vesely Importance Measures for Top Basic Events	3-304
Table 3.3-21	Risk Reduction Values for Basic Events	3-308
Table 3.3-22	Risk Increase Values for Basic Events	3-311
Table 3.4-1	Comparison of Functional Accident Sequences to NRC Screening Criteria	3-317
Table 4.1-1	Summary of SONGS Containment Data	4-5
Table 4.3-1	Plant Damage State Identifiers for ECCS Status	4-43
Table 4.3-2	"Transient" EET Sequences with Frequencies Greater Than 10^{-6} /yr	4-47
Table 4.3-3	"Large LOCA" EET Sequences With Frequencies Greater Than 10^{-6} /yr	4-49
Table 4.3-4	"Small LOCA" EET Sequences With Frequencies Greater Than 10^{-6} /yr	4-50
Table 4.3-5	Containment Bypass EET Sequences With Frequencies Greater Than 10^{-6} /yr	4-53
Table 4.3-6	Plant Damage States	4-55
Table 4.3-7	Sequence Selection to Meet Requirements of GL 88-20, Appendix 2	4-56
Table 4.3-8	Plant Damage States Analyzed for Source Term	4-57

<u>LIST OF TABLES</u> (continued)		<u>PAGE</u>
Table 4.4-1	Pressure Capacities for the Controlling Failure Modes	4-61
Table 4.4-2	Median Leak Areas and Variabilities	4-62
Table 4.4-3	Phenomenological Evaluation Summaries on Postulated Containment Failure Modes	4-74
Table 4.7-1	Initial SONGS 2/3 Inventory of Fission Product Groups	4-89
Table 4.7-2	IPE Back-end Sequence Selection Summary for SONGS 2/3	4-91
Table 4.7-3	Release Category Definitions	4-93
Table 4.7-4	Airborne Fission Product Release (%) 48 Hours after Accident Initiation	4-96
Table 4.7-5	SONGS Units 2 and 3 Airborne Release Category and Probability	4-99
Table 4.7-6	Source-Term Analysis Results - MAAP Run Summary Table	4-100
Table 4.7-7	SONGS 2/3 Sensitivity Analyses to Address Uncertainties Identified in NUREG-1335	4-112
Table 4.7-8	Source Term Sensitivity Analysis Results - MAAP Run Summary Table	4-116
Table 4.7-9	Accident Sequences with the Potential for Long Term Containment Failure	4-127
Table 4.8-1	SONGS Units 2 and 3 Airborne Release Category and Probability	4-131

	<u>LIST OF FIGURES</u>	<u>PAGE</u>
Figure 1.2-1	SONGS 2/3 Simplified P&ID	1-3
Figure 1.4-1	SONGS 2/3 Level I Results: Contribution by Initiator	1-7
Figure 1.4-2	SONGS 2/3 Level I Results: Contribution by Functional Accident Class	1-10
Figure 1.4-3	SONGS 2/3 Level I and Level II Results	1-14
Figure 3.1-1	Example Event Tree	3-18
Figure 3.1-2	Relationship Between Radioactive Release Barriers, Safety Functions and Systems	3-23
Figure 3.1-3	Transient with PCS Initially Available (TT) Event Tree	3-28
Figure 3.1-4	Loss of Power Conversion System (PCS) Event Tree	3-36
Figure 3.1-5	Anticipated Transient Without Scram (TWS) Event Tree	3-44
Figure 3.1-6	Loss of Offsite Power (LOP) Event Tree	3-53
Figure 3.1-7	Station Blackout (SBO) Event Tree	3-62
Figure 3.1-8	Main Steam Line Break (SLB) Event Tree	3-68
Figure 3.1-9	Large LOCA (LL) Event Tree	3-74
Figure 3.1-10	Medium LOCA (ML) Event Tree	3-80
Figure 3.1-11	Small LOCA (SL) Event Tree	3-86
Figure 3.1-12	Small-Small LOCA (SSL) Event Tree	3-93
Figure 3.1-13	Steam Generator Tube Rupture (SGR) Event Tree	3-99
Figure 3.1-14	Support System (SS) Event Tree	3-106
Figure 3.1-15	Loss of CCW (CCW) Event Tree	3-109
Figure 3.2-1	AFW Simplified P&ID	3-116

<u>LIST OF FIGURES</u> (continued)		<u>PAGE</u>
Figure 3.2-2	MFW/COND Simplified P&ID	3-119
Figure 3.2-3	MSS Simplified P&ID	3-124
Figure 3.2-4	SIT Simplified P&ID	3-126
Figure 3.2-5	HPSI Simplified P&ID	3-128
Figure 3.2-6	LPSI Simplified P&ID	3-130
Figure 3.2-7	CVCS Simplified P&ID	3-133
Figure 3.2-8	CS Simplified P&ID	3-136
Figure 3.2-9	CEFC Simplified P&ID	3-137
Figure 3.2-10	RCS Pressure Control Simplified P&ID	3-139
Figure 3.2-11	CCW Simplified P&ID	3-141
Figure 3.2-12	SWC Simplified P&ID	3-144
Figure 3.2-13	IA Simplified P&ID	3-147
Figure 3.2-14	ESF Switchgear HVAC Simplified P&ID	3-149
Figure 3.2-15	Chilled Water System Simplified P&ID	3-150
Figure 3.2-16	Chiller Room HVAC Simplified P&ID	3-151
Figure 3.2-17	1E AC Electric Power Simplified P&ID	3-157
Figure 3.2-18	1E DC Electric Power Simplified P&ID	3-158
Figure 3.2-19	Non-1E AC Electric Power Simplified P&ID	3-159
Figure 3.2-20	Non-1E DC Electric Power Simplified P&ID	3-160
Figure 3.2-21	ESFAS Functional Block Diagram	3-167
Figure 3.2-22	ESFAS Primary Block Diagram	3-168
Figure 3.2-23	RPS Functional Block Diagram	3-169
Figure 3.2-24	RPS Primary Block Diagram	3-170
Figure 3.2-25	Containment Isolation Simplified P&ID	3-175

<u>LIST OF FIGURES</u> (continued)		<u>PAGE</u>
Figure 3.3-1	Plant-Specific Data Collection and Evaluation Process	3-189
Figure 3.3-2	Pre-Initiator Human Error Probability Calculation Worksheet	3-210
Figure 3.3-3	Sample Operator Action Summary Data Sheet	3-220
Figure 3.3-4	Sample Post-Initiator Human Error Probability Calculation Worksheet	3-221
Figure 3.3-5	Sample Screening Process	3-257
Figure 3.3-6	Simplified P&ID: Penetrations 48 thru 51	3-285
Figure 3.3-7	Simplified P&ID: Penetration 9	3-286
Figure 3.4 1	Steam Generator Overfill Event Tree	3-329
Figure 4.1-1	Containment, Vertical Section Facing West	4-2
Figure 4.1-2	Containment, Vertical Section Facing North	4-3
Figure 4.1-3	Configuration of the Reactor Cavity and Lower Compartment	4-6
Figure 4.1-4	Plan View of Cavity and Cavity Cooling Ducts	4-8
Figure 4.1-5	Containment Spray System Schematics	4-11
Figure 4.1-6	Containment Emergency Fan Cooler System Schematics	4-12
Figure 4.2-1	SONGS Level II Methodology	4-16
Figure 4.3-1a	Extended Event Tree: Transient with Power Conversion System (PCS) initially available (TT) - Part I	4-19
Figure 4.3-1b	Extended Event Tree: Transient with Power Conversion System (PCS) initially available (TT) - Part II	4-20

<u>LIST OF FIGURES</u> (continued)		<u>PAGE</u>
Figure 4.3-2a	Extended Event Tree: Loss of Power Conversion System (PCS) - Part I	4-21
Figure 4.3-2b	Extended Event Tree: Loss of Power Conversion System (PCS) - Part II	4-22
Figure 4.3-3	Extended Event Tree: Anticipated Transient Without Scram (TWS)	4-23
Figure 4.3-4	Extended Event Tree: Loss of Offsite Power (LOP)	4-24
Figure 4.3-5	Extended Event Tree: Station Blackout (SBO)	4-25
Figure 4.3-6	Extended Event Tree: Main Steam Line Break (SLB)	4-26
Figure 4.3-7	Extended Event Tree: Large LOCA (LL)	4-27
Figure 4.3-8	Extended Event Tree: Medium LOCA (ML)	4-28
Figure 4.3-9	Extended Event Tree: Small LOCA (SL)	4-29
Figure 4.3-10	Extended Event Tree: Small-Small LOCA (SSL)	4-30
Figure 4.3-11a	Extended Event Tree: Steam Generator Tube Rupture - Part I	4-31
Figure 4.3-11b	Extended Event Tree: Steam Generator Tube Rupture - Part II	4-32
Figure 4.3-12	Extended Event Tree: Interfacing Systems LOCA (V-Sequence)	4-33
Figure 4.3-13	Extended Event Tree: Loss of Component Cooling Water	4-34
Figure 4.3-14	Extended Event Tree: Loss of 125V DC Bus (LDC)	4-35
Figure 4.4-1	Fuel Transfer Tube Bellows Inside the Containment Building	4-59
Figure 4.4-2	Vertical Section of Equipment Hatch	4-60

<u>LIST OF FIGURES</u> (continued)		<u>PAGE</u>
Figure 4.5-1	Containment Event Tree	4-77
Figure 5-1	SONGS 2/3 IPE Project Organization Chart	5-3
Figure A.1	Section of Containment, Auxiliary Feedwater Pump Building, and Auxiliary Building (Radwaste Area)	A-2
Figure A.2	Section of Safety Equipment Building and Auxiliary Building (Control Area)	A-3
Figure A.3	Reactor Cavity Ventilation Duct and Personnel Hatch for Reactor Cavity	A-4
Figure A.4	Containment Emergency Fan Coolers and Air Flow Path	A-5
Figure A.5	Ventilation Air Duct of the Emergency Fan Cooler	A-6
Figure A.6	Containment Structure General Arrangement	A-7

TABLE OF ACRONYMS

ADV	Atmospheric Dump Valve
AFW	Auxiliary Feedwater
AOI	Abnormal Operating Instruction
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
BAMU	Boric Acid Makeup
BNL	Brookhaven National Laboratory
CC	Common Cause
CCAS	Containment Cooling Actuation Signal
CCW	Component Cooling Water
CDF	Core Damage Frequency
CE	Combustion Engineering
CEDM	Control Element Drive Mechanism
CEFC	Containment Emergency Fan Cooler
CEOG	Combustion Engineering Owners Group
CET	Containment Event Tree
CIAS	Containment Isolation Actuation Signal
CIS	Containment Isolation System
CPIS	Containment Purge Isolation Signal
CRIS	Control Room Isolation Signal
CRS	Control Room Supervisor
CS	Containment Spray
CSAS	Containment Spray Actuation Signal
CSR	Containment Spray Recirculation
CST	Condensate Storage Tank
CVCS	Chemical Volume and Control System
ECCS	Emergency Core Cooling System
ECW	Emergency Chilled Water
EDG	Emergency Diesel Generator
EET	Extended Event Tree
EHC	Electro-Hydraulic Control
EOI	Emergency Operating Instruction
ERIN	ERIN Engineering and Research, Inc.
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
FAI	Fauske and Associates, Inc.
FHIS	Fuel Handling Building Isolation Actuation Signal
FMEA	Failure Modes and Effects Analysis
FTAP	Fault Tree Analysis Program
FWIS	Feedwater Isolation Signal
FWIV	Feedwater Isolation Valve
GL	Generic Letter
HEP	Human Error Probability
HPSI	High Pressure Safety Injection
HRA	Human Reliability Analysis
HVAC	Heating, Ventilating, and Air Conditioning

TABLE OF ACRONYMS
(continued)

IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
IPE	Individual Plant Examination
IPEEE	Individual Examination of External Events
IPEP	IPE Partnership, Inc.
ISA	Instrument & Service Air
ISLOCA	Interfacing System Loss of Coolant Accident
LCO	Limiting Condition For Operation
LDC	Initiator/Event Tree Reference to Loss of 125V DC
LL	Initiator/Event Tree Reference to Large LOCA
LOCA	Loss of Coolant Accident
LOP	Loss of Offsite Power
LOSP	Loss of Offsite Power
LOVS	Loss of Voltage Signal
LPSI	Low Pressure Safety Injection
MAAP	Modular Accident Analysis Program
MCCI	Molten Core-Concrete Interaction
MFW	Main Feedwater
M/G	Motor Generator
MGL	Multiple Greek Letter
ML	Initiator/Event Tree Reference to Medium LOCA
MOV	Motor-Operated Valve
MSIS	Main Steam Isolation Signal
MSIV	Main Steam Isolation Valve
MSS	Main Steam System
MSSV	Main Steam Safety Valves
MTC	Moderator Temperature Coefficient
NEDO	Nuclear Engineering Design Organization
NRC	Nuclear Regulatory Commission
NSAC	Nuclear Safety Analysis Center
NSSS	Nuclear Steam Supply System
NUMARC	Nuclear Management and Resource Council
OI	Operating Instruction
P&ID	Piping and Instrumentation Diagram
PCS	Power Conversion System
PDS	Plant Damage State
PIV	Pressure Isolation Valve
PORV	Power Operated relief Valves
PPS	Plant Protection System
PRA	Probabilistic Risk Assessment
PTS	Pressurized Thermal Shock
PWR	Pressurized Water Reactor
PZR	Pressurizer
QA	Quality Assurance
RAS	Recirculation Actuation Signal
RCP	Reactor Coolant Pump

TABLE OF ACRONYMS
(continued)

RCS	Reactor Coolant System
REBECA	Reliability Engineering Building-Block Environment for Computer Analysis
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RTO	Reactor Trip Override
RWST	Refueling Water Storage Tank
SBO	Station Blackout
SCE	Southern California Edison
SDC	Shutdown Cooling
SDCHX	Shutdown Cooling Heat Exchangers
SEQPRO	Sequence Processor
SG	Steam Generator
SGR	Initiator/Event Tree Reference to SGTR
SGTR	Steam Generator Tube Rupture
SIAS	Safety Injection Actuation Signal
SIT	Safety Injection Tank
SL	Small LOCA
SLB	Steam Line and Feedwater Line Breaks
SNL	Sandia National Laboratories
SONGS	San Onofre Nuclear Generating Station
SPTA	Standard Post-Trip Actions
SSL	Small-Small LOCA
STA	Shift Technical Advisor
SV	Safety Valve
SWC	Salt Water Cooling
TGIS	Toxic Gas Isolation System
TT	Transient With PCS Initially Available
TWS	Initiator/Event Tree Reference to
UFSAR	Updated Final Safety Analysis Report
UPS	Uninterruptible Power Supply
USI	Unresolved Safety Issue
VL	Initiator/Event Tree Reference to ISLOCA
VR	Initiator/Event Tree Reference to Reactor Vessel Rupture
gpm	gallons per minute
pcm	10^{-5} dp
ppm	parts per million
psia	pounds per square inch atmosphere
psig	pounds per square inch gauge

1.0 EXECUTIVE SUMMARY

1.1 Background and Objectives

In November of 1988, the NRC issued Generic Letter 88-20 (Reference 1.0-1, without Supplements 1-4) requesting that all U.S. nuclear utilities perform a plant-specific Individual Plant Examination for severe accident vulnerabilities. This effort was to involve an integrated analysis of plant and system response to a wide spectrum of internal, randomly initiated events such as reactor trips, loss of off-site power, and loss of coolant accidents (LOCAs) with an emphasis on quantification of plant core damage frequency and evaluation of containment performance. The specific objectives of the analysis, as stated in the Generic Letter, were for each utility:

- (1) to develop an appreciation of severe accident behavior,
- (2) to understand the most likely severe accident sequences that could occur at its plant,
- (3) to gain a more quantitative understanding of the overall probabilities of core damage and fission product releases, and
- (4) if necessary, to reduce the overall probabilities of core damage and fission product releases by modifying, where appropriate, hardware and procedures that would help prevent or mitigate severe accidents.

1.2 Plant Familiarization

The San Onofre Nuclear Generating Station (SONGS) is located on the coast of southern California, in San Diego County, approximately 62 miles southeast of Los Angeles and approximately 51 miles northwest of San Diego. The station is located entirely within the Camp Pendleton Marine Corps Base. The station includes three reactors. Unit 1, which operated until late 1992, is located northwest of and immediately adjacent to Units 2 and 3. Units 2 and 3 are essentially identical operating units and have the provision for limited sharing of AC power systems and cooling water intake structures. The plants also share a common control room complex, radwaste facilities, instrument air/nitrogen and emergency HVAC systems. Other than the above noted commonalities SONGS 2 and 3 operate as independent entities.

SONGS Unit 2 received its operating license in February 1982 and began commercial operation in August 1983. SONGS Unit 3 received its operating license in November 1982 and began commercial operation in April 1984.

The San Onofre Nuclear Generating Station Units 2 and 3 comprise two pressurized water reactor (PWR) nuclear steam supply systems (NSSS) each with a nominal thermal output of approximately 3410 MWt and a maximum dependable capacity (MDC) gross of 1127 MWe. Each NSSS, manufactured by Combustion Engineering, contains two independent primary coolant loops, each of which has two reactor coolant pumps, a steam generator, a 42-inch ID outlet (hot) pipe and two 30-inch outlet (cold) pipes. An electrically heated pressurizer is connected to one of the loops, and safety injection lines are connected to each of four cold legs and two hot legs. Pressurized water circulates by means of electric motor-driven, single stage, centrifugal reactor coolant pumps downward between the reactor vessel shell and the core support barrel, upward through the reactor core, through the tube side of the vertical U-tube steam generators, and back to the reactor coolant pumps. The main saturated steam produced in the steam generators is passed to the high-pressure turbine element of the turbine. The extraction steam from the high-pressure turbine exhaust passes to the reheater and then to the low-pressure section of the main turbine and the feedwater pump turbine drive.

Figure 1.2-1 is a simplified P&ID of the SONGS 2/3 nuclear plants. A summary of some of the key design features of SONGS 2/3 is provided in Table 1.2-1.

SAN ONOFRE NUCLEAR C

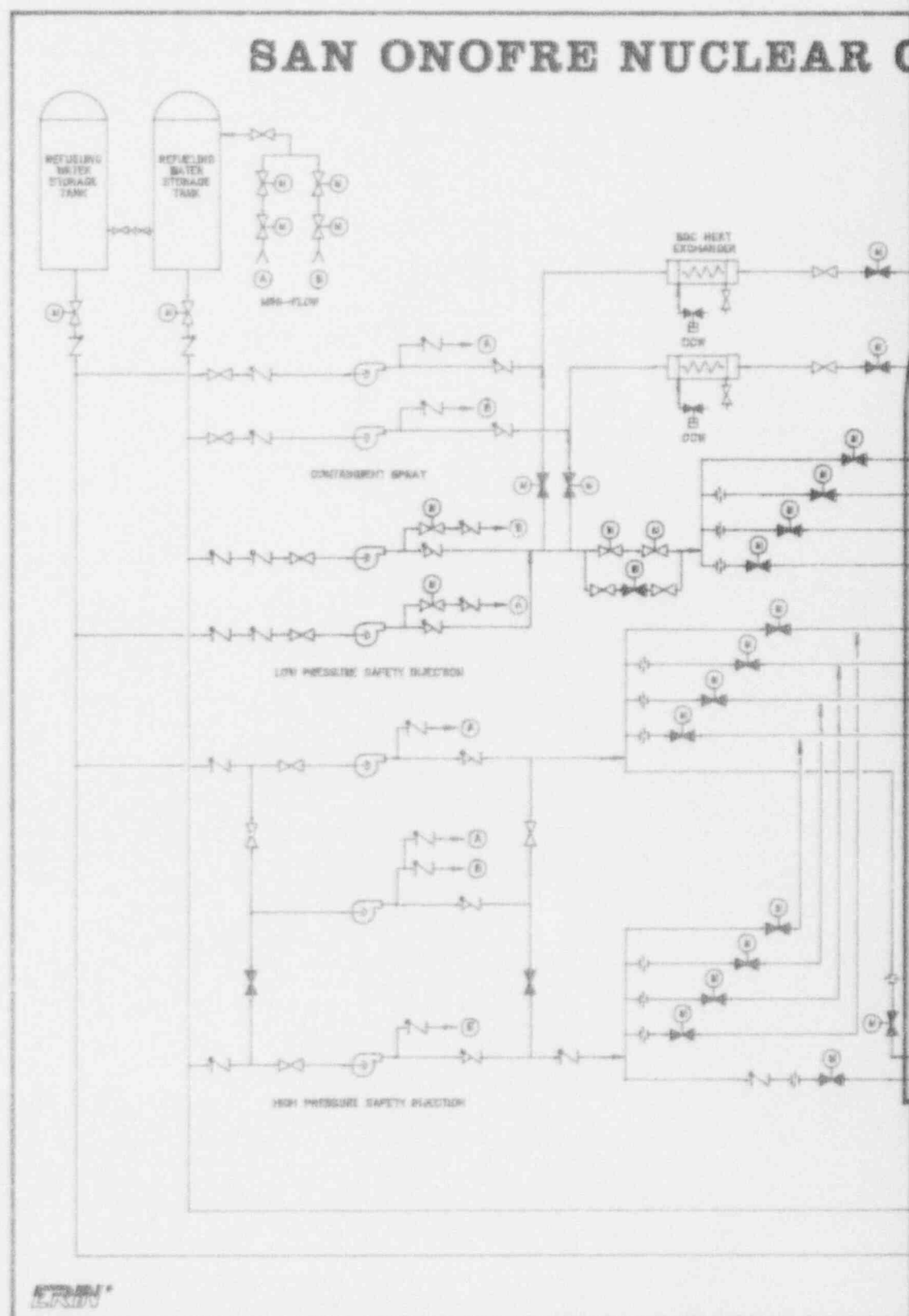
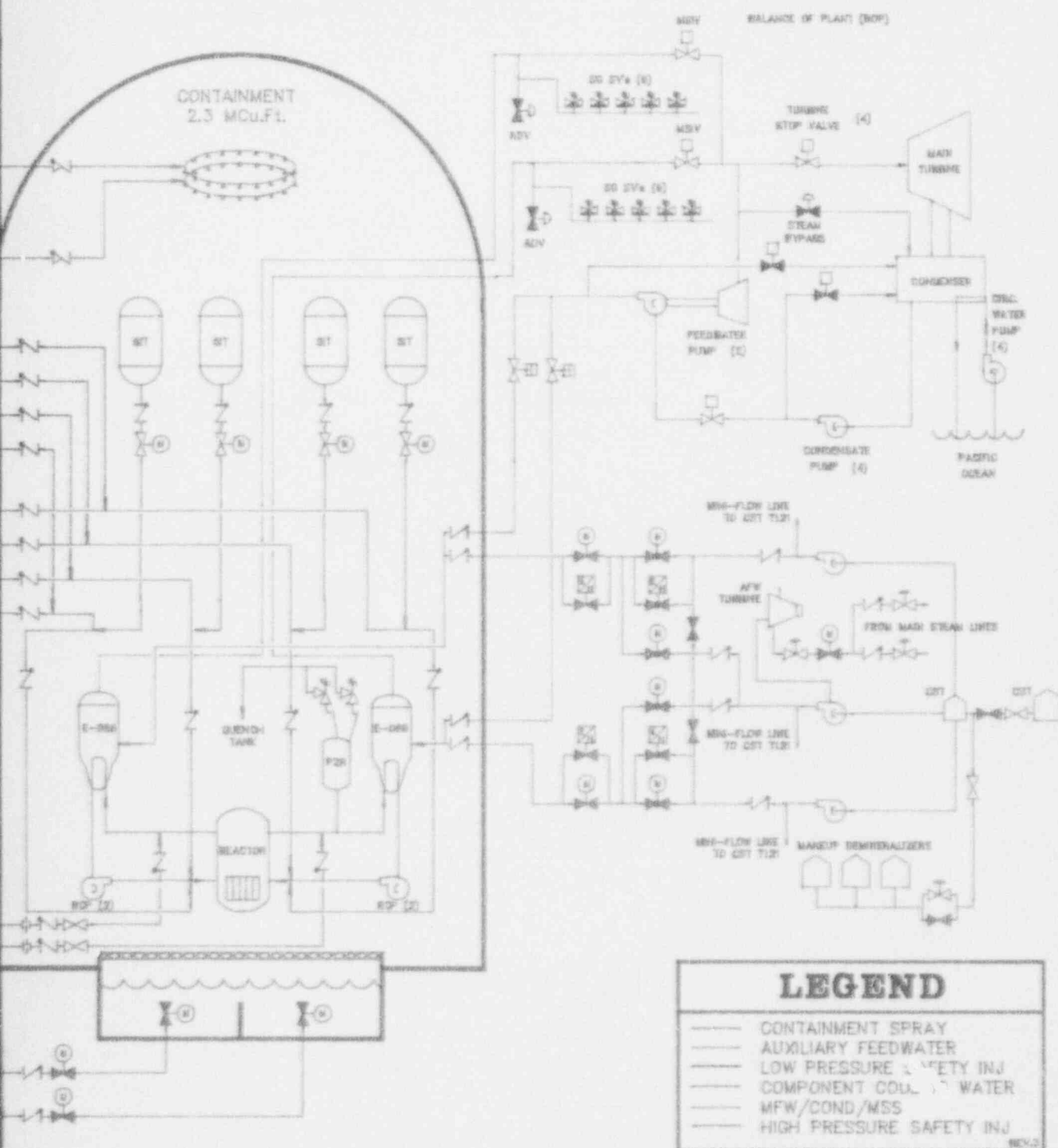


Figure 1.2-1
2/3 SIMPLIFIED P&ID

GENERATING STATION UNITS 2/3



9305040247-01-

Table 1.2-1

SUMMARY OF SONGS 2/3 DESIGN FEATURES

SAFETY FUNCTION	KEY SYSTEMS/FEATURES
Reactivity Control	<ol style="list-style-type: none"> 1) Reactor Protection System 2) Control Rods 3) Emergency Boration via Chemical Volume and Control System from the Refueling Water Storage Tank or the Boric Acid Makeup System
RCS Inventory and Pressure Control	<ol style="list-style-type: none"> 1) Three High Pressure Safety Injection Pumps <ul style="list-style-type: none"> - Injection - Recirculation 2) Two Low Pressure Safety Injection Pumps - Injection Only 3) Four Safety Injection Tanks 4) Two Pressurizer Safety Valves
RCS Heat Removal	<ol style="list-style-type: none"> 1) Main Steam Relief <ul style="list-style-type: none"> - Nine Main Steam Safety Valves per Steam Generator - One Atmospheric Dump Valve per Steam Generator - Four Turbine Bypass Valves 2) Two Main Feedwater Pumps 3) Auxiliary Feedwater <ul style="list-style-type: none"> - Two Motor-Driven Pumps - One Turbine-Driven Pump 4) Alternate Low Pressure Feedwater <ul style="list-style-type: none"> - Four Condensate Pumps
Containment Heat Removal	<ol style="list-style-type: none"> 1) Four Containment Emergency Fan Coolers 2) Two Containment Spray Trains with Heat Exchangers <ul style="list-style-type: none"> - Injection - Recirculation

Table 1.2-1

SUMMARY OF SONGS 2/3 DESIGN FEATURES
(continued)

SAFETY FUNCTION	KEY SYSTEMS/FEATURES
Key Support Systems	<ol style="list-style-type: none">1) 4kV and 480V Crosstie Capability to Opposite Unit2) 8 hour life on two of four Batteries3) 2 Emergency Diesel Generators per Unit4) Common Switchyard for Units 2 and 3<ul style="list-style-type: none">- One Main, two Auxiliary and three Reserve Transformers per unit5) Four Separate and Redundant 125V DC Buses for ESF Loads6) Four ESF 120V AC Buses, each capable of being supplied from two sources
Primary Containment Structure	<ol style="list-style-type: none">1) Large Dry Containment - 150 ft Inside Diameter, 172 ft Height2) 2,335,000 cubic ft Nominal Free Volume3) 60 psig Design Pressure

1.3 Overall Methodology

The SONGS 2/3 IPE utilized PRA methodology in accordance with that described in NUREG/CR-2300 (Reference 1.0-3), NUREG/CR-2815 (Reference 1.0-4), NUREG-1150 (Reference 1.0-5), the guidelines presented in GL 88-20 (Reference 1.0-1), its supplements and appendices including NUREG-1335 (Reference 1.0-2), and SCE IPE Procedures. The IPE includes a Level I (Front-End) analysis of core damage frequencies and a Level II (Back-End) analysis of phenomena affecting containment behavior and the release of radionuclides to the environment. Sensitivity and importance analyses on the results were used to determine the importance of systems, structures, components, and procedures. All results are reported in terms of mean values unless otherwise indicated.

1.4 Summary of Major Findings

The subsequent sections of this summary present the results of the PRA in a "top-down" manner. First, the top tier of results (total core damage frequency or large release frequency) are discussed, followed by the lower tiers of results (specific contributors).

1.4.1 Level I Results

The total mean core damage frequency (CDF) for internal events at SONGS 2/3 was calculated to be 3.0×10^{-5} /yr or roughly 1 in 33,000 years. This is approximately a factor of three below the NRC's proposed safety goal of 1 in 10,000 years (or 1×10^{-4} /yr) and compares favorably with the core damage frequencies reported for other PWRs.

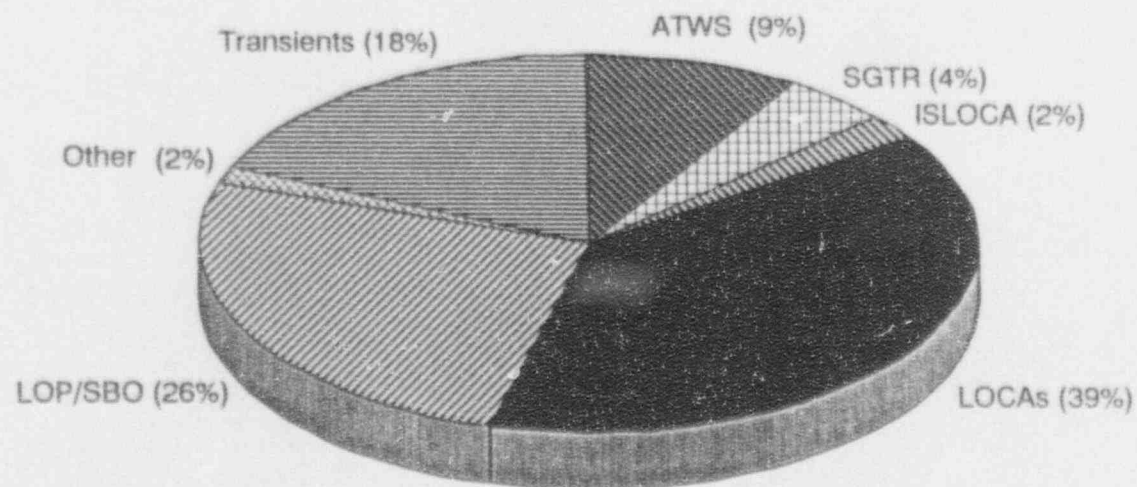
Figure 1.4-1 depicts the relative contributions of key event classes, i.e., LOCA, LOP/SBO, transients, ATWS, SGTR, ISLOCA, and others.

The contribution of specific initiating events to the total core damage frequency is provided in Table 1.4-1.

Finally, Table 1.4-2 and Figure 1.4-2 depict the relative contributions of Functional Accident Classes to the total CDF.

Figure 1.4-1

**SONGS 2/3 LEVEL I RESULTS
Contribution By Initiator**



TOTAL CDF = $3.0E-05/\text{yr}$

LEGEND

ISLOCA - Interfacing System LOCA
ATWS - Anticipated Transient w/o Scram
SGTR - Steam Generator Tube Rupture
LOP/SBO - Loss of Offsite Power/Station Blackout

Table 1.4-1

SONGS 2/3 LEVEL I IPE RESULTS
Contribution of Initiating Events To CDF

Total CDF = $3.0E-5/\text{yr}$

Initiator	Initiator Frequency	Core Damage Frequency	Fraction of CDF
Loss of Offsite Power Initiating Event	0.11	$7.8E-06$	0.26
Transient With Power Conversion System Initially Available Initiating Event	3.8	$4.4E-06$	0.15
Medium LOCA Initiating Event	$1.0E-03$	$4.0E-06$	0.14
Large LOCA Initiating Event	$5.0E-04$	$3.3E-06$	0.11
Loss of Power Conversion System Initiating Event	0.53	$3.2E-06$	0.11
Small LOCA Initiating Event	$1.0E-03$	$2.9E-06$	0.10
Steam Generator Tube Rupture Initiating Event	$1.0E-02$	$1.2E-06$	$4.2E-02$
Small-small LOCA Initiating Event	$1.3E-02$	$1.0E-06$	$3.4E-02$
Interfacing System LOCA	$6.6E-07$	$6.6E-07$	$2.2E-02$
Steam Line Break and Feedwater Line Break Initiating Event	$5.4E-04$	$4.1E-07$	$1.4E-02$
Loss of DC Power 125 VDC Bus D1/D2	$1.6E-03$	$2.6E-07$	$8.7E-03$
Reactor Pressure Vessel Rupture	$2.7E-04$	$2.0E-07$	$6.8E-03$
Loss of Component Cooling Water	$2.5E-04$	$1.4E-07$	$4.6E-03$

- Remarks:
- (1) The Anticipated Transient Without Scram contribution to the total CDF is included with the CDF contribution of the source initiating event which causes the demand for a plant trip or scram.
 - (2) The Station Blackout contribution to the total CDF is included with the CDF contribution of the Loss of Offsite Power.
 - (3) Figure 1.4-1 depicts the fractional contributions for the ATWS and Station Blackout initiating events separate from the initiators listed in this table.

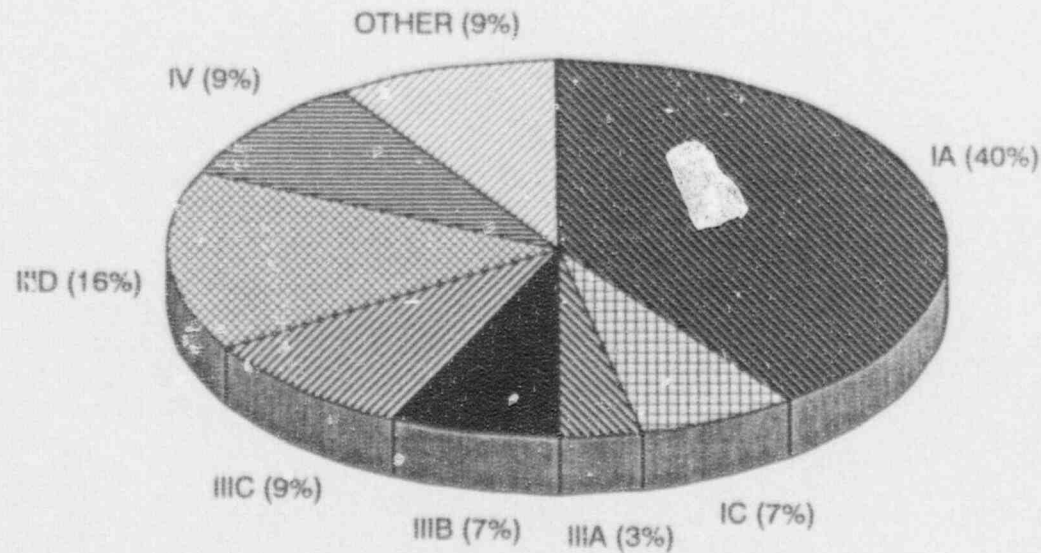
Table 1.4-2

SONGS 2/3 LEVEL 1 IPE RESULTS
Contribution of Functional Accident Classes to CDF

Functional Accident Class	Definition	Contribution To CDF	Fraction of CDF
IA	Accident sequences involving loss of both primary and secondary coolant makeup in the injection phase	1.2E-5	0.40
IB	Accident sequences involving loss of both primary and secondary coolant makeup in the recirculation phase	N/A	N/A
IC	Accident sequences involving loss of both primary and secondary coolant makeup due to Station Blackout	2.0E-6	0.07
IIA	Accident sequences involving an induced small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the injection phase	5.1E-7	0.02
IIB	Accident sequences involving an induced small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the recirculation phase	9.0E-7	0.03
IIIA	Accident sequences initiated by a small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the injection phase	9.8E-7	0.03
IIIB	Accident sequences initiated by a small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the recirculation phase	2.1E-6	0.07
IIIC	Accident sequences initiated by medium or large LOCA with loss of primary coolant makeup in the injection phase	2.7E-6	0.09
IIID	Accident sequences initiated by a medium or large LOCA with loss of primary coolant makeup or adequate heat removal in the recirculation phase	4.6E-6	0.16
IV	Accident sequences involving failure of reactivity control	2.7E-6	0.09
VA	Systems LOCA outside containment leading to loss of effective primary coolant inventory makeup	6.6E-7	0.02
VB	Steam generator tube rupture leading to loss of effective primary coolant inventory makeup	7.2E-7	0.02

Figure 1.4-2

SONGS 2/3 LEVEL I RESULTS Contribution By Functional Accident Class



TOTAL CDF = 3.0E-05/yr

LEGEND

- IA - Loss of Both Primary and Secondary Makeup in Injection Phase
- IC - Loss of Both Primary and Secondary Makeup due to Station Blackout
- IIIA - Small LOCA's with Loss of Primary Makeup or Loss of Adequate Heat Removal in Injection Phase
- IIIB - Small LOCA's with Loss of Primary Makeup or Loss of Adequate Heat Removal in Recirculation Phase
- IIIC - Medium or Large LOCA's with Loss of Primary Makeup in the Injection Phase
- IICD - Medium or Large LOCA's with Loss of Primary Makeup in the Recirculation Phase
- IV - Sequences Involving Loss of Reactivity Control

1.4.2 Level II Results

Results of the SONGS 2/3 Level II analysis are summarized in Table 1.4-3. This table provides the release categories, range of volatile fission products released, frequency of the release category, and the conditional probability of the release category given a core damage event has occurred.

The results indicate that, given core damage, there is an 84% probability that the containment will successfully maintain its integrity and prevent an uncontrolled fission product release.

The most likely mode of release from the containment is a late overpressure failure whose conditional probability is 9.4%. Containment bypass, with a conditional probability of 6.7%, is the next most likely mode of fission product release. Of these bypass sequences 70% are attributable to steam generator tube rupture with the remaining 30% attributable to interfacing system LOCAs. Finally, failure of the containment to isolate is expected to occur with a conditional probability of 0.1% per core damage event.

The overall conditional containment failure probability of 16% is comparable with other PWRs.

Table 1.4-3

SONGS UNITS 2/3 LEVEL II IPE RESULTS
AIRBORNE RELEASE CATEGORY AND PROBABILITY

Release Category	Definition	Release Frequency (per year)	P(RC CD) ¹
S	Success, no containment failure within 48 hrs, < 0.1% volatiles released	2.6×10^{-5}	0.838
T	Containment bypassed, > 10% volatiles released	6.5×10^{-7}	0.021
B	Containment bypassed, < 0.1% volatiles released	2.2×10^{-7}	0.007
D	Containment bypassed, up to 10% volatiles released	1.2×10^{-6}	0.039
G	Isolation failure, Containment failure prior to vessel failure, up to 10% volatiles released	2.0×10^{-6}	0.001
L	Late containment failure, up to 1% volatiles released	2.2×10^{-6}	0.072
W	Late containment failure, more than 10% volatiles released	6.9×10^{-7}	0.022

1. Conditional probability of release category given core damage.

1.4.3 Conclusion

The objectives of the NRC for Generic Letter 88-20 were essentially: 1) development by the utility of an understanding of plant specific responses to severe accidents, and 2) implementation of changes where indicated to address vulnerabilities. These objectives were met in the Individual Plant Examination of San Onofre Units 2 and 3.

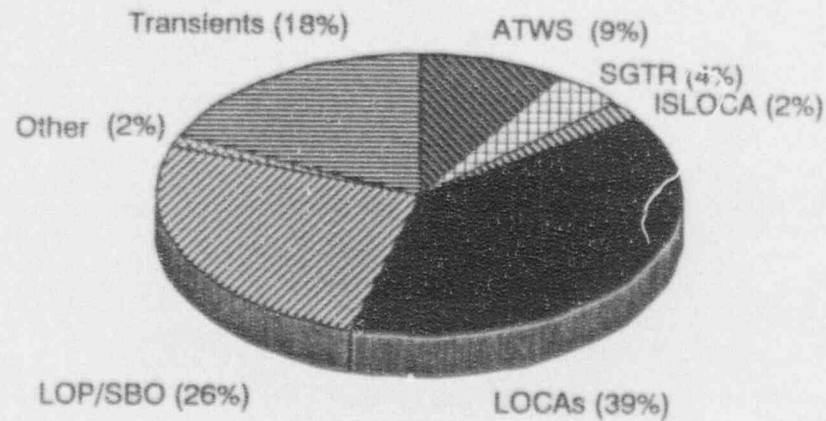
The majority of the modeling, quantification, and prioritization of core damage and significant release sequences associated with the IPE was performed by in-house personnel, thus assuring that a detailed appreciation of severe accident behavior was developed within SCE.

In the course of the IPE, preliminary calculations indicated the possibility of a severe accident vulnerability associated with potentially inadequate annunciation of high ambient temperature in inverter/distribution rooms. Without further detailed analysis, SCE installed high temperature alarms in these rooms (four rooms at each unit). The impact of this plant modification was roughly estimated to be a factor of three reduction in core damage frequency. The results reported in this Submittal reflect plant risk with the temperature alarms installed. No additional modifications to either plant design or procedures were indicated.

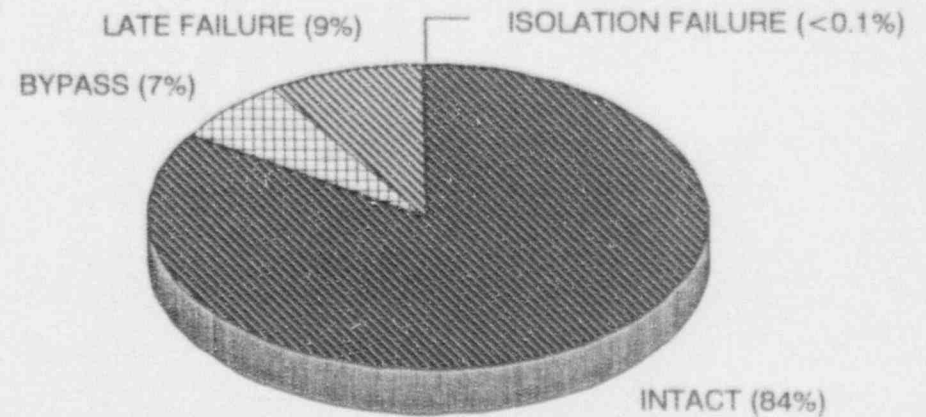
The final overall Level I and Level II results are portrayed in Figure 1.4-3.

Figure 1.4-3

SONGS 2/3 LEVEL I AND LEVEL II RESULTS



TOTAL CDF = $3.0E-05/\text{yr}$



CONDITIONAL PROBABILITY OF
CONTAINMENT FAILURE = 0.16

LEGEND

ISLOCA - Interfacing System LOCA
ATWS - Anticipated Transient w/o Scram
SGTR - Steam Generator Tube Rupture
LOP/SBO - Loss of Offsite Power/Station Blackout

1.5 References

- 1.0-1 Generic Letter No. 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR §50.54(f)," USNRC, dated November 23, 1988 including Supplements 1-4.
- 1.0-2 NUREG-1335, "Individual Plant Examination Submittal Guidance, Final Report, USNRC, dated August 1989.
- 1.0-3 NUREG/CR-2300, "PRA (Probabilistic Risk Assessment) Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," Volumes I and II, USNRC, dated January 1983.
- 1.0-4 NUREG/CR-2815, "Probabilistic Safety Analysis Procedures Guide," USNRC, dated August 1985.
- 1.0-5 NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," USNRC, dated December 1990.

2.0 EXAMINATION DESCRIPTION

2.1 Introduction

In response to GL 88-20 (Reference 2.0-1), SCE performed a probabilistic risk assessment of the SONGS 2/3 plants involving an integrated analysis of plant and system response to a wide spectrum of postulated internal, randomly initiated events in order to evaluate and quantify plant core damage frequency and evaluate containment performance.

2.2 Conformance with Generic Letter 88-20 and Supporting Material

The IPE of SONGS 2/3 as summarized in this submittal conforms to the NRC guidance contained in GL 88-20 and NUREG-1335 (Reference 2.0-2). SCE submitted a letter dated November 3, 1989, to the NRC outlining the proposed SCE IPE Program Plan for SONGS 2/3. The examination method chosen was a Level I PRA as described in NUREG/CR-2300, (Reference 2.0-3) plus a Containment Analysis as described by the NRC in Section 4 of the Generic Letter. Supplement No. 2, "Accident Management Strategies for Consideration in the IPE Process," and Supplement 3, "Completion of Containment Performance Improvement Program and Forwarding of Insights for Use in the IPE for Severe Accident Vulnerabilities," were also considered in the development of the IPE.

The criteria used in selecting important severe accident sequences were in accordance with Appendix 2 of GL 88-20. Documentation of examination results was maintained in a traceable manner under in-house document control as required by Section 10 of GL 88-20. This IPE report contains the information required by Appendix 4 of GL 88-20, and follows the format described in Table 2.1 of NUREG-1335.

2.3 General Methodology

The IPE includes a Level I (Front-End) analysis of core damage frequencies and a Level II (Back-End) analysis of phenomena affecting containment behavior and the release of radionuclides to the environment.

The SONGS 2/3 "Front-End" analysis used functionally descriptive event trees to model the accident sequences leading to safe or plant damage states. After the initiating event heading, each subsequent heading represents a function performed by SONGS 2/3 specific systems whose success or failure are modeled by detailed fault trees. The system fault trees were solved for the probability of system failure. The PRA model used general system functions in the event tree heading and modeled the system fault

trees in detail to the component level (the small event tree, large fault tree approach). The probabilistic analysis of modeling and quantification was performed using the *Reliability Engineering Building-Block Environment for Computer Analysis* (REBECA) computer code (Reference 2.0-4), and the containment thermal hydraulic response and source term analyses were performed with the Modular Accident Analysis Program (MAAP) code (Reference 2.0-13).

Common cause failure and mutually exclusive events were explicitly addressed in the fault tree and event tree solutions using post-processing features of REBECA.

The SONGS 2/3 "Back-End" Analysis was patterned after the IDCOR method as reviewed by the NRC. It coupled a probabilistic assessment of containment response to postulated initiating events with a physical model to examine plant response. Detailed papers addressing phenomenological issues and plant response were prepared based on SONGS 2/3 design features.

The Level II probabilistic models were embodied in the Extended Event Trees (EETs) which considered the systems, operator actions, and containment functional events required to respond to a core damage event and prevent or mitigate the release of radioactive fission products from the containment. The plant physical model was defined in the MAAP parameter file. This parameter file provided MAAP with information required to perform calculations of plant specific fission product transport and thermal hydraulic response to postulated accident sequences. It was also used to study the sensitivity of the source term to phenomenological uncertainties. The source term analysis used plant-specific values for MAAP model parameters. The sensitivity analysis identified any variations from this approach. The MAAP analyses were supplemented with phenomenological evaluation summaries to provide a complete physical representation of SONGS 2/3.

Results obtained with the probabilistic and physical plant models were closely linked. For instance, the EET structure depended on MAAP analyses to 1) define EET nodal success criteria and 2) determine the accident sequence outcome. Furthermore, sequences demonstrated by the quantification task to be either dominant contributors to the overall core damage frequency or of structural interest became the basis for MAAP calculations in support of the source term analysis. Finally, MAAP analyses and phenomenological evaluation summaries were used to investigate the effect of phenomenological uncertainties on the source term assessment. The use of MAAP as suggested above provided the necessary deterministic complement to the probabilistic assessment.

The SONGS 2/3 IPE utilized a modified version of MAAP PWR 3.0B Revision 17.02 to perform the containment and source term analysis. This version of the 17.02 code was modified slightly to more correctly model the SONGS 2/3 reactor cavity flow configuration and to employ the MAAP PWR 3.0B Revision 18.01 fan cooler model.

Source term analyses were performed following accident sequence quantification and designation of plant damage states. Plant damage states that were representative of containment performance had their source terms quantified in MAAP analyses. The purpose of the source term analysis was to define and quantify the radionuclide release characteristics for a given accident sequence, including specification of containment failure timing and fission product release magnitudes. MAAP calculations provided release magnitudes for selected fission product groups, release timing, and associated energy rates.

Since assumptions regarding key severe accident phenomena may dictate the analysis outcome, due consideration of phenomenological uncertainties was essential to the containment and source term analysis. The SONGS 2/3 IPE methodology addressed the phenomenological issues through plant-specific phenomenological evaluations and MAAP sensitivity studies. This two-pronged approach provided a bounding assessment of source term release timing and magnitude.

The SONGS 2/3 phenomenological evaluation summaries were the principal means of addressing the impact of phenomenological uncertainties on plant response. These summaries addressed a wide range of phenomenological issues and provided an in-depth review of plant specific features which influenced the uncertainty or acted to mitigate the consequences of such phenomena. The phenomenological evaluation summaries investigated both the likelihood of occurrence and the probable consequences of key severe accident phenomena.

The SONGS 2/3 phenomenological evaluation summaries were supported by plant specific calculations, available experimental information from open literature, as well as information developed using Fauske and Associates, Inc. (FAI) experimental facilities. Results of the FAI experimental efforts were incorporated into the appropriate phenomenological evaluation summaries.

The purpose of sensitivity studies was to determine which remaining phenomenological uncertainties had a significant impact on the likelihood or timing of containment failure and the magnitude of the source term release. In performing the SONGS 2/3 MAAP calculations, a limited number of model parameters was

investigated with respect to the influence of modeling uncertainties on the radionuclide source terms. In particular, uncertainties in the various physical processes were considered as documented in the IDCOR/NRC issue resolution process. The various phenomena and the uncertainties were described in letters from T. Speis of the NRC to A. Buhl of IT Corporation. GL 88-20 and NUREG-1335 provided summaries of those parameters judged to have a significant effect on containment failure and source terms.

In summary, the integrated approach to the assessment of total plant response adopted in the SONGS 2/3 IPE linked together probabilistic models in the EETs with physical plant models contained within MAAP. These models were supplemented through the use of SONGS 2/3 phenomenological evaluation summaries to provide in-depth technical arguments which reduced phenomenological uncertainties and examined realistic plant response to severe accident phenomena.

2.3.1 Applicability of Results to Both Units

The IPE model was developed based on design drawings and procedures for Unit 2 but is intended to portray the severe accident behavior of both Units 2 and 3.

San Onofre Units 2 and 3 were designed as twin mirror-image plants with some shared systems. SCE has maintained the units in as close to identical configuration as possible and design changes effected at one unit are effected at the opposite unit as soon as practical.

Units 2 and 3 share the same operating staff and operating crews routinely rotate back and forth between units. Units 2 and 3 share common operating procedures, e.g. the emergency operating instruction used for a loss of coolant accident at either unit would be procedure SO23-12-3. Operator training in the classroom and on the simulator is, with rare exceptions, non-unit specific. Finally, the Operating Licenses for both Units 2 and 3 are virtually identical.

Some past PRAs have identified dual unit initiating events as potential contributors to core damage risk. The possibility of this was investigated as part of the SONGS 2/3 IPE. In general, the SONGS 2/3 IPE model only credits the systems from a single unit. In some cases (e.g., 4160V cross-tie), credit was taken for use of systems from the adjacent unit. However, in all cases when credit was taken, the model reflects the specific likelihood that the system might be either affected by the initiator, required at the other unit due to plant status or initiator, or unavailable due to refueling outages, etc. Thus, the PRA model

of each of the initiating events accounts for any dual unit and shared system interactions and can be thought of as reflecting the core damage frequency of each unit.

As a result, the SONGS 2/3 IPE model based on Unit 2 design and operation is judged to be an applicable and accurate representation of the core damage frequency and contributors at both units.

2.4 Information Assembly

The procurement of information to support the IPE included reviews of past PRA studies, system walkdowns, personnel interviews, and assembly of documentation describing plant design and operation.

Past PRA studies reviewed as part of the IPE effort included:

1. WASH-1400, Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants (Reference 2.0-5).
2. Commonwealth Edison Company, Zion Probabilistic Safety Study, 1992 (Reference 2.0-6).
3. NUREG/CR-4550, Analysis of Core Damage Frequency From Internal Events: Sequoyah Unit 1 (Reference 2.0-7).
4. NUREG-1150, Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (Reference 2.0-8).
5. NUREG/CR-3511, Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant (Reference 2.0-9).
6. Pacific Gas & Electric, Diablo Canyon IPE Report, April 1992 (Reference 2.0-10).
7. Arkansas Nuclear One Unit 2 IPE Submittal, August 1992 (Reference 2.0-11).
8. Trojan IPE Submittal, November 1992 (Reference 2.0-12).

Pre-planned IPE plant walkdowns were undertaken by SCE IPE Team members, SCE system engineers and contractor personnel. Each system was walked down with a checklist for evaluating system performance and operator interfaces as part of the system analysis effort. In addition to the system walkdowns, each system analyst interviewed the cognizant plant system engineer to ensure current and historical operational and design

considerations are reflected appropriately. Human reliability analysts performed walk-throughs for key operator actions and documented key aspects of operator performance. In addition, the SONGS 2/3 simulator was utilized for both HRA data collection and plant response information and in some cases video tapes were made for further analysis. The internal flooding effort included additional walkdowns to verify component locations and flood sources. The Level II PRA for the Back-End analysis involved specific walkdowns performed to identify and document important plant features. Other walkdowns were performed as necessary to verify plant details.

System Notebooks were compiled for each plant system modeled in the IPE. These notebooks, generally consisting of several binders for each system, provided the IPE project team and reviewers with a ready information source for Updated Safety Analysis Report (UFSAR) data, system descriptions, training information pertaining to the system, technical specifications, operating procedures, maintenance procedures, as well as design drawings and other useful information.

All major work products (i.e., initiating event reports, event tree reports, system notebooks, etc.) were subjected to a multi-disciplinary review by SCE personnel to ensure that the plant, systems, and procedures were reflected accurately.

2.5 References

- 2.0-1 Generic Letter No. 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR §50.54(f)," USNRC, dated November 23, 1988 (including Supplements 1-4).
- 2.0-2 NUREG-1335, "Individual Plant Examination Submittal Guidance, Final Report," USNRC, dated August 1989.
- 2.0-3 NUREG/CR-2300, "PRA (Probabilistic Risk Assessment) Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," Volumes I and II, USNRC, dated January 1983.
- 2.0-4 "Reliability Engineering Building Block Environment for Computer Analysis (REBECA)," Version 3.0B, dated September 1992, a code based on FTAP and IMPORTANCE.
- 2.0-5 WASH-1400, "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," USAEC, dated August 1974.
- 2.0-6 "Zion Nuclear Generating Station, Units 1 and 2, Individual Plant Examination, Submittal Report," dated April 1992, attached to Letter from Marcia A. Jackson (CECo) to Dr. Thomas E. Murley (USNRC), dated April 24, 1992.
- 2.0-7 NUREG/CR-4550, "Analysis of Core Damage Frequency: Sequoyah, Unit 1, Internal Events," USNRC, dated April 1990.
- 2.0-8 NUREG-1150, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," USNRC, dated December 1990.
- 2.0-9 NUREG/CR-3511, "Interim Reliability Evaluation Program, Analysis of Calvert Cliffs, Unit 1, Nuclear Power Plant," USNRC, dated May 1984.
- 2.0-10 "Individual Plant Examination Report for Diablo Canyon Units 1 and 2 in Response to Generic Letter 88-20," Pacific Gas and Electric Company, April 1992.
- 2.0-11 "Arkansas Nuclear One, Unit 2 Probabilistic Risk Assessment: Individual Plant Examination Submittal for Arkansas Nuclear One, Unit 2", August 1992.

- 2.0-12 "Individual Plant Examination Report for the Trojan Nuclear Power Plant in Response to Generic Letter 88-20," dated November 1992.
- 2.0-13 "MAAP-3.0B - Modular Accident Analysis Program for LWR Power Plants, " EPRI NP-7071-CCML, Volume 1 and 2, November 1990.

3.0 FRONT-END ANALYSIS

3.1 Initiating Event and Plant Response Analysis

An initiating event is defined as a plant occurrence which challenges the continued safe operation of the facility. It causes a plant response which can be monitored and analyzed. Usually it leads to a plant trip due to protective systems which respond automatically to such an occurrence. A PRA begins by evaluating the plant design, design basis documents and studies, and plant history to identify a comprehensive set of initiating events. This process is described in Section 3.1.1. The plant response is defined by investigating the as-designed response to postulated initiating events and evaluating off-normal system performance or plant response. The result is a set of event trees which depict a complete set of responses which are depicted in Section 3.1.2.

3.1.1 Initiating Events

Any event or plant occurrence which leads to a plant shutdown is evaluated in the PRA as a potential event which initiates a plant response. Should the intended response fail, an accident may occur. Therefore it is important to identify those plant events that could, in conjunction with additional equipment failures and/or human errors, lead to core damage. This report addresses internally initiated (caused by an occurrence originating within the plant) events including internal flooding. Internal fires were not evaluated within the scope of internal initiating events per the requirements of GL 88-20. The external events, such as earthquakes, external floods, tornadoes, internal fire, and other external hazards, will be evaluated as part of the Individual Plant Examination for External Events (IPEEE) effort.

In the context of the IPE, an initiating event is defined as follows:

Any event that disrupts the normal conditions in the plant and leads to the need for reactor subcriticality and decay heat removal.

In the process of developing the list of initiating events for further evaluation, several assumptions are made which directly impact the initiating event identification, grouping, and analysis. These initiating event assumptions, as well as several limitations of the analysis, are listed below:

- All initiating events are considered to occur during full power operations. This is considered to be the limiting condition for most events.

- Events occurring at low power, cold shutdown, or manual shutdowns for administrative reasons or during refueling are not included as initiating events in this study.
- External events, such as wind, tornado, internal and external fires, external flooding, earthquakes, and sabotage are not within the scope of this study. This analysis is limited to those events associated with plant equipment failure, loss of offsite power, and internal flooding.
- Realistic analysis is the underlying objective of this study and excessive conservatism is avoided.
- Special studies and plant-specific calculations are performed as needed to establish realistic success criteria. However, UFSAR information or valid analyses/calculations from other general sources are also used.

The assumptions and limitations described above provide a general boundary of the scope for identifying initiating events. Based on these premises, the number of events satisfying the initiating event definition can be quite enormous. In order to transform the quantity of initiating events to a manageable number, a binning process was used to group the events into general initiating event categories. These general initiating event categories were sub-divided further as required to adequately capture the unique characteristic of events which could not be bounded within the general initiating event category.

The SONGS 2/3 plant shutdown histories were reviewed to develop a list of the shutdowns that have occurred since initial plant criticality. Based on this list and a review of the initiating event grouping performed in past studies, the general initiating event groups include:

- transient initiators
- loss of coolant accidents (LOCAs) initiators
- special initiators
- support system initiators

3.1.1.2 Transient Initiating Events

Transient initiating events represent a broad spectrum of events expected to occur during the life of the plant. These events result in a reactor scram and may impair operability of systems capable of supporting safe shutdown. Transient initiating events are classified into initiating event groups or categories based

upon common plant response and effects on the systems necessary to mitigate the transient.

Table 3.1-1 summarizes the binning of transient initiating events. Event categories defined to bound transient events include:

- TT transient events with Main Feedwater initially available
- TTa transient events with Main Feedwater impaired but initially available
- PCS transient events with Main Feedwater initially unavailable
- LOP transient events with Main Feedwater initially unavailable and non-1E power unavailable
- SS transient events not defined within the scope of TT, TTa, PCS and LOP evaluated separately as support systems

For analysis purposes, events defined within the TTa category were grouped with those defined in the TT category. The fractional contribution of TTa events (e.g., the ratio of the number of events in which one MFW train was impaired to the number of events in which MFW was available) was considered directly in the logic models.

A summary table used to quantify the plant-specific initiating event frequencies for the SONGS 2/3 transient initiating event categories is shown in Table 3.1-2. This table lists the number of occurrences and calculated frequencies for each of the three transient categories that are used for the SONGS 2/3 IPE.

Other transient initiators used in the SONGS 2/3 IPE include Main Steam Line/Feedwater Line Break (SLB), Anticipated Transient Without Scram (TWS), and Station Blackout (SBO). The main steam and feedwater line breaks are events that have not occurred at SONGS 2/3. Therefore, the initiating event frequencies are taken from generic industry data. The initiating event frequencies for both TWS and SBO are values transferred from other transient event trees. The TWS initiator is characterized by the occurrence of an initiating event with a failure of the reactor to scram. The SBO initiator is taken from the Loss of Offsite Power event tree characterized by a successful scram and a failure of both Emergency Diesel Generators (EDGs) to supply power initially.

Table 3.1-1

TRANSIENT INITIATING EVENTS

No.	Type	Transient Group
1	Loss of RCS Flow (1 loop)	TT
2	Uncontrolled Rod Withdrawal	TT
3	CEDM Problems and/or Rod Drop	TT
4	Leakage from Control Rods	TT
5	Leakage in Primary System	TT
6	Low Pressurizer Pressure	TT
7	Pressurizer Leakage	TT
8	High Pressurizer Pressure	TT
9	Inadvertent Safety Injection Signal	TT
10	Containment Pressure Problems	TT
11	CVCS Malfunction -- Boron Dilution	TT
12	Pressure/Temperature/Power Imbalance -- Rod Position Error	TT
13	Startup of Inactive Coolant Pump	TT
14	Total Loss of RCS Flow	TT
15	Loss or Reduction in Feedwater Flow (1 loop)	TTa
16	Total Loss of Feedwater Flow (all loops)	PCS
17	Full or Partial Closure of MSIV (1 loop)	TTa
18	Closure of All MSIVs	PCS
19	Increase in Feedwater Flow (1 loop)	TT
20	Increase in Feedwater Flow (all loops)	PCS
21	Feedwater Flow Instability -- Operator Error	PCS
22	Feedwater Flow Instability -- Miscellaneous Mechanical Causes	PCS
23	Loss of Condensate Pumps (1 loop)	TT
24	Loss of Condensate Pumps (all loops)	PCS
25	Loss of Condenser Vacuum	PCS
26	Steam Generator Leakage	TT
27	Condenser Leakage	TT

Table 3.1-1

TRANSIENT INITIATING EVENTS
(continued)

No.	Type	Transient Group
28	Miscellaneous Leakage in Secondary System	TT
29	Sudden Opening of Steam Relief Valves	TT
30	Loss of Circulating Water System	PCS
31	Loss of Component Cooling Water System	SS
32	Loss of Service Water System	SS
33	Turbine Trip, Throttle Valve Closure, EHC Problems	TT
34	Generator Trip or Generator Caused Faults	TT
35	Loss of All Offsite Power	LOP
36	Pressurizer Spray Failure	TT
37	Loss of Power to Necessary Plant Systems	SS
38	Spurious Trips -- Cause Unknown	TT
39	Automatic Trip -- No Transient Condition	TT
40	Manual Trip -- No Transient Condition	TT

Table 3.1-2

**SONGS 2/3 TRANSIENT
INITIATING EVENT FREQUENCIES**

Initiating Event Category	Plant	SONGS 2/3 Data Occurrences	SONGS 2/3 Data Frequency (per yr)	SONGS 2/3 IPE Value (per yr)
Transient with PCS Initially Available (TT)	SONGS 2	33	4.8	3.8
	SONGS 3	17	2.7	
	TOTAL	50		
Loss of Power Conversion System (PCS)	SONGS 2	2	0.29	0.53
	SONGS 3	5	0.80	
	TOTAL	7		
Loss of Offsite Power (LOP)	SONGS 2	0	0	0.11 ¹
	SONGS 3	0	0	
	TOTAL	0		

¹ From plant specific calculation based on NUREG-1032.

NOTE: SONGS 2 operating experience covers 6.9 years.
SONGS 3 operating experience covers 6.2 years.

3.1.1.3 LOCA Initiating Events

The LOCA initiating event group consists of loss of coolant accidents resulting from breaches of the primary system inside containment.

Loss of Coolant Accidents (LOCAs) include large LOCAs (>6"), medium LOCAs (2-6"), and small LOCAs (<2"). These three types of LOCAs are standard initiators used in plant PRAs. Plant specific thermal hydraulic analyses have been performed to verify that the break size ranges are appropriate for the SONGS 2/3 Emergency Core Cooling System (ECCS) capabilities. Also included is the small-small LOCA (<2"), which has evolved in the industry to primarily account for reactor coolant pump seal leaks that may have a unique contribution as initiators and for the steam generator tube rupture.

The values for these event frequencies were taken from NUREG/CR-4550, Revision 1 and are shown in Table 3.1-4. SONGS 2/3 RCS design features do not differ significantly from

the RCS design features of the PWR plants referenced in NUREG/CR-4550.

3.1.1.4 Special Initiating Events

For SONGS 2/3, two types of LOCAs are handled in a different manner than those LOCAs classified as part of the LOCA initiating event group. These two events are the Interfacing System LOCA (ISLOCA) and the Reactor Pressure Vessel Rupture. For both cases, it is conservatively assumed that there are no mitigating features of the plant to recover from these initiating events. As a result, the event frequency is taken to be the core damage frequency.

A SONGS 2/3 specific ISLOCA analysis has been performed based on the approach and data utilized in NUREG/CR-4550 and is discussed in more detail in Section 3.3.9.

The Reactor Pressure Vessel Rupture event has never occurred at any nuclear power plant and most other studies have excluded it as an initiator since the probability is extremely low. The SONGS 2/3 IPE includes it for completeness and to account for pressurized thermal shock scenarios. The frequency of the Reactor Pressure Vessel Rupture is estimated to be less than $2.0E-07/\text{yr}$ (based on WASH-1400).

3.1.1.5 Support System Initiating Events

A review of the SONGS 2/3 support systems has been performed to identify those systems whose failure causes a plant trip and degradation of an accident mitigating system. In general, postulated credible failures have been reviewed in each of the systems to determine whether a plant trip and degradation of a safety system occurs. If the results of the review indicate such, then the support system is considered an initiator, and an initiator frequency is developed.

The identification and evaluation of plant support systems follows the general guidance provided in NUREG/CR-4550 (Reference 3.1-1). System failures that result in a controlled plant shutdown (i.e., not a scram) are excluded from further review as they do not challenge plant safety systems.

If the resulting initiating event leads to a core damage frequency of less than $1.0E-07/\text{yr}$, the event is excluded from further evaluation, which is consistent with the methodology described in NUREG/CR-4550.

Based on the SONGS 2/3 system fault trees and the associated dependency matrices, the following support systems have been identified for evaluation:

- Electrical Support Systems (AC and DC)
- Mechanical Support Systems (SWC, CCW, ISA, HVAC, and ECW)

3.1.1.5.1 Electrical Support System Initiators

The Electric Power system at SONGS 2/3 consists of the following subsystems:

- 6.9 kV
- 4.16 kV
- 480 VAC
- 120 VAC
- 125 VDC

6.9 kV AC Power System

The 6.9 kV system is used to provide power to the reactor coolant pumps (RCPs). Loss of power at one or more of these buses will result in a plant trip due to loss of forced RCS flow. This failure has no impact on the availability of safety related equipment. In addition, the consequences of loss of power at the 6.9 kV bus is bounded by the Loss of Offsite Power (LOP) and the Loss of Power Conversion System (PCS) initiators. As such, loss of power on the 6.9 kV bus is not considered a potential support system initiator.

4.16 kV AC Power System

The 4.16 kV system is divided into safety related (SR) and non-safety related (NSR) portions. Loss of power on the non-safety related buses results in a plant trip due to loss of power to various balance of plant (BOP) loads. However, it does not have any impact on the availability of the accident mitigating systems. The consequences of loss of power on the non-safety related buses is bounded by the LOP and the PCS initiators. As such, loss of power on NSR 4.16 kV buses is not considered a potential support system initiator.

The safety related portion of the 4.16 kV system consists of buses 2A04 and 2A06 for SONGS 2 and 3A04 and 3A06 for SONGS 3. The discussion for loss of power at these buses is based on Unit 2, but the results are also applicable to Unit 3. Loss of a 4.16 kV bus A04(6) results in a loss of one train of safety related equipment, but does not result in an automatic or imminent plant trip. If a postulated failure was due to a bus fault, then one train of AC power would be lost regardless of the availability of alternate power sources. Since the bus failure does not result in an automatic or imminent plant trip, but a

controlled plant shutdown due to a technical specification Limiting Condition For Operation (LCO), it is not considered a potential support system initiator. Similarly, loss of both 4.16 kV ESF busses would not result in an automatic or imminent plant trip, but a controlled plant shutdown due to a technical specification LCO. Although a plant trip (manual scram) would be expected sooner for the case of two 4.16 kV ESF busses failing, the frequency of such an event is below the $1.0E-7$ /yr limit and is therefore not considered a separate support system initiator.

480 VAC Power System

The 480 VAC subsystem is configured such that each safety related 4.16 kV bus feeds a single safety related 480 VAC switchgear bus. Loss of a 480 VAC bus would result in loss of power to safety related equipment, and since the 480 VAC bus failure does not result in an automatic or imminent plant trip, but a controlled plant shutdown due to a technical specification LCO, it is not considered a separate support system initiator.

Similarly, failures of both 480 VAC buses or failures in combination with 4 kV bus failures would not result in an automatic or imminent plant trip, but a controlled plant shutdown due to technical specification LCO. The frequency of such an event is below the $1E-7$ /yr limit and is therefore not considered as a separate support system initiator.

120 VAC Power System

The safety related 120 VAC system (120 V vital AC) consists of 4 distribution buses. Each bus is normally supplied by a dedicated inverter, which is energized by the 125 VDC system described below. In the event inverter output is lost, the associated distribution bus would become de-energized until local operator action to transfer the bus to an alternate power source is completed. Loss of a single 120 VAC bus does not result in a plant trip, therefore, it is not evaluated as a support system initiator. However, loss of two 120 VAC buses would result in a plant trip with loss of some instrumentation channels of the Plant Protection System (PPS). Loss of power from two 120 VAC buses does not prevent ESF equipment from operating. The consequences of loss of two 120 VAC buses is bounded by the Loss of Power Conversion System (PCS) initiators. As such, loss of power on two 120 VAC buses is not considered a separate support system initiator.

125 VDC Power System

The SONGS 2/3 safety related 125 VDC system consists of four independent DC subsystems for each unit. Each subsystem is comprised of a battery bank, a battery charger, and a distribution bus. DC distribution panels D1P1 and D2P1 provide breaker control power to safety related 4.16 kV buses A04 and A06, respectively. Each subsystem also supplies power to a 120 VAC vital bus inverter: Bus D1 supplies inverter Y01, D2 supplies Y02, D3 supplies Y03, and D4 supplies Y04.

Loss of a 125 VDC subsystem results in a loss of the associated 120 VAC inverter bus until local operator action is taken to transfer the 120 VAC power supplies. Loss of DC bus D3 or D4 would not result in an automatic or imminent plant trip, but a controlled plant shutdown due to a technical specification LCO. Therefore, it is not considered a support system initiator. Loss of DC bus D1 or D2 would result in a plant trip due to closure of the feedwater isolation valves (FWIVs) and a main steam isolation valve (MSIV). Therefore, loss of power from DC bus D1 or D2 is treated as a support system initiator.

If loss of power occurred on distribution panel D1P1 or D2P1, loss of control power to one channel of safety related 4 kV power would also result. If this failure occurred during a PPS channel test of a different train, an automatic plant trip with significant loss of safety related equipment would result. A PPS channel check is performed once a month and involves introducing a tripped channel state for several minutes. Although the loss results in an automatic plant trip, the frequency of such an occurrence is below the $1.0E-7/\text{yr}$ limit. Therefore, loss of power on panel D1P1 or D2P1 is not considered a separate support system initiator.

Loss of two 125 VDC buses would result in an automatic plant trip due to loss of input power to the 120 VAC inverters. However, the frequency of such an event is below $1.0E-7/\text{yr}$. Therefore, it is not considered a separate support system initiator.

3.1.1.5.2 Mechanical Support System Initiators

The cooling systems that were evaluated for potential initiators are:

- Component Cooling Water (CCW) System
- Saltwater Cooling (SWC) System
- Heating, Ventilating, and Air Conditioning (HVAC)
- Emergency Chilled Water (ECW)

Component Cooling Water System

The Component Cooling Water (CCW) system at SONGS 2/3 is a closed loop system supplying cooling water to various plant equipment. The system is designed without provisions for "cross unit" connections when both plants are at power and is therefore not considered a common system. The heat in the CCW system is transferred to the SWC system via heat exchangers. Loss of a single train of CCW and/or SWC is not considered as a support system initiator since a plant trip does not occur.

If a total loss of SWC and/or CCW were to occur, a plant trip is expected to be manually initiated by the operators due to loss of cooling to the RCPs, the Control Element Drive Mechanisms (CEDMs), and the letdown heat exchanger. The initiator frequency for such an event is obtained from the CCW fault tree solution. The frequency for a total loss of CCW exceeds the $1.0E-7/\text{yr}$ limit. Therefore, it is considered a separate support system initiator.

Saltwater Cooling System

The Saltwater Cooling (SWC) system at SONGS 2/3 provides cooling water to only the CCW heat exchangers. In the event of loss of SWC, the effects are bounded by loss of CCW. As such, the evaluation of SWC as a support system initiator is performed concurrently with the evaluation of the CCW.

Heating, Ventilation and Air Conditioning Systems

The control of environmental conditions for plant areas at SONGS 2/3 is provided by various systems. For the purposes of this evaluation these systems are collectively referred to as the Heating, Ventilating, and Air Conditioning (HVAC) system. The loss of HVAC for certain areas such as the 4 kV and 480 VAC switchgear rooms and the control room could adversely impact plant systems and/or require a controlled plant shutdown. However, loss of HVAC does not cause nor require an immediate plant trip. Numerous operator actions such as starting emergency cooling units, reducing heat loads, opening doors, and providing portable fans are available to maintain area temperatures within acceptable limits. The very mild plant climate at SONGS extends the opportunity available for mitigative actions and contributes to the effectiveness of alternate cooling methods. Since mitigating actions are likely to occur and a plant trip is not expected, the loss of HVAC is not evaluated as a support system initiator.

Emergency Chilled Water System

SONGS 2/3 has an Emergency Chilled Water (ECW) system which provides cooling for essential plant equipment. The system is normally on standby and is automatically started on a Safety Injection Actuation Signal (SIAS). Failure of the ECW system does not cause nor require a plant trip and, therefore, failure of this system is not considered a support system initiator.

Instrument and Service Air System

The Instrument and Service Air (ISA) system at SONGS 2/3 consists of three air compressors and associated compressed air receivers, and a nitrogen backup system. Each air receiver is isolated from the others via check valves. Loss of all instrument air is expected to result in an automatic plant trip on both SONGS units. However, the loss of ISA does not adversely impact the availability of safety related equipment. The consequences of loss of ISA is bounded by the LOP and the Loss of Power Conversion System PCS initiators. As such, this system failure is not considered a separate support system initiator.

Table 3.1-3 provides a summary of support system initiators.

3.1.1.6 Internal Flood Initiating Event

The SONGS 2/3 Internal Flood Evaluation is described in Section 3.3.8. Based on this evaluation, the internal flood initiator was found to be bounded by the loss of PCS initiating event. Therefore, no separate internal flood initiator is evaluated.

3.1.1.7 Initiating Event Summary

Table 3.1-4 provides the list of initiating events used for the SONGS 2/3 IPE. Table 3.1-4 includes the frequency for each initiating event and the basis of the frequency. Table 3.1-5 summarizes the safety functions required or challenged by initiating events considered in the analysis.

3.1.2 EVENT TREES

3.1.2.1 General

Event tree models are used to depict a large number of failure scenarios or accident sequences that can result in serious plant conditions. These failure scenarios arise from certain failures of Engineered Safety Features (ESF) Systems to operate successfully following an initiating event. Each event tree depicts the functional response of the plant to a given initiating event, considering the systems required for successful mitigation of the plant challenge imposed by the initiator.

Table 3.1-3
SUMMARY OF SUPPORT SYSTEM INITIATORS

No.	Support System Failure	Impact on Normal Operation	Impacts on Safety Systems	Estimated Frequency	Resolution
1	4 kV 1E Single Bus	None	Loss of one train of safety related equipment	NA	Exclude based on no automatic trip
	4 kV 1E Multiple Buses	Plant trip (manual) due to loss of power	Loss of all safety related power	$< 1.0E-7$	Not evaluated based on low frequency of occurrence
2	480 VAC	Enveloped by 4 kV	Enveloped by 4 kV	NA	Combine with item no. 1
3	120 VAC Single Bus	No adverse impact	Loss of one channel of instrumentation	NA	Exclude based on no trip
	120 VAC Multiple Buses	Plant trip due to spurious PPS signal	Loss of multiple instrumentation channels and loss of main feedwater due to false CIAS	NA	Enveloped by loss of PCS Initiator
4	125 VDC Single Bus	Plant trip due to MSIV closure and MFW isolation	Loss of one train of safety related equipment.	$1.8E-3$	Evaluate as a support system initiator
	125 VDC Multiple Buses	Loss of breaker control power and automatic plant trip.	Loss of multiple trains of safety related equipment.	$< 1.0E-7$	Not evaluated based on low frequency of occurrence
5	Component Cooling Water Single Train	None	Loss of one train of safety related equipment	NA	Exclude based on no trip
	Component Cooling Water Multiple Trains	Loss of all CCW cooling to the RCP's and letdown heat exchanger - manual plant trip	Loss of cooling to the HPSI and LPSI pumps, and the shutdown heat exchanger	$2.5E-4$	Evaluate as a support system initiator
6	Saltwater Cooling Single Train	Loss of cooling to one CCW heat exchanger	Loss of cooling to one train of ECCS equipment	NA	Evaluate as part of loss of CCW
	Saltwater Cooling Multiple Trains	Loss of cooling to both CCW heat exchangers	Loss of cooling to the HPSI and LPSI pumps, and the shutdown heat exchanger	NA	Evaluate as part of loss of CCW
7	Instrument Air	Plant trip due to loss of control air supply	None	NA	Enveloped by LOP and PCS Initiators
8	HVAC	None unless action not taken to provide alternate ventilation	No immediate failures	NA	Exclude based on no trip
9	Emergency Chilled Water	None	Loss of emergency cooling to one train of ESF equipment rooms	NA	Exclude based on no trip

Table 3.1-4
SONGS 2/3 INITIATING EVENT SUMMARY AND BASIS

Abbreviation	Initiator	Frequency (/yr)	Basis
TT	Transient with PCS Initially Available	3.8	SONGS 2/3 plant specific data
PCS	Loss of Power Conversion System	0.53	SONGS 2/3 plant specific data
LOP	Loss of Offsite Power	0.11	SONGS 2/3 plant specific calculation based on NUREG-1032 (Reference 3.1-2)
SLB	Main Steam Line/Feedwater Line Break	5.4E-4	EPRI NP-6992-L (Reference 3.1-11)
LL	Large LOCA (> 6")	5.0E-4	NUREG/CR-4550, Rev. 1 (Reference 3.1-1)
ML	Medium LOCA (2" - 6")	1.0E-3	NUREG/CR-4550, Rev. 1 (Reference 3.1-1)
SL	Small LOCA (< 2")	1.0E-3	NUREG/CR-4550, Rev. 1 (Reference 3.1-1)
SSL	Small-Small LOCA (< 2")	1.3E-2	NUREG/CR-4550, Rev. 1 (Reference 3.1-1)
SGR	Steam Generator Tube Rupture	1.0E-2	NUREG/CR-4550, Rev. 1 (Reference 3.1-1)
VL	Interfacing System LOCA	6.6E-7	SONGS 2/3 plant specific evaluation (see Section 3.3.9)
VR	Reactor Pressure Vessel Rupture	<2.0E-7	WASH-1400 (Reference 3.1-4)
LDC	Loss of Single 125 VDC Bus	1.6E-3	NUREG/CR-2815 (Reference 3.1-13)
CCW	Loss of Component Cooling Water	2.5E-4	Based on analysis of the CCW fault tree

Table 3.1-5

SAFETY FUNCTION REQUIREMENTS VS. INITIATING EVENT CATEGORY

Initiating Event Category	Safety Function						
	Reactivity Control	RCS Heat Removal	RCS Pressure Control	RCS Inventory Control	Core Heat Removal	Containment	Vital Auxiliaries
Turbine Trip (TT)	Required.	Required.	Required. Not challenged by initiator, but may be degraded due to a stuck open pressurizer safety relief valve.	Not required unless heat sink or RCS pressure control safety functions are challenged.	Not required unless RCS Heat Removal or RCS pressure control functions fail.	Not required unless RCS heat removal or RCS pressure control are lost.	Required to support frontline systems.
Loss of Power Conversion System (PCS)	Required.	Required. Main feedwater, condensate and condenser initially unavailable due to initiator.	Required. Not challenged by initiator, but may be degraded due to a stuck open pressurizer safety relief valve.	Not required unless heat sink or RCS pressure control safety functions are challenged.	Not required unless RCS Heat Removal or RCS pressure control functions fail.	Not required unless RCS heat removal or RCS pressure control are lost.	Required to support frontline systems.
Loss of Offsite Power (LOP)	Required.	Required. All systems unaffected by initiator, except BOP equipment such as MFW, condensate and electric AFW, which may not be available.	Challenged due to loss of shutdown and RCP trip.	Not required unless heat sink or RCS pressure control safety functions are challenged.	Not required unless RCS heat removal or RCS pressure control functions fail.	Not required unless RCS heat removal or RCS pressure control are lost.	Required to support frontline systems.
Station Blackout (SBO)	Required.	Challenged. Only turbine-driven AFW pump available.	Challenged.	Not required unless heat sink or RCS pressure control safety functions are challenged. However, required systems are unavailable.	Not required unless RCS heat removal or RCS pressure control functions fail. However, required systems are unavailable.	Not required unless RCS heat removal or RCS pressure control are lost.	Required to support frontline systems. Degraded due to loss of offsite and onsite 4160/480 VAC.
Main Steam Line/Feedwater Line Break (SLB)	Required.	Required. Main Feedwater and Condensate may be affected by initiator. Success requires isolation of faulted S/G.	Required. Not challenged by initiator, but may be lost due to stuck open relief valves.	Not required unless heat sink or RCS integrity safety functions are challenged.	Not required unless heat sink or RCS integrity functions fail.	Challenged if SLB is inside containment.	Required to support frontline systems.
Large LOCA (LL)	Not required due to boron injection during core reflood.	Not required.	Challenged due to initiator.	Challenged due to loss of inventory caused by large LOCA.	Challenged. Accumulators required to ensure core cooling prior to ECCS flow reaching core.	Challenged by blowdown of RCS.	Required to support frontline systems.

Table 3.1-5

SAFETY FUNCTION REQUIREMENTS VS. INITIATING EVENT CATEGORY
(continued)

Initiating Event Category	Safety Function						
	Reactivity Control	RCS Heat Removal	RCS Pressure Control	RCS Inventory Control	Core Heat Removal	Containment	Vital Auxiliaries
Medium LOCA (ML)	Required.	Not required.	Challenged due to initiator.	Challenged due to inventory loss through RCS break.	Not required unless RCS inventory function is not maintained.	Challenged by blowdown of RCS.	Required to support frontline systems.
Small LOCA (SL)	Required.	Required.	Challenged due to initiator.	Challenged due to inventory loss through RCS break.	Not required unless RCS inventory function is not maintained.	Challenged by blowdown of RCS.	Required to support frontline systems.
Small-Small LOCA (SSL)	Required.	Required.	Challenged due to initiator. Cooldown to SDC initiator can mitigate loss of integrity.	Challenged due to inventory loss through RCS break.	Not required unless RCS inventory function is not maintained.	Challenged by blowdown of RCS.	Required to support frontline systems.
Steam Generator Tube Rupture (SGR)	Required.	Required.	Lost due to initiator.	Challenged due to inventory loss through RCS break.	Not required unless RCS inventory function is not maintained.	Not required.	Required to support frontline systems.
Interfacing System LOCA (VL)	Not evaluated due to low frequency of initiator.	Not required.	Lost due to initiator.	Lost due to initiator.	Lost due to initiator.	Bypassed due to initiator.	Required to support frontline systems.
Anticipated Transient without Scram (TWS)	Challenged. Shutdown of nuclear reaction required to achieve safe, stable state.	Challenged. Requires high flow rate to SGs.	Challenged. RCS pressure relief required to handle high heat generation rates.	Challenged. RCS makeup required to makeup for inventory loss due to pressure relief.	Challenged by mismatch in core power level and heat removal.	Challenged due to PZR relief valves opening.	Required to support frontline systems.
Loss of 125 VDC Bus (LDC)	Required.	Required. One ESF train of AFW affected.	Required. Not challenged by initiator, but may be degraded due to a stuck open pressurizer safety relief valve.	Not required unless heat sink or RCS pressure control safety functions are challenged. One train of ECCS affected.	Not required unless RCS Heat Removal or RCS pressure control functions fail.	Not required unless RCS heat removal or RCS pressure control are lost. One ESF Cont. spray pump affected.	Required to support frontline systems.
Loss of CCW (CCW)	Required.	Required.	Challenged. Failure to trip RCP can result in seal LOCA.	Challenged. All ECCS pumps except CVCS affected.	Not required unless RCS Heat Removal or RCS pressure control functions fail.	Not required unless RCS heat removal or RCS pressure control are lost.	Required to support frontline systems. Degraded due to loss of CCW cooling to ECCS pumps.

The ESF and Systems modeled provide the essential plant response actions that satisfy safety functions required to achieve stable conditions. The successful control and fulfillment of the safety functions form the basis by which successful mitigation of the accident is defined.

Each event tree is characterized by a subject title, initiator node, functional node, structured logic diagram, sequence number, sequence designation, accident class, and sequence frequency as depicted in Figure 3.1-1. The subject title refers to the initiating event group evaluated in the event tree. The first node in the event tree is defined as the initiating event group.

An event tree is developed for each initiating event group defined in Section 3.1.1.

Nodes following to the right of the initiator node represent functions that must be satisfied to achieve successful accident mitigation based on the challenge to the plant caused by the initiator. The success or failure of the function to be satisfied determines the subsequent functions required for plant safety. Although the functional nodes are most often listed in the order of sequential response or hierarchy of critical safety functions, this is not always the rule. In some cases nodes are placed in an alternate sequence to capture the impact of system availability on timing effects influencing success of subsequent nodes. This reordering helps identify the success or failure of a particular function more explicitly. Event tree structure logic diagrams depict the points in the model where certain functions are required. If a function pertains to the node in question, a branch is modeled. The upward path in the branch represents success of the function while the downward path represents failure of the function.

The end point of the event tree structure is represented by the sequence number, sequence designation, and accident class. The sequence number is used to reference the sequences in the event tree sequence discussions. The sequence designation represents, in abbreviated form, the node elements which comprise the sequence definition. Sequence designations consist of the node code definitions of the initiator and any functional node failure along the sequence path. For example, sequence #5 in Figure 3.1-1 is defined as "I-ND1-ND3" which signifies occurrence of initiator "I" with failure of node functions defined in node 1 (ND1) and node 3 (ND3).

The accident class field is used for multiple purposes depending on the assessment of the sequence. For cases in which sequences represent successful plant response to the initiating event, the accident class is defined as "OK" (sequence #1, Figure 3.1-1).

For cases in which sequences are not evaluated (e.g., due to previous assessment of the insignificance of the sequence frequency), the accident class field is left blank with the words "UNANALYZED" in the sequence frequency field (see sequence #3, Figure 3.1-1). For cases in which the sequence transfers to another event tree due to commonality of the event tree end state with the entry condition of another event tree model, the term "XFER" (signifying transfer) and the initiator code of event tree to which the sequence transfers is entered in this field (see sequence #5, Figure 3.1-1).

In most cases the accident class field represents a functional accident class (see sequences #2 and #4, Figure 3.1-1). The functional accident class indicates the condition of the plant following the sequence of events. Accident classes are used for the purpose of binning the Level I (Front-End) model results for comparison to NRC screening criteria. These classes are further subdivided into plant damage states as part of the Level II (Back-End) containment analysis. Table 3.1-6 defines the functional accident classes used in the SONGS 2/3 IPE. These functional accident classes are the same as those defined in NUMARC 91-04, "Severe Accident Issue Closure Guidelines" (Reference 3.1-5).

3.1.2.2 Critical Safety Functions

The concept of safety functions introduces a systematic approach to plant operations based on a hierarchy of protective actions. The protective actions are directed at mitigating the consequences of an event and, once fulfilled, ensure proper control of the event in progress. A safety function is defined as a condition or action that prevents core damage or minimizes radiation release to the public. A complete set of safety functions needs to be fulfilled to ensure proper operator control of the event and public safety.

The safety functions considered are directed at mitigating an event and containing and/or controlling radioactivity releases. Release is prevented by maintaining the barriers to radioactive release which include: (1) the fuel matrix and cladding; (2) the reactor coolant system (pressure vessel and piping in the closed primary loop); and (3) the containment structure. Each of the barriers to radioactive release is supported by one or more safety function. Similarly, each safety function is supported by one or more frontline systems which require support systems for operability.

The safety functions for SONGS 2/3 are defined in the Combustion Engineering Emergency Procedure Guidelines, Section 1.5.2

Table 3.1-6

FUNCTIONAL ACCIDENT SEQUENCE DEFINITION

Functional Accident Class	Definition
IA	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Injection Phase (e.g., loss of secondary heat sink and failure of bleed and feed)
IB	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Recirculation Phase
IC	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup Due To Station Blackout
IIA	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase
IIB	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase
IIIA	Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase
IIIB	Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase
IIIC	Accident Sequences Initiated By Medium or Large LOCA With Loss of Primary Coolant Makeup In The Injection Phase
IIID	Accident Sequences Initiated By A Medium or Large LOCA With Loss of Primary Coolant Makeup or Adequate Heat Removal In The Recirculation Phase
IV	Accident Sequences Involving Failure of Reactivity Control
VA	Systems LOCA Outside Containment Leading to Loss of Effective Primary Coolant Inventory Makeup
VB	Steam Generator Tube Rupture Leading to Loss of Effective Primary Coolant Inventory Makeup

(Reference 3.1-6). These safety functions are grouped into four major classes as follows:

- Anti-core melt safety functions
- Containment integrity safety functions
- Indirect radioactive releases safety function
- Maintenance of vital auxiliaries

The anti-core melt safety function class and the maintenance of vital auxiliaries are the primary concerns of the IPE Front-End analysis. The anti-core melt safety function is further subdivided into five safety functions:

- Reactivity control
- RCS inventory control
- RCS pressure control
- Core heat removal
- RCS heat removal

Reactivity Control refers to the shutdown of the reactor core to cease power generation by fission in the reactor. Shutdown of the reactor is accomplished by control rod insertion or emergency boration to introduce sufficient negative reactivity into the core for reduced thermal neutron interactions and ultimately cease fission power generation in the primary system.

RCS Inventory and Pressure Control refers to maintaining the reactor core covered with an effective coolant medium. RCS inventory and pressure control are interdependent for SONGS 2/3. Actions taken to effect inventory control affect pressure control and vice versa.

Core Heat Removal pertains to the removal of decay heat from the primary system. Core Heat Removal is achieved by transfer of primary system heat to the secondary system or through breaks in the primary system in the case of LOCAs.

RCS Heat Removal refers to the removal of heat from the primary system using secondary systems. Primary system heat is removed from the primary system using one or more steam generators.

The maintenance of vital auxiliaries safety function refers to maintaining operability of key systems necessary to support the other safety functions. The importance of maintaining vital auxiliaries is realized from the capacity of support system to affect multiple components and systems. For example, support systems such as electric power and component cooling water can affect the multiple frontline systems and the safety functions they support.

The safety function concept incorporates a principle of safety function hierarchy. Some safety functions have precedence over others in terms of their sequence of implementation during an event. Reactivity control is the most important safety function since it responds most quickly to changes in plant conditions and subsequent functions are dependent upon its success. Similarly, RCS inventory control must be satisfied before core heat removal can be effected (i.e., there must be a medium to remove heat) and, in general, loss of inventory can occur within a shorter time frame than that required for core heat removal. This hierarchy concept is important in the design of systems used to fulfill each function and is also employed in the Emergency Operating Instructions (EOIs). The EOIs identify each of the safety functions and the acceptance criteria which reflect successful accomplishment of each function.

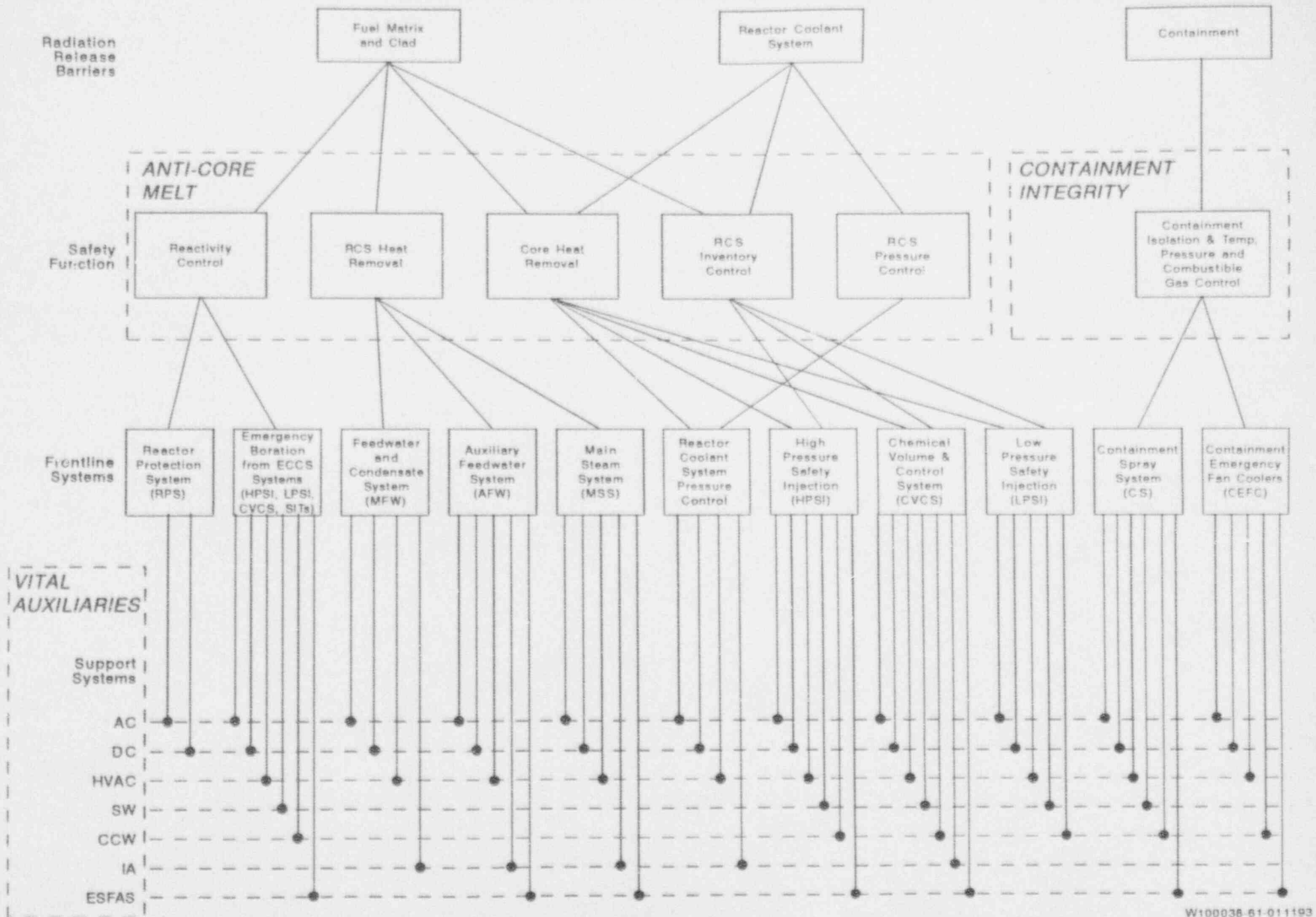
Figure 3.1-2 provides a graphic representation of the relationship of the safety functions considered in the Level I PRA and the SONGS 2/3 frontline and support systems modeled.

3.1.2.3 Event Tree Assumptions

Model assumptions were developed to establish common bases for accident sequences constructed in the event tree models. The modeling assumptions listed below are generic to the event tree models. These assumptions are consistent with NUREG/CR-4550 and common PRA practices. Assumptions having applicability to specific event trees are listed in the discussion of the individual event tree model.

1. All successful sequences are evaluated to the point where stable long term cooling conditions are established.
2. RCS inventory makeup is not required if RCS integrity is maintained. This implies normal pressurizer water level is sufficient to accommodate RCS inventory shrinkage from full power to hot shutdown and any pre-accident leakage permitted by Technical Specifications. RCS volume control via normal makeup and letdown is not addressed for any initiator.
3. Boration of the reactor is not required if hot shutdown temperatures and RCS integrity are maintained.

RELATIONSHIP BETWEEN RADIOACTIVE RELEASE BARRIERS, SAFETY FUNCTIONS AND SYSTEMS



4. Depressurization for RCS pressure control is either inherent in the accident response (LOCAs) or primary system pressure is controlled through the use of secondary systems.
5. Operator actions modeled include those tasks required by procedure to actuate and control necessary systems and to mitigate failed components.
6. RCS overcooling is not addressed in individual event trees. Operators are assumed to cooldown the plant as specified by the Emergency Operating Instructions.
7. Failure of the reactor pressure vessel for events characterized by overcooling and high system pressure is not addressed in the individual event trees. Through-wall crack formation for CE plants is conservatively estimated to be less than $1.0E-07/\text{yr}$ based on NUREG/CR-4483 (Reference 3.1-9). The frequency of a through-wall crack in which crack growth is not arrested leading to leakage above the capabilities of ECCS system is estimated to be less than the conservative estimate in NUREG/CR-4483. Therefore, the failure of the reactor pressure vessel due to pressurized thermal shock (PTS) is considered subsumed within the reactor pressure vessel rupture event tree.
8. Injection refers to ECCS injection from the RWST. The time phase of injection is referred to as early.
9. Recirculation refers to ECCS injection sourced from the containment sump. The time phase of recirculation is referred to as late.
10. The plant is considered to be operating at 100% power prior to the initiating event.
11. The criteria for core damage is conservatively assumed to be core uncover. Large LOCA is considered an exception due to temporary core uncover during the blowdown phase.
12. Combustion Engineering (CE) Document NPSD-537, "An Evaluation of the RCP Seal Integrity Issue GI-23," September 1989 (Reference 3.1-7) and SCE analysis (Reference 3.1-12) support the assessment that the SONGS 2/3 reactor coolant pump (RCP) seals will remain intact at least 24 hours without seal cooling, given

the RCPs are tripped. EOI S023-12-3, "Loss of Coolant Accident" indicates that the RCPs are tripped for all LOCA events. It is assumed for transient events that the probability of random failure or unavailability of the CCW system and failure of the operator to trip the RCPs given high seal temperature indication is negligible. If high containment pressure conditions exist, as in the case of LOCA events, a loss of cooling to the RCPs results due to the isolation of the CCW non-critical loop. RCP seal integrity for these scenarios is bounded by the frequency of the LOCA occurrence and does not preclude the availability of ECCS associated with a loss of all CCW.

13. Automatic reactor trip is successful if a reactor trip signal is generated and all CEAs are inserted into the core. EOI S023-12-1, "Standard Post Trip Actions" requires the operators to perform emergency boration if more than one CEA does not insert following trip of the reactor.
14. Reactor vessel head and pressurizer venting are not credited as a means of effective RCS heat removal.
15. Failure of main steam relief is negligible. That is, adequate redundancy exists for secondary pressure relief via the main steam bypass control system and 18 steam generator safety valves such that the probability of overpressurizing the secondary side is numerically insignificant. This is consistent with Surry and Sequoyah models in NUREG-4550.

3.1.2.4 Front-line Transient Event Trees

3.1.2.4.1 Transient with PCS Initially Available

Initiating Group Summary

The Transient with Power Conversion System Initially Available initiating event group (TT) includes all initiating events which lead to a reactor trip, but which do not directly disable systems required to maintain critical safety functions. Initial conditions for this accident scenario include availability of MFW, the condenser, turbine bypass valves, and offsite power at the time of the initiating event.

An example of a TT initiating event is a main turbine trip on turbine generator overload. As each of the high pressure turbine stop valves close, a valve close signal is generated and sent to

the Reactor Protection System (RPS). Any two of the four high pressure turbine stop valve close signals generate a "loss of load" reactor trip signal. This type of general transient initiating event challenges, but does not directly disable, critical plant safety functions or disable the PCS.

Plant Response to Initiating Event

Following the turbine trip, all turbine stop valves and governor valves are closed by springs when the trip signal releases hydraulic fluid in each of the actuators. Each of the four high pressure turbine stop valves sends an actuator hydraulic fluid low pressure signal to the RPS. Any two of the four signals cause the RPS to generate a "loss of load" reactor trip signal.

The steam bypass control system (SBCS) is normally in automatic mode and available upon turbine trip. If the SBCS is unavailable, the steam generator safety valves open to relieve steam and provide an ultimate heat sink. The atmospheric dump valves can also be used by the operators to remove decay heat. Each reactor trip incurs some probability that MFW is lost. A reactor trip override (RTO) signal, which is generated by every reactor trip, closes the MFW regulating valve, partially opens the feedwater bypass valve, and reduces the speed of the MFW pumps. Unlike some PWR plant designs, the SONGS 2/3 MFW remains available following these types of trips as the primary heat removal system.

Should the MFW system fail, the AFW system will automatically actuate on low steam generator level to provide feedwater and maintain level in the steam generators. Emergency Operating Instruction EOI SO23-12-2, "Reactor Trip Recovery" directs the operator to terminate automatic operation and commence manual operation of the AFW system in order to maintain steam generator level.

In the event both MFW and AFW are unavailable for secondary system heat removal, EOI SO23-12-9, "Functional Recovery," Attachment 8, directs the operator to establish low pressure alternate feedwater to the steam generators. The operator is required to reduce steam generator pressure to less than 500 psia and manually align the condensate system to provide feedwater to the steam generators. The steam generators can be depressurized successfully by utilizing the atmospheric dump valves.

Event Tree Assumptions

The following assumption was used in the event tree construction of the plant response to a transient event:

Assumption	Basis
Primary system pressure will not normally exceed the setpoint of the pressurizer safety valves, therefore, RCS integrity is only challenged for a fraction of the transient events.	FSAR Section 15.2.1.2 indicates that no challenge will occur. The fraction of events which challenge the pressurizer safety valves is driven by setpoint miscalibration. The frequency is based on the occurrence of one event in the past plant history involving premature opening of a pressurizer safety valve. This accounts for spurious openings and setpoint drift.

Event Tree Model

The event tree model for Transient with PCS Initially Available (TT) is depicted in Figure 3.1-3. The safety function and success criteria for each constituent node of this event tree are presented in Table 3.1-7.

The **Transient with PCS Available** node (TT) represents the occurrence of the turbine trip initiating event. The second node **Automatic Reactor Trip** (K) addresses the requirement for a reactor trip to achieve subcriticality following the turbine trip. This node addresses only the Reactor Protection System automatic reactor trip functions. Manual reactor trip is addressed separately in the Anticipated Transient Without Scram (TWS) event tree.

The **Main Steam Relief Available** (T) node represents removal of secondary system steam through the turbine bypass valves, atmospheric dump valves or main steam safety valves.

The **Pressurizer Safety Valves Reclose** (YTT) node evaluates the potential for pressurizer safety valves to be challenged and fail to reclose. The **HPSI In Cold Leg Injection Mode** (HI) and **Containment Spray In RCS Injection Mode** (NI) nodes evaluate the RCS makeup systems required to respond in the event of a stuck open pressurizer safety valve.

The **MPW Available to 1 of 2 Steam Generators** (F) and **APW Available to 1 of 2 Steam Generators** (L) nodes represent operation of secondary heat removal systems to remove decay heat from the primary system.

Figure 3.1-3: Transient with PCS Initially Available (TT) Event Tree

TRANSIENT WITH PCS INITIALLY AVAILABLE (TT)

SAN ONOFRE IPE - UNITS 2 & 3

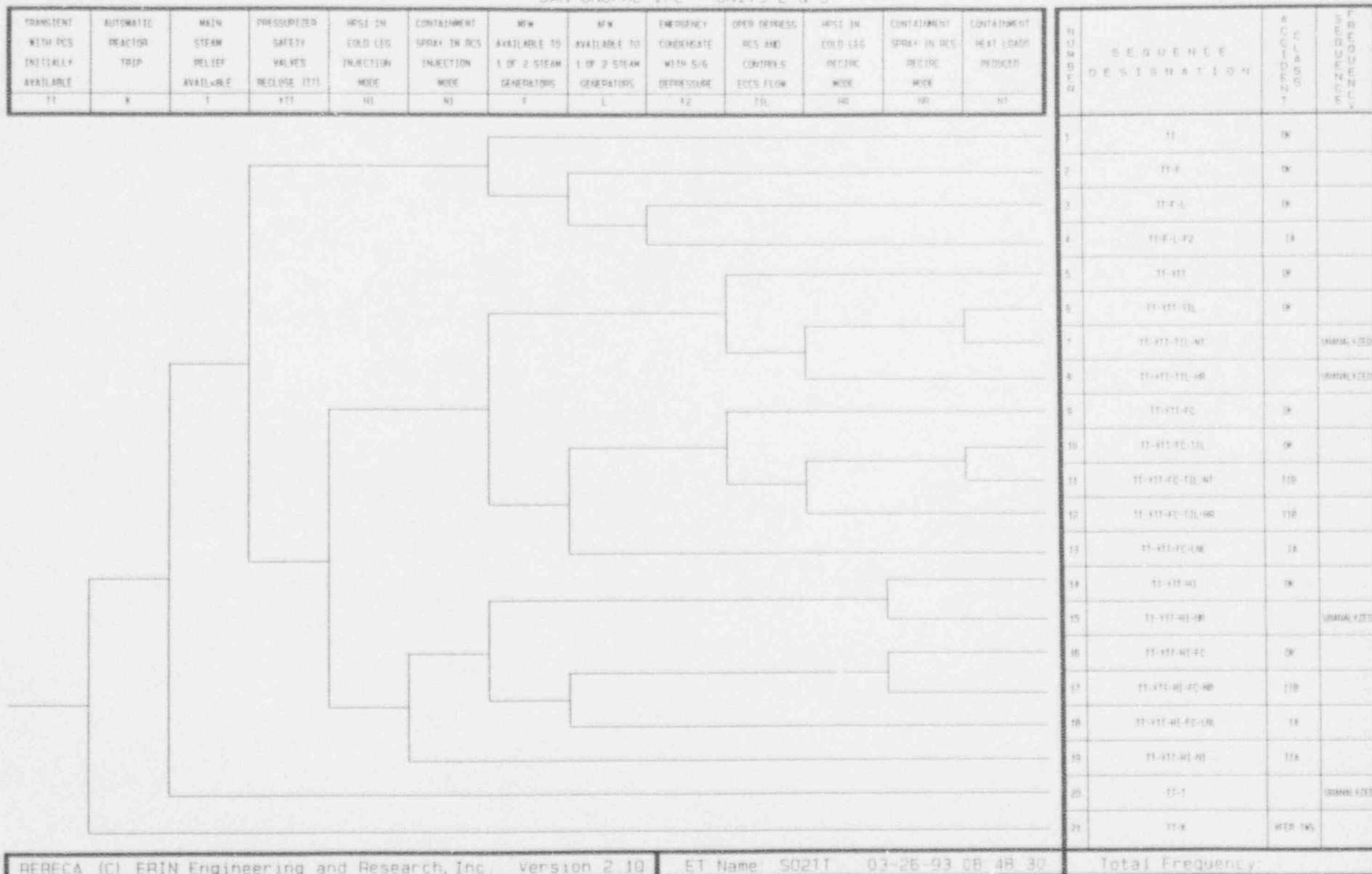


TABLE 3.1-7: TT EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: TT - Transient with PCS Initially Available

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of a reactor trip signal and insertion of all control rods into core.	None	EOI S023-12-2, Reactor Trip Recovery, step 1.c
Main Steam Relief Available (T)	RCS Heat Removal RCS Pressure RCS Inventory	3 of 9 main steam safety valves, 1 of 4 turbine bypass per steam generator open to relieve secondary system pressure.	Operator throttles ADVs (required) or backs up turbine bypass valve operation.	Plant MAAP Specific Analysis S023-12-1, Standard Post Trip Actions, step 8.c and S023-12-2, Reactor Trip Recovery, step 6.a
Pressurizer Safety Valves Reclose (TT) (YTT)	RCS Inventory	2 of 2 pressurizer safety valves reclose following spurious opening.	None	N/A
HPSI in Cold Leg Injection Mode (HI)	Reactivity Control RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject borated water from the RWST to 2 of 4 cold legs.	None	S023-12-3, Loss of Coolant Accident
Containment Spray in RCS Injection Mode (NI)	Reactivity Control RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 2 Containment Spray pumps inject borated water from the RWST to 2 of 4 cold legs.	Depressurize RCS and align containment spray for RCS injection.	S023-12-3, Loss of Coolant Accident
MFW Available to 1 of 2 Steam Generators (F)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 2 MFW pumps delivers flow to 1 of 2 steam generators.	Control feedwater flow to SGs.	S023-12-2, Reactor Trip Recovery, Attachment 1, step 6.a
AFW Available to 1 of 2 Steam Generators (L)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 3 AFW pumps delivers flow to 1 of 2 steam generators.	Manually actuate EFAS if not automatically initiated.	S023-12-2, Reactor Trip Recovery, Step 8.a

TABLE 3.1-7: TT EVENT TREE SUCCESS CRITERIA (continued)

INITIATING EVENT GROUP: TT - Transient with PCS Initially Available

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Emergency Condensate with S/G Depressurized (F2)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 4 condensate pumps delivers flow to 1 of 2 depressurized (<500 psia) steam generators.	Manually align low pressure alternate feedwater.	S023-12-9, Functional Recovery, Attachment 8, Step 6
Oper Depress RCS and Controls ECCS Flow (TIL)	RCS Pressure RCS Inventory	Operator initiates cooldown and limits/ terminates ECCS per procedures to prevent need for recirculation from containment sump.	Cooldown RCS with MFW/AFW and shut off ECCS pumps as required.	S023-12-3, Loss of Coolant Accident
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS realignment	S023-12-3, Loss of Coolant Accident, Attachment 5
Containment Spray in RCS Recirc Mode (NR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 2 containment spray pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS realignment	S023-12-3, Loss of Coolant Accident, Attachment 5
Containment Heat Loads Reduced (NT)	Containment Pressure	1 of 4 containment emergency fan coolers or 1 of 2 containment spray pumps taking suction from RWST	None	Plant Specific MAAP Analysis For CEFCs/CS Heat Removal

The **Emergency Condensate with S/G Depressurized (F2)** node represents use of the emergency condensate system as a backup to MFW and AFW. The non-safety related condensate pumps can be used to provide low head feedwater if offsite power is available and the ADVs are available to reduce steam generator pressure. The **Oper Depress RCS And Controls ECCS Flow (TIL)** node evaluates the likelihood of operator response following a stuck open pressurizer safety valve in controlling RCS temperature and ECCS flow to prevent the need to switchover from the RWST to the containment recirculation sump for ECCS makeup. The **HPSI In Cold Leg Recirc Mode (HR)** and **Containment Spray In RCS Recirc Mode (NR)** nodes evaluate the RCS makeup capability in the event recirculation switchover is required. The **Containment Heat Loads Reduced (NT)** node evaluates the management of containment heat through the use of containment heat removal systems (Containment Emergency Fan Coolers and Containment Spray).

FAILURE SEQUENCES

Sequence #4 represents successful reactor trip in order to achieve subcriticality, but failure to provide secondary heat removal via the AFW, MFW, or emergency condensate systems. The functional accident sequence is defined as IA, an accident sequence involving loss of adequate heat removal in the injection phase.

Sequences #7 and #11 represent successful automatic reactor trip and secondary heat removal with the MFW (sequence #7) or AFW (sequence #11) systems. However, a stuck open pressurizer safety valve requires RCS makeup from the HPSI system. Failure of the operator to successfully cooldown and reduce ECCS flow results in a containment pressure challenge which is not met in these sequences. Sequence #11 is defined as functional accident sequence class IIB, accident sequences involving an induced LOCA with failure of ECCS in the recirculation phase. Sequence #7 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequences #8 and #12 are similar to sequences #7 and #11 except long term ECCS flow is lost when HPSI fails in the recirculation phase. Consequently, sequence #12 is defined as functional accident sequence class IIB, accident sequences involving an induced LOCA with failure of ECCS in the recirculation phase. Sequence #8 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequences #13 and #18 are similar to sequence #4 except a stuck open pressurizer safety valve is also present with RCS makeup available from HPSI (Sequence #13) or CS (Sequence #18). The presence of the stuck open safety valve does not impact the functional reason for core damage (i.e., inadequate secondary heat removal). Consequently, the sequence was also defined as

functional sequence class IA, accident sequences involving loss of adequate heat removal in the injection phase.

Sequences #15 and #17 represent success of injection early by depressurizing the RCS and aligning containment spray for RCS injection following the occurrence of a stuck open pressurizer safety and failure of HPSI. RCS makeup is lost late following failure of containment spray injection during recirculation. Sequence #17 is defined as functional accident class IIB, accident sequences involving an induced LOCA with failure of ECCS in the recirculation phase. Sequence #15 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequence #19 represents successful automatic reactor trip with a stuck open pressurizer safety valve and inadequate RCS makeup from the HPSI and Containment Spray systems in the injection mode. This sequence is defined as functional accident sequence class IIA, an accident sequence involving an induced LOCA with failure of ECCS in the injection phase.

Sequence #20 represents successful automatic reactor trip and feedwater flow via the AFW or MFW systems, but failure to provide secondary steam relief. Consequently, adequate RCS heat removal cannot be achieved. The functional sequence is defined as IA, an accident sequence involving loss of adequate heat removal in the injection phase for this case. Sequence #20 is unanalyzed due to the negligible likelihood of main steam relief failure.

Sequence #21 involves an unsuccessful reactor trip leading to an ATWS condition. The plant and operator response to this event is evaluated in the ATWS event tree (Section 3.1.2.4.3).

3.1.2.4.2 Loss of Power Conversion System (PCS)

Initiating Group Summary

The Loss of PCS initiating event group includes transients which disable the MFW or Condensate systems. Initiators such as loss of condenser vacuum, loss of condensate pumps, or loss of steam bypass to the condenser are considered within the scope of the Loss of PCS initiating event group. Initial conditions for this accident scenario include availability of offsite power in response to the plant challenge and unavailability of MFW and Condensate systems.

Plant Response to Initiating Event

The Loss of PCS scenario assumes an instantaneous stop of feedwater flow to both steam generators. The Plant Protection System (PPS) provides protection against the loss of the secondary heat sink by the steam generator low water level reactor trip and the automatic initiation of the AFW system. The

high pressurizer pressure reactor trip provides protection in the event the RCS pressure limit is approached. The maximum RCS pressure anticipated during the Loss of PCS scenario is based on the most conservative Loss of PCS event, the loss of condenser vacuum. FSAR Table 15.2-1 and Figure 15.2-3 indicate the RCS will reach a pressure which is above the pressurizer safety valve setpoint. Due to the conservatism in the FSAR analysis assumptions, there is some probability the pressurizer safety valve setpoint will not be reached for most Loss of PCS events.

Following the automatic reactor trip, plant response is similar to the Transient With PCS Initially Available event. Secondary heat removal is provided immediately by the turbine bypass valves. Should the turbine bypass system be rendered unavailable, the main steam safety valves will relieve secondary system pressure and provide secondary heat removal.

Continued secondary heat removal is achieved by the AFW system which is automatically actuated on low steam generator level. EOI SO23-12-6, "Loss of Feedwater" directs the operator to initiate AFW manually if it is not automatically actuated. It is assumed the RCP seals will remain intact throughout the duration of the transient. Without loss of RCS integrity due to RCP seal failure, the plant can achieve stable hot standby and subsequent safe shutdown conditions.

Should the AFW system be rendered unavailable for secondary heat removal, the operators will attempt to recover the PCS. Although the initiator implies failure and non-recovery of the PCS, procedural actions to recover the PCS are assumed to continue throughout the event. Per EOI SO23-12-9, "Functional Recovery," the operators will continue attempts to provide feedwater flow to the steam generators via the MFW and Condensate systems. A node is included in the Loss of PCS event tree to account for the possibility that the power conversion system is recovered. This node represents the recovery of MFW or use of the Condensate system in conjunction with steam generator depressurization.

Should the pressurizer safety valves open in response to elevated pressure in the RCS, there is some probability the valves will fail to reseal. In this event, the plant will respond in a manner assumed equivalent to a small LOCA. RCS inventory control is initially lost since the break flow rate exceeds the available charging pump capacity. Primary system pressure decreases with the inventory loss through the break. When pressurizer pressure decreases below the SIAS setpoint or if containment pressure reaches the high containment pressure setpoint, a SIAS will be initiated automatically. It is expected that the primary system pressure will exceed the injection head capability of the LPSI pumps or the pressure at which the Safety Injection Tank discharges. The HPSI pumps automatically start with the SIAS and

repressurize the RCS through the cold legs with borated water from the RWST.

For the pressurizer safety valve(s) induced small LOCA, decay heat removal is achieved through the steam generators. It is assumed sufficient decay heat removal cannot be achieved through the stuck open safety valve. As primary system pressure decreases, the rate of inventory loss decreases and the rate of HPSI injection increases. It is conservatively assumed the reduced RWST inventory causes a demand for recirculation prior to the time shutdown cooling conditions are achieved. The decreasing RWST inventory throughout the event should correspond to an increasing containment sump level.

As inventory is lost through the induced break, the containment atmosphere absorbs heat from the RCS resulting in elevated temperatures and pressures. If containment pressure reaches the high containment pressure setpoint, a containment cooling actuation signal (CCAS) automatically starts the emergency fan coolers. If the containment pressure reaches the high-high pressure setpoint, a containment spray actuation signal (CSAS) starts the containment spray pumps which initially take suction from the RWST. Actuation of the containment spray system increases the inventory demands on the RWST and expedites depletion of the tank. When the RWST level reaches the low level setpoint, a Recirculation Actuation Signal (RAS) is automatically initiated. The operator manually closes the RWST isolation valves after sufficient suction from the sump to the HPSI and containment spray pumps is confirmed.

Event Tree Assumptions

The following assumptions were used in event tree construction of the plant response to a Loss of PCS event:

Assumption	Basis
The maximum RCS pressure anticipated during a Loss of PCS event is 2160 psia. The pressurizer safety valves are not required for RCS pressure relief, but may open due to the uncertainty associated with the high pressure transient and safety valve calibration. A conservative estimate of 0.1 is used for the probability of a safety valve will open.	Conservative relative to NUREG/CR-3511, Calvert Cliffs IREP FSAR Table 15.2-6
Although not required for RCS pressure relief, there is some probability the PZR safety valves lift during the loss of PCS event. A node is included to account for the possibility that the safety valves <u>do not reseal</u> subsequent to lifting.	Consistent with NUREG/CR-3511 Conservatism

Assumption	Basis
RCS Inventory demand following an induced LOCA (stuck open SRV) results in a RAS before shutdown cooling can be established.	Conservatism

Event Tree Model

The event tree model for the Loss of the PCS is depicted in Figure 3.1-4. The safety function and success criteria for each constituent node of the event tree is presented in Table 3.1-8.

The **Loss of PCS Initiator (PCS)** node represents the occurrence of the loss of power conversion system event. The second node **Automatic Reactor Trip (K)** addresses the requirement for a reactor trip to achieve subcriticality following the loss of power conversion systems. This node addresses only the automatic reactor trip functions. Manual reactor trip is addressed in the Anticipated Transient Without Scram (TWS) Event Tree. The **Main Steam Relief (T)** node represents removal of secondary system steam through the turbine bypass valves, atmospheric dump valves or main steam safety valves.

The **Pressurizer Safety Valves Reclose (YRC)** node represents the possibility that the safety valves open in response to the RCS pressure increase immediately following the Loss of PCS transient and successfully reseal. Each of the safety valves that open is required to close after the RCS pressure has decreased to the valve closure setpoint. Failure of any valve to reclose results in a coolant loss condition assumed equivalent to a small break LOCA. The **HPSI In Cold Leg Injection Mode (HI)** and **Containment Spray In RCS Injection Mode (NI)** nodes evaluate the RCS makeup systems required to respond in the event of a stuck open pressurizer safety valve.

The **APW Available to 1 of 2 Steam Generators (L)** node represents operation of the APW system in order to provide feedwater to the steam generators for secondary heat removal.

The **Recovery of Main Feedwater (FR)** node represents recovery of Main Feedwater system in order to provide secondary heat removal. The success of this node can be achieved through recovery of one MPW train with one condensate train. The **Recovery of Condensate With S/G Depressure (F2R)** node represents recovery of Condensate system. However, in order for the Condensate system alone to provide adequate secondary heat removal, a steam generator must be depressurized. The success of this node can be achieved through recovery of one condensate train in conjunction with

TABLE 3.1-8: PCS EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: PCS - Loss of Power Conversion System

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of a reactor trip signal and insertion of all control rods into core.	None	S023-12-1, Standard Post Trip Actions, step 3.a
Main Steam Relief Available (T)	RCS Heat Removal RCS Inventory RCS Pressure	1 of 3 main steam safety valves, 1 of 4 turbine bypass, or 1 of 2 ADVs per steam generator open to relieve secondary system pressure.	Operator throttles ADVs (required) or backs up turbine bypass valve operation.	Plant Specific MAAP Analysis
Pressurizer Safety Valves Reclose (TT) (YRC)	RCS Inventory	2 of 2 pressurizer safety valves reclose following events requiring opening.	None	N/A
HPSI in Cold Leg Injection Mode (HI)	Reactivity Control RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject borated water from the RWST to 2 of 4 cold legs.	None	S023-12-3, Loss of Coolant Accident
Containment Spray in RCS Injection Mode (NI)	Reactivity Control RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 2 Containment Spray pumps inject borated water from the RWST to 2 of 4 cold legs.	Depressurize RCS, align containment spray for RCS injection.	S023-12-3, Loss of Coolant Accident
AFW Available to 1 of 2 Steam Generators (LI)	RCS Heat Removal RCS Inventory RCS Pressure	1 of 3 AFW pumps deliver flow to 1 of 2 steam generators.	Manually actuate EFA's, throttle AFW pump, if not auto initiated.	S023-12-6, Loss of Feedwater, step 2.6
Recovery of Main Feedwater (FR)	RCS Heat Removal	1 train MFW and 1 train condensate available to provide feedwater to steam generator	Manual alignment to recover initial fault.	S023-12-9, Functional Recovery, Attachment 8
Recovery of Condensate With S/G Depressure (FZR)	RCS Heat Removal	1 steam generator depressurized and one train condensate available and manually aligned to provide feedwater.	Manual alignment of condensate to steam generator.	S023-12-9, Functional Recovery, Attachment 8
Oper Depress RCS and Controls ECCS Flow (TIL)	RCS Pressure RCS Inventory	Operator initiates cooldown and limits/ terminates ECCS per procedures to prevent need for recirculation from containment sump.	Cooldown RCS with MFW/AFW and shut off ECCS pumps as required.	S023-12-3, Loss of Coolant Accident

TABLE 3.1-8: PCS EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: PCS - Loss of Power Conversion System

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS realignment	SD23-12-3, Loss of Coolant Accident, Attachment 5
Containment Spray in RCS Recirc Mode (NR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 2 containment spray pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS realignment	SD23-12-3, Loss of Coolant Accident, Attachment 5
Containment Heat Loads Reduced (NT)	Containment Pressure	1 of 4 containment emergency fan coolers or 1 of 2 containment spray pumps taking suction from RWST	None	Plant Specific MAAP Analysis For CEFCs/CS Heat Removal

depressurization of a steam generator to allow low head condensate flow.

The Oper Depress RCS And Controls ECCS Flow (TIL) node evaluates the likelihood of proper operator response following a stuck open pressurizer safety valve in controlling RCS temperature and ECCS flow to prevent the need to switchover from the RWST to the containment recirculation sump for ECCS makeup. The HPSI In Cold Leg Recirc Mode (HR) and Containment Spray In RCS Recirc Mode (NR) nodes evaluate the RCS makeup capability in the event recirculation switchover is required. However, the use of containment spray in recirculation has been conservatively omitted as a success path in the current PRA model and is assumed to fail. The Containment Heat Loads Reduced (NT) node evaluates the management of containment heat through the use of containment heat removal systems (Containment Emergency Fan Coolers and Containment Spray).

FAILURE SEQUENCES

Sequence #4 represents failure to establish a secondary heat sink by using the AFW system or recovering some portion of the power conversion system. The absence of secondary heat removal results in inadequate RCS heat removal. The functional accident sequence is defined as IA, an accident sequence involving loss of adequate heat removal in the injection phase.

Sequences #7 and 11 represent successful automatic reactor trip and secondary heat removal with the MFW (sequence #11) or AFW (sequence #7) systems. However, a stuck open pressurizer safety valve requires RCS makeup from the HPSI system. Failure of the operator to successfully cooldown and reduce ECCS flow results in a containment pressure challenge which is not met in these sequences. Sequence #7 is defined as functional accident sequence class IIB, accident sequences involving an induced LOCA with failure of ECCS in the recirculation phase. Sequence #11 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequences #8 and #12 are similar to sequences #7 and #11 except long term ECCS flow is lost when HPSI fails in the recirculation phase. Consequently, sequence #8 is defined as functional accident sequence class IIB, accident sequences involving an induced LOCA with failure of ECCS in the recirculation phase. Sequence #12 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequences #13 and #18 are similar to sequence #4 except a stuck open pressurizer safety valve is also present with successful RCS makeup (Sequence #13) or unavailable (Sequence #18). The presence of the stuck open safety valve does not impact the functional reason for core damage (i.e., inadequate secondary

heat removal). Consequently, these sequences were also defined as functional sequence class IA, accident sequences involving loss of adequate heat removal in the injection phase.

Sequences #15 and #17 represent success of injection early by depressurizing the RCS and aligning containment spray for RCS injection following the occurrence of a stuck open pressurizer safety and failure of HPSI. RCS makeup is lost late following failure of containment spray injection during recirculation. Sequence #15 is defined as functional accident class IIB, accident sequences involving an induced LOCA with failure of ECCS in the recirculation phase. Sequence #17 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequence #19 represents successful automatic reactor trip with a stuck open pressurizer safety valve and inadequate RCS makeup from the HPSI and Containment Spray systems in the injection mode. This sequence is defined as functional accident sequence class IIA, an accident sequence involving an induced LOCA with failure of ECCS in the injection phase.

Sequence #20 represents successful automatic reactor trip and feedwater flow via the AFW or MFW systems, but failure to provide secondary steam relief. Consequently, adequate RCS heat removal cannot be achieved. This sequence is unanalyzed due to the negligible likelihood of main steam relief failure.

Sequence #21 represents failure of the RPS to initiate an automatic reactor trip. This sequence transfers to the Anticipated Transient without Scram (TWS) event tree.

3.1.2.4.3 Anticipated Transient Without Scram (ATWS)

Initiating Group Summary

The Anticipated Transient Without Scram (TWS) initiating event group consists of transfer sequences characterized by the failure of the reactor protection system to automatically trip the reactor. The title "initiating event" for the TWS event is somewhat of a misnomer since the entry condition into the TWS event tree is a transient initiating event and failure of the reactor protection system as defined in other event trees. The common attribute of failing to automatically trip the reactor forms the basis for the TWS initiating event grouping. This basis is somewhat different than the traditional TWS basis which is failure of automatic and manual attempts to shutdown the reactor during the initial event time period. Transient events transferring into the TWS event tree include Transient with PCS Available, Loss of PCS, Loss of Offsite Power, Steam Generator Tube Rupture, Main Steamline Break, Medium LOCA, Small-Small LOCA, and Small LOCA.

Plant Response to Initiating Event

Following the failed automatic reactor trip in the transient event, immediate action is taken by the operator to achieve a subcritical state in the reactor. Initially, EOI SO23-12-1, "Standard Post-Trip Actions," directs the operator to manually trip the reactor in order to insert the Control Element Assemblies (CEAs) into the reactor core. If more than one CEA is not inserted, the operator is then directed to trip Load Center B-15 and B-16 supply breakers, open all reactor trip circuit breakers locally, open all motor/generator (M/G) set input and output breakers locally and initiate emergency boration. These actions should override electrical faults in the RPS and insert the CEAs into the core.

Failure of a significant number of control rods to insert continues the process of fission heat production occurring faster than the rate heat can be removed by the secondary system. The degree of the pressure and temperature excursion is a function of the power level prior to the transient, the amount of heat removal available to the primary system, and the negative reactivity created by the Moderator Temperature Coefficient (MTC). The initiation of the TWS event at a high power level provides less margin for pressure increase than that available if the event is initiated at low power.

The MTC is a measure of the amount of reactivity decrease (or increase) based on the relationship between the reactivity and temperature. A negative MTC indicates a reduction in power generation which occurs with increased temperature due to the reduction in the thermal cross section of the fuel for neutron interactions. This negative reactivity feedback feature of the reactor neutron interactions provides a self-correcting mechanism during the RCS temperature excursion.

The MTC value changes during the life of the core. Early in core life MTC is a small negative value or a slightly positive value. This value decreases during the core life. A less severe transient is experienced with a more negative MTC (near the end of core life). There is a critical value of MTC above which there is insufficient negative reactivity to prevent pressure in the primary system from exceeding the yield point of the reactor pressure boundary if the transient occurs at high power. The failure to trip results in core damage under these circumstances. There is also a critical MTC value below which no pressure challenge occurs based on the margin provided by the inherent negative feedback mechanism.

In order to prevent reactor power increases following the initial time period of the transient, RCS temperature is maintained constant, if possible, until reactivity control is regained. Temperature is not reduced in the RCS to prevent reactor power

increases due to the negative MTC. As part of the standard post trip actions, EOI S023-12-1 directs the operator to trip the turbine to avoid excessive cooling of the primary system (introducing positive reactivity). If the turbine trip fails, the operator is directed to close the MSIVs.

As the steam generator inventory decreases, heat transfer to the primary system decreases, increasing the primary system temperature. Even if the steam generators remain full of feedwater, the pressurizer safety valves must open to relieve primary system pressure. This is due to the large mismatch between reactor power (>110%) and steam generator heat removal capability (110%). The AFW system actuates on a low steam generator level signal and the operators are directed to manually start AFW if not initiated automatically.

After attempting to manually trip the reactor and open all of the reactor trip breakers, EOI S023-12-9, "Functional Recovery", directs the operators to begin emergency boration. The operator verifies at least one charging pump and boric acid makeup (BAMU) pump is available for boration. The operator is instructed to align the charging pump suction to the BAMU tanks via the BAMU pumps or the gravity feed lines.

If the BAMU tanks are not available, the operator aligns the charging pump suction to the RWST. The operator is directed to maintain a boron addition rate of 40 gpm (1 charging pump) and continue emergency boration until the Technical Specification shutdown margin is achieved.

Event Tree Assumptions

The following assumptions were used in event tree construction of the plant response to an ATWS event:

Assumptions	Bases
Reactor trip with insertion of all CEAs during an ATWS event is equivalent to success. Successful manual trip of the reactor eliminates the challenge to the Reactivity Control critical safety function. Subsequent mitigation of the sequence progression would be the same as modeled in the event tree transferring into the ATWS event tree. Consequently, the cutsets produced from detailed modeling of the accident progression in the ATWS event tree would include failure of the reactor to trip and successful manual recovery in addition to the cutset solution from the transfer-in event tree. These cutsets would be insignificant relative to the cutsets from the transfer-in event tree.	Consistent with NUREG/CR-4550.

Assumptions	Bases
The Moderator Temperature Coefficient is negative for 95% of the fuel cycle such that RCS pressure under high power conditions does not lead to vessel failure. Consequently, the likelihood of Low or Medium MTC conditions existing at the time of the ATWS event occurrence is .05.	Plant Specific RETRAN Analysis
High power is defined as greater than 20% core power	Consistent with Surry and Sequoyah in NUREG/CR-4550.
Failure to trip the turbine in 1 minute is more likely to occur due to the operator failing to act rather than any hardware failure. Therefore, the KTT node of the event tree is treated as a point estimate.	Consistent with Surry and Sequoyah in NUREG/CR-4550.
Turbine trip is not required for low power operating conditions	Adequate time is available for local operation and adequate margin exists to prevent overpressure conditions in the primary system. Consistent with Sequoyah and Surry in NUREG/CR-4550.
Main Feedwater is not available for secondary heat removal	Conservative assumption. Consistent with Sequoyah and Surry in NUREG/CR-4550.

Event Tree Model

The event tree model for Anticipated Transient Without Scram is depicted in Figure 3.1-5. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-9.

The **Anticipated Transient Without Scram Initiator (TWS)** represents the entry condition into the event tree model which consists of transient conditions with failure of the reactor to scram automatically. The second node **Manual Reactor Trip Successful (KMO)** characterizes the immediate actions by the operator to trip the reactor from the control room, open the reactor trip breakers and de-energize the CEAs. The **Power Level Greater than 20% (Z1)** is modeled following the KMO node to distinguish between the success criteria requirements for high and low power operations. A second plant condition of concern is represented at the fourth node **Low/Med MTC Conditions Exist (EOL) (Z2)**. MTC conditions are evaluated at this node since recovery from the pressure transient is not possible from high power operations with high MTC conditions. The downward path on the

Figure 3.1-5: Anticipated Transient Without Scram (TWS) Event Tree

ANTICIPATED TRANSIENT WITHOUT SCRAM EVENT TREE (TWS)

SAN ONOFRE IPE - UNITS 2 & 3

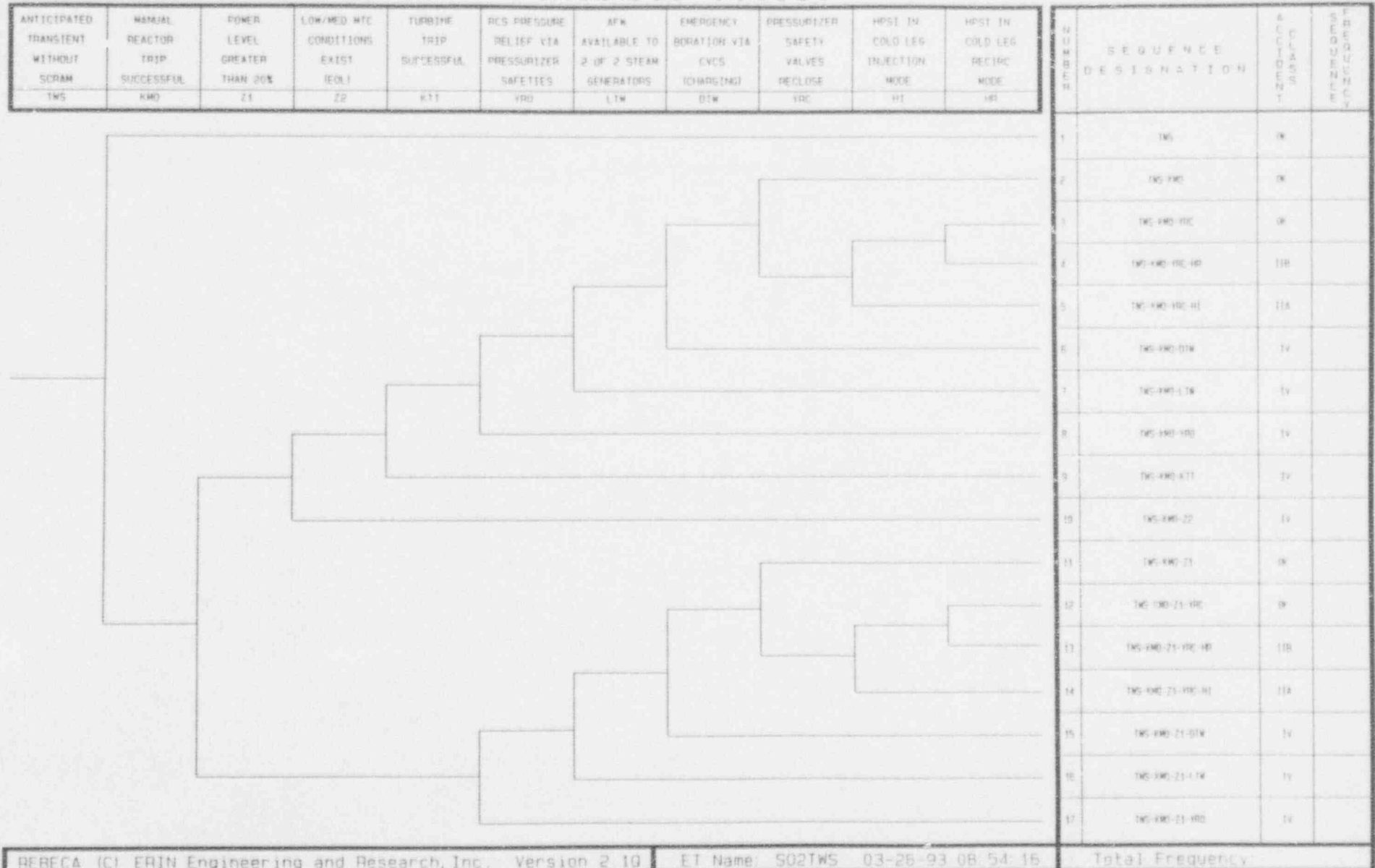


TABLE 3.1-9: TWS EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: TWS - Anticipated Transient Without Scram

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Manual Reactor Trip Successful (KMO)	Reactivity Control	Operator inserts all control rods with sufficient negative reactivity to shutdown the core	Manually trip the reactor or de-energize the CEDM from the control room or locally de-energize the CEDM	SO23-12-9, Functional Recovery, step 1.b
Power Level Greater Than 20% (Z1)	Reactivity Control	Power level prior to initiating event is less than 20%	None	NUREG/CR-4550, Vol. 3, 5 (Surry, Sequoyah)
Low/Med MTC Conditions Exist (Z2)	Reactivity Control	MTC condition following 5% of operating cycle.	None	Plant specific RETRAN analysis
Turbine Trip Successful (KTT)	Reactivity Control	Manual trip of the turbine is completed within 1 minute of initiating event	Manually trip the turbine	EOI SO23-12-1, Standard Post Trip Actions, step 4.a, NUREG/CR-4550, Vol. 3,5 (Surry, Sequoyah)
RCS Pressure Relief Via Pressurizer Safeties (YRO)	Core Heat Removal	2 of 2 pressurizer relief valves open to relieve RCS pressure	None	Plant specific RETRAN analysis
AFW Available to 2 of 2 Steam Generators (LTW)	RCS Heat Removal	1 of 3 AFW pumps supply water from the CST to 2 of 2 steam generators	Operator manually initiates AFW, if required	EOI SO23-12-1, Standard Post Trip Actions, step 8, NUREG/CR-4550, Vol 3,5 (Surry, Sequoyah)
Emergency Boration Via CVCS (Charging) (DTW)	Reactivity Control RCS Inventory	1 of 3 charging pumps taking suction from BAMU system or RWST deliver borated water to RCS	Operator manually aligns charging pumps for emergency boration	EOI SO23-12-9, Functional Recovery, Attachment 4, step 1, NUREG/CR 4550, Vol 3,5 (Surry, Sequoyah)

TABLE 3.1-9: TWS EVENT TREE SUCCESS CRITERIA (continued)

INITIATING EVENT GROUP: TWS - Anticipated Transient Without Scram

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Pressurizer Safety Valves Reclose (YRC)	RCS Inventory RCS Pressure Containment	2 of 2 open pressurizer relief valves reclose	None	NUREG/CR-4550, Vol 3,5 (Surry, Sequoyah)
HPSI in Cold Leg Injection Mode (HI)	Reactivity Control RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject borated water from the RWST to 2 of 4 cold legs.	None	Plant specific MAAP analysis for induced LOCA
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after recirc alignment.	S023-12-3, Loss of Coolant Accident, Attachment 5

event tree represents the more favorable low MTC condition. The **Turbine Trip Successful (KTT)** node addresses the need to eliminate sources of positive reactivity caused by excessive primary system cooling from the secondary system. The **MTC Conditions (Z2)** and **Turbine Trip (KTT)** nodes are not evaluated for the low power operating condition path since excessive RCS pressure challenges are not encountered due to the margin available for pressure relief and reactivity control.

RCS pressure relief through the pressurizer safety valves and secondary heat removal using AFW are required for both high and low power initial conditions as depicted by the descriptions **RCS Pressure Relief Via Pressurizer Safeties** and **AFW Available to 2 of 2 Steam Generators** in nodes YRO and LTW, respectively. AFW is required to remove secondary heat to lower the RCS temperature. The temperature decrease shrinks the RCS, enabling the CVCS to inject borated water into the RCS in order to reach subcriticality.

Negative reactivity insertion and coolant makeup for inventory losses through the primary system pressure relief valves are provided by the CVCS Charging pump injecting borated water as represented in the node **Emergency Boration Via CVCS (Charging) (DTW)** node. Primary system makeup and reactivity control from the injection of borated water restore reactivity control and RCS inventory. Successful closure of the pressurizer safety valves following restoration of reactivity control ensures primary system integrity. This integrity issue is addressed in node YRC, **Pressurizer Safety Valves Reclose**.

Failure of the valves to reclose continues the breach of primary system integrity requiring recirculation similar to a Small LOCA condition. The **HPSI in Cold Leg Injection Mode (HI)** represents the high pressure injection requirement. The **HPSI in Cold Leg Recirc Mode (HR)** node models the requirement to establish high pressure recirculation if the primary system is not depressurized before the level in the RWST requires transfer to recirculation operations.

FAILURE SEQUENCES

Sequences #4, #5, #13, and #14 represent cases when the pressurizer safety valves fail to reseal, resulting in an induced Small LOCA. Sequences #5 and #14 represent failure of the high pressure safety injection system. Without makeup, the primary system inventory depletes resulting in core uncover. Since the core damage is induced after the ATWS has been successfully mitigated, functional accident sequences #5 and #14 are defined as IIA, accident sequences initiated by induced LOCAs with loss of primary coolant makeup or loss of adequate heat removal in the injection phase.

Sequences #4 and #13 represent failures resulting from failures of high pressure injection during recirculation following an induced Small LOCA. RCS heat removal and inventory are lost resulting in core uncover. Here again, the ATWS is not the reason for core damage, and the functional accident sequences are defined as IIB, accident sequences initiated by induced LOCAs with loss of primary coolant makeup or loss of adequate heat removal in the recirculation phase.

Sequences #6 and #15 represent failures to provide emergency boration via the CVCS charging pumps. In the case of sequence #6, failure to inject borated water results in the inability to render the core subcritical due to the initial high power conditions. The low power complement to this event (sequence #15) results in failure to provide sufficient makeup to the RCS following pressure relief resulting in core uncover. In the case of sequence #15, failure of secondary heat removal and inability to reduce RCS pressure results in the inability of the charging pumps to provide sufficient borated RCS makeup. These functional accident sequences are defined as IV, accident sequences involving failure of reactivity control for these cases.

Sequences #7 and #16 represent failures to achieve subcriticality for conditions in which power operations are high following the transient. Subcriticality is not achieved in sequence #7 due to failure of the AFW system in providing primary pressure reduction to allow for emergency boration. These conditions result in early failure and are classified by functional accident sequence IV, accident sequences involving failure of reactivity control.

In sequence #10, an unfavorable MTC causes the reactivity control mechanism in the reactor to fail. These conditions result in early failure and are classified by functional accident sequence IV, accident sequences involving failure of reactivity control.

Sequences #8 and #17 represent failures to provide adequate pressure relief during the power excursion following failure to trip the reactor. The RCS pressure continues to rise, challenging the reactor coolant system boundary integrity. The functional accident sequence is defined as IV, accident sequences involving failure of reactivity control in both cases.

Sequence #9 represents failure to trip the turbine successfully under high power conditions. Continued secondary system steam relief results in uncontrolled cooling of the primary system and introduction of positive reactivity. The functional accident sequence is defined as IV, an accident sequence involving failure of reactivity control in this case.

3.1.2.4.4 Loss of Offsite Power

Initiating Group Summary

The Loss of Offsite Power (LOP) initiating event is a transient event in which AC power is lost from the unit auxiliary and reserve auxiliary transformers. The initiating event considers both loss of offsite power to the station auxiliaries SONGS 2/3 220 kV switchyard and loss of power from the unit auxiliary and reserve auxiliary transformers.

Plant Response to Initiating Event

The LOP from offsite sources scenario begins with a loss of all AC electric power to the plant's 220 kV switchyard. The loss of normal AC power results in the loss of all power to the station auxiliaries and a concurrent turbine generator trip signal. Only the 120 VAC buses supplied by inverters and the DC buses supplying them continue to receive power. This situation could result either from a complete loss of external grid (offsite) or a loss of the on-site AC distribution system. As a result of the loss of non-vital AC power, electric power is interrupted to the CEDMs resulting in a reactor trip. Power is lost to the reactor coolant pumps, condensate pumps, main circulating water pumps, steam bypass control system, and normal pressurizer control systems. Under such circumstances, the plant experiences a simultaneous loss of turbine load, main feedwater flow, and forced reactor coolant flow.

The LOP from the unit and reserve auxiliary transformers scenarios involves switchyard related losses of power. Offsite power is available, however, offsite power to the reserve auxiliary transformer is unavailable. Class Non-1E power fails following fast transfer from the unit auxiliary transformer to the de-energized reserve auxiliary transformer. The Class 1E power supply transfers to the opposite unit supplied by offsite power. Failure of the Class 1E supply to transfer to the opposite unit presents conditions similar to the loss of offsite power from offsite sources scenario.

At time zero, when all normal AC power to the plant is lost, the turbine stop valves and control valves close. The steam generator feedwater flow to both steam generators stops due to loss of the condensate pumps and consequent trip of the MFW pumps. The reactor coolant pumps coast down and the reactor coolant flow begins to decrease. Even if the turbine fails to trip or if no reactor trip signal is generated upon turbine trip, a low DNBR (RCP speed) reactor trip occurs. In addition, the pressure increases in the RCS and steam generators following the reactor trip are limited by the reduction in reactor power, the pressurizer sprays, and the steam generator safety valves. The pressurizer safety relief valves may open due to setpoint shift

or very high initial RCS pressure. Should the pressurizer safety valves open, there is some possibility the valves may fail to reseal. In this event, the plant responds in a manner equivalent to a small LOCA.

The loss of all normal AC power is followed by an automatic startup signal to the emergency diesel generators (EDGs). The power output of one EDG is sufficient to supply electrical power to all necessary engineered safety features (ESF) systems and to provide the capability of maintaining the plant in a safe shutdown condition. When the buses are energized by the EDGs, ESF loads are sequenced back on their respective buses. With essential power restored by the EDGs, the accident assumes the characteristics similar to a Turbine Trip transient event. Subsequent to the reactor trip, stored and fission product decay energy must be dissipated by the RCS and main steam system. In the absence of forced convective reactor coolant flow, free convective heat transfer reactor coolant flow (natural circulation) is utilized. Initially, the residual water inventory in the steam generators is used as a heat sink and steam is released to atmosphere by the spring-loaded main steam safety valves (MSSVs).

If power is not initially available on the 4.16 kV AC buses, EOI SO23-12-1 directs the operator to EOI SO23-12-7, "Loss of Forced Circulation/Loss of Offsite Power." Following verification of reactor trip/turbine-generator trip, RCS inventory and pressure control, and EFAS actuation, the operator attempts to restore power per EOI SO23-12-7, "Loss of Offsite Power", Attachment 7.

An Emergency Feedwater Actuation Signal (EFAS) is generated on steam generator level. The EFAS signal automatically starts the 2 motor-driven and 1 turbine-driven AFW pumps. The EFAS signal then automatically turns off AFW when approximately 5% of narrow range level in the steam generator is restored. EOI SO23-12-7 directs the operator to override automatic level control and adjust AFW discharge valves to maintain steam generator inventory between 40% and 80% narrow range level.

Should AFW be rendered unavailable, the EOI SO23-12-9 directs the operator to attempt recovery of secondary heat sink. Alignment of MFW is attempted following non-recovery of AFW. Since the condensate pumps and main steam controls for the MFW pumps are non-ESF equipment and are not powered from the EDGs, recovery of MFW is not possible until power is restored.

In the event a pressurizer safety valve sticks open and an induced small LOCA results, RCS inventory control is impaired. When pressurizer pressure decreases below the SIAS pressurizer low pressure setpoint or containment pressure reaches the high containment pressure setpoint, a SIAS is initiated automatically. The primary system pressure exceeds the injection head capability

of the LPSI pumps, and precludes Safety Injection Tank discharge. Therefore, the HPSI pumps are utilized for inventory control. The HPSI pumps are ESF components powered by the operating EDGs. Decay heat removal is achieved through the steam generators in conjunction with limited heat removal through the pressurizer. It is conservatively assumed the RWST inventory depletes prior to the time shutdown cooling conditions are achieved. The decreasing RWST inventory throughout the event should correspond to an increasing containment sump level.

Increased inventory demands on the RWST may occur if the containment spray system actuates due to the containment pressure increase following a stuck open pressurizer safety condition and expedites depletion of the tank. Because the containment spray system is powered by the EDGs, it remains available during the LOP event. When the RWST level reaches the low level setpoint, a RAS is automatically initiated. The operator manually closes the RWST isolation valves after sufficient suction from the sump to the HPSI and containment spray pumps is confirmed.

Event Tree Assumptions

The following assumptions were used in the event tree construction of the plant response to a LOP event:

Assumption	Basis
The maximum RCS pressure anticipated during a LOSP is 2441 psia. The pwr safety valves are not required for RCS pressure relief, but may open due to the uncertainty associated with the high pressure transient and safety valve calibration. A conservative estimate of 0.1 is used for the probability of a safety valve will open.	Conservative with respect to NUREG/CR-3511 FSAR Table 15.2-3
Although not required for RCS pressure relief, there is some probability the pwr safety valves lift during the loss of PCS event. A node is included to account for the possibility that the pwr safety valves do not reseal subsequent to lifting.	Consistent with NUREG/CR-3511 Conservatism
A stuck open safety valve is equivalent to a small break LOCA with respect to RCS inventory makeup requirements.	Conservative. Plant Specific MAAP Analysis
RCS inventory demand following an induced LOCA (stuck open pwr relief valve) results in a RAS before shutdown cooling can be established	Conservatism. Plant Specific MAAP Analysis

Assumption	Basis
Sixty minutes exist for recovery of secondary heat removal following the LOP occurrence.	Plant Specific RETRAN Analysis

Event Tree Model

The event tree model for the LOP transient is depicted in Figure 3.1-6. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-10.

The **Loss of Offsite Power (LOP)** node represents the occurrence of the loss of offsite power event. The second node **Automatic Reactor Trip (K)** represents the requirement for a reactor trip to achieve subcriticality following the loss of secondary heat removal systems. This node addresses only the mechanical faults that could preclude a reactor trip given loss of power to the CEDM. Failure to achieve reactor trip is addressed in the Anticipated Transient Without Scram (TWS) event tree.

The **Emergency AC Power Available (U)** node represents the requirement to recover AC power using the EDGs. Evaluation of plant conditions, without onsite or offsite 4.16 kV AC power available and if power is not recovered from at least one EDG, is performed in the SBO event tree.

The **Main Steam Relief Available (T)** node represents removal of secondary system steam through the turbine bypass valves, atmospheric dump valves or main steam safety valves. Steam relief is required within a minute of the offsite power loss for early secondary heat removal and is required later in conjunction with the AFW system for continued heat removal.

The **Recovery of Offsite Power Within 60 Minutes (U0)** node accounts for the considerable likelihood that offsite power could be restored before steam generator dryout. Recovery of power restores the plant systems to their availability before the initiating event and is assumed to result in such a low probability of unsuccessful mitigation that it is not analyzed.

AFW Available to 1 of 2 Steam Generators (L) node represents operation of the AFW system in order to provide feedwater to the steam generators for secondary heat removal.

The **Pressurizer Safety Valves Open and Reclose (YRO)** node represents the possibility that the safety valves open in response to the RCS pressure increase immediately following the LOP transient and successfully reclose. Each of the safety valves that open is required to close after the RCS pressure has decreased to the valve closure setpoint. Failure of any valve to

Figure 3.1-6: Loss of Offsite Power (LOP) Event Tree

LOSS OF OFFSITE POWER EVENT TREE (LOP)

SAN ONOFRE IPE - UNITS 2 & 3

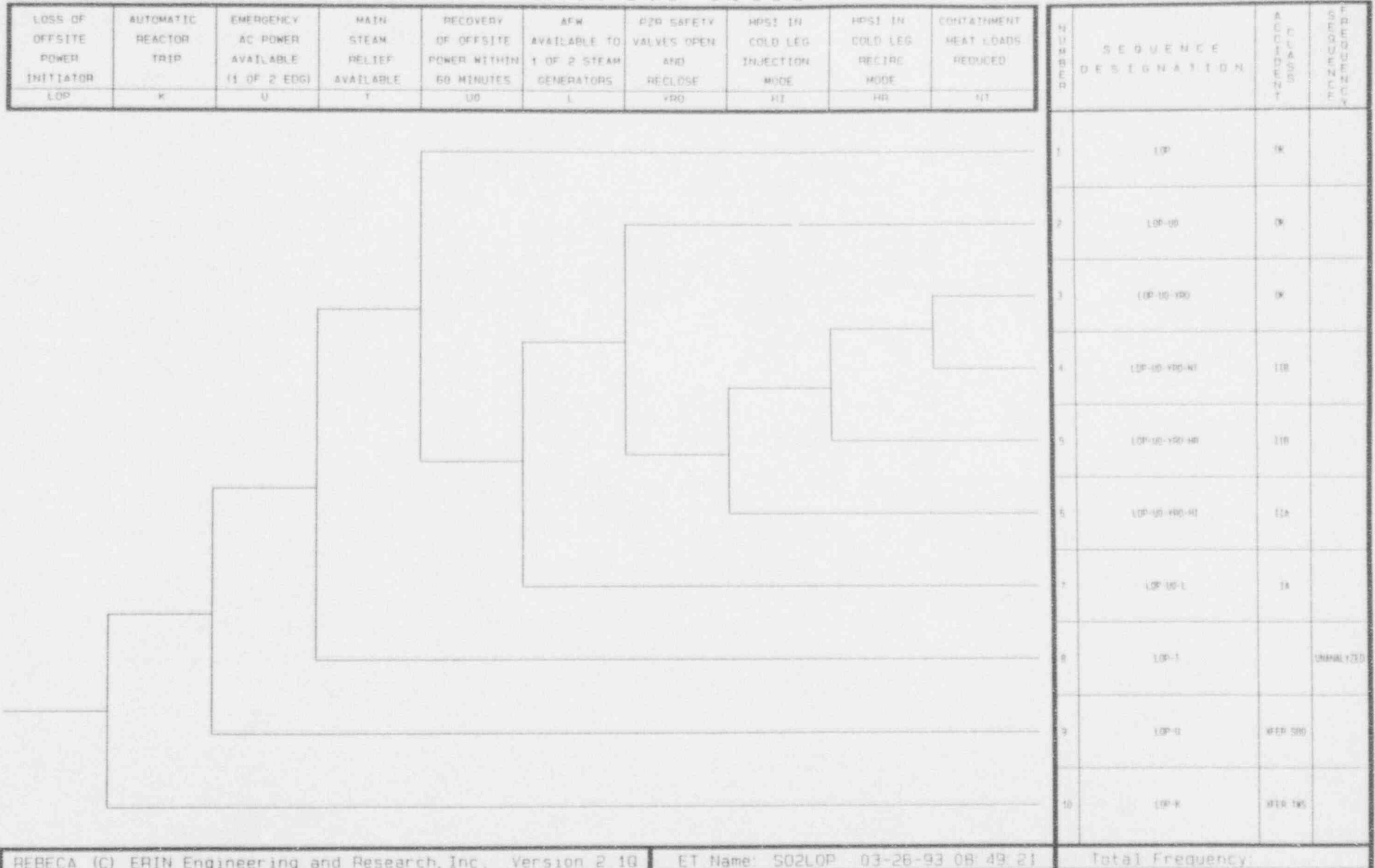


TABLE 3.1-10: LOP EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: LOP - Loss of Offsite Power

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of a reactor trip signal and insertion of rods into core.	None	S023-12-1, Standard Post Trip Actions, step 3.a
Emergency AC Power Available (1 of 2 EDG) (U)	Vital Auxiliaries	1 of 2 onsite emergency diesel generators starts and runs to power ESF loads.	Manual start/load of EDG if required.	S023-12-7, Loss of Offsite Power, step 2.d
Main Steam Relief Available (T)	RCS Heat Removal RCS Inventory RCS Pressure	1 of 9 main steam safety valves, 1 of 4 turbine bypass, or 1 of 2 ADVs per steam generator open to relieve secondary system pressure.	Operator throttles ADVs (required) backs up turbine bypass valves operation.	Plant Specific MAAP Analysis
Recovery of Offsite Power Within 60 Minutes (UO)	Vital Auxiliaries	Offsite power restored to the unit within 60 minutes of loss (e.g., before core uncover).	Restoration of faults and re-alignment of busses.	S023-12-7, Loss of Offsite Power
AFW Available to 1 of 2 Steam Generators (L)	RCS Heat Removal RCS Inventory RCS Pressure	1 of 3 AFW pumps deliver flow to 1 of 2 steam generators.	Manually backup EFAS if required, throttle AFW pumps if not auto initiated.	S023-12-7, Loss of Offsite Power, step 9
Pressurizer Safety Valves Open and Reclose (YRO)	RCS Inventory RCS Pressure	Pressurizer safety valves completely reseal following lift in response to pressure spike.	None	Plant Specific MAAP Analysis Conservatism
HPSI in Cold Leg Injection Mode (HI)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject borated water from the RWST to 2 of 4 cold legs.	None	S023-12-3, Loss of Coolant Accident
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS HPSI realignment.	S023-12-3, Loss of Coolant Accident, Attachment 5

TABLE 3.1-10: LOP EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: LOP - Loss of Offsite Power

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Containment Heat Loads Reduced (NT)	Containment Pressure	1 of 4 containment emergency fan coolers or 1 of 2 containment spray pumps taking suction from RWST	None	Plant Specific MAAP Analysis For CEFCs/CS Heat Removal

reclose results in a coolant loss condition equivalent to a small break LOCA.

The HPSI in Cold Leg Injection Mode (HI), and HPSI in Cold Leg Recirc Mode (HR) nodes represent the system requirements in the event a small LOCA results from a stuck open pressurizer safety valve.

The Containment Heat Loads Reduced (NT) node evaluates the management of containment heat through the use of containment heat removal systems (Containment Emergency Fan Coolers and Containment Spray).

FAILURE SEQUENCES

Sequences #4, #5 and #6 represent cases of an induced small LOCA following the loss of offsite power. Sequence #4 represents the case in which HPSI operates successfully in injection and recirculation following an induced LOCA. Containment cooling systems fail to reduce heat loads to containment leading to failure late in the event. The accident is defined as IIB, accident sequences involving an induced LOCA with failure of ECCS in recirculation.

Sequence #5 represents failure due to inadequate RCS makeup during the recirculation phase. The functional accident sequence is defined as IIB, accident sequences initiated by an induced LOCA with loss of primary coolant makeup or loss of adequate heat removal in the recirculation phase.

Sequence #6 represents failure during the injection phase. The functional accident sequence is defined as IIA, accident sequences initiated by an induced LOCA with loss of primary coolant makeup or loss of adequate heat removal in the injection phase in this case.

Sequence #7 represents successful reactor trip, RCS integrity, main steam relief, and onsite AC power, but failure to establish a long term secondary heat sink by using the AFW system. The absence of secondary heat removal results in inadequate RCS heat removal. The functional accident sequence is defined as IA, accident sequences involving loss of adequate heat removal in the injection phase.

Sequence #8 represents successful reactor trip in order to achieve subcriticality, but failure to provide early secondary system heat relief via main steam relief. Consequently, adequate RCS heat removal cannot be achieved such that RCS pressure and integrity are challenged. Sequence #8 is unanalyzed due to the negligible likelihood of main steam relief failure.

Sequence #9 represents successful reactor trip, but failure of onsite 4.16 kV power from the EDGs and, in the case of switchyard failure initiators, failure to transfer to offsite power from the opposite unit. This sequence transfers to the SBO event tree.

Sequence #10 represents failure of the RPS to initiate an automatic reactor trip. This sequence transfers to the Anticipated Transient without Scram (TWS) event tree.

3.1.2.4.5 Station Blackout

Initiating Group Summary

The SBO initiating event is characterized by failure of both offsite and onsite AC power sources. The loss of AC power results in the loss of all power to the station auxiliaries and a concurrent turbine generator trip signal. Loss of onsite power results from events leading to failure of both EDGs to provide on-site AC power. The initial condition for this initiator includes LOP to the unit, unavailability of power from the opposite unit, loss of onsite power from EDGs and successful reactor trip.

Plant Response to Initiating Event

Immediately following the reactor trip and failure of the diesel generators to supply emergency AC power, the pressurizer level decreases due to shrinkage caused by the cooling from the turbine trip. Once the turbine stop and control valves shut following the reactor trip, steam generator pressure increases rapidly. Pressure continues to increase until the MSSVs open. The MSSVs cycle open and close until the operators take control of steam generator pressure via the ADVs. The MSSVs maintain steam generator pressure at 1100 psia. The secondary safeties must reseal after each opening. Failure to reseal lowers steam generator pressure and jeopardizes the operability of the steam driven AFW pump. The operators can utilize the ADVs since they are powered from vital 125 V DC batteries A and B. Additionally, the ADVs can be manually operated locally.

The steam generator level decreases during the transient. The AFW system is automatically actuated by an EFAS signal on low steam generator level and utilizes the steam-driven AFW feedwater pump. Following automatic actuation, the AFW cycles automatically to maintain steam generator level. The operators normally take manual control of the AFW feed system control valves after conditions have stabilized.

EOI SO23-12-7 directs the operator to EOI SO23-12-8, "Station Blackout," upon failure of the EDGs. After verifying the SBO diagnosis, the operator initiates a MSIS to isolate the secondary systems, and verifies RCS Heat Removal is available. The

operator starts the turbine-driven auxiliary feedwater pump, if the pump is not already running, and overrides and manually controls the AFW system if automatic operation is no longer desired. The operator attempts to energize the Class 1E buses by means which include cross-connecting to the opposite unit. Sources of RCS leakage are ensured isolated to limit inventory losses.

Failure of the onsite AC power source following the LOP event eliminates charging of the Class 1E 125 VDC batteries. These batteries provide the nominal power for essential 125 VDC and 120 VAC controls and indications during the SBO event. To extend the battery life, EOI SO23-12-8, directs the operators to reduce non-essential loads on the Class 1E batteries.

The Condensate Storage Tank (CST) level is monitored closely to insure adequate inventory is available to AFW pumps for injection to the steam generators. An alarm is generated on low CST level. Should the CSTs reach a specified low level, the operator is directed to provide alternate makeup to the CST in accordance with SO23-9-5, "Condensate Storage and Transfer System."

The ability of the turbine-driven AFW pump and associated control valves to maintain adequate steam generator makeup until AC power is recovered is dependent upon the capability of the 125 VDC power system and the 120 V vital AC power system. There are four independent battery buses, each of which powers a 120 V vital AC bus through an inverter. The battery life differs due to the differences in the size and number of loads on each train. Battery life expectancy calculations indicate that the A and B batteries can provide power following a station blackout for at least 90 minutes. The C and D batteries have fewer loads and consequently have a greater lifetime. Batteries C and D can provide power under blackout conditions for at least 8 hours.

Based on plant specific calculations, the battery life assumptions are as follows:

BATTERY	EXPECTED BATTERY LIFE IN SBO	
	W/O LOADSHED	WITH LOADSHED
A (B007)	90 min	4 hours
B (B008)	90 min	4 hours
C (B009)	8 hours	8 hours
D (B010)	8 hours	8 hours

Loadshed must be initiated within 30 minutes of loss of power to charger. This action is the second step of the SBO EOI S023-12-8.

The vital bus inverters can operate only within a certain environmental temperature range and are provided with AC powered room cooling systems to maintain appropriate operating conditions in the inverter rooms. Following a loss of AC power, the inverter rooms begin to heat up due to the presence of heat sources, namely the inverters, in the room. The inverters are designed to operate continuously at room temperatures up to 104°F and for periods up to 4 hours at temperatures between 104° and 122°F. The analysis indicates that if the room temperature exceeds 122°F at any time, the inverters may fail.

Based on plant specific calculations performed for the SONGS 2/3 SBO analysis, the class 1E DC distribution rooms are not expected to exceed 119°F within 4 hours. However, this is based on a worst case initial room temperature of 95°F. A more realistic initial room temperature is 80°F, which would result in the distribution room being at roughly 104°F in 4 hours. This is within the equipment qualification basis for the equipment in the room. The calculated room heatup rate over the 2 to 4 hour period was less than 2°F per hour (roughly 3°F rise in the last 2 hours). In 8 hours the class 1E DC distribution room temperature should not exceed 112°F. Thus, distribution room cooling is not required to ensure inverter performance.

AFW pump room cooling is not required for an SBO event. Calculations performed for the SONGS 2/3 SBO analysis found that the temperature rise in the AFW pump room was low (only 3°F in 4 hours). Therefore, no room cooling requirements were assumed for SBO.

Manual manipulation of the AFW flow control valves is credited for sequences where battery depletion has resulted in loss of control power. The AFW flow valves are readily accessible to the plant operators and would only require minor adjustment since they would already be positioned by the operators to meet the decay heat requirements prior to battery depletion.

Operator action to manually control the turbine-driven AFW pump (P-140) upon loss of control power was omitted from the model since power would be available for the 8 hour SBO coping duration.

The time for restoration of AC power is based on RETRAN analyses performed for the IPE:

CASE	TIME BETWEEN LOP/SBO AND LOSS OF AFW	TIME BETWEEN LOP/SBO AND CORE UNCOVERY
1	90 Minutes	3 Hours
2	3.0 Hours	5 Hours
3	4.0 Hours	6.4 Hours
4	7.5 Hours	11 Hours

Based on operator actions to shed loads and/or take manual control of the turbine-driven AFW pump, the SBO event tree considers four time frames for loss of AFW: immediate, 1.5 hours, 4 hours, and 8 hours. An appropriate time to core uncover is then added to the time at which AFW is lost to determine the maximum available time for AC power recovery. One-half hour is subtracted from the core uncover time to estimate the time available for AC power recovery, as shown in the following table:

CASE DESCRIPTION	EVENT TREE SEQ. NO.	TIME AFW LOST	TIME TO CORE UNCOVERY	TIME AVAILABLE TO RECOVER AC POWER
Immediate Loss (Initial Failure of Turbine-Driven AFW Pump)	16	0	> 1 Hour	1 Hour
A & B Battery Depletion Without Load Shedding (@ 90 min) and Failure To Control AFW Valves Manually	14	1.5 Hours	3 Hours	2.5 Hours
Loss after A & B Battery Depletion With Load Shedding (@ 4 hrs) and Failure To Control AFW Valves Manually	8	4 Hours	6 Hours	5.5 Hours
Loss after C & D Battery Depletion (@ 8 hrs) leading to loss of control power to Pump P-140. (Includes cases where A & B battery depletion was overcome by manual control of AFW flow)	5, 11	8 Hours	~11.5 Hours	11 Hours

Event Tree Assumptions

The following assumptions were used in the event tree construction of the plant response to the SBO event:

Assumptions	Bases
Core uncover occurs at approximately 60 minutes unless feedwater is supplied.	Plant Specific RETRAN Analysis
Adequate inventory is available in the Condensate Storage Tank to supply the steam generators for 8 hours. Makeup to the CST is not required.	Plant Specific MAAP Analysis
The mission time for the turbine-driven AFW pump is conservatively modeled as 24 hours. For the station blackout event, however, the maximum time for which the turbine-driven pump is required is 8 hours at which time the batteries deplete.	Conservatism.

Event Tree Model

The event tree model for the SBO event is depicted in Figure 3.1-7. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-11.

The **Station Blackout Initiator (SBO)** node represents the occurrence of an event in which offsite power is lost, onsite AC power is unavailable and the reactor successfully trips. The Station Blackout event can be successfully mitigated if AC power is recovered within 60 minutes prior to core uncover. The **AC Power Recovered Within 60 Min (U1)** node represents the occurrence of this event.

Decay heat removal is accomplished by using the turbine-driven Auxiliary Feedwater pump and the atmospheric dump valves. The node **Turbine Driven AFW Pump Train Operates (LTD)** addresses the availability of these systems.

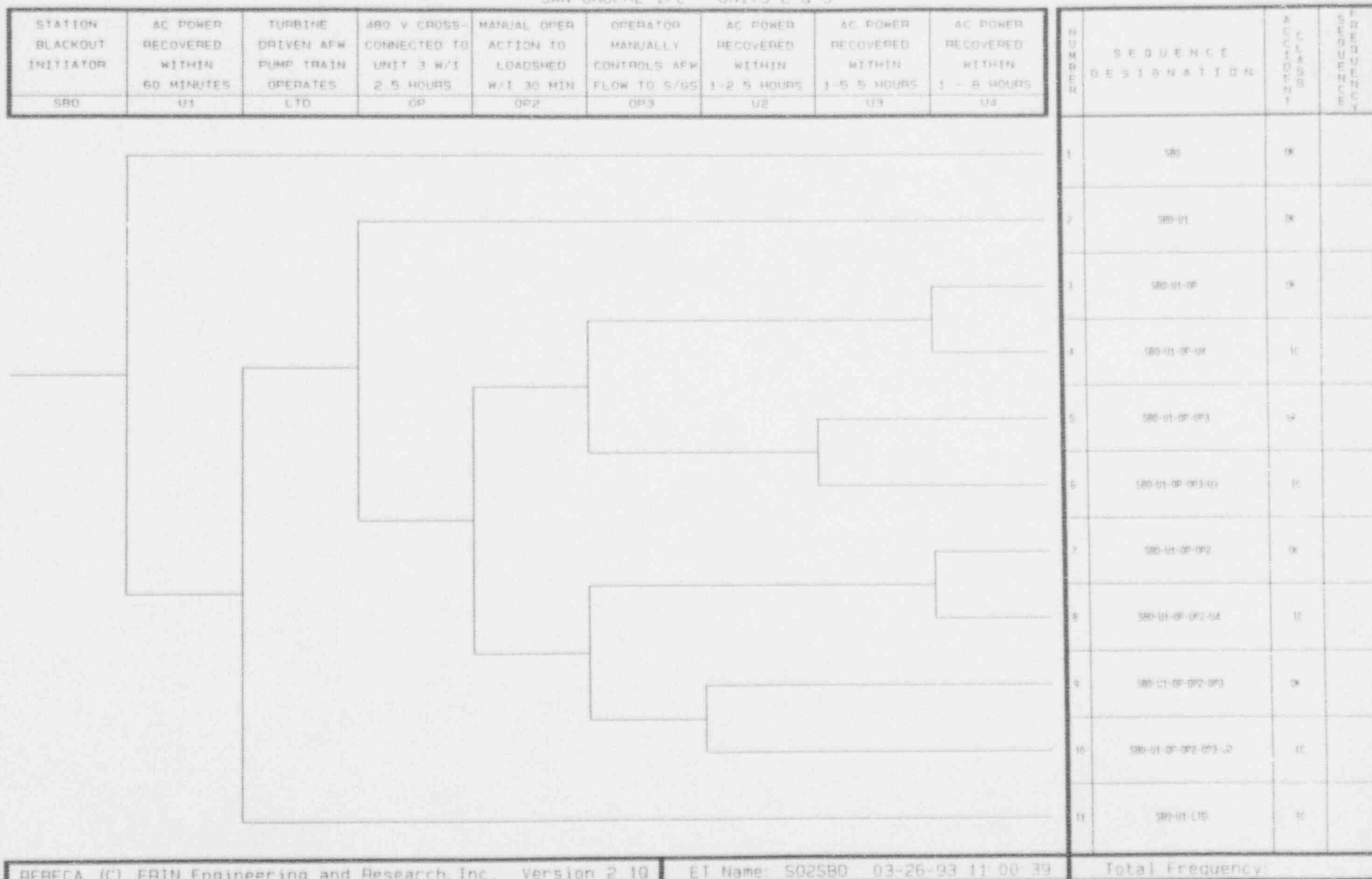
The **480V Cross-Connected To Unit 3 W/I 2.5 Hours (OP)** node accounts for the potential to cross-connect 480 VAC busses between the units to provide power to battery chargers and inverters.

As described above, load shedding of the batteries can have a significant impact on battery life. The operator actions required to shed non-essential loads are accounted in the node **Manual Oper Action To Loadshed W/I 30 Min (OP2)**. Upon depletion of the batteries, the plant operators can manually operate the turbine-driven AFW pump train by manually operating the flow control valves to the steam generators. However, this method of operation will only be successful if instrumentation is available to monitor steam generator level. This is accounted for in the node **Operator Manually Controls AFW Flow To S/Gs (OP3)**.

The likelihood of recovering AC power within time to prevent core damage is accounted for in three nodes, depending upon the

Figure 3.1-7: Station Blackout (SBO) Event Tree
STATION BLACKOUT EVENT TREE (SBO)

SAN ONOFRE IPE - UNITS 2 & 3



REBECA (C) ERIN Engineering and Research, Inc. Version 2.10

ET Name: S02SBO 03-26-93 11:00:39

Total Frequency:

TABLE 3.1-11: SBO EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SBO - Station Blackout

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
AC Power Recovered W/1 60 Minutes (U1)	Vital Auxiliaries RCS Heat Removal	One of two emergency diesel generators or offsite power is recovered within 60 minutes (before core uncover)	Operator attempts to restore power from any available source	S023-12-8, Station Blackout, step 5 and Attachment 7
Turbine Driven AFW Pump Operates 24 H (LTD)	RCS Heat Removal RCS Inventory RCS Pressure	Turbine driven AFW pump P-140 provides feedwater to 1 of 2 steam generators	Operator locally manually operates P-140	S023-12-8, Station Blackout, step 5.b
480V Cross Connected To Unit 3 W/1 2.5 Hours (OP)	Vital Auxiliaries	Cross-tie vital 480 VAC busses between units to provide battery charging and inverter power within 2.5 hours.	Operator action to manually open/close breakers	S023-12-8, Station Blackout
Manual Oper Action to Loadshed W/1 30 Min (OP2)	Vital Auxiliaries	Non-essential loads are shed from vital buses to maximize battery life	Operator sheds non-essential loads from inverters	E01 S023-12-8, "Station Blackout" Attachment 4
Operator Manually Controls AFW Flow To S/Gs (OP3)	RCS Heat Removal RCS Inventory RCS Pressure	AFW control valves throttled to control steam generator level	Operator throttles DC powered AFW control valves locally to control auxiliary feedwater flow to steam generators	S023-12-9, Attachment 8
AC Power Recovered Within 1-2.5 Hours (U2)	Vital Auxiliaries RCS Heat Removal	One of two emergency diesel generators or offsite power is recovered within 2.5 hours	Operator attempts to restore power from any available source	S023-12-8, Station Blackout, step 6 and Attachment 7
AC Power Recovered Within 1-5.5 Hours (U3)	Vital Auxiliaries RCS Heat Removal	One of two emergency diesel generators or offsite power is recovered within 5.5 hours	Operator attempts to restore power from any available source	S023-12-8, Station Blackout, step 6 and Attachment 7
AC Power Recovered Within 1-8 Hours (U4)	Vital Auxiliaries RCS Heat Removal	One of two emergency diesel generators or offsite power is recovered within 8 hours	Operator attempts to restore power from any available source	S023-12-8, Station Blackout, step 6 and Attachment 7

sequence of events (e.g., success or failure of operator actions). These nodes are AC Power Recovered Within 1-2.5 Hours (U2), AC Power Recovered Within 1-5.5 Hours (U3), and AC Power Recovered Within 1-8 Hours (U4).

FAILURE SEQUENCES

Sequences #4 and #8 represent successful secondary heat removal and successful manual control of AFW, but failure to restore AC power within 8 hours. This corresponds to the time when indications of steam generator level will be lost. Inverter load shedding is successful in sequence #4 and unsuccessful in sequence #8. In these cases, load shedding does not directly impact the time for power recovery due to the success of manual control actions. The functional accident sequence is defined as IC, accident sequences involving loss of both primary and secondary coolant makeup due to SBO.

Sequence #6 represents the scenario in which secondary heat removal is available and the operators successfully load shed the inverters, but fail to manually control AFW flow manually. This is assumed to lead to loss of AFW flow at 4 hours, leading to core uncover at 6 hours. This allows 5.5 hours for power recovery. The functional accident sequence is defined as IC, accident sequences involving loss of both primary and secondary coolant makeup due to SBO.

Sequence #10 represents failure to recover AC power within 2.5 hours after failing to shed non-essential loads from the inverters and failure to manually control the AFW flow control valves. In this case core uncover is expected in about 3 hours, allowing 2.5 hours for power recovery. The functional accident sequence is defined as IC, accident sequences involving loss of both primary and secondary coolant makeup due to SBO.

Sequence #11 represents early failure to provide secondary heat sink. The MSSVs successfully relieve secondary steam, but the turbine-driven AFW pump does not provide makeup to the steam generators leading to steam generator dryout. The functional accident sequence is defined as IC, accident sequences involving loss of both primary and secondary coolant makeup due to SBO.

3.1.2.4.7 Main Steam Line Break

Initiating Event Group Summary

The Main Steam Line Break initiating event group (SLB) consists of transient events which cause significant, uncontrolled depressurization of the secondary coolant system. Steam line breaks considered within the scope of the Main Steam Line Break initiating event group include all steam line breaks upstream and downstream of the main steam isolation valves (MSIVs). Division

of steam line breaks based on the break location serves to properly characterize the plant challenge and operational response to these events.

For the case of a steam line break downstream of the MSIVs, the uncontrolled cooldown is less severe since the line break can be effectively isolated by the MSIVs to restore control of the cooldown process. A break upstream of the MSIVs results in a rapid, uncontrolled depressurization of at least one steam generator which cannot be isolated.

Feedwater line breaks in the piping downstream of the last isolation check valve in the Feedwater system (before the steam generator) are considered within the scope of the main steam line break. The plant response following a feedwater line break in this region is similar to that experienced in a steam line break. Feedwater line breaks upstream of the last isolation check valve are considered within the boundary of the loss of PCS initiating event.

Plant Response to Initiating Event

Following the steam line rupture, steam flow increases as blowdown occurs through the break reducing steam line pressure. The accelerated secondary heat removal results in a rapid decrease in primary system pressure and temperature. These conditions rapidly generate a SIAS. The low steam line pressure initiates a MSIS. The MSIS closes the MSIVs, the MSIV bypass valves, the ADVs, the AFW isolation valves, the steam generator blow down valves and the steam generator sample valves. Provided the steam line break is downstream of the MSIVs, closure of the MSIVs isolates the steam generators from the break enabling the re-establishment of secondary heat removal control. EOI SO23-12-5, "Excessive Steam Demand Event," directs the operator to manually initiate an MSIS if an MSIS was not automatically actuated. If the line break is upstream of the MSIVs, the affected steam generator is isolated.

A reactor trip is generated from either the core protection calculators (CPC), low steam generator pressure, high linear power level, or high containment pressure. Even with successful reactor trip, the core may become critical and return to power due to the effect of the rapid RCS cooldown on the negative MTC. The "RETRAN Analysis for MSLB Event - RCS Volume Shrinkage and Restart Potential," dated April 1987, concluded the negative effect on MTC is insufficient to result in a return to power during a main steam line break event. Additionally, this analysis indicated that the HPSI system is not required to prevent core damage following a steam line break.

The loss of secondary system steam through the break decreases the level in the steam generators, actuating the AFW system on

low steam generator level. The EFAS identifies the affected steam generator by the steam generator differential pressure and automatically feeds the intact steam generator. The operator is directed by EOI S023-12-5 to identify the affected steam generator and initiate AFW to the intact steam generator manually if not automatically actuated.

Event Tree Assumptions

The following assumptions were used in the event tree construction of the plant response to a steam line break event:

Assumptions	Bases
High pressure safety injection is not required to maintain RCS inventory for a main steam line break.	"RETRAN Analysis for MSLB" indicates that HPSI flow, although desirable, is not required to prevent core damage following a steam line break.
A reactor trip is sufficient to maintain subcriticality during a main steam line break event.	"RETRAN Analysis for MSLB" concludes that the negative moderator temperature coefficient effects resulting from RCS cooldown and shrinkage are not sufficient to result in a return to power.
Isolation of a main steam line break located downstream of the MSIVs successfully mitigates the steam line break accident.	With the MSIS successfully isolating a break downstream of the MSIVs, the accident becomes similar to a loss of PCS event except lower RCS pressure exists.
A steam line break inside containment may cause the initiation of a Containment Isolation Actuation Signal (CIAS) due to the elevated containment pressure.	The frequency of steam line/feed line break occurring with failure of the operator to respond to an annunciator is bounded by the loss of CCW evaluation.
Location of the steam line break with respect to the containment structure is considered irrelevant. The high containment pressure resulting from the steam line break does not affect the ability to maintain RCS heat removal and is considered a Level II issue.	Containment spray is not required to assist in decay heat removal for a main steam line break. Natural circulation in conjunction with secondary heat removal from the intact steam generator provides RCS heat removal. Containment environmental conditions are considered in the Level II analysis. The high containment pressure may actuate SIAS. The effects of inadvertent ECCS actuation with respect to RCS integrity are addressed in the FSAR Section 15.5.1.2 and are assumed to present no challenge during a main steam line break.
All CEAs are assumed to insert.	Failures to scram are transferred to the ATWS tree.

Assumptions	Bases
No credit is taken for recovering main feedwater following an MSIS.	Conservatism with successful isolation, the MSIS can be overridden and MFW restored.

Event Tree Model

The event tree model for Main Steam Line Break is depicted in Figure 3.1-8. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-12.

The **Main Steam Line Break Initiating Event (SLB)** represents the occurrence of a steam line break upstream or downstream of the MSIV. Steam release from the break commences to rapidly depressurize the secondary system and rapidly cool the primary system. The second node **Automatic Reactor Trip (K)** represents successful reactor trip in order to achieve subcriticality.

The **Steam Line Break Downstream of MSIVs (TDS)** node represents the differentiation between breaks upstream and downstream of the MSIVs. The challenges to safety systems and operational responses vary depending on break location. The **One Main Steam Line Isolated (MSIS) (TIS)** node represents the automatic isolation of one steam generator by the Engineered Safety Features Actuation System (ESFAS). The **Both Steam Lines Isolated (MSIS) (TSB)** node represents the automatic isolation of both steam generators by the Engineered Safety Features Actuation System (ESFAS).

The success or failure of adequately controlling steam flow from the break determines the subsequent response of the plant. If the affected steam generator cannot be isolated or the break is located upstream of the MSIVs, cooldown rate can be controlled by feeding only the intact steam generator and allowing the affected generator to boil dry.

The **APW Available to Intact S/G (LMU)** and **MPW Available To Intact S/G (F2)** nodes represent operation of the APW or Main Feedwater systems in order to provide feedwater to the intact steam generator for controlled secondary heat removal. MFW is rendered unavailable due to the presence of an MSIS. For the case of a steamline break occurring inside containment, a CIAS will provide a secondary automatic isolation of MFW.

Figure 3.1-8: Main Steam Line Break (SLB) Event Tree

MAIN STEAM/MAIN FEEDWATER LINE BREAK (SLB)

SAN ONOFRE IPE - UNITS 2 & 3

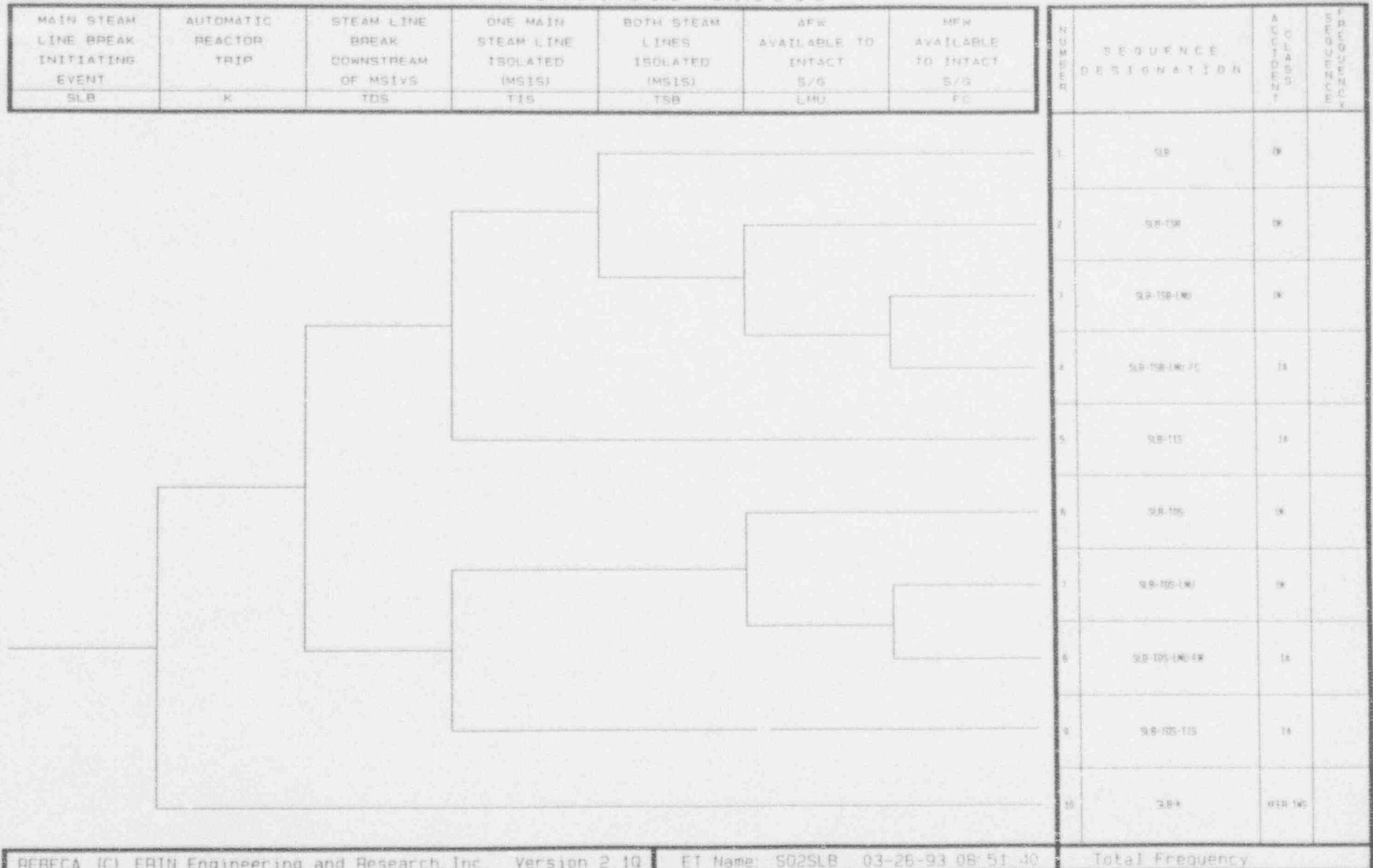


TABLE 3.1-12: SLB EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SLB - Main Steam Line Break

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of a reactor trip signal and insertion of all rods into core	None	S023-12-1, Standard Post Trip Actions, step 3.a
Steam Line Break Downstream of MSIVs (TDS)	RCS Heat Removal RCS Pressure Control	Break in steam line is located downstream of the main steam isolation valves	None	RETRAN SCE Nuclear Analysis 608290
One Main Steam Line Isolated (MSIS) (TIS)	RCS Heat Removal RCS Pressure Control	Main Steam Isolation Signal (MSIS) automatically isolates the affected steam generator by closing MSIVs, MSIV bypass valves, MFIVs, ADVs, AFW isolation valves, steam generator blowdown and steam generator sample isolation valves.	Operator action to backup MSIS if necessary	S023-12-5, Excess Steam Demand, step 6
Both Main Steam Lines Isolated (MSIS) (TSB)	RCS Heat Removal RCS Pressure Control	Main Steam Isolation Signal (MSIS) automatically isolates both steam generators by closing MSIVs, MSIV bypass valves, MFIVs, ADVs, AFW isolation valves, steam generator blowdown and steam generator sample isolation valves.	Operator action to backup MSIS if necessary	S023-12-5, Excess Steam Demand, step 6
AFW Available to Intact Steam Generator (LSB)	RCS Heat Removal RCS Pressure Control Inventory Control	1 of 3 AFW pumps deliver flow to 1 of 1 intact steam generator.	Operator manually actuates AFW system to maintain unaffected S/G level.	S023-12-5, Excess Steam Demand, step 13.i
MFW Available To Intact S/G (FC)	RCS Heat Removal RCS Pressure Control Inventory Control	For breaks outside containment, 1 of 2 MFW pumps with 1 of 4 condensate pumps to 1 of 1 steam generators For breaks inside containment, MFW is unavailable due to CIAS.	None	N/A

FAILURE SEQUENCES

Sequences #4 and #8 represent successful isolation of the faulted steam generator but failure to provide feedwater to the intact steam generator, resulting in a loss of controlled secondary heat sink. The functional accident sequence is defined as IA, accident sequence involving loss of both primary and secondary coolant makeup in the injection phase.

Sequences #5 and #9 represent failure to successfully isolate the faulted steam generator resulting in extensive over-cooling of the primary system. The MSIS, EFAS and operator action are unsuccessful in isolating the affected steam generator to control cooling before core damage ensues. The accident sequence designation for these sequences is IA, accident sequences involving loss of both primary and secondary coolant makeup in the injection phase.

Sequence #10 represents failure of the RPS to initiate an automatic reactor trip. This sequence transfers to the Anticipated Transient Without Scram (TWS) event tree.

3.1.2.5 Front-line Loss of Coolant Accident (LOCA) Event Trees

3.1.2.5.1 Large LOCA

Initiating Group Summary

For the SONGS 2/3 IPE, the Large LOCA event tree initiating event group (LL) consists of breaks in the primary system ranging nominally from 6 inches in diameter to a double-ended guillotine break of RCS loop piping. For the purposes of discussing plant response to this event, the limiting event, a double-ended guillotine break of an RCS loop, is described.

Plant Response to Initiating Event

Immediately following the large LOCA initiating event, the primary system experiences a rapid cooldown and depressurization as inventory escapes through the break. This phase is known as the initial blowdown. The sudden pressure drop causes a significant portion of the primary inventory to flash to steam. A two-phase mixture of steam and water rapidly escapes through the break until stable conditions are established between the primary system and containment atmosphere. During the blowdown phase, the nuclear reaction is terminated by moderator voiding.

When pressurizer pressure decreases below the SIAS setpoint, or if containment pressure reaches the high containment pressure setpoint, a SIAS is initiated automatically. If this does not occur, EOI SO23-12-3, "Loss of Coolant Accident" directs the operator to manually initiate a SIAS.

Once the pressure drops in the primary system below the 615 psia nitrogen pressure of the safety injection tanks (SITs), the tanks can inject their contents into the core. The SIT discharge flows into the downcomer, fills the lower plenum and refloods the core, preventing excessive peak cladding temperatures. A significant portion of the injection escapes through the break during the blowdown phase.

Following the blowdown process, the Safety Injection (SI) system also becomes effective in providing inventory to refill the vessel. With little opposing system pressure, the vessel rapidly fills to the level above the core region. EOI SO23-12-3 directs the operators to establish maximum SI flow. Additionally, the operator is directed to attempt to isolate potential sources of leakage to minimize RCS inventory losses. The SI system continues to inject borated water in the primary system to cool the core which eventually escapes through the break to the containment sump.

During the initial blowdown process, containment pressure rises from relief of primary system steam and fluid through the break. If the containment pressure rises above the high containment pressure setpoint, an automatic Containment Isolation Actuation Signal (CIAS) and in addition if a SIAS is already initiated, a Containment Cooling Actuation Signal (CCAS) should be initiated. The CCAS starts the emergency containment fan coolers which operate in conjunction with the normal containment cooling and air recirculation systems. The containment spray pumps start on a SIAS but the spray flow is not initiated until containment pressure reaches the high-high containment pressure setpoint. When the containment pressure reaches the high-high setpoint following a SIAS actuation, an automatic CSAS is initiated opening the containment spray header isolation valves and allowing flow to the spray headers. If the automatic signals fail, the operator can manually actuate the system per EOI SO23-12-1. The containment spray system initially takes suction from the RWST. The containment is adequately cooled when any single spray pump or fan cooler is available to provide cooling capacity assisting in RCS decay heat removal.

EOI SO23-12-3 directs the operator to initiate RCS heat removal via the steam generators. For a large LOCA, the RCS depressurizes to an equilibrium pressure with the containment. In this condition, the RCS fluid is at a lower temperature than that of the steam generators. The steam generators, therefore, act as a heat source, superheating any steam in the RCS which may be flowing through the steam generators. The operators are directed by EOI SO23-12-3 to cool down the steam generators to reduce heat input to the RCS. However, it should be noted adequate heat removal can be achieved by circulating primary coolant through the break and using containment cooling systems for decay heat removal.

Throughout the event, the operators monitor RWST level. The LPSI pumps and containment spray pumps take suction from the RWST which is depleted in approximately 30 minutes. The decreasing RWST level should correspond to an increasing containment sump level. The operators are able to trend RWST level and anticipate possible problems in actuating a RAS at the RWST low level setpoint.

When the RWST reaches the low level setpoint, a RAS is initiated automatically. The operators are then directed by procedure to ensure that the sump valves have opened and the LPSI pumps have stopped. The operators verify the SI and containment spray pump mini-flow isolation valves are closed and containment spray flow is greater than 1750 gpm. The RWST isolation valves are closed manually after the containment emergency sump level is verified. Note that operator action to close the RWST isolation valve is a redundant isolation of the line in case a check valve fails to close.

During cooldown, if shutdown cooling system entrance conditions cannot be met, then simultaneous hot and cold leg injection is required within 4 hours following LOCA initiation. In this mode, the HPSI pump discharge lines are realigned so the total injection flow is divided equally between the hot and cold legs. This alignment is used as a mechanism to prevent the precipitation of boric acid in the reactor vessel.

Event Tree Assumptions

The following event tree assumptions were used in the event tree construction of the plant response to a large LOCA event:

Assumptions	Basis
Reactor trip is not required to achieve subcriticality.	Moderator voiding during blowdown. Emergency boration by safety injection system.
Each containment spray pump can provide 100% capacity containment cooling and each emergency cooling fan can provide 100% capacity. Thus, any containment heat removal train is sufficient to remove RCS decay heat during the injection and recirculation phases. Failure of containment cooling is assumed to result in an early loss of containment integrity and flashing of the sump inventory, leading to a failure of recirculation.	Plant Specific MAAP Analysis

Assumptions	Basis
It is recognized the containment spray pumps can be utilized as a backup for LPSI cold leg injection per the Functional Recovery EOI. This alignment is conservatively not modeled even though alignment of containment spray as an injection source would occur (since the core heat removal safety function has priority over containment).	Conservatism
EOI SO23-12-3 directs the operator to ensure all available charging pumps are operating. Due to the relatively small contribution of the charging pumps to RCS inventory makeup (relative to other injection sources under low pressure RCS conditions), the charging pumps are assumed not to be required.	Plant Specific MAAP Analysis
Use of LPSI and containment spray as backups to HPSI for recirculation is not credited.	Conservatism.
HPSI is not required during the injection phase of the Large LOCA accident scenario. LPSI can provide all makeup required during injection.	Plant-Specific MAAP Analysis

Event Tree Model

The event tree model for Large LOCA is depicted in Figure 3.1-9. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-13.

The **Large LOCA Initiate (LL)** node represents occurrence of the initiating event. Subsequent to initial core blowdown, the Safety Injection Tanks discharge into the downcomer through the cold legs to reflood the core. This is represented by the **SITs Discharge to 3/3 Intact Cold Legs (V)** node. The **LPSI in Cold Leg Injection Mode (AI)** represents injection of coolant from the Refueling Water Storage Tank (RWST) into the cold legs by the LPSI system. The low pressure environment in the RCS following blowdown permits high volume, low pressure injection in order to cover the reactor core.

Blowdown following the break increases the containment pressure, causing the containment emergency fan coolers to actuate. As containment pressure continues to increase, a containment spray actuation signal is automatically initiated. **100% Capacity CMNT Cooling w/CEFCs & CS In Injection (NE)** represents a combination of containment emergency coolers and containment spray pumps providing early decay heat removal. The **100% Capacity CMNT Cooling w/CEFCs & CS in Recirc (NL)** node represents the realignment of the containment spray pumps to take suction from

Figure 3.1-9: Large LOCA (LL) Event Tree

LARGE LOCA EVENT TREE (LL)

SAN ONOFRE IPE - UNITS 2 & 3

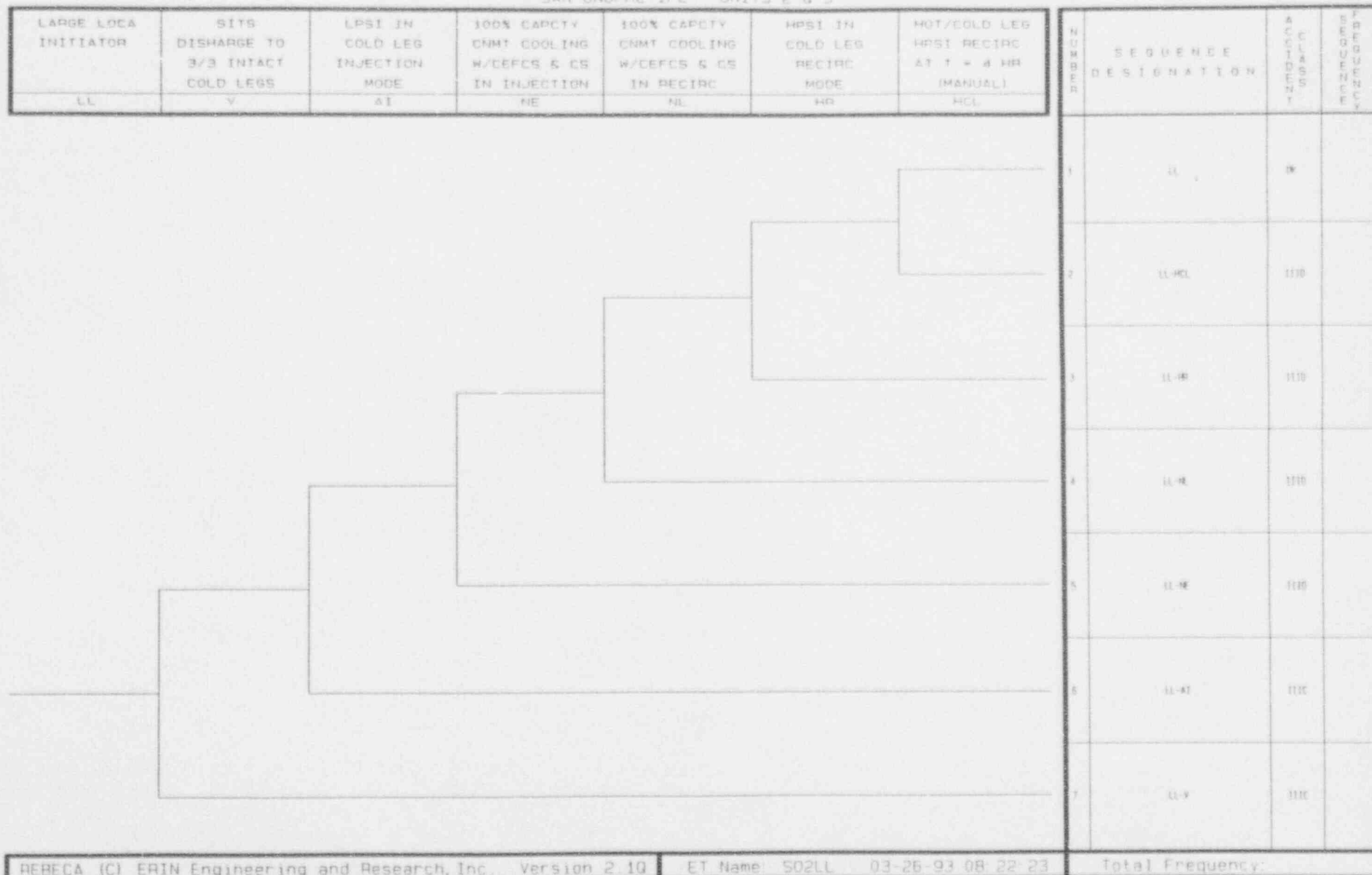


TABLE 3.1-13: LL EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: LL - Large LOCA

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
SITs Discharge to 3 of 3 Intact Cold Legs (V)	Reactivity Control RCS Inventory RCS Heat Removal	3 of 3 SITs discharge into intact RCS legs	None	FSAR Section 15.6.3.3
LPSI in Cold Leg Injection Mode (AI)	Reactivity Control RCS Inventory RCS Heat Removal	1 of 2 LPSI pumps inject borated water into the RCS from RWST through two intact cold legs	None	Plant Specific MAAP Analysis
100% Capacity Cnmt Cooling w/CEFCs & CS In Injection (NE)	RCS Heat Removal	One of two CS pumps and shutdown cooling heat exchanger with suction from the RWST or One of four emergency fans	None	Plant Specific MAAP Analysis
100% Capacity Cnmt Cooling w/CEFCs & CS in Recirc (NL)	RCS Heat Removal	One of two CS pumps and shutdown cooling heat exchanger with suction from the containment sump or One of four emergency fans	Operator isolates RWST after automatic RAS containment spray realignment.	S023-12-3, Loss of Coolant Accident, Attachment 5
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal	1 of 3 HPSI pumps inject water from containment sump into the RCS through two intact cold legs	Operator isolates RWST after automatic RAS HPSI realignment	S023-12-3, Loss of Coolant Accident, Attachment 5
Hot/Cold Leg HPSI Recirc at T-4 Hr (HCL)	RCS Inventory RCS Heat Removal	1 of 2 hot leg valves open, with HPSI in recirc to valve	Operator aligns for simultaneous hot/cold leg recirculation	S023-12-3, Loss of Coolant Accident, Attachment 5

the containment sump as the RWST depletes for late decay heat removal.

The HPSI in Cold Leg Recirc Mode (HR) node addresses the requirement to change over to recirculation as the RWST inventory depletes and accumulates in the sump. Approximately four hours after the LOCA, injection is switched over to simultaneous hot and cold leg injection to prevent boron precipitation. The Hot/Cold Leg HPSI Recirc at T=4 Hr (HCL) node represents this alignment.

FAILURE SEQUENCES

Sequence #2 represents successful mitigation of challenges to the plant early, but failure to establish simultaneous hot/cold leg recirculation. Boron precipitation in the core eventually causes loss of RCS heat removal. The functional accident sequence is classified as IIID, accident sequence initiated by a Medium or Large LOCA with loss of primary coolant makeup or adequate heat removal in the recirculation phase.

Sequence #3 represents successful reflooding of the vessel, but failure to establish HPSI recirculation. RWST inventory depletes resulting in loss of circulation and RCS heat removal. The functional accident sequence is classified as IIID, accident sequence initiated by a Medium or Large LOCA with loss of primary coolant makeup or adequate heat removal in the recirculation phase.

Sequence #4 represents successful reflooding of the core and switchover to recirculation, but failure to realign containment spray to take suction from the containment sump and failure of all the CEFCs. Decay heat cannot be adequately removed from the containment sump resulting in inadequate RCS heat removal. The functional accident sequence is classified as IIID, accident sequence initiated by a Medium or Large LOCA with loss of primary coolant makeup or adequate heat removal in the recirculation phase.

Sequence #5 represents failure of the containment cooling systems to remove adequate decay heat early. This sequence is defined by a IIID, accident sequence initiated by Medium or Large LOCA with loss of primary coolant makeup in the recirculation phase.

Sequences #6 and #7 represent failure during the injection phase following the large break LOCA. The failure of the safety injection tanks results in failure to restore RCS heat removal in sufficient time following blowdown. Failure of injection from LPSI causes loss of the only high volume injection source (after SIT injection) to be lost resulting in the inability to provide inventory control and heat removal in sufficient time following blowdown. The functional accident sequences are defined as IIIC,

accident sequences initiated by Medium or Large LOCA with loss of primary coolant makeup in the injection phase.

3.1.2.5.2 Medium LOCA

Initiating Group Summary

The Medium LOCA event tree group consists of primary system leakage through breaks ranging from 2 inches to 6 inches in diameter.

Plant Response to Initiating Event

Immediately following the Medium LOCA event, fluid from the primary system escapes through the break. The sudden pressure drop at the break location flashes the fluid to steam. Break size and back pressure from the fluid/steam flashing precludes the degree of sudden depressurization and vessel voiding evident in a Large LOCA event.

When primary system pressure decreases below the SIAS low pressurizer pressure setpoint, or containment pressure reaches the high pressure setpoint, a SIAS and CCAS is initiated automatically and the reactor is tripped. If this does not occur, EOI SO23-12-3 directs the operator to manually initiate a SIAS. The HPSI system begins to inject borated water into the RCS.

HPSI provides the necessary makeup to maintain core heat removal and adequate inventory in the RCS. For a Medium LOCA, it is assumed the primary system pressure remains above the shutoff head of the LPSI pumps. Continued relief of primary coolant to the containment increases the containment pressure and temperature. Emergency containment fan coolers start automatically following CCAS actuation to provide containment heat removal. The containment spray pumps start automatically upon SIAS actuation and recirculate inventory back to RWST. Following the SIAS actuation, a containment pressure increase to the high-high containment pressure setpoint will initiate a CSAS which automatically starts containment spray system by opening the spray discharge valves.

Operator actions check and verify plant conditions during the injection phases of the accident. The operators utilize EOI SO23-12-3 and remain in this procedure for the duration of the accident since the termination criteria are not met.

The RWST level decreases rapidly due to HPSI and containment spray operation. When the RWST level reaches low level, a RAS is initiated automatically. The operators then verify the sump valves have opened and the LPSI pumps are stopped. The operators isolate the RWST after sufficient suction to the HPSI and

containment spray pumps is confirmed. During the recirculation phase the containment cooling systems provide decay heat removal and prevent sump pool boiling.

The HPSI pumps take suction from the containment sump and recirculate primary fluid through the cold legs and vessel to cool the core. Inventory also flows out the break to the sump. This process continues for 4 hours following the LOCA initiating event. If shutdown cooling entrance conditions cannot be achieved during this 4 hour time period, then simultaneous hot and cold leg recirculation is required within 4 hours to prevent boron precipitation. Hot/cold leg recirculation continues until the primary system reaches shutdown cooling entry conditions. When shutdown cooling is available, the LPSI system is realigned for shutdown cooling.

Event Tree Assumptions

The following assumptions were used in the event tree construction of the plant response to a medium LOCA event:

Assumptions	Basis
Safety injection tanks (SIT) are not required as they only provide an interim source of makeup. Other long term sources of makeup can provide necessary makeup without use of SITs.	There is no void pressure range in which the ECCS can provide makeup between the HPSI injection head and LPSI injection head. Plant Specific MAAP Analysis
Primary system pressure remains above the shutoff head of the LPSI pumps.	Conservatism
An automatic reactor trip is required for a Medium LOCA to maintain sufficient reactivity control. Failure of containment cooling is assumed to result in an early loss of containment integrity and flashing of the sump inventory, leading to a failure of recirculation.	Conservatism
Unlike other events requiring reactor trip, the Medium LOCA event does not credit emergency boration.	Conservatism With failure of the RPS during a Medium LOCA, pressure is assumed to remain high, above the shutoff head of the HPSI pumps.
Both the containment emergency coolers and the containment spray system actuate during a Medium LOCA.	Plant Specific MAAP Analysis
Decay heat can be removed from the containment sump during recirculation by either on train of the containment spray system or one containment emergency air cooler.	Plant Specific MAAP Analysis

Assumptions	Basis
Transfer to simultaneous hot/cold injection is required at T=4 hours for successful accident mitigation.	EOI SO23-12-3
EOI SO23-12-3 directs the operator to ensure all available charging pumps are operating. Due to their relatively small contribution of the charging pumps to RCS inventory makeup (relative to other injection sources under low pressure RCS conditions), the charging pumps are assumed not to be required.	Plant Specific MAAP Analysis

Event Tree Model

The event tree model for Medium LOCA is depicted in Figure 3.1-10. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-14.

The **Medium LOCA Initiator (ML)** node represents occurrence of the initiating event. **Automatic Reactor Trip (K)** is required to maintain adequate reactivity control. Primary system leakage following the break occurrence actuates SI providing the necessary high head injection to maintain core heat removal. The nodes **HPSI in Cold Leg Injection Mode (HI)** and **Containment Spray In Cold Leg Injection (NI)** represent the injection phase makeup to the RCS. Containment spray can act as a backup to HPSI for these events, if the operators depressurize the RCS. In either case, the loss of the inventory through the break, increases containment pressure and temperature causing containment emergency cooling actuation and sprays. The node **100% Capacity CNMT Cooling w/CEFCs & CS in Injection (NE)** represents the need for containment cooling systems to remove decay heat to prevent sump pool boiling and maintain effective core heat removal. The node **100% Capacity CNMT Cooling w/CEFCs & CS in Recirc (NL)** addresses the requirement to realign containment spray to take suction from the sump or utilize a CEFC for continued decay heat removal.

The nodes **HPSI in Cold Leg Recirc Mode (HR)** and **Containment Spray in Cold Leg Recirc (NR)** address the requirement to change over to recirculation as the RWST inventory depletes and accumulates in the sump. The recirculation process continues for approximately four hours at which time manual switchover to simultaneous hot and cold leg recirculation is performed. The hot/cold leg switchover is represented by the final node **Hot/Cold Leg HPSI Recirc at T=4 HR (MANUAL) (HCL)**.

Figure 3.1-10: Medium LOCA (ML) Event Tree

MEDIUM LOCA EVENT TREE (ML)

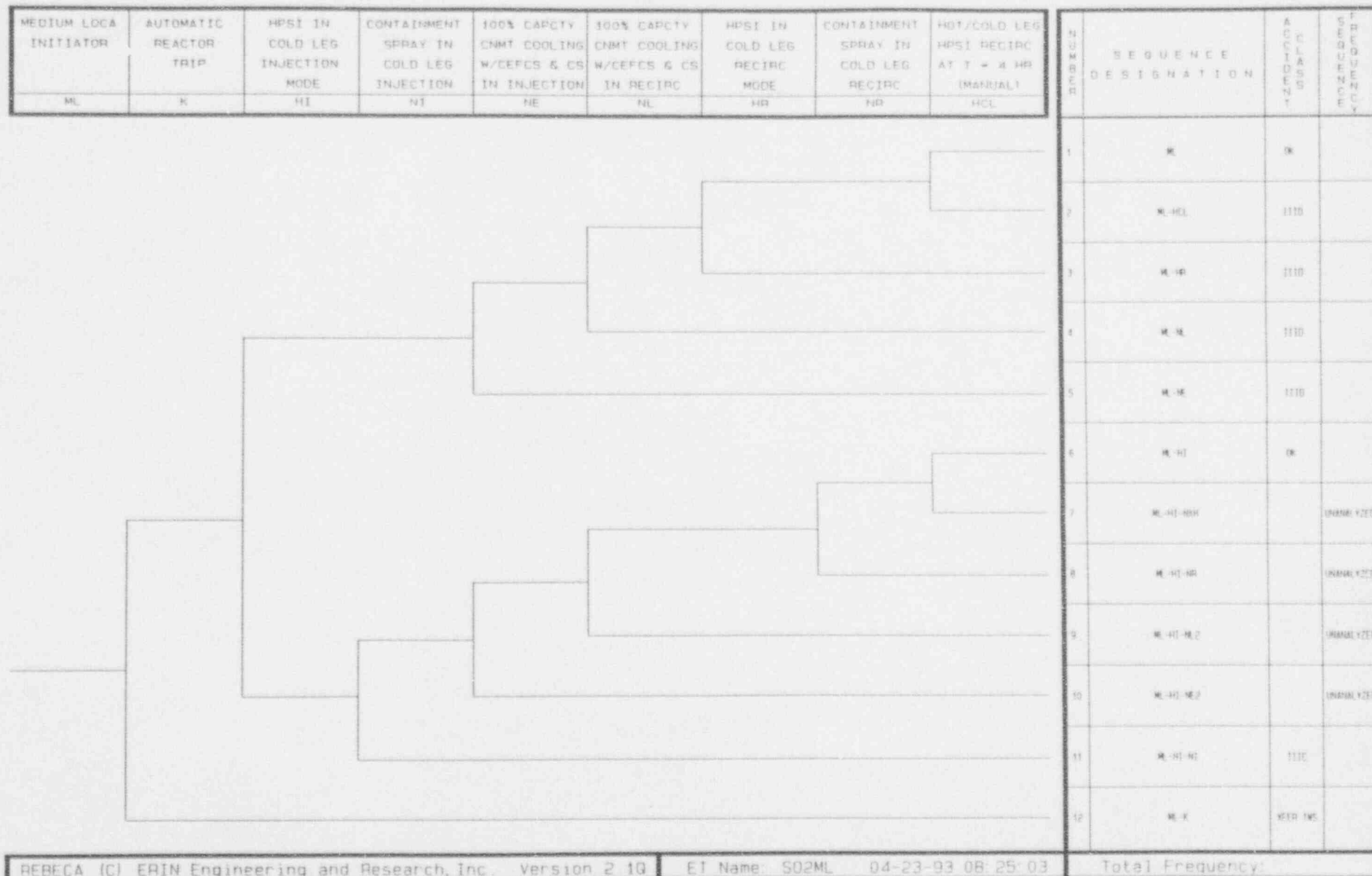


TABLE 3.1-14: ML EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: ML - Medium LOCA

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of reactor trip signal and insertion of all rods into core.	None	S023-12-1, Standard Post Trip actions, step 3.a
HPSI in Cold Leg Injection Mode (HI)	Reactivity Control RCS Inventory RCS Heat Removal	1 of 3 HPSI pumps inject borated water from RWST to cold legs.	None	S023-12-3, Loss of Coolant Accident
Containment Spray in Cold Leg Injection (NI)	Reactivity Control RCS Inventory RCS Heat Removal	1 of 2 containment spray pumps inject borated water from RWST to cold legs.	Align containment spray for RCS injection	S023-12-3, Loss of Coolant Accident
100% Capacity Cnmt Cooling w/CEFCs & CS in Injection (NE)	RCS Heat Removal Containment	One of two CS pumps and shutdown cooling heat exchanger with RWST suction or One of four emergency fans	None	Plant Specific MAAP Analysis
100% Capacity Cnmt Cooling w/CEFCs & CS in Recirc (NL)	RCS Heat Removal Containment	One of two CS pumps and shutdown cooling heat exchanger with suction from the containment sump or One of four emergency fans	Operator isolates RWST after automatic RAS containment spray realignment.	S023-12-3, Loss of Coolant Accident, Attachment 5
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal	1 of 3 HPSI pumps inject water from the containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS HPSI realignment.	S023-12-3, Loss of Coolant Accident, Attachment 5
Hot/Cold Leg HPSI Recirc at T-4 Hr (HCL)	RCS Inventory RCS Heat Removal	1 of 2 hot leg valves open with HPSI in recirc mode to valve.	Operator aligns for simultaneous hot/cold leg recirculation.	S023-12-3, Loss of Coolant Accident, Attachment 4

FAILURE SEQUENCES

Sequences #2 and #7 represent successful mitigation of challenges to the plant early, but failure to establish simultaneous hot/cold leg recirculation. Boron precipitation in the core causes loss of heat removal. In sequence #2, HPSI is relied upon for recirculation, whereas, in sequence #7, containment spray is utilized. Accident sequence #2 is classified as IIID, accident sequences initiated by a Medium or Large LOCAs with loss of primary coolant makeup or adequate heat removal in the recirculation phase. Sequence #7 is unanalyzed due to the expected failure to align containment for injection early in the sequence progression.

Sequence #3 represents success of HPSI cold leg injection of the vessel, but failure to establish HPSI cold leg recirculation. RWST inventory depletes resulting in loss of circulation and heat removal in the vessel. The functional accident sequence is classified as IIID, accident sequences initiated by a Medium or Large LOCAs with loss of primary coolant makeup or adequate heat removal in the recirculation phase.

Sequences #4 and #9 represent successful HPSI injection and recirculation, but failure to establish late containment cooling for sump decay heat removal. In sequence #4, HPSI is relied upon for recirculation, whereas, in sequence #9, containment spray is utilized. Accident sequence #4 is defined as IIID, accident sequences initiated by a Medium or Large LOCAs with loss of primary coolant makeup or adequate heat removal in the recirculation phase. Sequence #9 is unanalyzed due to the expected failure to align containment for injection early in the sequence progression.

Sequences #5 and #10 represent failure to establish early heat removal using containment cooling systems. In sequence #5, HPSI is relied upon for recirculation, whereas, in sequence #10, containment spray is utilized. Sequence #5 is defined by IIID, accident sequences initiated by a Medium or Large LOCAs with loss of primary coolant makeup or adequate heat removal in the recirculation phase, functional accident sequence classification. Sequence #10 is unanalyzed due to the expected failure to align containment for injection early in the sequence progression.

Sequence #8 represents failure of containment spray in the RCS injection alignment during recirculation. Sequence #8 is unanalyzed due to the expected failure to align containment for injection early in the sequence progression.

Sequence #11 represents failure during the injection phase following the medium break LOCA. Failure of injection from the HPSI and containment spray systems causes a loss of heat removal early. The functional accident sequence is defined as IIIC,

accident sequences initiated by Medium or Large LOCA with loss of primary coolant makeup in the injection phase.

Sequence #12 represents failure of the RPS to initiate an automatic reactor trip. This sequence transfers to the Anticipated Transient without Scram (TWS) event tree.

3.1.2.5.3 Small LOCA

Initiating Group Summary

The Small LOCA initiating event group includes breaks in the primary system ranging from 3/8 inch to 2 inches in diameter.

Plant Response to Initiating Event

RCS inventory control is initially lost since the break flow rate exceeds the available charging pump capacity. Primary system pressure decreases with the inventory loss through the break. When pressurizer pressure decreases below the low pressure setpoint, or containment pressure reaches the high containment pressure setpoint, a SIAS and CCAS should be initiated automatically. If this does not occur, EOI SO23-12-3 directs the operator to manually initiate a SIAS. The low pressurizer pressure, low DNBR, high containment pressure or manual operator action initiate a reactor trip which quickly reduces core power to decay heat.

The high primary system pressure exceeds the injection head capability of the LPSI pumps, and precludes Safety Injection Tank discharge. The HPSI pumps automatically start with the SIAS and replenish the RCS through the cold legs with borated water from the RWST. The HPSI pump injection eventually surpasses the leak flow rate and the RCS begins to refill.

During this period of refilling before RCS pressure control has been regained there may be significant voiding in the RCS. The voided areas may be located in the reactor vessel head region, the RCS loops, or the steam generator U-tubes and may consist of steam or non-condensable gases. RCS heat removal is not jeopardized by the gases since a significant number of steam generator tubes are not blocked. Considerable oxidation of fuel cladding does not occur for a Small LOCA.

For a Small LOCA, decay heat removal is achieved principally through the steam generators in conjunction with some heat removed through the break. Secondary heat removal is provided following the turbine trip immediately by the turbine bypass system, ADVs and/or the MSSVs. Continued secondary heat removal requires that main or auxiliary feedwater is provided to the steam generators in conjunction with adequate steam relief. The AFW system automatically starts given low steam generator level.

RCS heat removal is maintained by natural circulation. In the event the AFW system does not actuate automatically, the EOI SO23-12-3 directs the operator to manually initiate AFW or MFW.

The temperature in the primary system decreases as heat removal from secondary systems and through the break matches or exceeds decay heat. Break size and flow hold the primary system pressure high, continuing the net inventory loss as the break flow exceeds the injection flow. As primary system pressure decreases, the rate of inventory loss decreases and the rate of HPSI injection increases. Cumulative RCS inventory losses reduce the RWST inventory, causing an automatic transfer to RAS prior to the time shutdown cooling conditions are achieved. Throughout the event, the operators monitor RWST level. The decreasing RWST should correspond to an increasing containment sump level.

As inventory is lost through the break, the containment atmosphere absorbs heat from the RCS resulting in elevated temperatures and pressures. A CCAS automatically starts the emergency fan coolers. If the pressure reaches the high-high containment pressure setpoint, a CSAS allows spray flow to the spray header (the containment spray pumps start on a SIAS). Initially containment spray takes suction from the RWST. This increases the inventory demands on the RWST and expedites depletion of the tank. Containment cooling systems are not included in the small LOCA event tree as they are not required for decay heat removal since secondary cooling is available. Early containment failure will not occur due to containment cooling system failure. Thus, flashing of sump inventory is not a concern.

When the RWST level reaches the low level setpoint, a RAS is automatically initiated. The operators ensure containment sump valves have opened, the LPSI pumps are stopped, pump mini-flow valves are closed and that the proper flow has been established. The operator then manually closes the RWST isolation valves after sufficient suction from the sump to the HPSI and containment spray pumps is confirmed.

Event Tree Assumptions

The following assumptions were used in the event tree construction of the plant response to a Small LOCA event:

Assumptions	Basis
It is assumed the RWST depletes within the 24 hour mission time, requiring recirculation mode for safety injection before shutdown cooling can be implemented.	Conservatism Plant Specific MAAP Analysis

Assumptions	Basis
Simultaneous hot and cold leg injection is not required to preclude boron precipitation for a Small LOCA.	EOI SO23-12-3, Loss of Coolant Accident Forward flow of liquid maintained through the core.
Emergency Condensate may be available for secondary heat removal, however, this system is not included in the event tree model.	Containment pressure above the high pressure setpoint closes FWIVs and no credit is taken for actions beyond control board override capability in this case.
The FWIVs close on receipt of a CIAS should containment pressure reach the high pressure setpoint.	Conservatism
Flow from the CVCS charging pumps is not modeled in the event tree due to the insignificant contribution to primary system makeup relative to the HPSI pumps.	Conservatism

Event Tree Model

The event tree model for Small LOCA event is depicted in Figure 3.1-11. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-15.

The **Small LOCA Initiator** node (SL) represents occurrence of the Small LOCA initiating event. The second node **Automatic Reactor Trip** (K) addresses the requirement for a reactor trip in order to achieve subcriticality. Failure to trip the reactor transfers to the Anticipated Transient Without Scram (TWS) event tree. The **Main Steam Relief Available** (T) node represents removal of secondary system steam through the turbine bypass valves, ADVs, or MSSVs.

Following the successful reactor trip, the loss of coolant through the break requires makeup. Primary system pressure remains high, requiring high pressure injection. The nodes **HPSI in Cold Leg Injection Mode** (HI) and **Containment Spray In Cold Leg Injection** (NI) represent the injection phase makeup to the RCS. Containment spray can only act as a backup to HPSI for these events, if the operators depressurize the RCS.

The **APW Available to 1 of 2 Steam Generators** (LNL), and **MPW (CIAS) Available to 1 of 2 Steam Generators** (F) nodes represent operation of secondary heat removal systems to remove decay heat from the primary system.

Figure 3.1-11: Small LOCA (SL) Event Tree

SMALL LOCA EVENT TREE (SL)

SAN ONOFRE IPE - UNITS 2 & 3

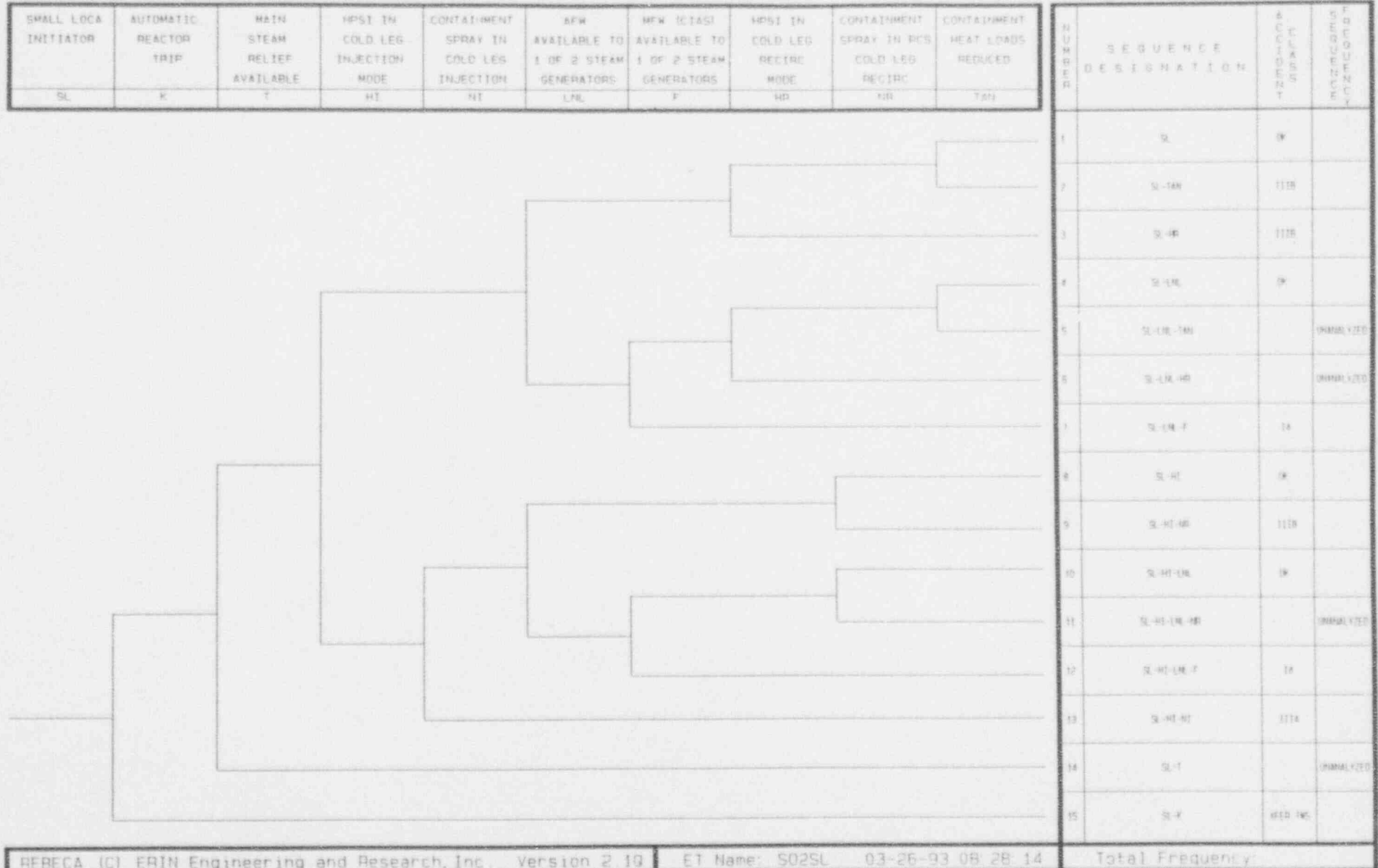


TABLE 3.1-15: SL EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SL - Small LOCA

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of reactor trip signal and insertion of all rods to core.	None	S023-12-1, Standard Post Trip Action, step 3.a
Main Steam Relief Available (T)	RCS Heat Removal	3 of 9 main steam safety valves, 1 of 4 turbine bypass, or 1 of 2 ADVs lift to relieve secondary system pressure per steam generator.	Operator throttles ADVs (required) or backs up turbine bypass valve operation.	Plant Specific MAAP Analysis
HPSI in Cold Leg Injection Mode (HI)	Reactivity Control RCS Inventory RCS Heat Removal	1 of 3 HPSI pumps inject borated water from the RWST to 2 of 4 cold legs	None	Plant Specific MAAP Analysis
Containment Spray in Cold Leg Injection (NI)	Reactivity Control RCS Inventory RCS Heat Removal	1 of 2 containment spray pumps inject borated water from RWST to cold legs.	Align containment spray for RCS injection	S023-12-3, Loss of Coolant Accident
AFW Available to 1 of 2 Steam Generators (LNL)	RCS Heat Removal	1 of 3 AFW pumps deliver flow to 1 of 2 working steam generator.	None	S023-12-3, Loss of Coolant Accident, step 11
MFW Available to 1 of 2 Steam Generators (F)	RCS Heat Removal	1 of 2 MFW pumps deliver flow to 1 of 2 working steam generators.	None.	S023-12-9, Functional Recovery, Attachment 8, step 6
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal	1 of 3 HPSI pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS HPSI realignment.	S023-12-3, Loss of Coolant Accident, Attachment 5
Containment Spray in RCS Recirc Mode (NR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 2 containment spray pumps inject water from containment sump into 2 of 4 cold legs.	Operator isolates RWST after automatic RAS HPSI realignment	S023-12-3, Loss of Coolant Accident, Attachment 5

TABLE 3.1-15: SL EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SL - Small LOCA

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Containment Heat Loads Reduced (TAN)	Containment Pressure	1 of 4 containment emergency fan coolers or 1 of 2 containment spray pumps taking suction from RWST	None	Plant Specific MAAP Analysis For CEFCs/CS Heat Removal

The node **HPSI in Cold Leg Recirc Mode** (HR) models the requirement to establish high pressure recirculation when the level in the RWST requires transfer to recirculation operations. The **Containment Spray In RCS Cold Leg Recirc** (NR) node evaluates the RCS makeup capability in the event recirculation switchover is required when containment spray is being utilized for RCS makeup. The **Containment Heat Loads Reduced** (NT) node evaluates the management of containment heat through the use of containment heat removal systems (Containment Emergency Fan Coolers and Containment Spray).

FAILURE SEQUENCES

Sequences #2 and #5 represent failure resulting from failures of high pressure injection during recirculation due to failure to control containment heat loads. RCS heat removal and inventory are lost resulting in core uncover. The primary difference in these sequences is that AFW is used to remove RCS heat in sequence #2 and MFW is used in sequence #5. Accident sequence #2 is defined as IIIB, accident sequences initiated by a Small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the recirculation phase. Sequence #5 is unanalyzed due to expected isolation of MFW in the presence of an CIAS.

Sequences #3 and #6 represent failure resulting from failures of high pressure injection system during recirculation. RCS heat removal and inventory are lost resulting in core uncover. The primary difference in these sequences is that AFW is used to remove RCS heat in sequence #3 and MFW is used in sequence #6. Accident sequence #3 is defined as IIIB, accident sequences initiated by a Small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the recirculation phase. Sequence #3 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequences #7 and #12 represent failure due to inadequate secondary heat removal from the MFW and AFW systems. Decay heat removal through the break is inadequate causing primary system temperature to rise. The primary difference in these sequences is that HPSI is used to provide RCS makeup in sequence #7 and containment spray is used in sequence #12. The primary system pressure remains high limiting HPSI injection resulting in inventory depletion and core uncover. The functional accident sequences are defined as IA, accident sequences with loss of adequate heat removal in the injection phase.

Sequences #9 and #11 represent failure resulting from failures of containment spray injection system during recirculation. RCS heat removal and inventory are lost resulting in core uncover. The primary difference in these sequences is that AFW is used to remove RCS heat in sequence #9 and MFW is used in sequence #11. Accident sequence #9 is defined as IIIB, accident sequences

initiated by a Small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the recirculation phase. Sequence #11 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequences #13 represents the unavailability of the adequate RCS makeup. This sequence represents failure of the HPSI and containment spray systems to provide makeup. Without makeup, the primary system inventory depletes resulting in core uncover. The functional accident sequences are defined as IIIA, accident sequences initiated by a Small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the injection phase.

Sequence #14 represents failure due to inadequate main steam relief, resulting in inadequate secondary heat removal. This sequence is unanalyzed due to the negligible likelihood of main steam relief failure.

Sequence #15 represents failure of the RPS to initiate an automatic reactor trip. This sequence transfers to the Anticipated Transient Without Scram (TWS) event tree.

3.1.2.5.4 Small-Small LOCA

Initiating Group Summary

The Small-Small LOCA initiating event group includes breaks in the primary system approximately 3/8 inch in diameter. The lower bounds of the Small-Small LOCA category are the breaks for which makeup can be provided by the charging system without leading to a reactor trip.

Plant Response to Initiating Event

After the Small-Small break LOCA occurrence, primary system pressure decreases with inventory loss through the break. The rate of primary system depressurization is slow. Based on either primary system pressure decreasing below 1740 psig or manual actuation by the operator (EOI S023-12-3, "Loss of Coolant Accident"), the SI system actuates. The low pressurizer pressure or more likely a manual trip initiates a reactor trip which quickly reduces core power to decay heat.

The high primary system pressure exceeds the injection head capability of the LPSI pumps, and precludes SIT discharge. The HPSI pumps and idle charging pumps automatically start with the SIAS and begin to inject borated water from the RWST to the RCS cold legs. The charging and HPSI pump injection eventually surpasses the leak flow rate and the RCS begins to refill.

For a Small-Small LOCA, decay heat removal is achieved through the steam generators in conjunction with the minor heat removed

through the break. Immediate secondary heat removal following the turbine trip is provided by the turbine bypass system, ADVs or the MSSVs. Continued secondary heat removal is automatically provided by the AFW system in conjunction with main steam relief. In accordance with EOI SO23-12-3 EFAS or manual action by the operator to backup EFAS actuates the AFW system should the MFW system be unavailable. The AFW system automatically starts given a low steam generator level or pressure. RCS heat removal is maintained by either forced circulation RCPs (provided RCS pressure greater than 1430 psia with no CCW leakage indication) or natural circulation. It is assumed, however, that the RCPs are tripped for all LOCAs in accordance with EOI SO23-12-3.

Temperature in the primary system decreases as heat removal from the secondary systems matches or exceeds decay heat. Decay heat holds the primary system pressure high, continuing the net inventory loss as the break flow exceeds the injection flow. As primary system pressure decreases, the rate of inventory loss decreases and the rate of charging and HPSI injection increases. When the RCS pressure and temperature are sufficiently reduced, RCS heat removal can be provided by the SDC system.

During a Small-Small LOCA, the containment pressure rises very slowly from relief of primary system steam and fluid through the break. Because the release is small, the normal containment ventilation systems can maintain the containment atmospheric conditions. Therefore, the emergency fan coolers and containment spray are not required.

As the primary system pressure decreases due to secondary heat removal, the rate of inventory loss decreases and the rate of charging and HPSI injection increases. Since the leak is very slow, the continued operation of all charging and HPSI injection sources can result in maintaining pressure higher than SDC entrance pressure or filling the pressurizer solid. EOI SO23-12-3 directs the operator to throttle the HPSI and charging pumps as necessary to maintain the pressurizer level between 30% and 60% narrow range and to continue to depressurize by cooling via the steam generators in preparation for restarting the RCPs and/or SDC.

The injection phase operates over an extended period due to the reduced makeup requirements to the primary system. Without demands on the RWST inventory from containment spray actuation, the operator has sufficient time to cooldown and depressurize the primary system before transfer to recirculation is required. SDC conditions can be established before RWST depletion.

Event Tree Assumptions

Assumptions	Basis
The feedwater isolation valves close on receipt of a CIAS should containment pressure reach 3.4 psig. A basic event is included in the MFW tree to account for the manual operator action required to override the CIAS signal.	Conservatism.
Shutdown cooling is not modeled because secondary heat removal can be sustained for the 24 hour mission time.	Consistent with NUREG/CR-3511, Calvert Cliffs IREP
Sequence #9 of the Small-Small LOCA event tree transfers to the TWS event tree. Although failure of the RPS precludes use of HPSI (due to RCS pressure above the shutoff head) the charging system can provide both sufficient boration and makeup for the Small-Small LOCA event.	Consistent with NUREG/CR-3511, Calvert Cliffs IREP
A Small-Small LOCA does not deplete the RWST within the 24 hour mission time, therefore, recirculation is not required.	Consistent with NUREG/CR-3511, Calvert Cliffs IREP
Because recirculation is not required for a Small-Small LOCA, containment cooling for sump decay heat removal is not necessary.	Consistent with NUREG/CR-3511, Calvert Cliffs IREP
It is assumed for a Small-Small LOCA, EOI SO23-12-3, Loss of Coolant Accident, is followed and the RCPs are tripped.	EOI SO23-12-3, Loss of Coolant Accident
Transfer to simultaneous hot and cold leg injection is not required for a Small-Small LOCA.	EOI SO23-12-3, Loss of Coolant Accident Forward flow of liquid maintained through the core.

Event Tree Model

The event tree model for Small-Small LOCA event is depicted in Figure 3.1-12. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1.2-16.

The Small-Small LOCA Initiator node (SSL) represents occurrence of the Small-Small LOCA initiating event. The second node Automatic Reactor Trip (K) addresses the requirement for a reactor trip in order to achieve subcriticality. Failure to trip the reactor transfers to the Anticipated Transient Without Scram (TWS) event tree.

Figure 3.1-12: Small-Small LOCA (SSL) Event Tree

SMALL SMALL LOCA EVENT TREE (SSL)

SAN ONOFRE IPE - UNITS 2 & 3

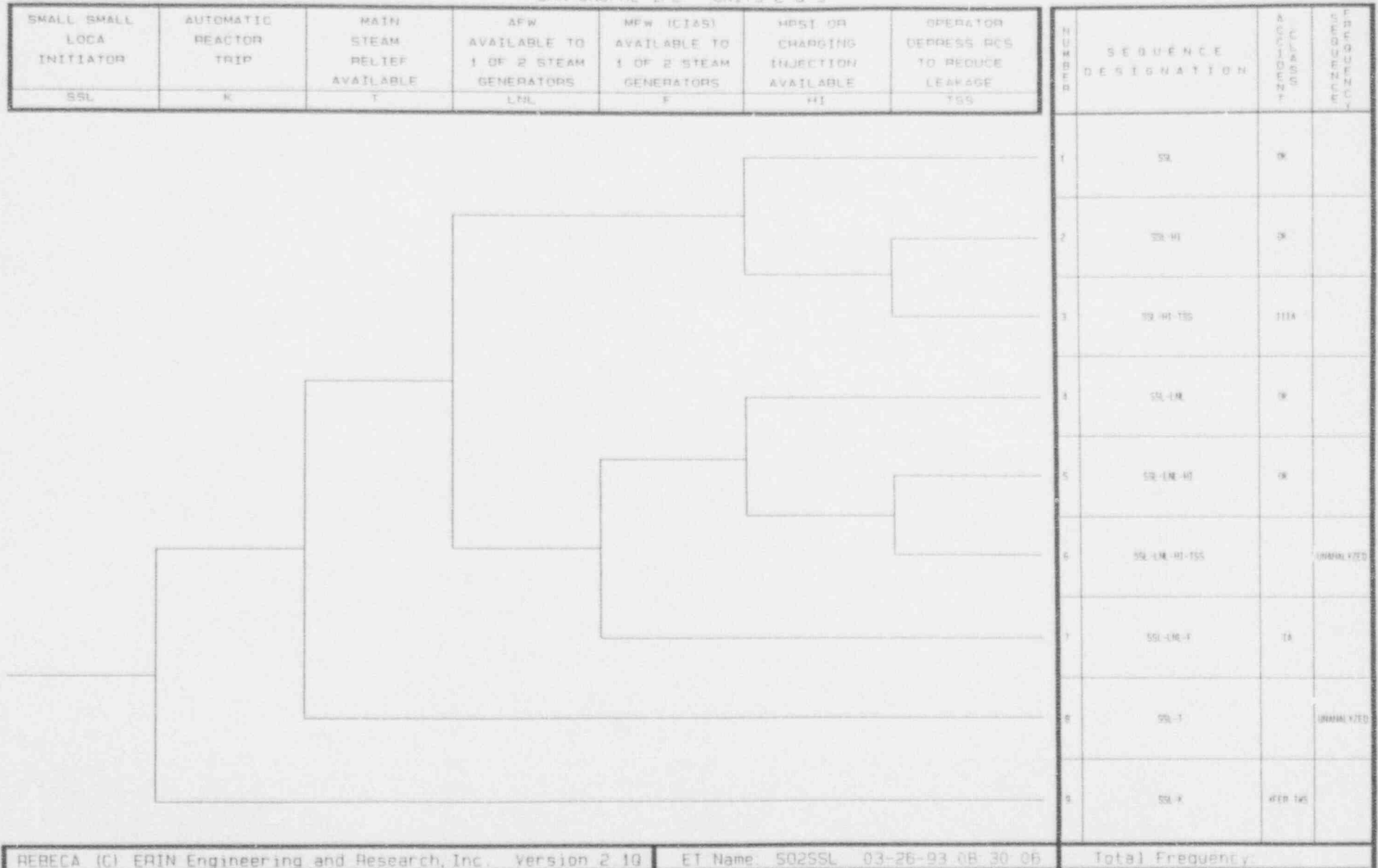


TABLE 3.1-16: SSL EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SLL - Small-Small LOCA

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of reactor trip signal and insertion of all rods into core.	None	S023-12-1, Standard Post Trip Actions, step 3.a
Main Steam Relief Available (T)	RCS Heat Removal	3 of 9 main steam safety valves, 1 of 4 turbine bypass, or 1 of 2 ADVs open to relieve secondary system pressure per steam generator.	Operator throttles ADVs (required) or backs up turbine bypass valve operation, if available.	Plant Specific MAAP Analysis
AFW Available to 1 of 2 Steam Generators (LNL)	RCS Heat Removal	1 of 3 AFW pumps deliver flow to 1 of 2 working steam generators.	None	S023-12-3, Loss of Coolant accident, step 11
MFV Available to 1 of 2 Steam Generators (F)	RCS Heat Removal	1 of 2 MFV pumps deliver flow to 1 of 2 working steam generators.	None	S023-12-3, Loss of Coolant accident, step 11
Operator Depress RCS To Reduce Leakage (TSS)	RCS Inventory	Operator depressurizes RCS to reduce leakage to prevent need for HPSI	Depressurize RCS by using the secondary heat removal systems	S023-12-3, Loss of Coolant accident
HPSI or Charging Injection Available (HI)	RCS Inventory Control RCS Pressure RCS Heat Removal	1 of 3 HPSI pumps or 3/3 Charging pumps inject borated water from the RWST to cold legs.	None	Plant Specific MAAP Analysis

The Main Steam Relief Available (T) node represents removal of secondary system steam through the turbine bypass valves, ADVs, or MSSVs.

The AFW Available To 1 of 2 Steam Generators (LNL) and MFW (CIAS) Available To 1 of 2 Steam Generators (F) nodes represent operation of secondary heat removal systems to remove decay heat from the primary system. Operation of the MFW system for a small-small LOCA is assumed to be precluded by the presence of a CIAS signal. In the event primary system pressure remains high, high pressure injection would be required to maintain RCS inventory. The node HPSI or Charging Injection Available (HI) represents makeup from either the Charging system or HPSI.

The node Operator Depress RCS To Reduce Leakage (TSS) evaluates the potential for operator action to reduce RCS leakage down to a level which can be maintained by normal charging. This is only applicable when adequate secondary heat removal exists.

FAILURE SEQUENCES

Sequences #3 and #6 represent success of main steam relief and secondary heat removal, but failure to reduce leakage and failure of the high pressure safety injection system. Without makeup, the primary system inventory depletes resulting in core uncover. The primary difference between these sequences is that in sequence #3, AFW is providing secondary heat removal and in sequence #8, main feedwater provides secondary heat removal. Accident sequence #3 is defined as IIIA, an accident sequence involving a Small LOCA with loss of primary coolant makeup or loss of adequate heat removal in the injection phase for this case. Sequence #6 is unanalyzed due to the expected isolation of MFW in the presence of a CIAS.

Sequence #7 represents failure due to inadequate secondary heat removal due to unavailability of the MFW and AFW systems. Decay heat removal through the break is inadequate causing primary system temperature to rise. The primary system pressure remains high limiting HPSI injection which results in inventory depletion and core uncover. The functional accident sequence is defined as IA, an accident sequence with loss of adequate heat removal in the injection phase.

Sequence #8 represents inadequate main steam relief. Sequence #8 is unanalyzed due to the negligible likelihood of main steam relief failure.

Sequence #9 represents failure of the RPS to initiate an automatic reactor trip. This sequence transfers to the Anticipated Transient Without Scram (TWS) event tree.

3.1.2.5.5 Steam Generator Tube Rupture

Initiating Group Summary

The Steam Generator Tube Rupture initiating event is characterized by a penetration of the barrier between the RCS and the main steam system and results from a failure of a steam generator U-tube. In terms of break size, the worst case is a postulated double-ended tube rupture of one tube. The steam generator tube rupture event is similar to a small-small LOCA event based on the quantity of inventory lost from the primary system. Concurrent with the loss of coolant is a breach of the primary-secondary boundary. This presents a unique challenge for mitigating the event as reactor coolant is lost outside the containment unless the break flow is limited through operator action.

Plant Response to Initiating Event

Following the steam generator tube rupture, the RCS pressure gradually decreases. The primary-to-secondary leak rate and drop in RCS pressure results in all Chemical Volume and Control System (CVCS) charging pumps being brought on line and reactor trip due to low pressurizer pressure. Following reactor trip, the steam system pressure increases until the turbine bypass valves open to control the main steam system pressure. If turbine bypass is unavailable, secondary steam pressure is controlled either by operator action to open the ADVs or steam generator safety valves opening automatically to control the main steam system pressure.

Diagnosis of the steam generator tube rupture is facilitated by indication from radiation monitors in the blowdown sample lines, blowdown processing sump discharge seal line, and in the condenser air ejector discharge line in addition to changes in the steam generator levels. These monitors initiate alarms in the control room and inform the operator of abnormal activity levels.

EOI SO23-12-4, "Steam Generator Tube Rupture," initially directs the operator to confirm the accident diagnosis. As a result of the low RCS pressure, a SIAS may be generated. The operators are directed to maximize the safety injection flow to the RCS to ensure the RCS inventory is replenished. The combined safety injection and charging pump flows compensate for the loss of reactor coolant inventory through the ruptured tube. During this period, the main steam system pressure is reduced and the steam generator safety valves reseal.

Per SO23-12-4, the operators initiate lowering the RCS temperature and pressure through use of the MFW or AFW systems, pressurizer spray, and secondary steam relief. The affected

steam generator is cooled to less than 530°F prior to isolation to prevent MSSVs from lifting.

The operators identify and isolate the affected steam generator by closing the main steam isolation, main steam isolation bypass, atmospheric dump, main feed isolation, AFW blowdown and sample isolation valves to the steam generator.

With successful isolation of the steam generator from the secondary system, the ruptured steam generator becomes an extension of the primary system. As long as primary system pressure exceeds the pressure of the isolated steam generator, flow continues from the RCS to the steam generator. The steam generator safety valves are the only un-isolated (following successful manual isolators) boundary between the primary system and the environment. Operator actions are taken to prevent steam generator overfill and further radioactivity release. Safety injection pumps and charging are sequentially stopped as conditions permit. The process continues with control of RCS pressure and makeup to maintain constant inventories in the pressurizer and steam generator until SDC conditions are met.

Event Tree Assumptions

The following assumptions were used in the event tree construction of the plant response to a steam generator tube rupture event:

Assumptions	Basis
The primary to secondary leakage due to the steam generator tube rupture results in a gradual decrease in pressurizer level and pressure. RCS pressure does not reach the pressurizer safety valve setpoint at 2525 psia, and the valves do not open.	FSAR Section 15.6.3.2
Emergency condensate is not credited.	Conservatism
For sequences in which there is no early depressurization, makeup from the charging pumps is not credited.	Conservatism. This maintains flexibility in the model for adding long term makeup from the RWST.
Steam generator tube rupture event is defined as a double ended rupture of 1 tube. Rupture of multiple tubes is not considered.	Consistent with Surry and Sequoyah analysis in NUREG/CR-4550

Assumptions	Basis
Failure to depressurize the RCS results in unacceptable leakage into the secondary system whether or not the steam generator is isolated. Because inventory does not accumulate in the sump for a steam generator tube rupture event, recirculation cannot be established. Consequently core damage is assumed if the RCS is not cooled/depressurized to shutdown cooling or the RWST is not refilled.	In order to capture the impacts of radioactive release, it is necessary to evaluate the consequences of failing to permit release into the secondary system. This enables radioactive release to be captured in the Level II analysis. This is conservative since actions could be taken to mitigate core damage by permitting contamination of the secondary system.
Successful depressurization can be accomplished with ADVs or SBCS.	Plant Specific MAAP Analysis
Gagging a stuck open main steam safety valve is not credited.	Conservatism

Event Tree Model

The event tree model for Steam Generator Tube Rupture is depicted in Figure 3.1-13. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1-17.

The **Steam Generator Tube Rupture Initiator** node (SGR) represents occurrence of the initiating event. The second node **Automatic Reactor Trip** (K) addresses the need for a reactor trip in order to achieve subcriticality. Failure to trip the reactor transfers to the Anticipated Transient Without Scram (TWS) event tree.

The **Main Steam Relief Available** (T) node represents removal of secondary system steam through the turbine bypass valves, ADVs, or MSSVs. Steam relief is required early in the accident for secondary heat removal and later in conjunction with MFW or AFW for heat removal through the unaffected steam generator.

The node **Operator Diagnoses SGTR and Begin Depres Early** (YDE) evaluates the potential for prompt operator action to depressurize the intact steam generator or spray the pressurizer to reduce RCS pressure and thereby reduce flow out the broken steam generator tube. This early action prevents steam generator overfill and minimizes the potential for a stuck open main steam safety valve. If this action fails, then a stuck open main steam safety valve is assumed, resulting in a more difficult event to control.

Figure 3.1-13: Steam Generator Tube Rupture (SGR) Event Tree

STEAM GENERATOR TUBE RUPTURE EVENT TREE (SGR)

SAN ONOFRE IPE - UNITS 2 & 3

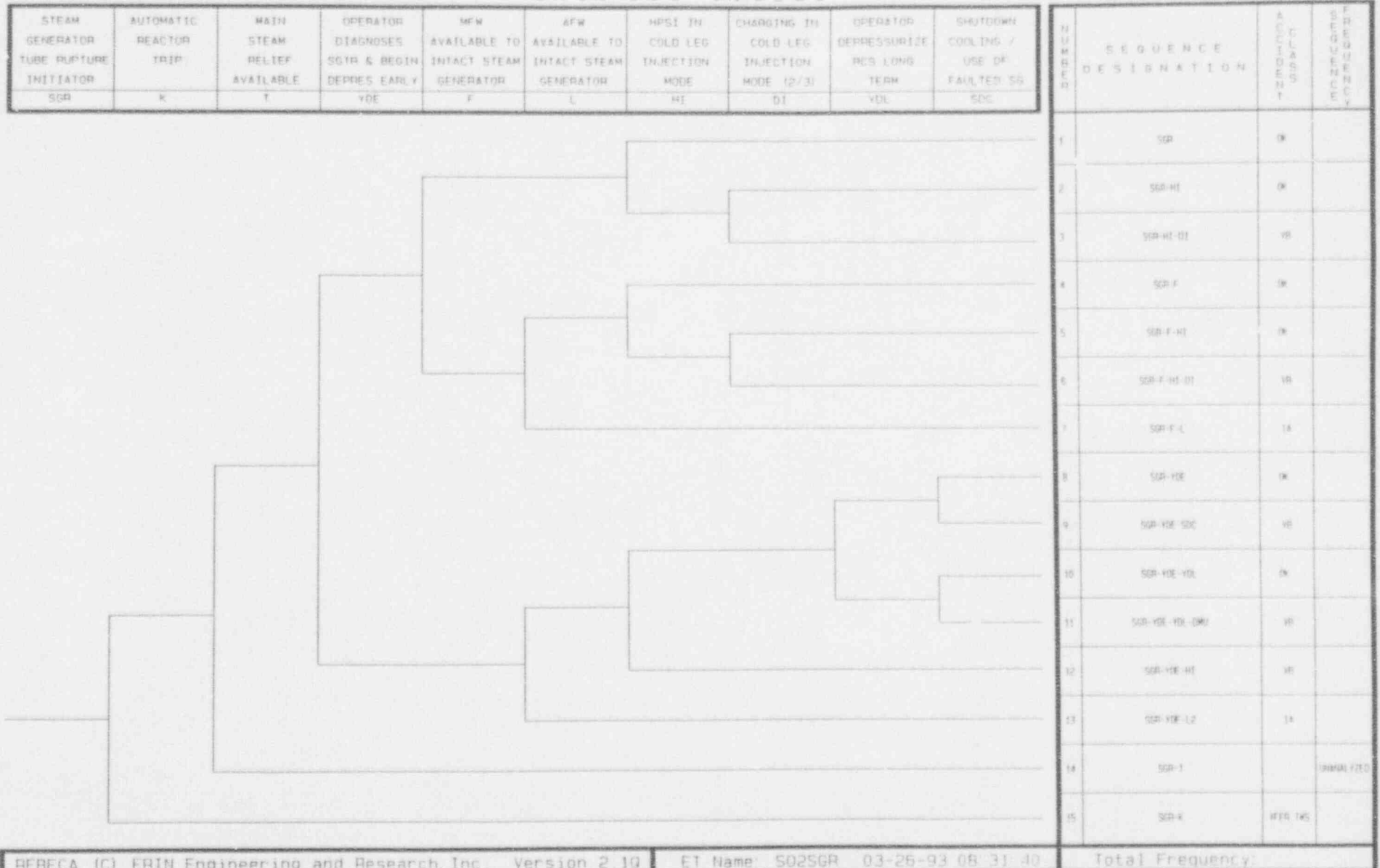


TABLE 3.1-17: SGR EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SGR - Steam Generator Tube Rupture

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of an automatic reactor trip signal and insertion of rods into core.	None	S023-12.1, Standard Post Trip Actions, step 3.a
Main Steam Relief Available (T)	RCS Heat Removal RCS Pressure RCS Inventory	One main steam safety valve, one turbine bypass, or one ADV associated with the intact steam generator opens to relieve secondary system pressure.	Operator throttles ADVs (required) or backs up turbine bypass valve operation.	Plant Specific MAAP Analysis
Operator Diagnoses SGTR and Begin Depress Early (YDE)	RCS Inventory Control	Operator closes MSIV of faulted S/G, stops 2 RCPs in affected loop, stops feedwater flow to damaged S/G & opens unaffected S/G ADV or uses steam bypass control system to begin plant cooldown. Cooldown and depressurization must be completed before steam generator overfill and water is passed through main steam safety valves.	Operate SBSCS or open ADV on intact steam generator. Start pressurizer spray. Control cooldown.	S023-12.4, Steam Generator Tube Rupture
MFWD Available to 1 of 2 Steam Generators (F)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 3 MFWD pumps deliver flow to 1/1 intact steam generator.	None	S023-12.4, Steam Generator Tube Rupture, step 7.b
AFW Available to 1 of 2 Steam Generators (L)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 3 AFW pumps deliver flow to intact steam generator.	Manual initiation of EFAS if not automatically actuated.	S023-12.4, Steam Generator Tube Rupture, step 7.b
HPSI in Cold Leg Injection (HI)	Inventory Control	1 of 3 HPSI pumps inject borated water from RWST into cold legs.	None	S023-12.4, Steam Generator Tube Rupture, step 5
Charging in Cold Leg Injection (2/3) (DI)	Inventory Control	2 of 3 charging pumps inject borated water from RWST into cold legs.	None	S023-12.4, Steam Generator Tube Rupture

TABLE 3.1-17: SGR EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SGR - Steam Generator Tube Rupture

Node	Critical Safety Function	Success Criteria	K ₁ - Operator Actions	Reference(s)
Operator Depressurize RCS Long Term (YOL)	RCS Pressure RCS Inventory	Operator closes MSIV of faulted S/G, stops RCPs in affected loop, stops feedwater flow to damaged S/G & uses SBCS or opens unaffected S/G ADV to begin plant cooldown. Cooldown and depressurization must be completed before RWST depletion.	Operator implements depressurization, RCS cooldown and S/G isolation	SO23-12.4, Steam Generator Tube Rupture, Steps 7-11
Shutdown Cooling/Use of Faulted SG	RCS Inventory	Enter shutdown cooling before RAS (late depressurization) or use faulted steam generator to depressurize.	Refill RWST.	Plant Specific MAAP Analysis

The MFW Available to Intact Steam Generator (F) and AFW Available to Intact Steam Generator (L) nodes represent operation of secondary heat removal systems to remove heat rapidly from the primary system.

Following the successful reactor trip, the loss of coolant through the ruptured tube requires makeup. Primary system pressure remains high, requiring high pressure injection. The nodes HPSI in Cold Leg Injection Mode (HI) and Charging in Cold Leg Injection Mode 2/3 (DI) represent the high pressure injection requirement during the tube rupture event. Charging is only an acceptable backup, if early depressurization has been successful.

The node Operator Depressurize RCS Long Term (YDL) evaluates the potential for long term stabilization if early efforts were unsuccessful. Operator action to depressurize late can permit entry into shutdown cooling before RAS occurrence and subsequent RWST depletion.

The node Shutdown Cooling/Use of Faulted SG evaluates the potential for controlling RCS inventory long-term or depressurizing with the faulted SG. With successful isolation of the faulted steam generator and operability of ADVs or SBCs, the RCS can be depressurized to shutdown cooling conditions.

FAILURE SEQUENCES

Sequences #3 and #6 represent successful reactor trip and heat removal via the AFW or MFW systems, but failure to replenish the primary system with either HPSI or charging. RCS losses through the ruptured tube can not be made up without high pressure safety injection or charging. The functional accident sequence is defined as VB, steam generator tube rupture leading to loss of effective primary coolant inventory makeup.

Sequence #7 represents core damage occurrence due to failure of the secondary heat sink. RCS heat removal is lost resulting in core damage. The functional accident sequence designation is defined as IA, accident sequence with loss of adequate heat removal in the injection phase.

Sequence #9 represent successful reactor trip, heat removal via the AFW system, operator action to successfully depressurize late and RCS makeup with HPSI, but failure of long term inventory control using shutdown cooling. Long term makeup from the RWST is not credited. The functional accident sequence is defined as VB, steam generator tube rupture leading to loss of effective primary coolant inventory makeup.

Sequence #11 represent successful reactor trip, heat removal via the AFW system, unsuccessful early and late depressurization, but successful RCS makeup with HPSI. Hardware failures prevent long

term inventory control which leads to core damage. The functional accident sequence is defined as VB, steam generator tube rupture leading to loss of effective primary coolant inventory makeup.

Sequence #12 represents successful reactor trip and heat removal via the AFW or MFW systems, but failure to depressurize early followed by failure to replenish the primary system with HPSI. RCS losses through the ruptured tube cannot be made up without high pressure safety injection. The functional accident sequence is defined as VB, steam generator tube rupture leading to loss of effective primary coolant inventory makeup.

Sequence #13 represents successful reactor trip with core damage occurrence due to failure of the secondary heat removal. In this sequence, MFW is not available because early depressurization was not successful and steam generator overfill occurred failing the MFW turbine driven pumps. RCS heat removal is lost resulting in core damage. The functional accident sequence designation is defined as IA, accident sequence with loss of adequate heat removal in the injection phase.

Sequence #14 represents inadequate main steam relief. This sequence is unanalyzed due to the negligible likelihood of main steam relief failure.

Sequence #15 represents failure of the RPS to initiate an automatic reactor trip. This sequence transfers to the Anticipated Transient Without Scram (TWS) event tree.

3.1.2.6 Special Event Trees

3.1.2.6.1 Interfacing System LOCA

Initiating Group Summary

The Interfacing System LOCA (VL) initiating event group includes events which result in significant leakage from the primary system through valves which normally isolate the high pressure reactor coolant system from low pressure piping of adjoining systems. Such an event may preclude long term cooling using recirculation due to inventory loss outside of containment and provides a potential avenue for containment bypass.

No event tree is developed for analysis of the Interfacing LOCA initiating event. It is conservatively assumed that no mitigation is available to isolate the break once the event occurs leading to eventual depletion of RCS makeup and subsequent core damage. The event occurrence is assumed to lead directly to core damage at a frequency of occurrence described in Section 3.1.1.5.

3.1.2.6.2 Reactor Pressure Vessel Rupture

Initiating Group Summary

The Reactor Pressure Vessel Rupture (VR) initiating event group is characterized by an event which results in spontaneous catastrophic failure of the reactor pressure vessel.

No event tree is developed for the reactor pressure vessel rupture initiating event. It is assumed that no mitigation is available to recover from the vessel rupture event leading to loss of core cooling and core damage. The event occurrence is assumed to lead directly to core damage at a frequency of occurrence described in Section 3.1.1.5.

3.1.2.7 Support System Event Trees

The SONGS 2/3 systems which provide support to components in frontline systems were evaluated as potential initiators in section 3.1.1.5, Support System and Special Initiating Events. Systems whose failure would disrupt normal plant operations, impact the availability of plant safety systems, and require a response not enveloped by the other plant initiators were identified. Based on the screening evaluation of SONGS 2/3 support systems, the following support system initiating events were selected for quantification.

- Loss of a Single 125 VDC Bus
- Loss of Component Cooling Water

In general, the plant response to a support system failure is equivalent to a general transient with the power conversion system available. The general support system event tree used to evaluate most of the support system initiators is shown in Figure 3.1-14. The support system event tree is used with a unique flag set and initiating event frequency to characterize the transient in terms of the plant response to the failed support system. The safety functions and success criteria for the loss of support system event tree nodes are presented in Table 3.1-18. Each of the support system initiators, the critical safety functions challenged, and the plant response are discussed below.

3.1.2.7.1 Loss of Single 125 VDC Bus

The SONGS 2/3 125 VDC system consists of four DC subsystems. Failure of one 125 VDC subsystem results in loss of the associated 120 VAC inverter bus. If the loss of DC bus D1 or D2 occurs, an automatic plant trip will occur with significant loss of safety related equipment results. The SS event tree is quantified for loss of a single 125 VDC bus.

3.1.2.7.2 Loss of Component Cooling Water

The CCW system at SONGS 2/3 is a two train closed loop system which supplies cooling water to various plant equipment. During normal operation, the CCW system supplies cooling water to the letdown heat exchangers, the RCP motor and seals, and the CEDMs. Loss of the entire CCW system results in an immediate manual plant trip due to loss of cooling to these components.

The only significant challenge to the plant posed by loss of CCW is the potential for an RCP seal LOCA which could not be mitigated. If the operator response to a loss of CCW event did not include tripping of the RCPs, then the RCP seals could overheat, resulting in an RCP seal LOCA. Without CCW available, HPSI, LPSI, and Containment Spray pumps would be unavailable for RCS inventory makeup and core damage could ensue.

The loss of CCW event is analyzed using a simplified event tree which addresses the key aspects of a loss of CCW induced RCP seal LOCA: annunciator and operator response.

Event Tree Model

The event tree model for Loss of Component Cooling Water (CCW) is depicted in Figure 3.1-15. The safety function and success criteria for each constituent node of the event tree are presented in Table 3.1.2-19.

The **Loss of CCW** node (CCW) represents occurrence of the initiating event. The second node **Automatic Reactor Trip (K)** addresses the need for a reactor trip in order to achieve

Figure 3.1-14: Support System (SS) Event Tree

SUPPORT SYSTEM INITIATOR EVENT TREE (SS)

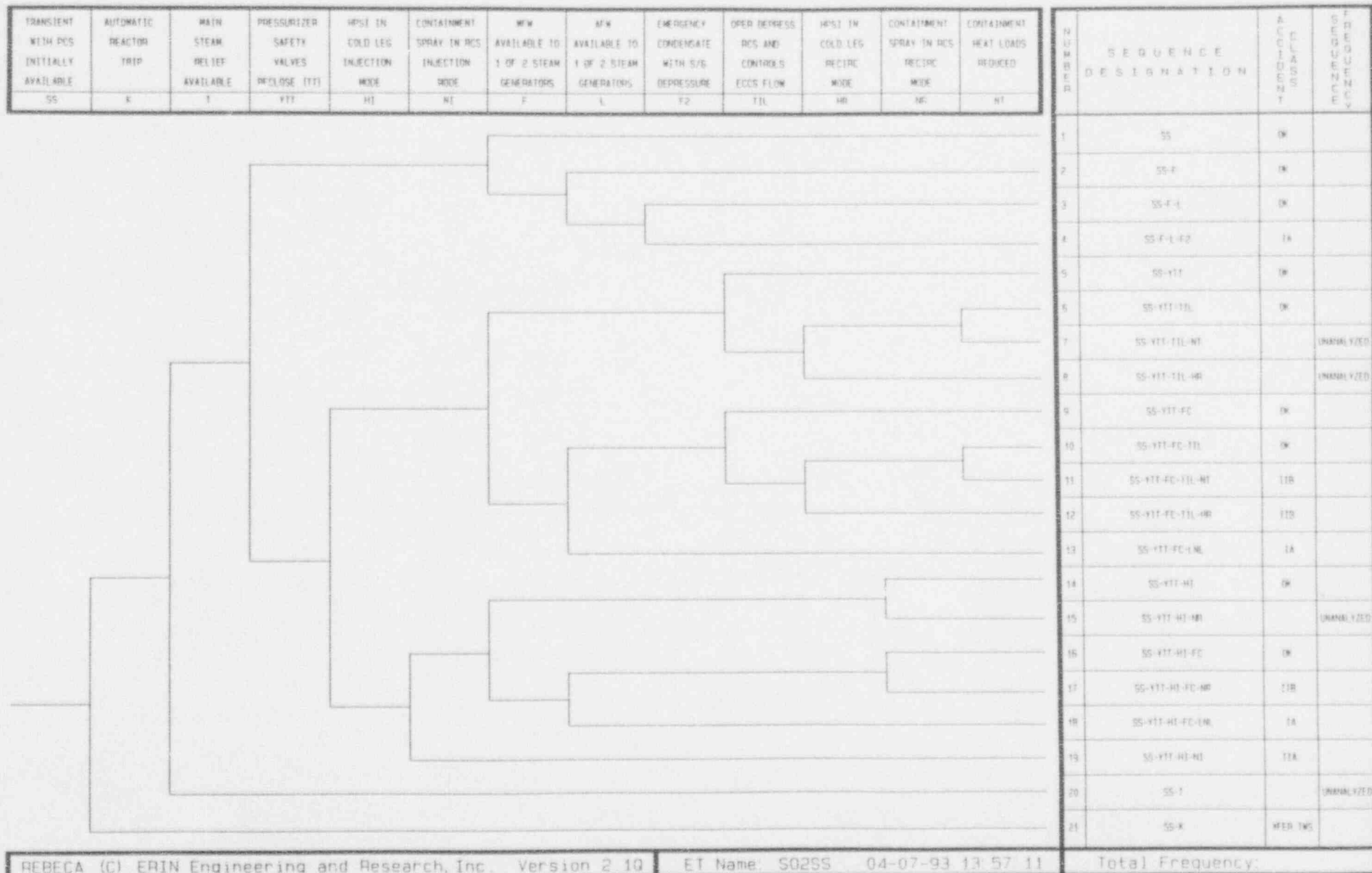


TABLE 3.1-18: SS EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: SS - Support System Initiator

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Automatic Reactor Trip (K)	Reactivity Control	Generation of a reactor trip signal and insertion of all control rods into core.	None	E01 S023-12-2, Reactor Trip Recovery, step 1.c
Main Steam Relief Available (T)	RCS Heat Removal RCS Pressure RCS Inventory	3 of 9 main steam safety valves, 1 of 4 turbine bypass or 1 of 2 ADVs per steam generator open to relieve secondary system pressure.	Operator throttles ADVs (required) or backs up turbine bypass valve operation.	Plant Specific MAAP Analysis, S023-12-1, Standard Post Trip Actions, step 8.c and S023-12-2, Reactor Trip Recovery, step 6.a
Pressurizer Safety Valves Reclose (TT) (YTT)	RCS Inventory	2 of 2 pressurizer safety valves reclose following events requiring opening (assumed to be 10% of TT events).	None	N/A
HPSI in Cold Leg Injection Mode (III)	Reactivity Control RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject borated water from the RWST to 2 of 4 cold legs.	None	S023-12-3, Loss of Coolant Accident
Containment Spray in RCS Injection Mode (NI)	Reactivity Control RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 2 Containment Spray pumps inject borated water from the RWST to 2 of 4 cold legs.	Align containment spray for RCS injection.	S023-12-3, Loss of Coolant Accident
MFW Available to 1 of 2 Steam Generators (F)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 2 MFW pumps delivers flow to 1 of 2 steam generators.	Control feedwater flow to SGs.	S023-12-2, Reactor Trip Recovery, Attachment 1, step 6.a
AFW Available to 1 of 2 Steam Generators (L)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 3 AFW pumps delivers flow to 1 of 2 steam generators.	Manually actuate EFAS if not automatically initiated.	S023-12-2, Reactor Trip Recovery, Step 8.a

TABLE 3.1-18: SS EVENT TREE SUCCESS CRITERIA (continued)

INITIATING EVENT GROUP: SS - Support System Initiator

Node	Critical Safety Function	Success Criteria	Key Operator Actions	Reference(s)
Emergency Condensate with S/G Depressurized (F2)	RCS Heat Removal RCS Pressure RCS Inventory	1 of 4 condensate pumps delivers flow to 1 of 2 depressurized (<500 psia) steam generators.	Manually align low pressure alternate feedwater.	S023-12-9, Functional Recovery, Attachment 8, Step 6
Oper Depress RCS and Controls ECCS Flow (TIL)	RCS Pressure RCS Inventory	Operator initiates cooldown and limits/ terminates ECCS per procedures to prevent need for recirculation from containment sump.	Cooldown RCS with MFW/AFW and shut off ECCS pumps as required.	S023-12-3, Loss of Coolant Accident
HPSI in Cold Leg Recirc Mode (HR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 3 HPSI pumps inject water from containment sump into 2 of 4 cold legs before RWST depletion.	Operator isolates RWST after automatic RAS HPSI realignment	S023-12-3, Loss of Coolant Accident, Attachment 5
Containment Spray in RCS Recirc Mode (NR)	RCS Inventory RCS Heat Removal (Induced LOCA only)	1 of 2 containment spray pumps inject water from containment sump into 2 of 4 cold legs before RWST depletion.	Operator isolates RWST after automatic RAS HPSI realignment	S023-12-3, Loss of Coolant Accident, Attachment 5
Containment Heat Loads Reduced (NT)	Containment Pressure	1 of 4 containment emergency fan coolers or 1 of 2 containment spray pumps taking suction from RWST	None	Plant Specific MAAP Analyses For CEFCs/CS Heat Removal

Figure 3.1-15 Loss of CCW (CCW) Event Tree

LOSS OF COMPONENT COOLING WATER EVENT TREE (CCW)

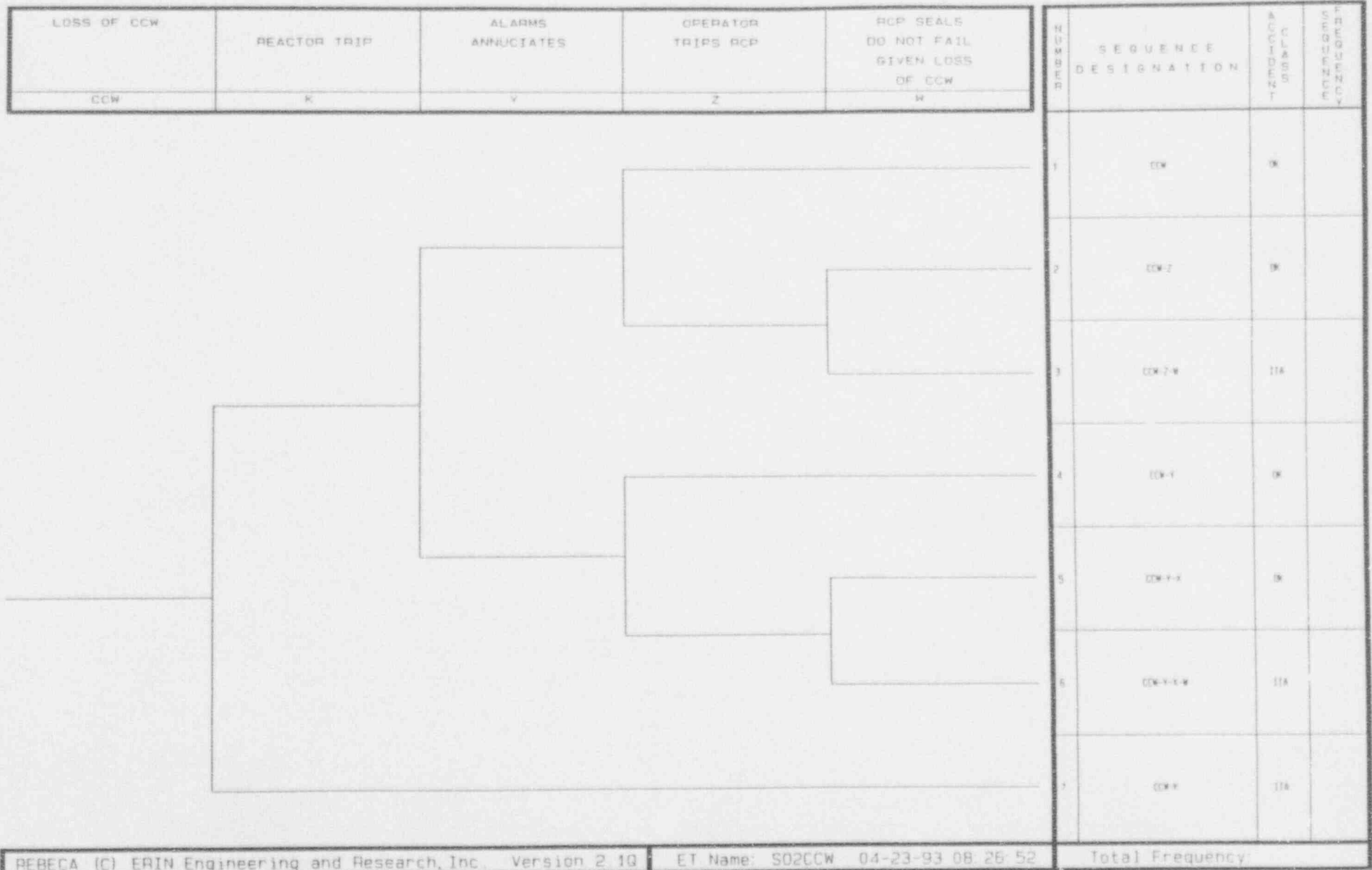


TABLE 3.1-19: CCW EVENT TREE SUCCESS CRITERIA

INITIATING EVENT GROUP: CCW - Loss of CCW Initiator

Node	Critical Safety Function	Success Criteria	Operator Actions	Reference(s)
Reactor Trip (K)	Reactivity Control	Generation of a reactor trip signal and insertion of all control rods into core.	Operator manually trips reactor	EOI S023-12-2, Reactor Trip Recovery, step 1.c
Alarm Annunciates (Y)	RCS Inventory	RCP high seal temperature alarm annunciates in control room.	None	N/A
Operator Trips RCPs (Z)	RCS Inventory	Operator trips four of four RCPs within 30 minutes of alarm to prevent seal challenge due to high temperatures.	Trip all four RCPs based on high thrust bearing temperature.	S023-13-7, Loss of Component Cooling Water /Saltwater Cooling
RCP Seals Do Not Fail Given Loss of CCW (W)	RCS Inventory	Four of four RCP seals remain intact while RCPs running without CCW cooling. Conservatively assumes that failure always occurs.	None	N/A

subcriticality. Failure to trip the reactor transfers to the Anticipated Transient Without Scram (TWS) event tree.

The next node **Alarm Annunciates** (Y) evaluates the likelihood of a failure in the RCP seal temperature alarm system which could result in inadequate operator notification. The node **Operator Trips RCP** (Z) evaluates operator response in events with and without the RCP seal temperature alarm. Finally, a node **RCP Seals Do Not Fail Given Loss of CCW** (W) evaluates the likelihood of RCP seal failure given failure to trip. For this analysis, this likelihood of failure of this node is assumed to be unity (1.0).

FAILURE SEQUENCES

Sequences #3 and #6 represent the potential RCP seal LOCA sequences of interest. One is due to operator error, with an alarm (sequence #3) and the other is with failure of the alarm (sequence #6).

Sequence #7 represents failure of the RPS to initiate an automatic reactor trip. The functional accident sequence is defined as IIA, accident sequences initiated by an induced LOCA with loss of primary makeup or loss of adequate secondary heat removal.

3.2 System Analysis

Extracts from detailed system analyses are summarized in this section. System analyses were performed for systems identified for evaluation based on event tree logic models described in section 3.1.2. The detailed system analysis reports include thorough evaluations of systems including the systems' function, normal and abnormal operation, dependencies, instrumentation and controls, test and maintenance, Technical Specification limitations, operator interface, walkdown and cognizant engineer interviews, and operating experience. Fault tree logic models developed based on the detailed analyses are included as part of the detailed analysis reports. The system analyses and fault trees represent the current design of SONGS Units 2 and 3 (Cycle 6).

The frontline and support systems analyzed include the following:

- Auxiliary Feedwater (AFW)
- Main Feedwater and Condensate (MFW/COND)
- Main Steam (MSS)
- Safety Injection Tanks (SIT)
- High Pressure Safety Injection (HPSI)
- Low Pressure Safety Injection (LPSI)
- Chemical Volume and Control (CVCS)
- Containment Spray and Containment Emergency Fan Coolers (CS/CEFC)
- Reactor Coolant System Pressure Control (RCSPC)
- Component Cooling Water (CCW)
- Saltwater Cooling (SWC)
- Instrument Air and Nitrogen (IA)
- Heating, Ventilation and Air-Conditioning (HVAC)
- Electric Power (EP and AC/DC)
- Actuation Signals (RPS/ESFAS)
- Containment Isolation (CI)

As evident from the list of systems analyzed, elemental systems of the Emergency Core Cooling System (ECCS) were modeled separately. Several non-essential support systems were not developed in detail. These support systems included Turbine Plant Cooling Water, Circulating Water, Nitrogen and Service Water.

Descriptions of the systems and simplified P&IDs (Section 3.2.1) and dependency matrices (Section 3.2.2) are reported as outlined in NUREG-1335. System fault trees are not provided in the submittal as specified in NUREG-1335.

3.2.1 Auxiliary Feedwater

The function of the AFW System modeled in the IPE is to supply feedwater to the steam generators for RCS Heat Removal.

The AFW system consists of three 100% capacity pumps, associated piping, controls, valves, and instrumentation. Two pumps (P-141, P-504) are electric motor-driven with each pump discharge piping aligned to one of the two steam generators. The discharge lines from the motor-driven AFW pump trains are equipped with AC motor-operated control valves (HV-4712, 4713) and AC, electro-hydraulic bypass control valves (HV-4762, 4763).

The third pump (P-140) is steam-driven and discharges to both steam generators via the same piping used by the motor-driven pumps. The discharge lines from the turbine-driven pump P-140 are equipped with DC motor-operated control valves (HV-4705, 4706). Flow-limiting, cavitating venturi at the discharge of each AFW pump prevents pump runout conditions by limiting the discharge flow to 1000 gpm.

Steam supply to the turbine-driven AFW pump is provided from two main steam lines between the containment penetrations and the main steam isolation valves. Each of the steam supply lines to the turbine includes a check valve and a pneumatically-actuated steam supply isolation valve (HV-8200, 8201). The steam from both supply lines combines before entering the turbine via a stop valve (HV-4716) and a governor valve (SV-4700). Both pneumatically-actuated isolation valves, the stop valve, and the controls to the governor are supplied with power from an emergency DC power source.

Each of three AFW pumps takes suction from a seismic Category I condensate storage tank (T-121) through separate suction lines. Makeup to the 150,000 (nominally 144,000) gallon tank is available from the 500,000 gallon condensate storage tank (T-120) and three 500,000 gallon demineralized water storage tanks (T-266, T-267, T-268). Mini-flow (100 gpm) recirculation lines from

each AFW pump discharge pipe return to condensate storage tank T-121.

Two parallel containment isolation valves are provided in each AFW line to each steam generator immediately outside containment. One isolation valve in each parallel path is AC electro-hydraulic powered (HV-4714,4731) while the other isolation valve is DC motor-powered (HV-4715,4730). This DC/AC power arrangement assures the flow paths to both steam generators are operable if valve failures occur concurrently with either a loss of AC or DC power.

Each AFW line passes through the containment wall and connects to a main feedwater line between a check valve and the steam generator inlet nozzle. The AFW lines include check valves close to the steam generator inlet nozzles. The check valves in both the MFW lines and the AFW lines provide system separation and reduce the likelihood of a steam generator blowdown if a MFW or AFW line break occurs.

During normal operations at power the AFW System is in standby with both the control valves and isolation valves closed. One steam supply valve to the turbine pump is also normally closed. During emergency conditions, the AFW system is automatically actuated by an EFAS on low steam generator level. The EFAS logic: 1) Starts the auxiliary feedwater pumps; 2) determines which steam generator(s) is intact and 3) opens the auxiliary feedwater valves (and a steam supply to turbine pump) to the intact steam generator(s). If the water level in a steam generator returns to the 30% narrow range level setpoint, AFW System discharge and isolation valves to the steam generator automatically close to prevent steam generator overfill. Operators assume control manually after initial EFAS response by overriding EFAS and throttling flow control valves to maintain steam generator water levels relatively constant.

Actuation of both a MSIS and an EFAS provides indication of a faulted steam generator condition. Initiation of an MSIS automatically shuts all remotely actuated AFW control valves and isolation valves. EFAS logic overrides the closure of a valve closed by an MSIS. The EFAS logic automatically isolates AFW flow to the faulted steam generator and controls flow to the intact steam generator.

A differential pressure type flow element is installed in each AFW supply line to a steam generator just upstream of the containment isolation valves. Flow indicators provide flow indication in the control room. Flow monitored by one of the flow elements is recorded on a recorder.

If required, one motor-driven pump may be aligned to feed either of the two steam generators or both simultaneously by opening manually-operated isolation valves in the 4" cross-tie that connects the two discharge lines of the motor-driven pumps.

The support systems for the AFW system include AC power, DC power, instrument air, the Plant Protection System and the Main Steam System. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the AFW System is presented in Figure 3.2-1.

3.2.2 Main Feedwater and Condensate System

The function of the MFW and Condensate System modeled in the IPE is to supply feedwater to the steam generators for RCS Heat Removal.

The MFW and Condensate System includes PCS components from the hotwell to the feedwater supply side of the steam generators. Four 33% capacity electric motor-driven condensate pumps (P-050,051,052,053) take suction from the four condenser hotwells and discharge to a common header. Flow from the common header passes through full flow condensate polishing demineralizers (FFCPD) to parallel paths including the air ejector condenser, gland steam condenser, blowdown heat exchanger, and a parallel bypass to the feedwater heaters. A normally closed cross-connect between Unit 2 and Unit 3 connects condensate downstream of the FFCPD to the opposite unit enabling condensate from one unit to be supplied to the opposite unit.

Two parallel 60% capacity turbine-driven feedwater pumps (P-062,063) deliver condensate from the first five point heaters through the high pressure heater and into a common feedwater header. Two feedwater injection lines branch off the common header, one to each steam generator. Flow through each injection line passes through a feedwater regulating valve (FV-1111,1121) and two isolation valves: feedwater isolation valves (HV-4052, HV-4048) and feedwater block valves (HV-4051, HV-4047). The regulating valve in each line is equipped with a bypass line which is normally isolated by an air-operated control valve (HV-1105,1106).

During normal plant operation at power the MFW and Condensate System is operating with condensate and feedwater pumps delivering condensate from the condenser hotwells to the steam generators. Nominally, three of the four condensate pumps are normally in operation along with both main feedwater pumps at 100% power. Flow to the steam generators is controlled by the feedwater regulating valves and the bypass valves. Each steam generator is equipped with a separate Feedwater Control System

Figure 3.2-1: AFW Simplified P&ID

SAN ONOFRE UNITS 2/3 AUXILIARY FEEDWATER SYSTEM

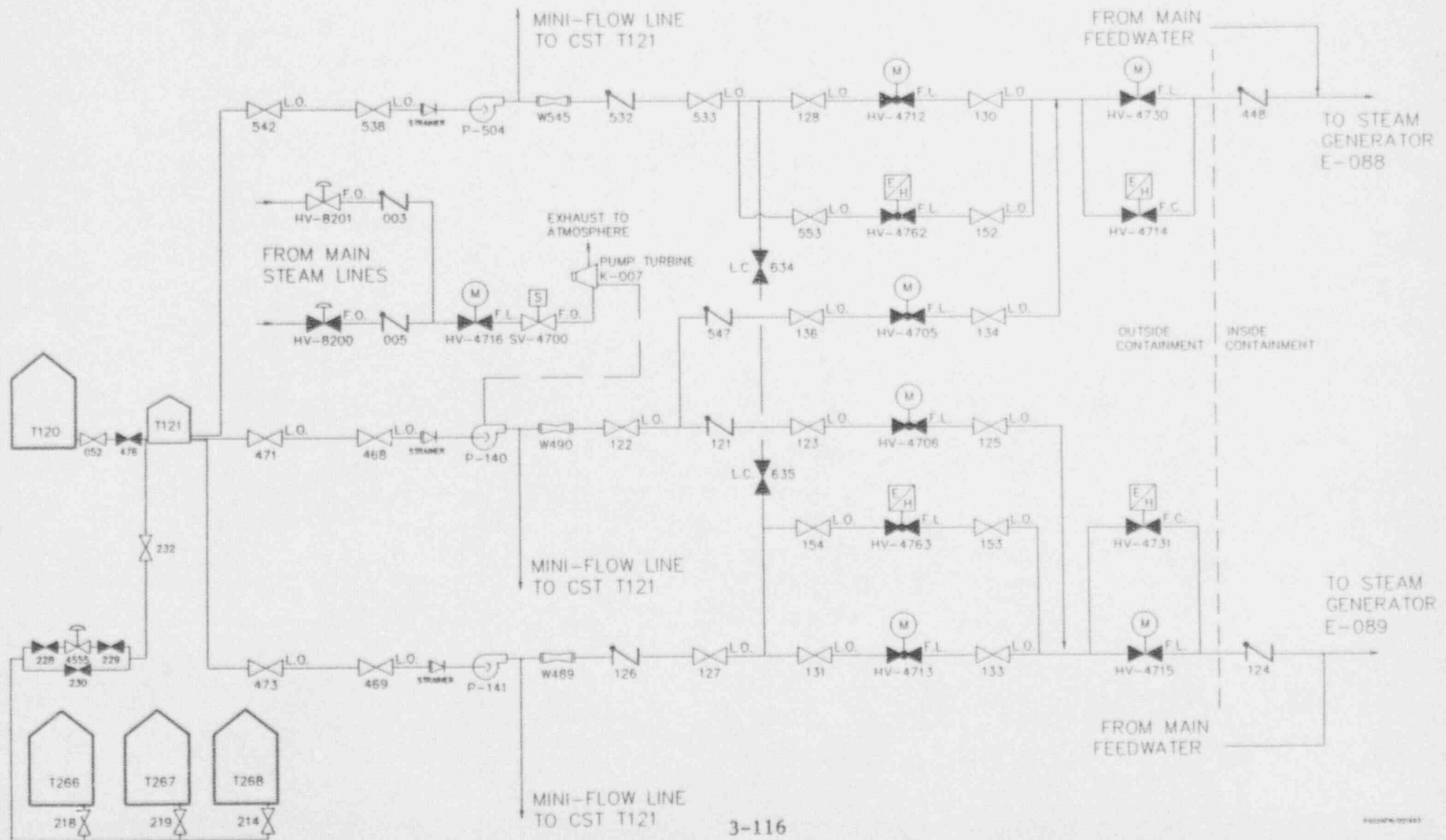


TABLE 3.2-1

SYSTEM DEPENDENCY TABLE

	AFW	MFW	MSS	SIT	HPSI	LPSI	CVCS	CS & CEFC	RCSPC	CCW	SWC	IA	HVAC	ACPWR	DCPWR	PPS	CI
AFW																	
MFW																	
MSS	X	X															
SIT																	
HPSI						1	1	1									
LPSI								2									
CVCS																	
CS/CEFC																	
RCSPC																	
CCW					X	X		X									
SWC										X							
IA		X		X					X								
HVAC							4					3		X			
ACPWR	X	X	X		X	X	X	X	X	X	X	X	X		X	X	X
DCPWR	X	X	X		X	X	X	X		X	X	X		X			
PPS	X		X		X	X	X	X					X	X			X
CI																	

<X> Direct Dependency

<1> RWST within HPSI system boundary (and Sump for LPSI and CS).

<2> CS ECCS injection path within LPSI system boundary.

<3> Turbine Plant Cooling Water within HVAC system boundary.

<4> Emergency Chilled Water within HVAC system boundary.

NOTE : Systems listed across the top row have dependencies on system listed in the left column. Dependencies are identified by an "X" for system dependency. Other dependencies, i.e., shared components or undeveloped systems, are identified by number and are described in notes.

(FWCS). The FWCS monitors steam flow, feedwater flow, and steam generator level in order to maintain the proper level in the steam generators. At low reactor power, the FWCS controls feedwater by operating the feedwater regulating valves. At high power, feedwater flow is controlled by adjusting feedwater turbine speed.

During abnormal operations following a reactor/turbine trip, the FWCS is overridden by Reactor Trip Override (RTO) Signal. The RTO controls reduce the feedwater turbine pump speed, closes the feedwater regulating valves, and opens the regulating bypass valves to match reduction in feedwater required post-trip and prevent steam generator overfill. Mini-flow paths for both the Main Feedwater pumps and the condensate pump open to circulate condensate back to the hotwell.

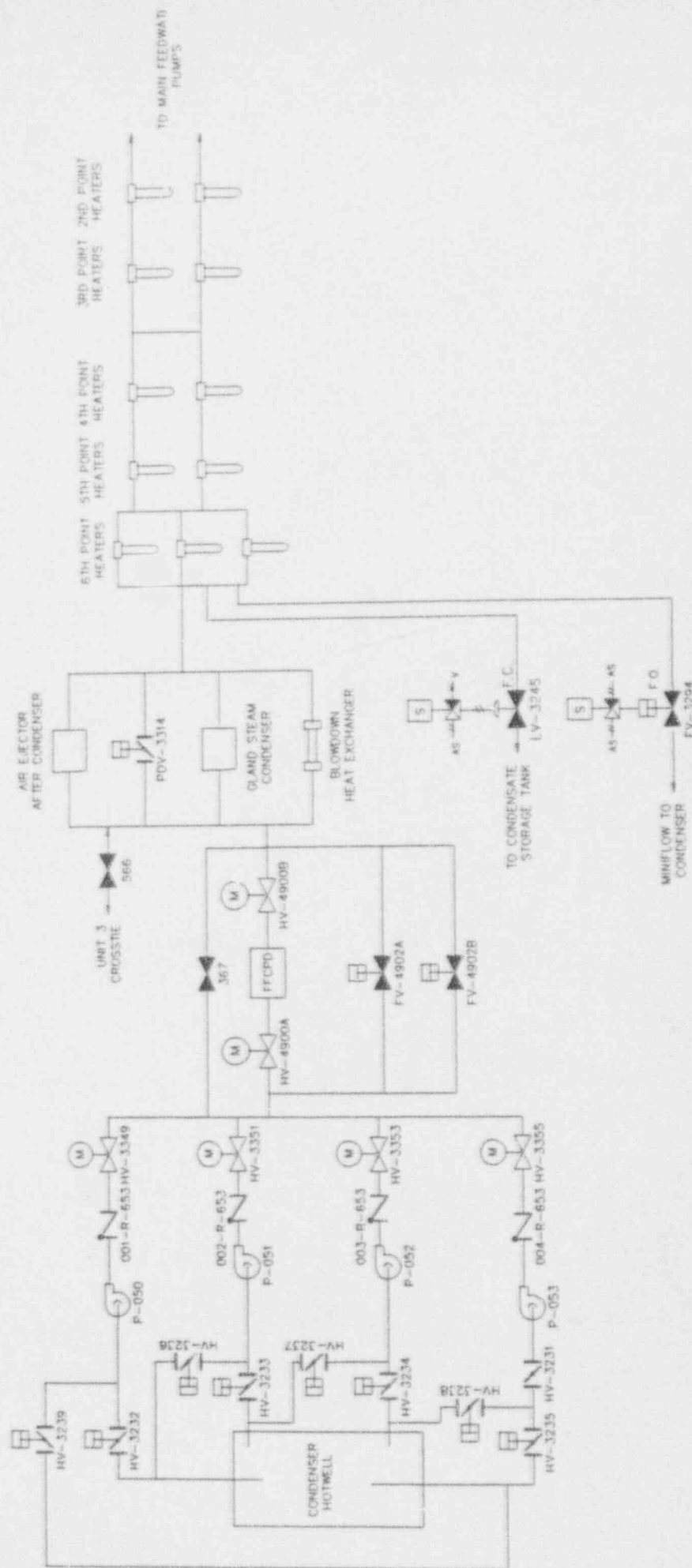
RTO operation is verified as part of standard post-trip actions. RTO clears approximately 10 minutes after initiation allowing FWCS to resume control, increasing the feed pump speed to increase flow and maintain the level in the steam generators. The operator may switch the FWCS to MANUAL mode and maintain steam generator level by adjusting the feedwater regulating valves.

In the event that both the MFW and AFW Systems are unable to adequately maintain level in the steam generators, the condensate pumps can be used to supply coolant from the hotwell to a steam generator. In order to use the condensate pumps, the operator must first depressurize the steam generators using the ADVs. Successful use of Emergency Condensate is conditional upon the preceding MFW failure not being attributable to condensate pump failure or loss of an injection path.

The feedwater isolation valves (HV-4052, HV-4048) and the feedwater block valves (HV-4051, HV-4047) automatically close on a containment isolation actuation signal (CIAS) to isolate the system from the steam generators. The feedwater isolation valves also close on a MSIS. No direct override of these signals is available to the operators from the control room.

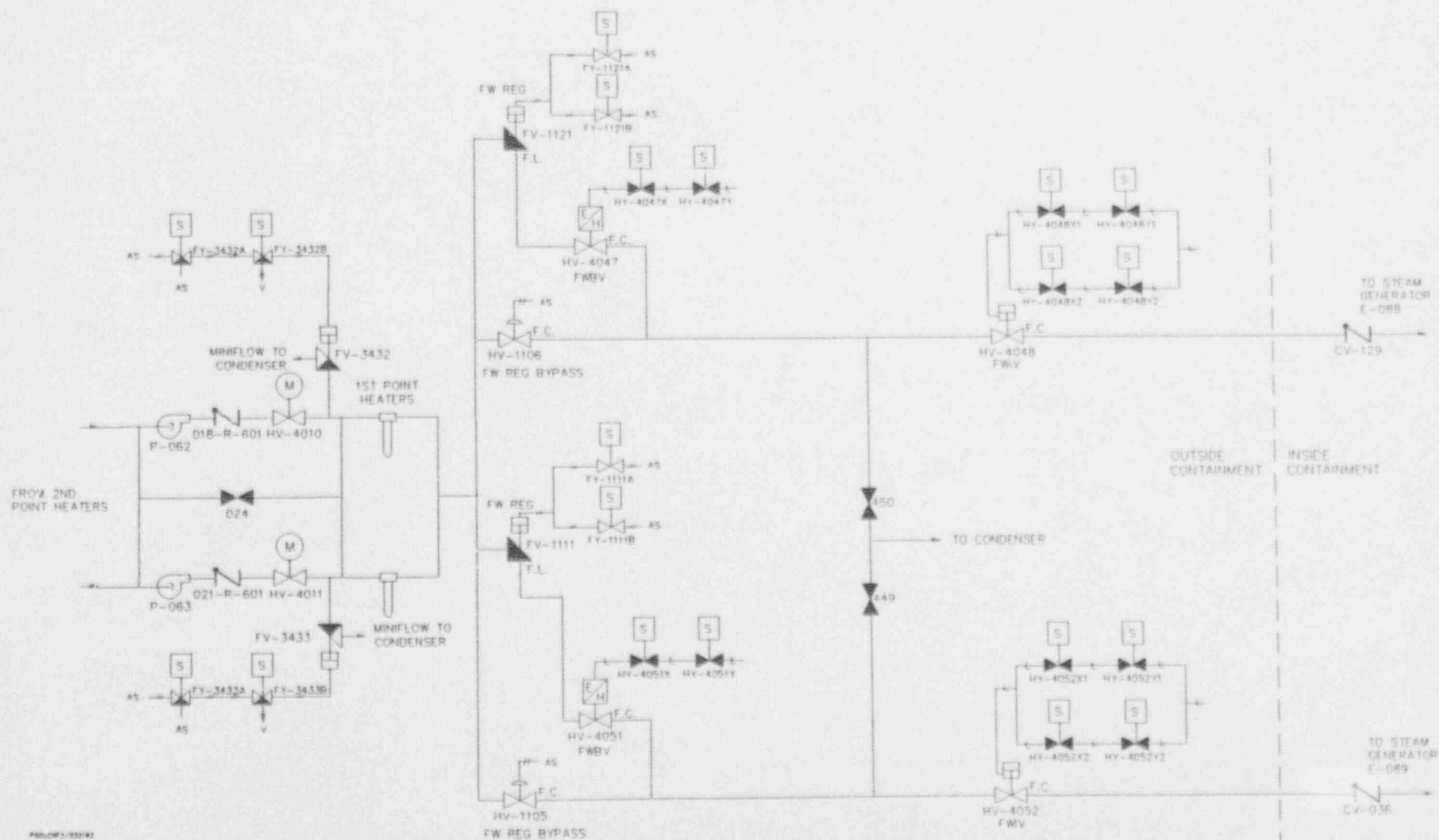
The support systems for the MFW and Condensate System include AC power, DC power, instrument air and the Main Steam System. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the MFW and Condensate System is presented in Figure 3.2-2.

(Page 1 of 2)



SAN ONOFRE UNITS 2/3 CONDENSATE/FEEDWATER SYSTEM

(Page 2 of 2)



3.2.3 Main Steam System

The functions of the Main Steam System (MSS) modeled in the IPE are: (1) to support decay heat removal from the RCS by main steam relief and main steam isolation and (2) to supply steam to the MFW pumps and turbine-driven AFW pump to support their operation. The MSS works in conjunction with the MFW, AFW, or Emergency Condensate to support RCS Heat Removal.

The MSS provides steam from the two steam generators to the high pressure turbine. The steam is piped from the steam generator nozzles through valves and associated controls to the turbine stop valves before reaching the high pressure turbine. The system is equipped with two ADVs, two main steam isolation valves (MSIVs), four Steam Bypass Control System (SBCS) valves, and eighteen MSSVs.

One steam line per steam generator penetrates the containment wall. The two main steam lines are cross-connected downstream of the MSIVs and upstream of the SBCS valves to equalize the steam pressure and flow between the two lines during normal and steam bypass operations. Auxiliary lines branch off at various points to provide process steam to turbine gland seal steam system, steam jet air ejectors, auxiliary boiler, MFW pump turbines and AFW pump turbine.

One main steam relief header branches off each main steam line upstream of the MSIV. Each relief header contains nine MSSVs and one pneumatic ADV. These relief header branch lines also provide the motive steam to the AFW pump turbines.

The MSSVs operate mechanically to maintain system pressure below their associated setpoints. The MSSVs have staggered setpoints ranging from 1100 to 1155 psia. The MSSVs are equipped with level arms to permit manual operation of the MSSVs if required. The MSSVs are designed to relieve in excess of 100% of design power.

Each ADV is capable of relieving 5% of design power. The ADVs (HV-8419,8421) can be set to operate automatically or manually from the control room. The ADVs can also be operated locally using a handwheel. The Instrument Air and Nitrogen systems in addition to a dedicated nitrogen backup provides the motive force for ADV operation. An isolation valve upstream of each ADV line is available to isolate the line in the event an ADV remains stuck open.

One MSIV and two parallel turbine stop valves are present in each main steam line. In addition, a normally closed pneumatic bypass valve (HV-8202,8203) is located parallel to each MSIV

(HV-8204,8205). Downstream of the MSIVs, motive steam is supplied to the turbines of the MFW pumps. Nitrogen is used as the motive force for closing the MSIVs. Compressed nitrogen exerts pressure on the top of the valve piston, while hydraulic fluid exerts pressure on the bottom of the valve piston. Upon receipt of a signal to close, the hydraulic fluid is dumped by two solenoid valves through two redundant dump lines to a hydraulic reservoir.

The SBCS valves discharge steam from the MSS to the condenser. Two parallel SBCS valves branch off each main steam line (HV-8423,8424 and HV-8425,8426). The SBCS valves are regulated by pneumatic positioners which receive input from current-pneumatic (I/P) transducers. Each valve is also equipped with solenoid valves that bypass the positioners to admit air for quick full opening of the valve. The SBCS is capable of relieving 45% of design power.

During normal full power operation both MSIVs are open and the MSSVs, ADVs, and SBCS valves are in the closed position. The ADVs are normally set in the manual mode and therefore do not provide automatic pressure relief. Steam normally flows through each turbine stop valve and passes through a turbine governor valve to the high pressure turbine. The SBCS valves open and close as required during fluctuating loads.

During abnormal operations (e.g., turbine trip), the "quick-open" feature of the control system automatically opens the SBCS valves within 1 second to their fully open position. Excessive secondary steam pressure is relieved by the MSSVs, although normally, the SBCS operation is sufficient to prevent demands on the MSSVs. For emergency operations such as Emergency Condensate or loss of offsite power, or failure of the secondary plant, the ADVs can be manually operated to depressurize a steam generator or accelerate cooldown and depressurization of the RCS.

A portion of the MSS, the main steam isolation system, is designed to isolate the steam generators and main steam lines to prevent the uncontrolled blowdown of more than one steam generator following the fault of a steam generator inside containment. In the event of a main steam line break outside containment, the isolation function of the MSS prevents uncontrolled blowdown of both steam generators and reduces the potential leakage of radioactivity to the environment in support of the containment isolation function. The MSIVs are automatically closed upon receipt of a MSIS or a CIAS. The MSIVs cannot be reopened until the MSIS and CIAS signals are reset.

The support systems for the MSS include AC power, DC power, and instrument air. The system dependencies are tabulated in Table

3.2-1. A simplified P&ID of the MSS is presented in Figure 3.2-3.

3.2.4 Safety Injection Tanks

The function of the SITs modeled in the IPE is to inject borated water into the Reactor Coolant System to flood and cool the core following the unlikely event of a large break LOCA accident for RCS Inventory Control.

The four SITs provide a means to flood the core with borated water following depressurization of the RCS. Borated water from each nitrogen pressurized SIT discharges through a check valve and a normally open motor-operated isolation valve into the four cold leg injection lines and then to the RCS through the four ECCS isolation check valves. For a large break LOCA, core reflooding by the SITs assists in core cooling until flow from the SI pumps becomes effective.

Each SIT (T-007,008,009,010) is provided with one wide range and two narrow range pressure transmitters and one wide range and two narrow range level transmitters. Each transmitter is connected to a separate indicator in the control room. The narrow range transmitters provide high/low and high-high/low-low alarms.

The discharge line of each SIT contains a motor-operated isolation valve (HV-9340,9350,9360,9370). When RCS pressure is above 700 psi, these valves are key-locked open, and power to the motor operators is locked out to prevent spurious movement. The valves receive an open signal following a SIAS.

Each SIT is provided with connections for filling, draining, pressurizing, venting and sampling. Inadvertent or spurious nitrogen vent valve actuation, which could result in SIT depressurization, is prevented by maintaining these valves normally locked closed with power removed.

During normal plant operation, each SIT is isolated from the RCS by two check valves in series.

During abnormal operations which depressurize the reactor coolant system, the SITs automatically discharge into the core through each of the cold legs when RCS pressure decreases below SIT pressure.

The only support system required for the SITs is the HPSI System. This dependency accounts for the final check valve in the SIT injection path which is within the system boundary defined for

the HPSI system. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the SITs is presented in Figure 3.2-4.

3.2.5 High Pressure Safety Injection

The function of the HPSI System modeled in the IPE is to inject borated water into the RCS to provide high pressure emergency makeup to reactor vessel following a LOCA for Core Heat Removal and RCS Inventory Control. The HPSI system operates in two modes: injection and recirculation.

The HPSI system consists of two 100% capacity trains with three HPSI pumps. The three HPSI pumps (P-017, P-018, and P-019) are centrifugal type pumps capable of delivering up to approximately 1000 gpm each. The swing HPSI pump (P018) can be manually aligned to supply either train. Support systems for the swing HPSI pump (power, CCW, mini-flow) are also capable of being aligned to either Train A or B.

Mini-flow for each HPSI pump recirculates back to the RWST T-005 through two motor-operated valves (HV-9347, HV-9348 for Train A and HV-9305, HV-9306 for Train B). Other ECCS pumps including the LPSI pumps and the CS pumps share the same mini-flow recirculation path.

For ECCS injection, borated water is supplied by two RWSTs (T-005, T-006). Each RWST has approximately 245,000 gallons of capacity (nominal 188,000 gallons required; alarms at 90% level or approximately 220,000 gallons). The RWSTs are cross-connected by two normal open isolation valves. Each RWST supplies a train of ECCS pumps including a LPSI pump, HPSI pump and CS pump.

For ECCS recirculation, borated water is supplied from the ECCS containment sump. Two isolation valves in each train (HV-9303, HV-9305 for Train A and HV-9302, HV-9304 for Train B) isolate the sump from the RWST suction to the ECCS pumps during injection.

Each train of HPSI discharges through a header supplying four cold leg injection lines and one hot leg injection line. Each high pressure injection train is provided with motor operated isolation valves (HV-9323/9324, HV-9326/9327, HV-9329/9330, HV-9332/9333) joining at a common header prior to penetrating containment. On each injection line, one valve is powered from "A" train, and the other is powered from "B" train.



The four common cold leg injection lines include a check valve upstream of the point where the SIT and LPSI join a common ECCS injection header. Flow from the common ECCS header into each of four cold legs passes through a check valve before reaching the RCS.

During normal plant operation, the HPSI system is in standby with the pump suctions aligned to the RWSTs. Three pumps are normally aligned for ECCS operation. Two HPSI pumps (the swing pump and the pump powered from the opposite train of support systems supplying the swing pump) start automatically upon receipt of a SIAS. The third HPSI pump is started manually. RWST isolation valves to the ECCS pump suctions (HV-9300 and HV-9301) are normally locked open with power removed and receive an open signal upon SIAS. Pump mini-flow valves are normally open and injection path motor-operated valves are normally closed.

During abnormal conditions which generate a SIAS, the aligned HPSI pumps start and the four cold leg injection valves open in each HPSI train open, allowing borated water from the RWST to be injected into the reactor coolant system. If RCS pressure exceeds the HPSI pump discharge pressure, the HPSI pumps continues to operate recirculating inventory through mini-flow until the RCS pressure decreases below the pump discharge pressure.

On low RWST level, a RAS automatically shifts the suctions of the HPSI pumps from the RWSTs to the containment sump. Sump isolation valves open automatically and ECCS mini-flow valves close. RWST valves HV-9300 and HV-9301 are closed manually per procedure to prevent diversion of flow to the RWST, if the check valve on the RWST supply line fails to close. The HPSI system continues to inject into the RCS throughout the pump suction transfer process.

The support systems required for the HPSI system include AC power, DC power, Component Cooling Water and the Plant Protection System. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the High Pressure Safety Injection System is presented in Figure 3.2-5.

3.2.6 Low Pressure Safety Injection

The function of the LPSI system modeled in the IPE is to inject borated water into the RCS to provide emergency makeup to the reactor vessel following a LOCA for Core Heat Removal and RCS Inventory Control.

The LPSI System is comprised of two redundant and independent trains. Each train includes one low pressure, high volume centrifugal pump (P-015 or P-016) capable of delivering approximately up to 5,000 gpm. The LPSI pumps are provided with minimum flow protection recirculation lines to prevent damage resulting from operation against a closed discharge valve. Mini-flow circulates back to the RWST T-005 through shared ECCS mini-flow motor-operated valves.

For ECCS injection, borated water is supplied to each LPSI pump from the RWSTs (T-005, T-006). For ECCS recirculation, the LPSI pumps are stopped automatically following a RAS. The discharge of each LPSI pump enters a common header to a normally open motor-operated isolation valve (HV-8161) and flow control valve (HV-8160) before branching into the four cold leg injection lines. Each LPSI cold leg injection line is provided with a motor operated isolation valve (HV-9322, 9325, 9328, 9331). Two valves are powered from "A" train, and the other two are powered from "B" train. Each LPSI injection line joins a common header with the HPSI system and the SIT.

During normal plant operation, the LPSI system is in standby with pump suctions aligned to the RWSTs. LPSI pump mini-flow valves are normally open. Injection path motor-operated valves are normally closed, but automatically open upon receipt of a SIAS.

During abnormal conditions which generate a SIAS, the LPSI pumps start and the four cold leg injection valves open, allowing borated water from the RWST to be injected into the RCS. If RCS pressure exceeds the LPSI pump discharge pressure, the LPSI pumps continue to operate recirculating inventory until the RCS pressure decreases below the pump discharge pressure. When the level in the RWST drops below the low level setpoint, a RAS automatically trips the LPSI pumps and closes the mini-flow recirculation valves.

The support systems required for the LPSI system include AC power, DC power, CCW and the PPS. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the LPSI system is presented in Figure 3.2-6.

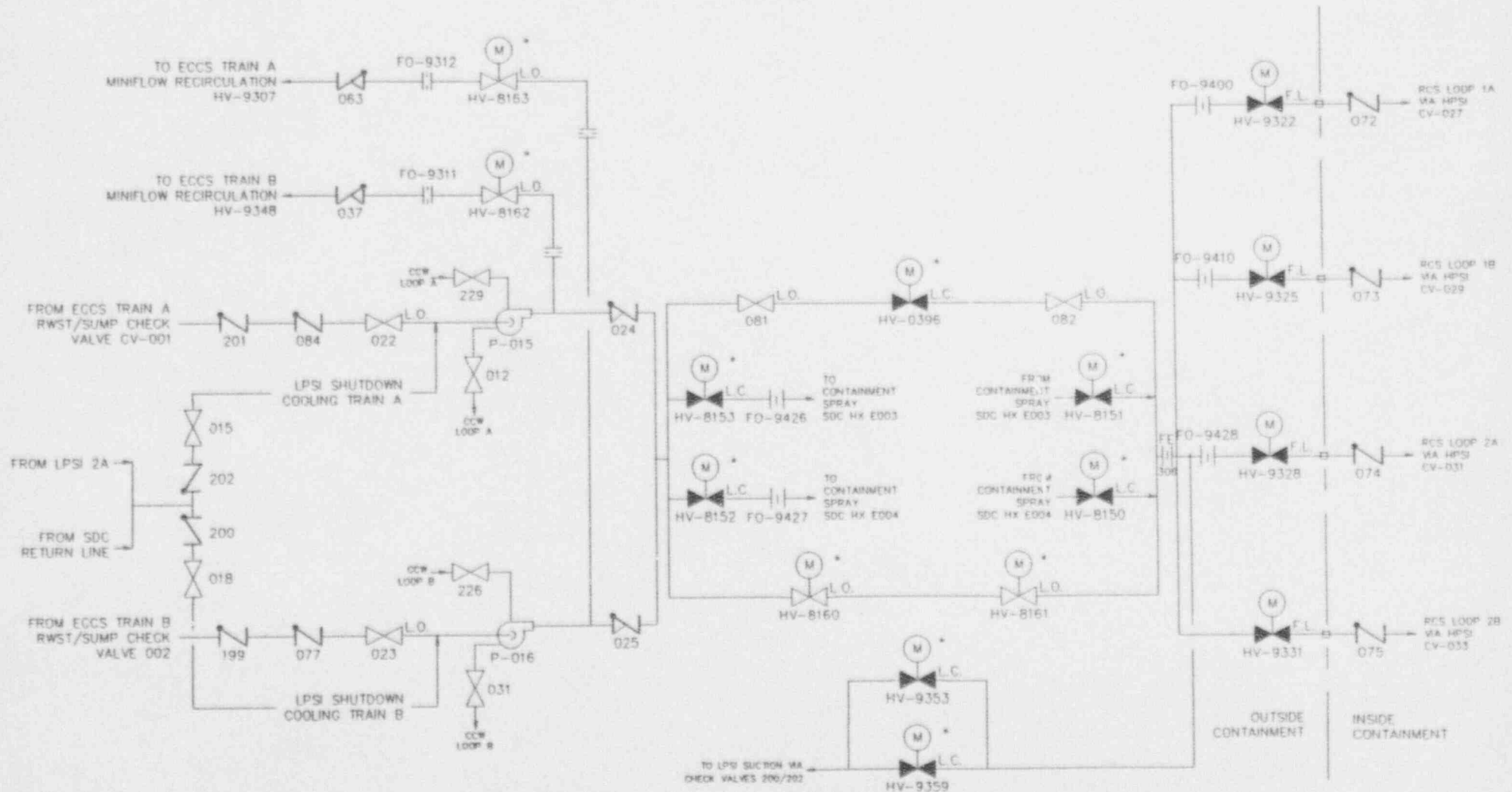
3.2.7 Chemical Volume and Control System

The functions of the CVCS modeled in the IPE are to: (1) inject borated water into the RCS to provide high pressure emergency makeup following a small-small loss of coolant accident for Core Heat Removal and RCS Inventory Control and (2) provide emergency boration to reduce core power for Reactivity Control.

The CVCS consists of the letdown subsystem, charging subsystem,

Figure 3.2-6: LPSI Simplified P&ID

SAN ONOFRE UNITS 2/3 LOW PRESSURE SAFETY INJECTION SYSTEM



and the BAMU subsystem. The letdown subsystem includes piping and components from the RCS loop to the volume control tank (VCT). The charging subsystem includes CVCS piping and components ranging from the VCT, RWST and BAMU subsystem to the point of injection back into the RCS. The BAMU portion of the CVCS consists of all paths from the two BAMU tanks to the suction of the charging pumps.

The Charging subsystem has three high head, low volume (44 gpm) positive displacement charging pumps: one pump for each of two trains (P-190, P-192) and a third swing pump (P-191) which can be powered from either Train A or B. The charging system is provided with borated coolant from the VCT or two emergency sources. One of the emergency sources is the cross-connected RWSTs supplied by gravity feed. The second source of borated coolant is from two BAMU tanks which supply borated coolant to the three charging pumps via either the BAMU pumps or through a gravity feed path.

The two BAMU pumps (P-174, 175) take suction from the BAMU tanks (T-071, 072) and pump the borated coolant into a common header to the suction of the charging pumps. The pumps and associated valves required to align flow to the charging pumps are Train A powered and actuated. The gravity feed path from the BAMU tanks is aligned by opening two valves (HV-9240, 9235) which are Train B powered and actuated.

The charging pumps discharge into a common header which normally directs flow back to the regenerative heat exchanger. From the heat exchanger, flow can be directed to the hot legs of RCS loop 1 or 2, or into the pressurizer for auxiliary spray. The common header on the discharge of the charging pumps also has alternate paths to direct charging flow to the SI header and pressurizer auxiliary spray. Both of these paths are normally isolated with closed manual valves.

During normal operations, the CVCS maintains RCS water chemistry, purity, and reactivity levels. In addition, the CVCS maintains RCS volume and provides a path for reactor coolant pump seal bleed-off which supports seal cooling. Normally, one charging pump is in operation, recycling letdown inventory from the VCT.

During abnormal operations with LOCAs, automatic operation of the standby charging pumps and/or modulation of the operating letdown control valve occurs to makeup decreasing RCS inventory. Following a SIAS, the VCT isolation valve, LV-0227C, closes and the RWST isolation valve, LV-0227C, opens to establish a gravity feed path of borated water to the suction of the charging pumps. The BAMU pumps, P-174 and 175, and associated discharge valve, HV-9247, as well as the BAMU tank gravity feed discharge valves

to the charging pumps suction, HV-9240 and 9235, all start or open as appropriate on a SIAS to provide concentrated boric acid to the charging pumps' suction.

Emergency boration following an Anticipated Transient Without Scram requires operator actions to align the CVCS charging system since no SIAS signal would be expected. The charging pumps take suction from the BAMU system and discharge to the RCS via the charging line.

For RCS depressurization without forced circulation (e.g., normal pressurizer spray is not available), the RCS can be depressurized using pressurizer auxiliary spray supplied by the charging pumps. The charging pumps take suction from the BAMU System and/or the RWST.

The support systems required for the CVCS include AC power, DC power, and the PPS. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the CVCS is presented in Figure 3.2-7.

3.2.8 Containment Spray and Containment Emergency Fan Coolers

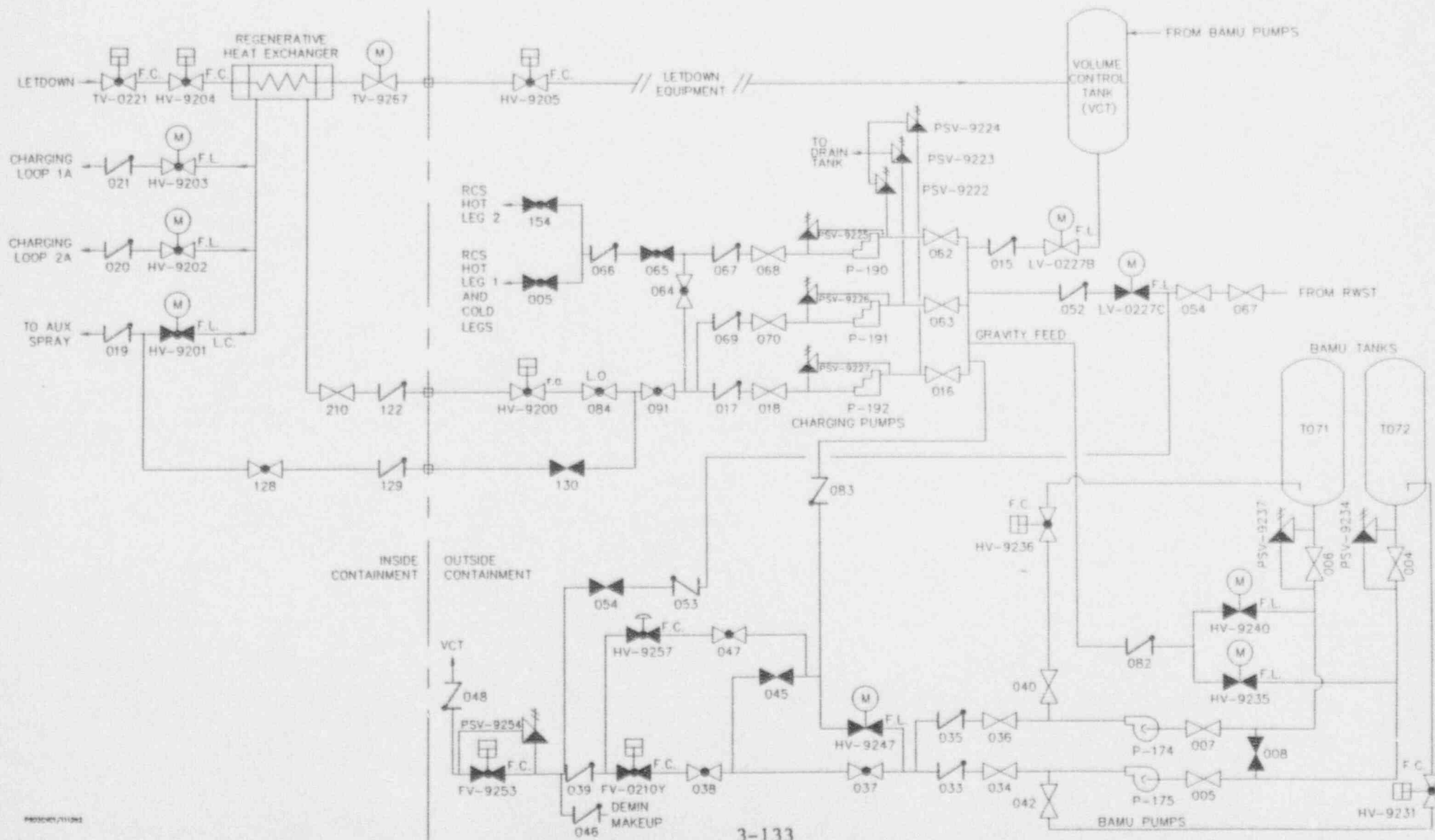
The functions of the Containment Spray and Containment Emergency Fan Coolers modeled in the IPE are: to remove energy from containment following events which release significant amounts of energy into the containment to support the Containment Integrity and to inject borated water into the Reactor Coolant System to provide backup injection to reactor vessel following loss of coolant accident for RCS Inventory Control and Core Heat Removal. The CS System is comprised of two trains of equipment designed to deliver borated water to the containment atmosphere for heat and iodine removal inside the containment. The CS pumps (P-012,013) are centrifugal type pumps with a shutoff head of 250 psig. The CS pumps share common suction headers with the HPSI pumps and the LPSI pumps. Inventory from either the RWSTs (injection) or the containment sump (recirculation) supplies the suction header.

Two Shutdown Cooling Heat Exchangers (SDCHXs) (E003,E004) remove heat from containment spray flow during recirculation. The SDCHXs reject heat to the CCW system. Cross-connect lines and isolation valves join the CS and LPSI Systems upstream and downstream of each SDCHX.

Two motor-operated valves (HV-9367,HV-9368) isolate the CS pumps from the containment spray headers. The CS nozzles are installed in two headers of three rings each, oriented to maximize effective coverage of the containment volume. The spray headers are located in the upper regions of the containment to allow the

Figure 3.2-7: CVCS Simplified P&ID

SAN ONOFRE UNITS 2/3 CHEMICAL AND VOLUME CONTROL SYSTEM



falling droplets time to reach thermal equilibrium with the steam-air atmosphere.

The Containment Emergency Fan Coolers (CEFC) system consists of four emergency fan cooling units (E-399,400,401,402). These units remove heat energy from the containment atmosphere during accident conditions. Each emergency fan cooling unit is supplied with cooling water from the CCW system. Two of the CEFCs are supplied by train A support systems while the other CEFCs are fed from the B train systems.

During normal plant operation, the CS pumps are in standby with mini-flow valves open and containment isolation valves closed. The CEFCs are also in standby with CCW supply valves open and CCW outlet valves closed.

During abnormal operations, a SIAS starts the CS pumps automatically. The Containment Spray containment isolation valves, HV-9367 and HV-9368, remain closed following the SIAS causing inventory to circulate back to the RWST through mini-flow valves.

The same conditions generating a SIAS signal trigger a CCAS which starts the CEFCs. Both the CCW supply and return valves to the CEFCs receive an open signal when a CCAS occurs. The normally closed return valves open following the CCAS. Forced circulation of the containment atmosphere across the CEFC coils removes heat from the containment atmosphere.

Continued increase in the containment pressure generates a CSAS. The CSAS signal opens HV-9367 and HV-9368 to commence spraying the containment. When RWST inventory reaches the low level, a RAS automatically realigns the CS pump suction source to the emergency sump. The pumps continue to operate throughout the process of transferring pump suction from the RWST to the emergency sump.

Heat removal from the containment is increased during the recirculation mode through the CS system. Sump inventory flows to the suction of each CS pump and discharges through a SDCHX which removes decay heat. The coolant flows through the CS isolation valves and spray headers return the cooled inventory to containment. The spray droplets fall to the containment floor, drain to the containment emergency sump, and recycle through the system.

Under abnormal LOCA conditions in which emergency RCS makeup from the HPSI is unavailable, CS pumps are used for ECCS injection. Operators depressurize the RCS and align CS pumps to supply

injection flow via the LPSI/HPSI injection flow path via HV-8150 or HV-8151.

The support systems required for the CS and CEFCs include AC power, DC power, CCW, and the PPS. The LPSI system also serves as a support system when the CS system operates in an ECCS capacity. The system dependencies are tabulated in Table 3.2-1. Simplified P&IDs of the CS and CEFCs are presented in Figures 3.2-8 and 3.2-9.

3.2.9 Reactor Coolant System Pressure Control

The functions of the RCS modeled in the IPE are to maintain RCS Pressure Control by providing pressure relief for the primary coolant system through pressure relief and to maintain primary system integrity for RCS Inventory Control.

The RCS contains the nuclear fuel (core) and includes components necessary to assure the core is structurally contained, cooled, and controlled from a reactivity standpoint. The RCS Pressure Control System analysis focuses on the cooling and structural integrity functions of RCS components. As such only the RCS pressurizer safety valves PSV-0200 and PSV-0201 and the normal pressurizer spray via PV-0100A and PV-0100B are considered. The pressurizer is equipped with two code safety relief valves PSV-0200 and PSV-0201 that limit RCS pressure below the maximum design pressure. The relief valves are 1.25" nominal diameter orifice size and are capable of relieving 504,874 lb/hr each, at the set pressure of 2500 lb/in². The safety valves relieve to the primary system quench tank (T-011) where the steam is condensed.

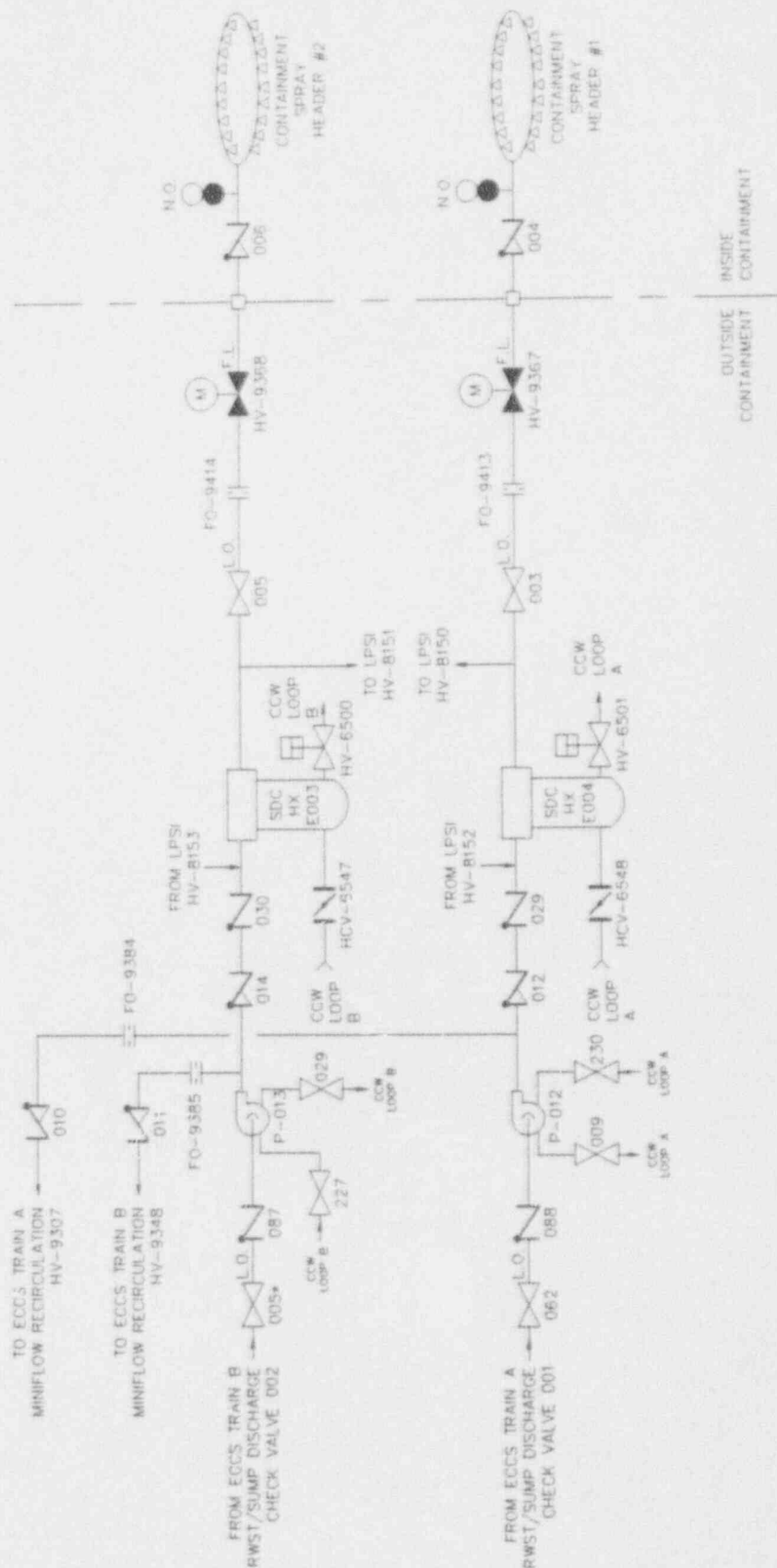
The normal pressurizer spray is supplied from the RCS cold legs 1A and 1B. Forced circulation from operation of RCPs 001 and 003 directs RCS inventory to the spray control valves PV-0100A and PV-0100B which supply the pressurizer spray header. A common header upstream of the spray header joins the normal spray supply line with the auxiliary spray line from the Charging System.

During normal operations, the RCS pressure relief valves are closed serving as part of the RCS Pressure Boundary. The normal pressurizer spray operates as required to support primary system pressure control during normal operations.

Following transient events that result in abnormally high primary system pressure, the pressurizer safeties open and the normal spray functions to provide RCS pressure relief. The lifting of the code safety valves is a mechanical function with no support system interactions or requirements. Following pressure transients causing the safeties to lift, the pressurizer safety

Figure 3.2-8: CS Simplified P&ID

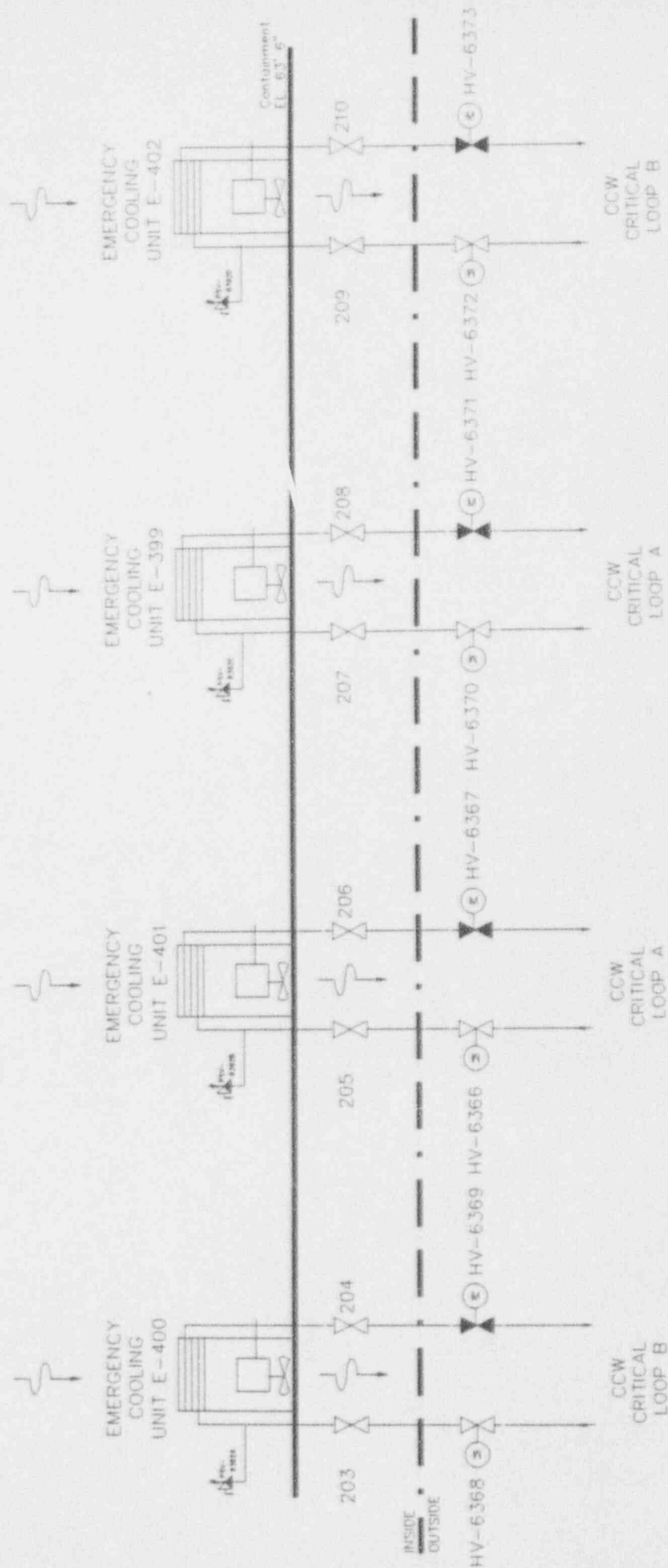
SAN ONOFRE UNITS 2/3 CONTAINMENT SPRAY SYSTEM



• VALVE DESIGNATED 005X DUE TO SIMILAR VALVE NUMBER IN SYSTEM BOUNDARY

Figure 3.2-9: CEFC Simplified P&ID

SAN ONOFRE UNITS 2/3 CONTAINMENT EMERGENCY COOLING SYSTEM



valves must reseal to restore RCS integrity.

Following events requiring the RCS to be depressurized, pressurizer spray may be used. Normal pressurizer spray requires the reactor coolant pumps to operate, while auxiliary pressurizer spray requires operation of the charging pumps.

The support systems required for the RCS Pressure Control include AC power, DC power, and IA. The CVCS also serves as a support system when pressurizer spray is supported by auxiliary spray from the Charging pumps. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the RCS Pressure Control System is presented in Figure 3.2-10.

3.2.10 Component Cooling Water

The functions of the CCW System modeled in the IPE are to provide general support for heat removal from operating components including pumps, cooling units and heat exchangers.

The CCW System provides continuous cooling water flow to components which handle potentially radioactive fluids. The system also forms a barrier between these radioactive systems and the SWC System. The CCW system is a closed loop, pressurized system.

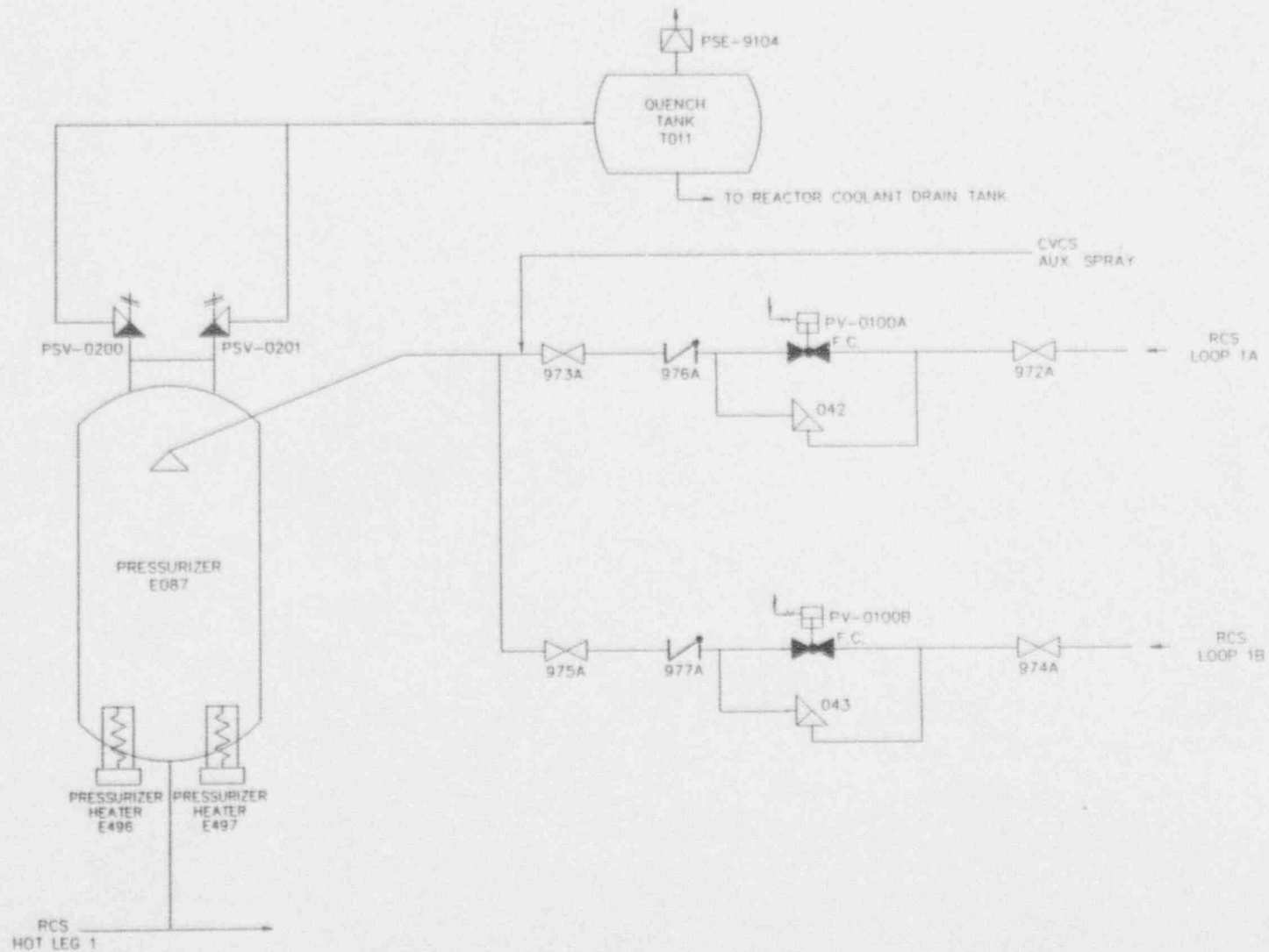
The system is arranged in two independent, full capacity, critical cooling loops and one noncritical cooling loop. One CCW pump (P-024,026) is installed in each critical loop to circulate the cooling water through a component cooling water heat exchanger where heat is transferred to the SWC system. Cooling water flows through cooled components and returns to the CCW water pump.

A third CCW pump (P-025) is provided as an installed spare and can be aligned to either critical loop. Physical and electrical independence of the two loops is maintained by double valve isolation and kirk-key breaker interlocks. Most of the valves in the system are manually operated with the exception of the valves associated with CCW swing pump P-025, surge tank isolation valves, and non-critical loop isolation valves.

Suction for CCW pump P-025 is aligned to one of two surge tanks through two AC motor-operated series butterfly valves (HV-6222A, 6222B, 6224A, 6224B). CCW pump discharge valves are AC motor-operated butterfly valves mounted in series from a common discharge line from pump P025. Flow from the discharge valves is directed to the CCW heat exchangers.

Figure 3.2-10: RCS Pressure Control Simplified P&ID

SAN ONOFRE UNITS 2/3 RCS PRESSURE CONTROL



Flow downstream of the CCW heat exchangers supplies both the critical and non-critical loops. Flow from the loops returns to the outlet of the surge tanks where it ties into the suctions of the CCW pumps. Each critical loop cools a HPSI pump and the third of a kind HPSI pump, a LPSI pump, a CS pump, shared letdown heat exchanger, two CEFCs, a shared emergency chiller, a SDCHX, a CCW pump and the third of a kind CCW pump, and a fuel handling building post-accident cleanup unit.

The CCW non-critical loop isolation valves are air-operated, butterfly valves (HV-6212,6213,6218,6219) which fail closed. The CCW surge tanks (T-003,004) maintain system pressure and provide for expansion and contraction of cooling water. Nuclear service water supplies makeup water to each surge tank when a surge tank low level is reached. Emergency makeup is available to the surge tanks from the fire water system. Normal and backup nitrogen is supplied to each CCW surge tank to maintain required system pressure.

The system is capable of meeting design heat load requirements with one critical loop operating supplying its respective critical loop and the non-critical loop, with the other loop in standby. Normally, in accordance with operations management requirements, both loops are in operation with the third of a kind CCW pump, P-025, aligned to the loop supplying the non-critical loop.

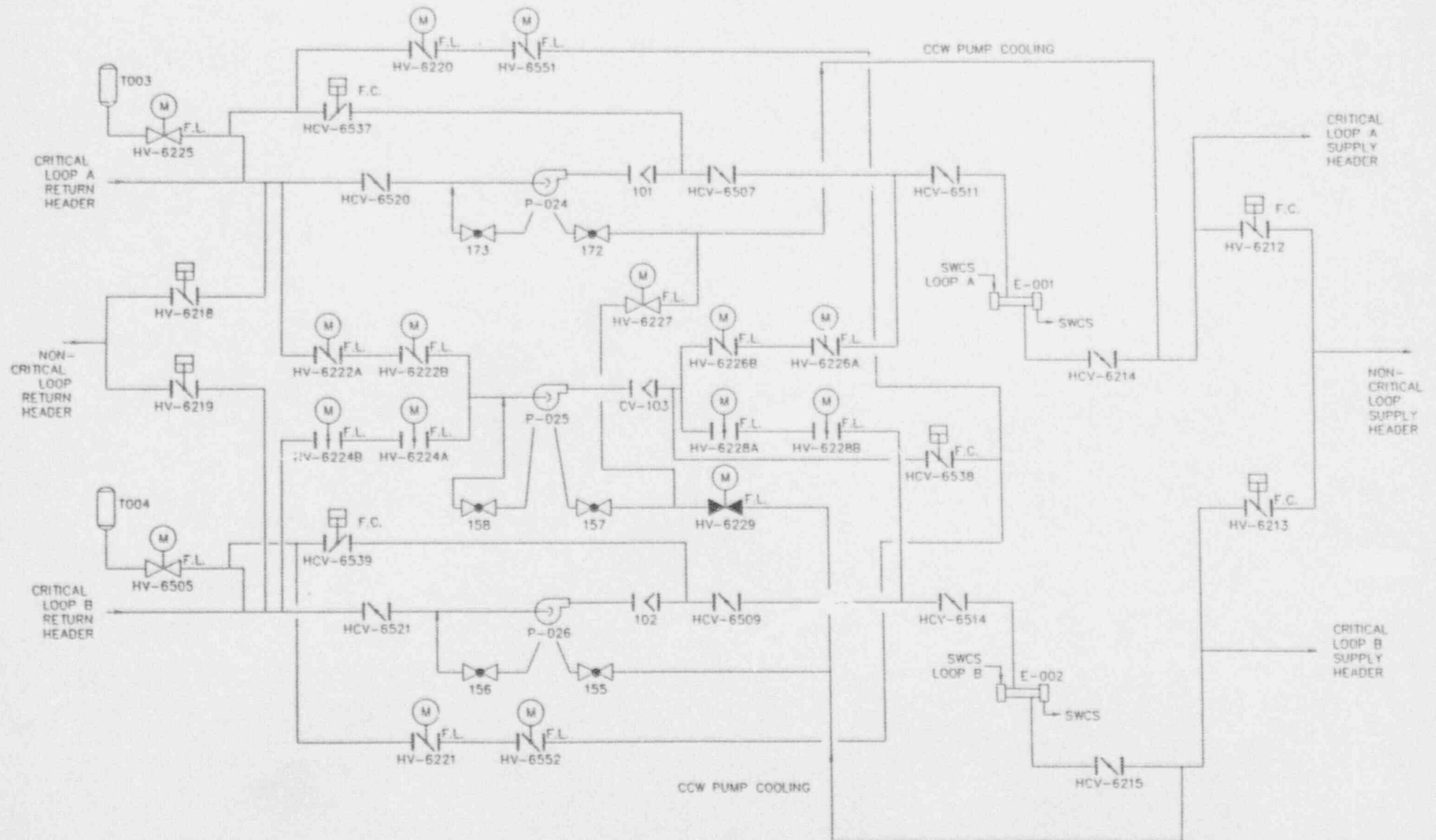
During abnormal operations, the CCW system operates to support actuation of emergency safety features. A SIAS ensures one CCW pump on each loop is started if not already operating. A CIAS isolates the non-critical loop by closing the supply and return valves to/from both loops, and isolates the cooling supply and return lines to the cooled components located within the containment. CCW to the CEFCs and the CS system open on CCAS and CSAS, respectively.

The isolation valves from loop A and from loop B are interlocked to provide loop separation and isolation of the associated non-critical loop when the respective CCW surge tank low-low level alarm or a CIAS signal is received.

The support systems required for the CCW system include AC power, DC power and the ESFAS systems. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the CCW system is presented in Figure 3.2-11.

Figure 3.2-11: CCW Simplified P&ID

SAN ONOFRE UNITS 2/3 COMPONENT COOLING WATER SYSTEM



3.2.11 Saltwater Cooling

The function of the Saltwater Cooling System modeled in the IPE is to provide heat removal from the Component Cooling Water heat exchangers.

The SWC system transfers heat from components to the ultimate heat sink (the Pacific Ocean). The system is an open cycle system which supplies seawater to the CCW heat exchangers (E-001,002) to remove heat from components cooled by the closed loop CCW System and returns the heated seawater to the Pacific Ocean.

The SWC system consists of four pumps (P-112, 113, 114, and 307), flow control valves, check valves, and various instrumentation. The SWC system is comprised of two independent and redundant trains. Each train is capable of providing 100% of the design cooling requirement for a unit.

Each SWC train has two pumps. One pump is located in the Unit 2 intake structure, and the other pump of the same train is located in the Unit 3 intake structure. This arrangement allows one units intake structure to be removed from service for heat treatment and while the other intake supplies full capacity flow to both redundant trains on both units.

Check valves and air-operated valves are provided at the discharge of the SWC pumps to facilitate flow delivery during pump operation and prevent reverse flow through the pumps when not in operation. Each air-operated discharge valve is equipped with an accumulator.

Each SWC train supplies cooling saltwater to a CCW heat exchanger. The saltwater flows through the tube side of the CCW heat exchanger and discharges to the sea through the circulating water box culvert. An emergency discharge line is provided to an overflow at the seawall. Manual valves immediately upstream and downstream of the CCW heat exchangers are provided to permit reversal of flow through the CCW heat exchangers during backwash operations.

Each SWC pump is equipped with a valve which supplies service water to the pump bearings. A low flow switch is installed in the service water supply to each saltwater cooling pump. Pump seals and bearings are flushed (cleared of particulate, cooled and lubricated) by the Service Water System. In the event of loss of service water, seal and bearing cooling and lubrication are provided from the operating pump's discharge. A cyclone separator filters particulate matter from the pump discharge before entering the pump seals.

Saltwater enters the CCW heat exchanger through the inlet nozzle at the bottom of the heat exchanger inlet channel. The inlet channel has a relief valve for overpressure protection and a vent valve. Saltwater flows through the heat exchanger tubes, cooling the component cooling water, and leaves at the opposite end of the heat exchanger through the outlet nozzle at the bottom of the outlet channel.

A kirk-key interlock is provided for each train's pair of SWC pumps to allow only one pump to be aligned for automatic actuation at any one time.

During normal operation, both SWC trains are operating. Each train has only one SWC pump operating. One train supplies the heat removal function while the standby train operates without heat loads. The operating pump in the standby train is aligned to the other unit's intake structure. This alignment prevents common mode failure of both trains if an intake structure becomes unavailable. During normal cooldown operations, heat loads are applied to both operating trains to reduce the time requirement to cool down the plant.

During abnormal operations, the SWC pumps receive a start signal automatically 20 seconds after receipt of a SIAS or after a 5 second delay of the CCW pump starting in the same train. If the standby pump was not in operation, the bearing seal water supply control valve, pump discharge valve, and CCW heat exchanger saltwater cooling outlet valve to circulating water box culvert open.

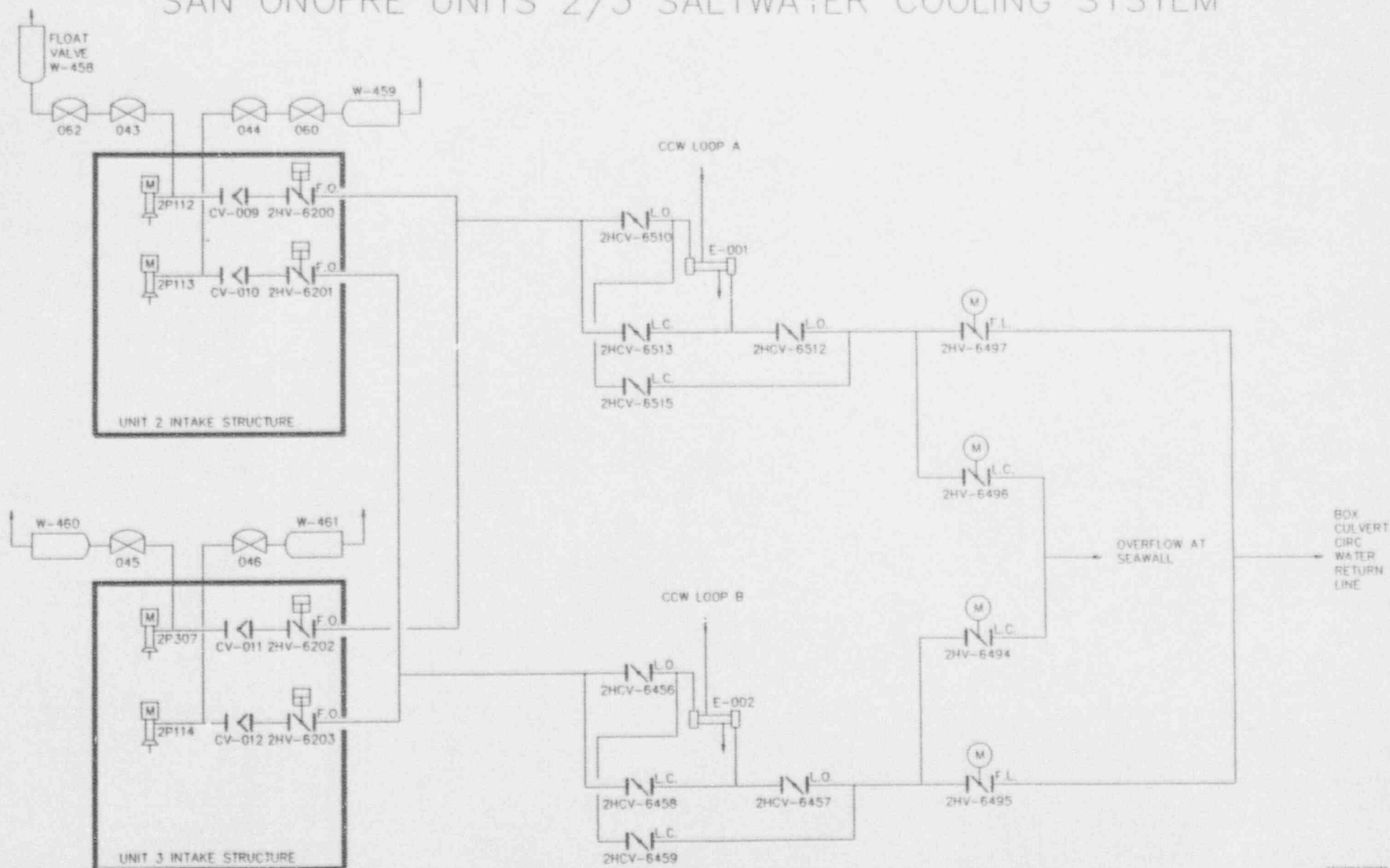
Flow is normally discharged to the circulating water return line through HV-6497 and HV-6495. The saltwater emergency discharge valves (HV-6494, HV-6496) can be remotely operated from the Control Room for emergency discharge from the CCW heat exchangers if a failure or blockage of the normal discharge path occurs.

During periods of degraded heat removal due to marine fouling, heat removal may be restored using several techniques including pump bumping, backflushing and heat treatment.

The support systems required for the SWC system include AC power, DC power, Instrument Air and Service Water. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the SWC system is presented in Figure 3.2-12.

Figure 3.2-12: SWC Simplified P&ID

SAN ONOFRE UNITS 2/3 SALTWATER COOLING SYSTEM



3.2.12 Instrument Air

The function of the Instrument Air System modeled in the IPE is to provide general support for operation of pneumatic devices.

The IA system provides a continuous supply of filtered, dry and essentially oil-free air for pneumatic instrumentation, controls and valve operations. The IA system is common to both Units 2 & 3 and includes three identical 100% capacity air compressing trains, each consisting of the following: air intake filter/silencer, two-stage compressor unit, intercooler and aftercooler with moisture separator, air receiver, dryers and filters.

The IA compressors are reciprocating, two-stage compressors cooled by the Turbine Plant Cooling Water (TPCW) System. The aftercoolers are counterflow heat exchangers cooled by TPCW and located above the air receivers. The IA dryers are water cooled refrigeration units which provide fully automatic, continuous dehumidification. Condensed moisture and oil are separated from the air using a centrifugal and baffled separator.

Air from within the turbine building is drawn in through the filter/silencer and directed to the first stage of the air compressor. The air is compressed, intercooled and directed to the second stage of the compressor. The air compressed in the second stage of the compressor is cooled in the aftercooler. Both stages of the air compressor and the intercooler are housed in one body.

The air cooled in the aftercooler passes through a moisture separator. In the moisture separator, water is removed from the air stream which then enters an air receiver. Three air receivers (E090, E091, E092) are connected in parallel to a common discharge header. This common air header supplies air to the IA System.

Air from the common air header is directed to one of the two IA dryers. In the IA dryer, moisture and oil from the air is separated and removed. Downstream of the air dryers is a check valve followed by a branch line from the Auxiliary Gas System supplying backup nitrogen to the IA system. Dry air (or nitrogen) then passes through three of four air filters. The air filters remove particulates from the air. The IA then enters each Unit's IA distribution header.

During normal power operation, one of the compressors is selected for continuous operation (LEAD), and serves the IA system demands. The second compressor serves as a standby (LAG-1). The third compressor is a second standby (LAG-2). Standby

compressors start automatically on low system pressure. If the system pressure is not maintained by the IA System, the passive Nitrogen System automatically supplies the IA header to all served components. Some components, such as the Automatic Depressurization Valves, have dedicated nitrogen supplies enabling component operation with both the IA and Nitrogen systems unavailable.

The support systems required for the IA System include AC power, DC power, and TPCW. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the IA System is presented in Figure 3.2-13.

3.2.13 Heating Ventilation and Air Conditioning

The function of the Heating, Ventilation and Air-Conditioning System modeled in the IPE is to provide room cooling to ESF switchgear and distribution rooms. Other ventilation and room cooling systems are considered within the boundary of the system served.

The ESF Switchgear room ventilation system is comprised of a normal and emergency cooling system. The switchgear and distribution rooms are capable of being cooled from normal and emergency cooling units. The normal cooling unit, E-430, draws outside air over cooling coils before entering the distribution rooms and exhausting to the atmosphere.

Chilled water to the E-430 cooling unit is supplied by chilled water pumps (P-158/P-159). The Chilled Water system, shared by Units 2 and 3, supplies cooling water to the HVAC loads that are in service during normal plant operations. Chilled water from the system loads flow through a separator/strainer unit to the chilled water pump suction.

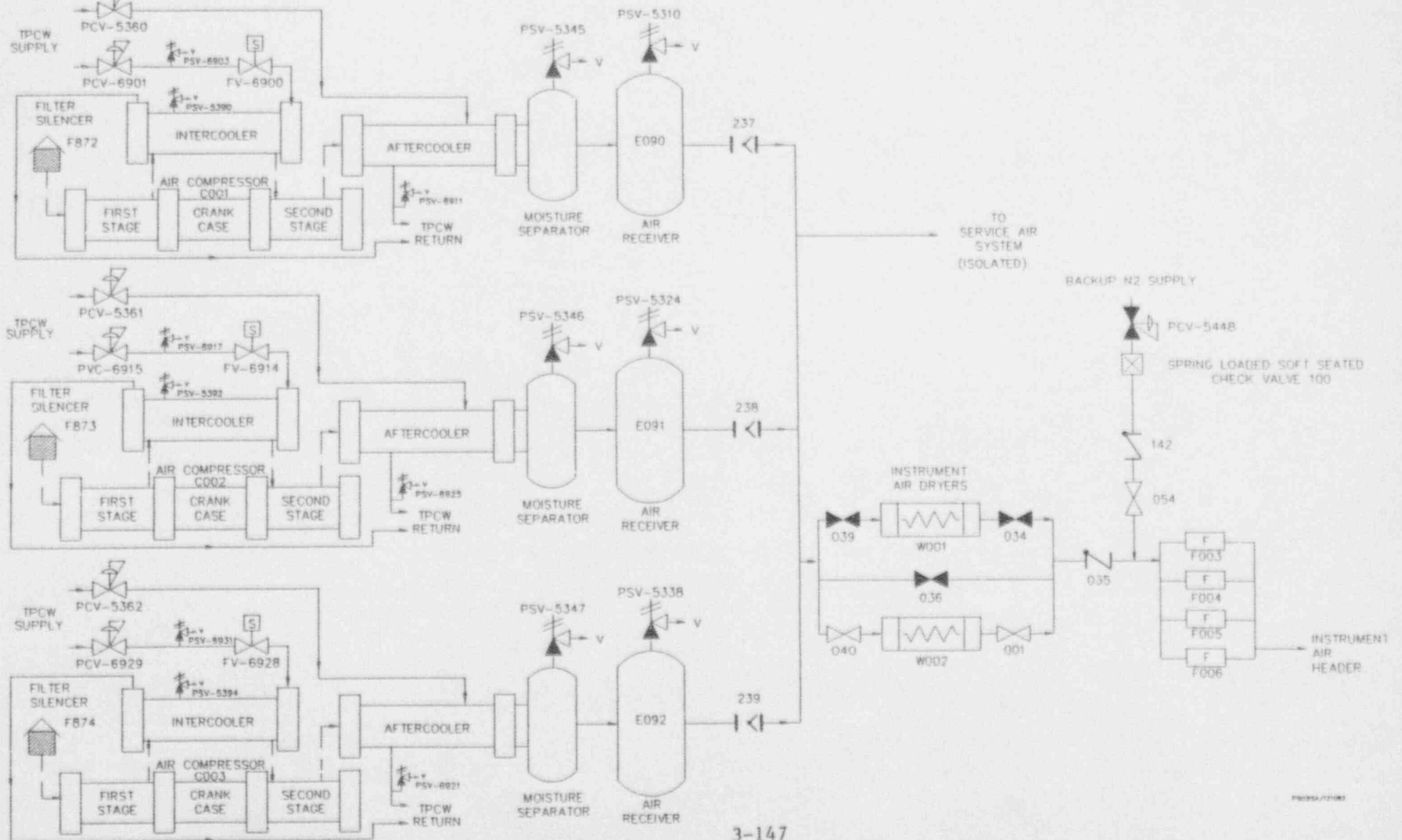
The chiller pumps discharge to a chiller unit (E-330/E-331). The chiller unit removes heat from the chilled water and transfers the heat to the turbine plant cooling water system. Chilled water from the chiller unit flows through the various system loads for both units and back to the suction of the chilled water pump.

The ESF Switchgear room emergency cooling system is made up of two emergency cooling units per unit, one for each train of ESF equipment. The emergency cooling units (E-255/E-257) provide recirculated air to the ESF Switchgear rooms.

The Emergency Chilled water system consists of two independent cooling trains A and B. Each train consists of a 400 ton chiller unit (E-336 & E-335) and one recirculating pump (P-162 & P-160).

Figure 3.2-13: IA Simplified P&ID

SAN ONOFRE UNITS 2/3 INSTRUMENT AIR SYSTEM



The emergency chillers can be cross-tied to the opposite unit's 4 kV bus should the normal power supply be rendered unavailable. Additionally, the CCW which supplies cooling water to the chillers can be cross-tied to the opposite unit.

The Normal & Emergency Chiller rooms ventilation system is comprised of a normal and emergency ventilation system. During normal operations the Normal & Emergency Chiller rooms are ventilated by means of a supply/exhaust fan combination. The normal supply fan (A-051) is designed to maintain the room temperature by drawing outside air into the normal chiller room and the two emergency chiller rooms. The exhaust fan (A-052) operates simultaneously with the supply fan, exhausting to atmosphere. The control circuit is provided with a lockout on normal exhaust fan operation.

The Emergency Chiller rooms emergency ventilating system is made up of a supply/exhaust fan combination. Operation of the fans occurs on startup of the Chiller units. The emergency supply fans (A-053/A-054) maintain the room temperature by drawing outside air into the rooms. The emergency exhaust fans (A-055/A-056) operate simultaneously with their respective supply fans, exhausting to atmosphere.

During normal operations the ESF Switchgear room is ventilated by means of a cooling unit, exhaust fan combination. The normal cooling unit (E-430) is designed to maintain the room temperature by drawing outside air through cooling coils. The exhaust fan (A-165) operates simultaneously with the cooling unit, exhausting to atmosphere. The cooling unit is controlled by a thermostat. The control circuit is provided with lockouts on a fire protection actuation, and exhaust fan low DP. During normal plant operation, one chilled water pump and one chiller unit are operating. The second pump is in stand-by, operating only when needed. The second chiller is secured and isolated.

The Emergency Chilled water system will automatically supply chilled water to various cooling units throughout both Units 2 and 3, upon receipt of a SIAS, TGIS, CRIS, or FHIS from either unit. The operational functions for the two trains are the same as the Normal Chilled water system with the exception of the heat from the chiller unit is removed by the CCW system.

The support systems required for the HVAC system include electric power, TPCW and CCW. The system dependencies are tabulated in Table 3.2-1. Simplified P&IDs of the ESF switchgear room coolers, chilled water system, and Chiller room HVAC are presented in Figures 3.2-14 through 3.2-16.

Figure 3.2-14: ESF Switchgear HVAC Simplified P&ID

SONGS 2/3 HVAC SYSTEM ESF SWITCHGEAR AND BATTERY EQUIPMENT ROOMS

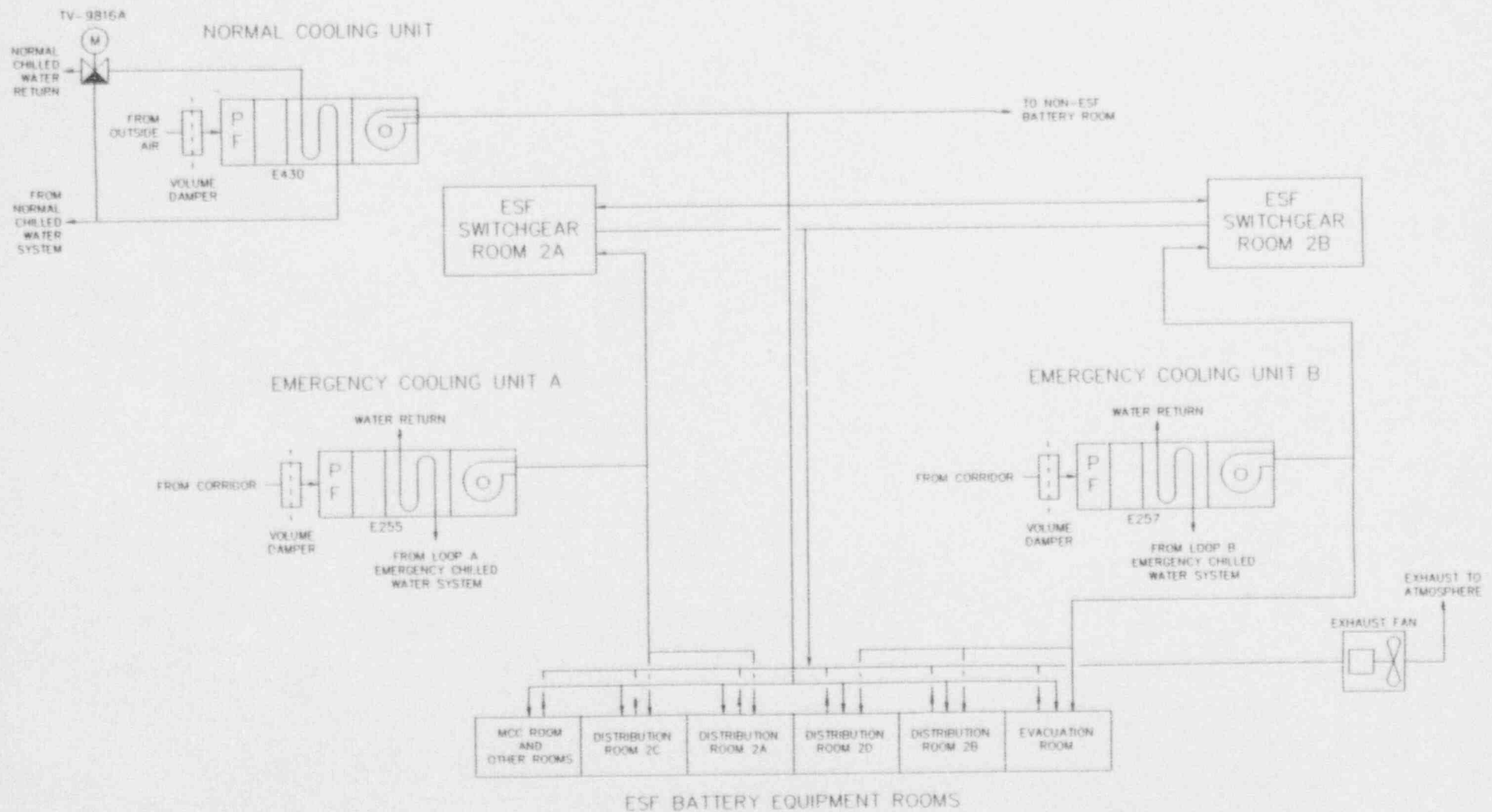


Figure 3.2 - 15: Chilled Water System Simplified P&ID

SONGS 2/3 CHILLED WATER SYSTEM

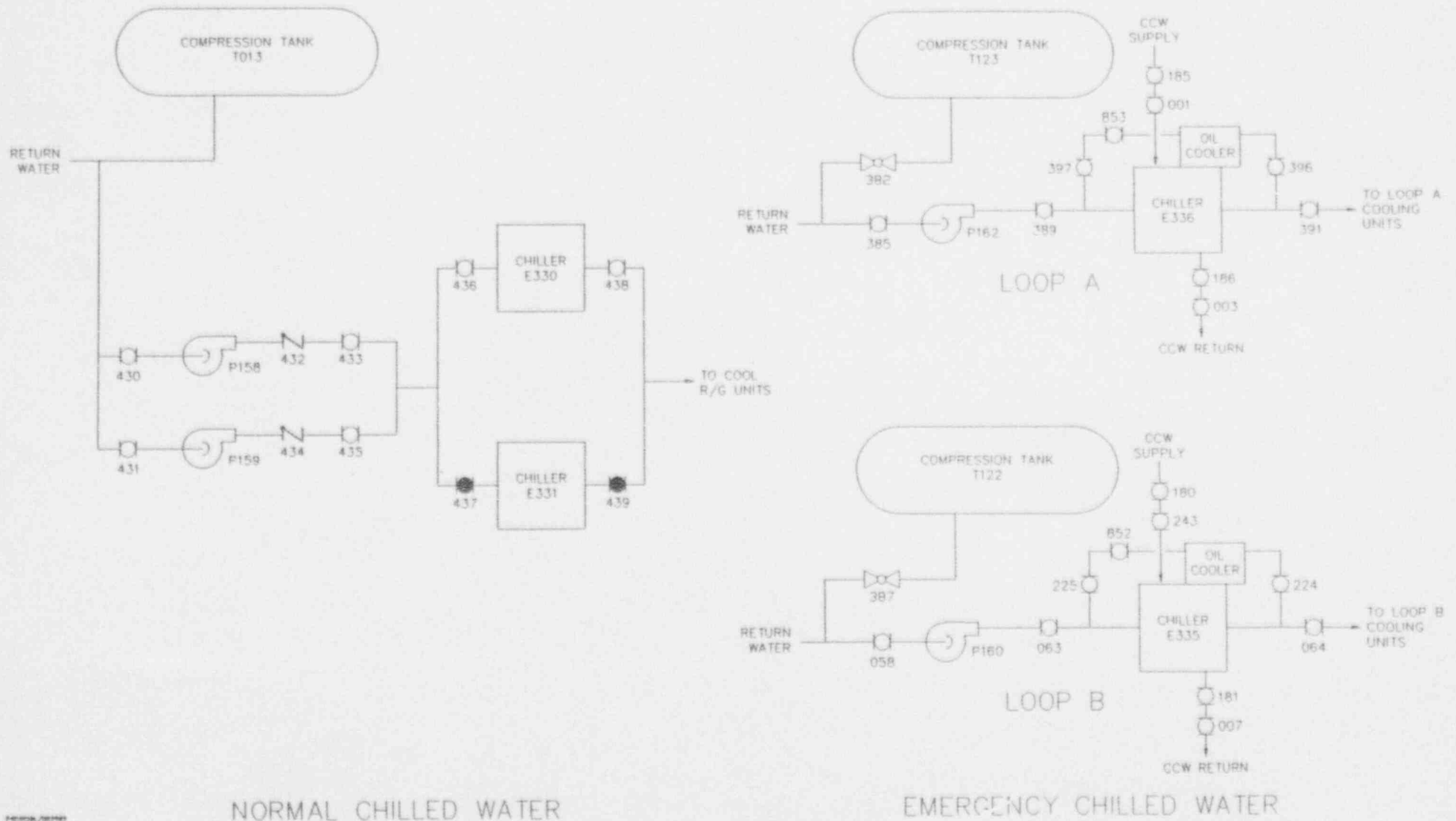
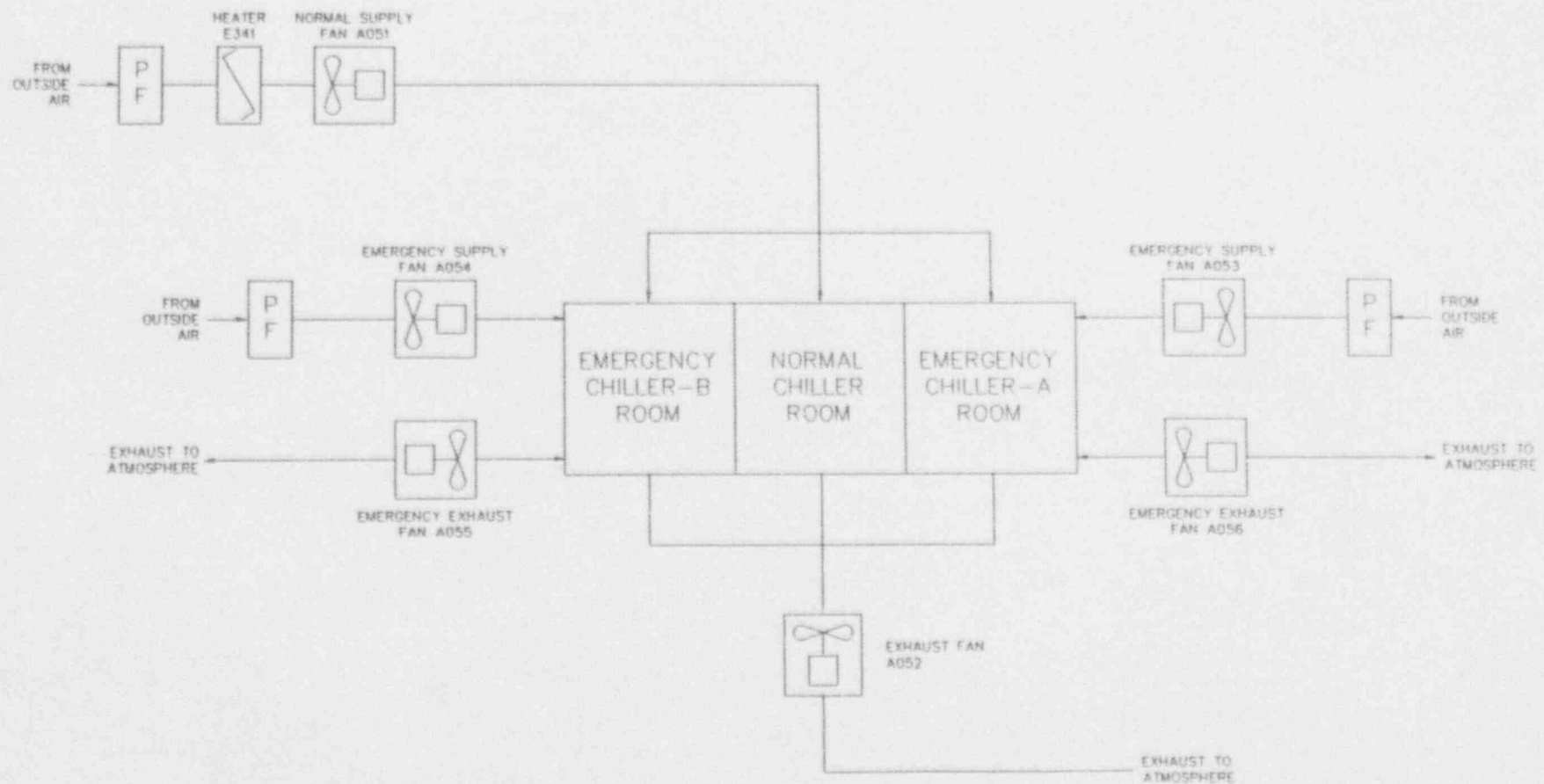


Figure 3.2-16: Chiller Room HVAC Simplified P&ID

SONGS 2/3 HVAC SYSTEM CHILLER ROOM HVAC



3.2.14 Electric Power

The function of the Electric Power System modeled in the IPE is to provide general support for operation of DC and AC powered electrical devices.

The AC Electric Power System at SONGS 2/3 consists of the 6.9 kV System, 4.16 kV System, the 480 VAC System, the 120 VAC System, and the Onsite AC Power System (composed of the diesel generators). The AC Electrical Power System includes both Class 1E and Class non-1E. The Class 1E system consists of two 4.16 kV buses per unit, their 480 V buses, and the 120 VAC Vital buses. The system is divided into two trains. Each train consists of one Class 1E 4.16 kV bus, one 480 V load center, four 480 V motor control centers (MCC's), a common 480 V MCC (common to Units 2 and 3), a 208/120 V distribution system, and two 120 VAC Vital buses. Each of the two 120 VAC Vital buses is powered by an inverter from a dedicated 125 VDC battery bus. Each 125 VDC battery bus is connected to a battery charger powered by a vital 480 VAC MCC.

Each 4.16 kV bus is normally supplied by one of two reserve auxiliary transformers in the same Unit. The connections are designed such that with both Units operating, the two redundant 4.16 kV ESF buses are never energized by the same transformer. If a loss of power on a 4.16 kV bus occurs, the bus will be automatically transferred to its companion bus on the other unit provided that it is powered by its reserve auxiliary transformer or unit auxiliary transformer. If this supply is unavailable, the train dedicated onsite EDG will automatically energize the bus. The two 4.16 kV buses can also be supplied by the same transformer of the other Unit provided the supplying Unit is shutdown.

The EDGs are designed to be redundant standby power sources capable of furnishing adequate power to safely shut down the reactor, remove reactor residual heat, and maintain the plant in a safe shutdown condition upon the loss of preferred power with or without a coincident design basis event (DBE).

Two tandem EDGs per unit are provided to generate and supply the required standby power to the redundant 4.16 kV ESF buses. These buses will supply all of the ESF loads and those non-ESF loads for which it is desirable to have manually switched over to the diesel generators.

Each EDG unit is designed to start automatically upon receipt of a start signal, attain rated speed and voltage within 10 seconds of receiving the start signal and to accept automatically

connected ESF loads in sequence, or manually connected loads required for shutdown without offsite power.

Each of the EDGs is provided with a dedicated cooling system. As such, there is no dependence on plant service water or CCW flow.

Each EDG is also provided with an air starting system. The air receivers provide sufficient air for five start attempts. Subsequent attempts, if required, would require the use of AC powered air compressors or other source of compressed air. Fuel for the EDG is provided by an independent fuel oil system.

Each fuel oil system consists of an underground storage tank, two transfer pumps (normal and standby), day tanks, and transfer piping. The normal transfer pump is designed to automatically start as necessary to refill the day tanks. If the normal transfer pump fails, manual operator action is required to start the standby transfer pump. Control circuits for each EDG operate from a separate Class 1E 125 VDC system supplied by Class 1E station battery.

The 120 VAC Vital System consists of two buses per train energized by dedicated inverters. Each inverter is connected to a dedicated DC subsystem. As such, loss of any individual Class 1E battery, bus, or chargers would impact only one 120 VAC Vital bus. Upon loss of the DC supply to an inverter, the associated 120 VAC bus will lose power. The transfer to an alternate AC power source for the vital bus is a manual transfer which must be performed at the inverter.

The Non-Class 1E system consists of four 4.16 kV buses per unit, their downstream 480 VAC buses, various 120 VAC buses, and the non-Class 1E UPS distribution panel, Q069. The 208/120 VAC UPS distribution panel Q069 is powered by an inverter from a 250 VDC battery bus. The 250 VDC bus is connected to a battery charger powered through transformer T014 by a circuit breaker in 1E 4.16 kV bus A04. In order to maintain adequate separation between 1E and non-1E equipment, this A04 circuit breaker trips open automatically when a SIAS occurs. Inverter Y012 provides the normal source of AC power for the 120 VAC non-1E instrument bus. A static transfer switch initiates transfer of the load from the inverter output to the alternate source upon loss of inverter. Inverters Y005, Y010 and Y011 do not supply any loads considered on the IPE models and are not described. The non-Class 1E AC system also consists of 6.9 kV buses which power the RCPs.

The DC Electric Power System at SONGS 2/3 consists of the 125 VDC and 250 VDC systems. The overall DC Electrical Power System includes both Class 1E and Non-Class 1E distribution systems.

The Class 1E system consists of four 125 VDC buses per unit, their associated batteries and chargers, and downstream distribution panels. The system is divided into two ESF trains. Each ESF train consists of two 125 VDC buses and their associated system components. There are no shared components between any of the four DC buses. The four buses are designated D1, D2, D3, and D4. Buses D1 and D2 provide control power for 4.16 kV and 480 V buses and the EDG control systems. Buses D1 and D2 also provide DC power to inverters Y001 and Y002, respectively. Provision exists to cross connect D2 and D4 in Modes 5 and 6. DC buses D3 and D4 provide power for NSSS control and DC power to inverters Y003 and Y004, as well as to the inverters Y006 and Y007 for the two redundant SDC system suction isolation valves.

The non-Class 1E systems consists of a 125 VDC distribution system (Bus D5), a 125 VDC system (HPCS), a 250 VDC distribution system (Bus D6) and a 250 VDC uninterruptible power system (UPS). One system is provided for each unit except for the HPCS which is common for both units. Each system consists of a battery, a battery charger, an inverter, and downstream distribution panels. Bus D6 is provided with one normal and one standby battery charger.

Bus D5 provides DC control power for the circuit breakers and protective relays associated with the 6.9 kV, the non-ESF 4160 V and 480 V switchgear. D5 also provides DC power to inverter Y005 which supplies 120 VAC power to the PMS computer distribution panel Q060. Bus D6 provides DC power to inverter Y010 which supplies 120 VAC power to the CFMS distribution panel Q071.

The 250 VDC UPS provides a primary source of power for the 208/120 VAC UPS distribution panel Q069. This panel provides power supplies for the Anticipated Transient Without Scram/Diverse Scram Systems via inverter Y012.

The battery chargers for D5 and D6 are powered from non-Class 1E 480 V MCCs and the charger for the HPCS is powered from Class-1E 480 V MCC common for both units. Because of the large size of inverter Y012, the charger for the UPS system is powered from 4.16 kV bus A04. Upon loss of power from inverter Y012, a static transfer switch integral to the inverter automatically transfers the load from the inverter output to the 480 V MCC bus B12, the alternate supply to Q069.

Each Class 1E 4.16 kV bus is provided with loss of voltage detection circuits. A Loss of Voltage Signal (LOVS) is generated upon actuation of at least two-out-of-four undervoltage relays on either 4160 VAC bus. If there is a loss of power or undervoltage condition on the bus, the following automatic actions take place in sequence until power is restored.

- The undervoltage condition at the bus actuates two-out-of-four undervoltage relays.
- After a delay of approximately 1 second, the undervoltage relays initiate a LOVS which trips the normal supply incoming feeder breaker.
- The LOVS sends a signal to start the EDG associated with the bus.
- After the bus voltage has decayed to 30% or less, a signal is sent to close the tie breaker to the other unit's bus provided that bus is supplied by its reserve auxiliary transformer or unit auxiliary transformer and has normal voltage.
- If the transfer to the other unit's bus is blocked, or is otherwise not completed within 4 seconds after initiation of the LOVS, all loads on the affected bus will be tripped except for the load center and HPSI pump feeders.
- After the EDG has obtained rated voltage and frequency, and the above conditions have been satisfied, the EDG breaker will close to energize the bus.

The 4.16 kV buses can also be supplied by the unit auxiliary transformer, but this requires significant manual operator action and is not credited for this analysis.

If a SIAS is generated, the EDGs will automatically start regardless of the availability of offsite power. In addition, the SIAS signal initiates load shed of Non-Class 1E loads that are energized from the Class 1E system. If no LOVS is present (the bus remains powered by offsite power), the EDG breaker will not close. If a SIAS and LOVS are both present, then the EDG breaker will close, and the Class 1E loads will be sequenced onto the bus at the appropriate times.

In the event of loss of power to a Class 1E 480 VAC bus, a manual cross connection of each train's 1E 480 VAC bus to the same bus in the other Unit through Common MCC BQ or BS is provided. For example, 2B04 can be cross-connected to 3B04 by deliberately overriding the Kirk-Key interlock in Common MCC BQ. This cross connection is meant to power very selected loads and cannot power all loads of 3B04 and 3B06.

The 120 VAC Vital buses are normally energized by the DC system. A manual transfer switch is provided to transfer a Vital bus to

an alternate AC supply in the event of inverter or DC supply failure. This transfer switch is located at the inverter.

Each of the non-Class 1E 4.16 KV buses is provided with undervoltage detection system. When the normal source of power for the Unit Auxiliary transformer is de-energized, an automatic transfer of each bus to the same Unit's Reserve Auxiliary transformers takes place. No provision exists for transfer of non-Class 1E 4.16 KV buses to transformers in the other Unit.

Each of the four Class 1E 125 VDC buses is normally supplied by a dedicated battery charger/station battery. The batteries for buses 2D1 and 2D2 are sized to carry the required safety loads for 90 minutes under normal conditions and for 4 hours during station blackout conditions with load shedding without battery charger support. The batteries for buses 2D3 and 2D4 are sized to carry the required safety loads for 8 hours without battery charger support. After these time periods, if the battery charger and/or its supply is not restored, the voltages available throughout the DC system may not be sufficient to ensure proper component operation.

Each of the non-Class 1E 125 VDC buses is normally supplied by a dedicated battery charger/battery. If a loss of AC power or charger failure should occur, the power will be supplied automatically by the stored energy in the battery for some period of time, after which the DC voltage available may not be sufficient to ensure proper component operation.

The support systems required for the Electric Power system include HVAC to the ESF switchgear rooms. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the Electric Power System is presented in Figures 3.2-17 through 3.2-20.

3.2.15 Plant Protection

The function of the Plant Protection System modeled in the IPE is to provide general support for operation of components in response to abnormal plant conditions.

The PPS maintains plant safety by monitoring various plant parameters, and initiating protective response if any parameter indicates a hazardous condition. The PPS consists of two separate subsystems: the RPS and ESFAS.

The RPS is designed for accident prevention and the ESFAS for accident response. The ESFAS generates the following signals: SIAS, RAS, CIAS, CSAS, MSIS, EFAS, and CCAS.

Figure 3.2-17: 1E AC Electric Power Simplified P&ID

SAN ONOFRE UNITS 2/3 CLASS 1E AC POWER SYSTEM

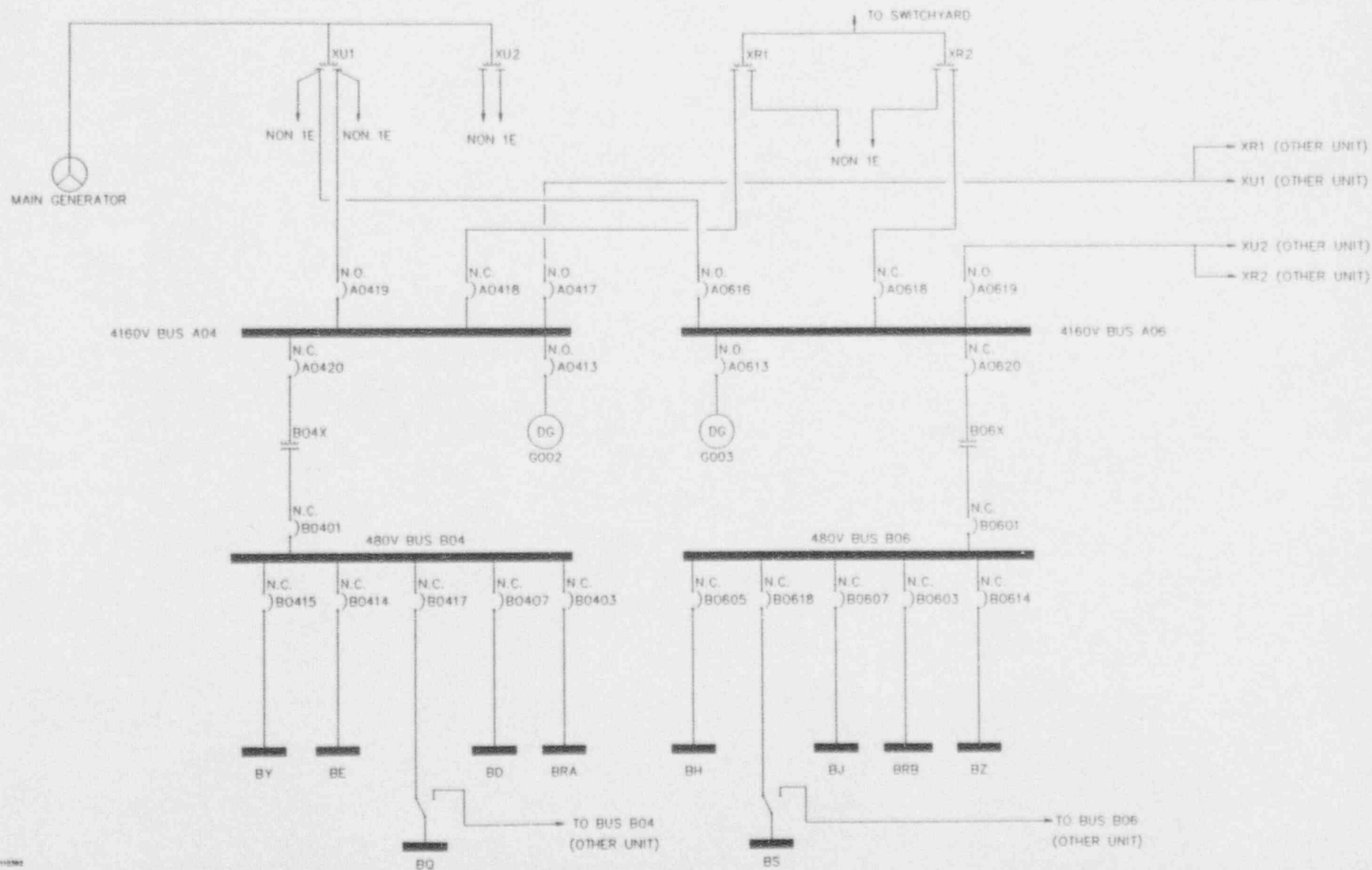
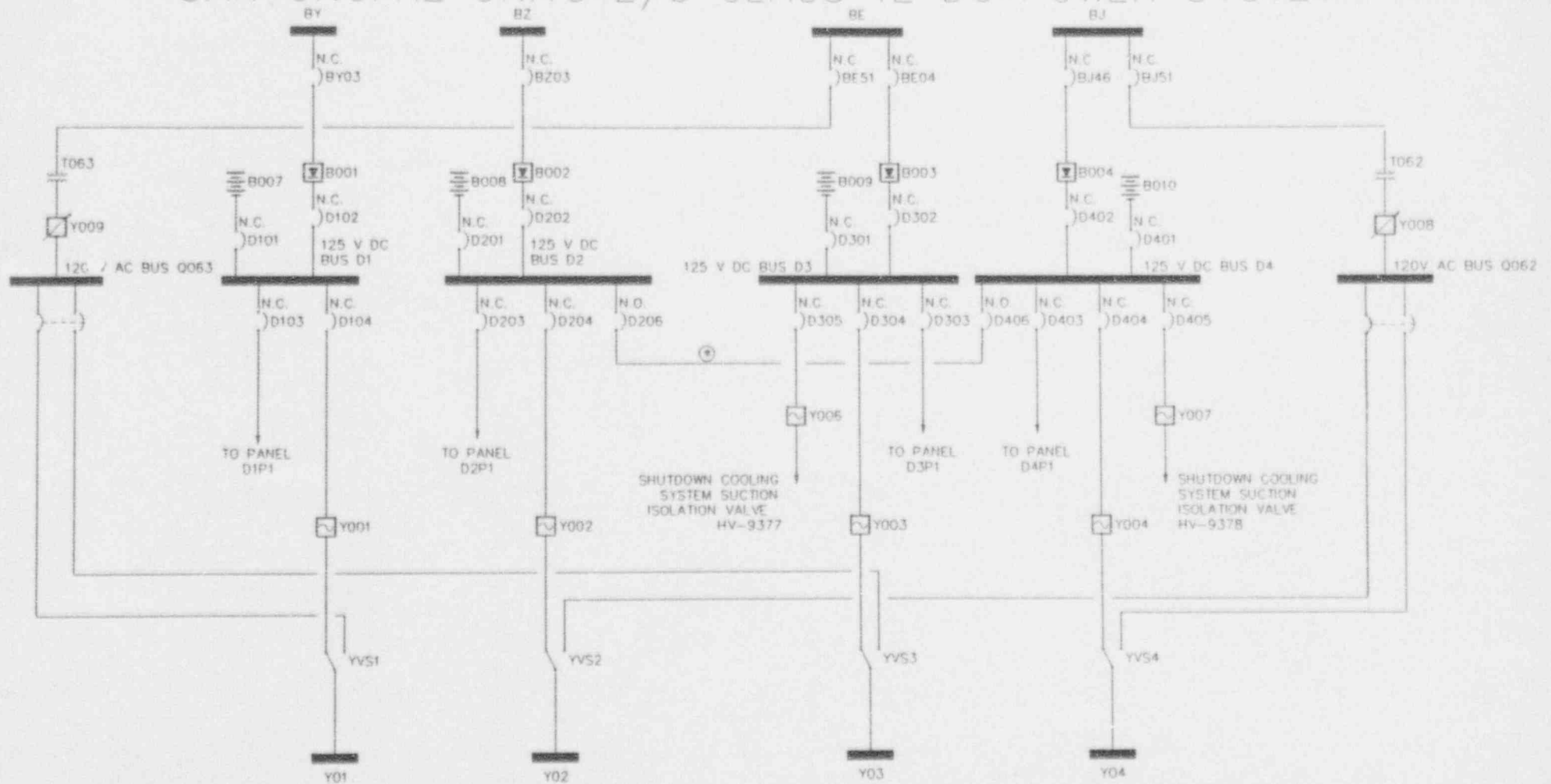


Figure 3.2-18: 1E DC Electric Power Simplified P&ID

SAN ONOFRE UNITS 2/3 CLASS 1E DC POWER SYSTEM



⊙ UNIT 2 ONLY

Figure 3.2-19: Non-1E AC Electric Power Simplified P&ID

SAN ONOFRE UNITS 2/3 NON-1E AC POWER SYSTEM

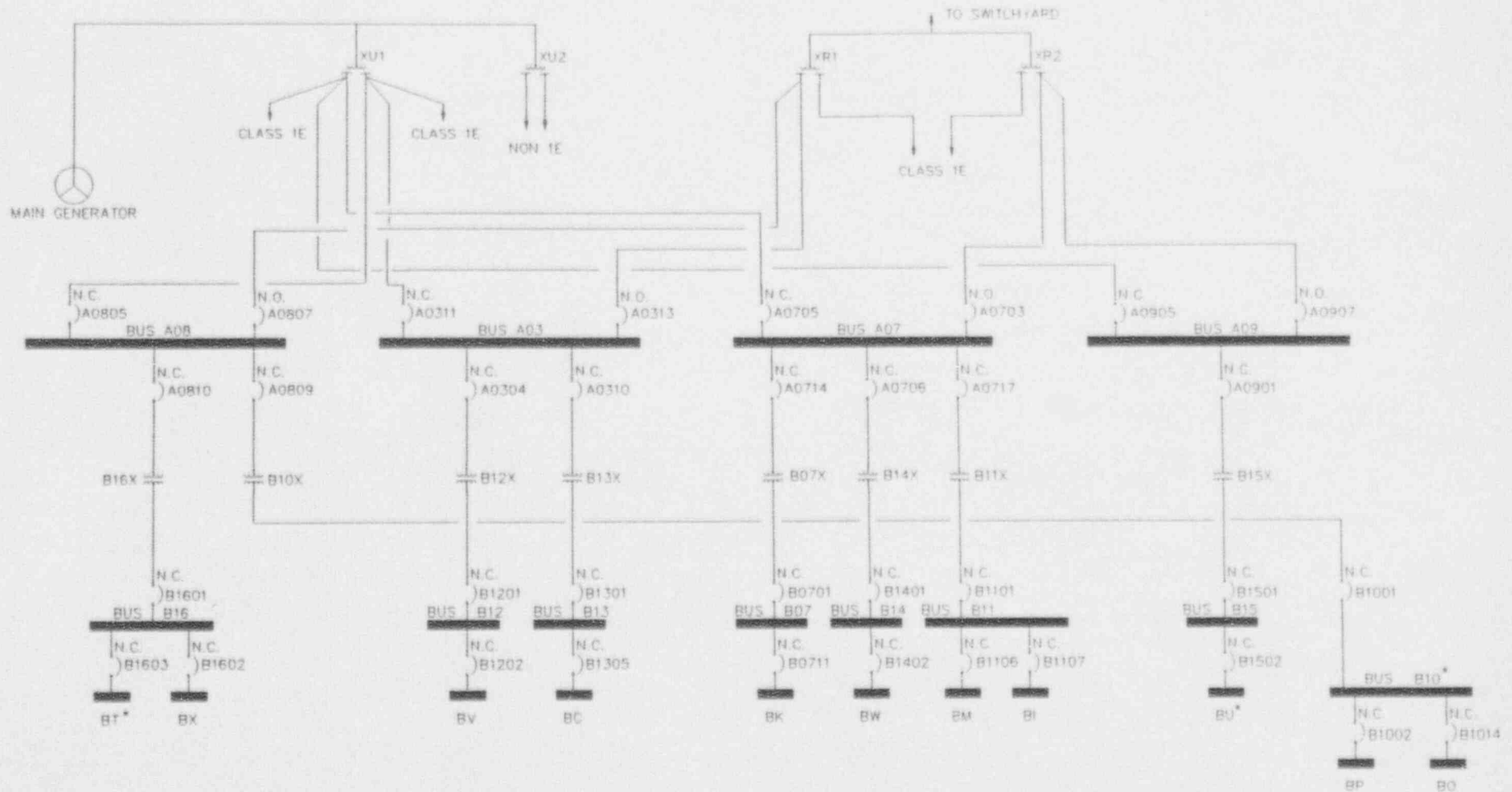
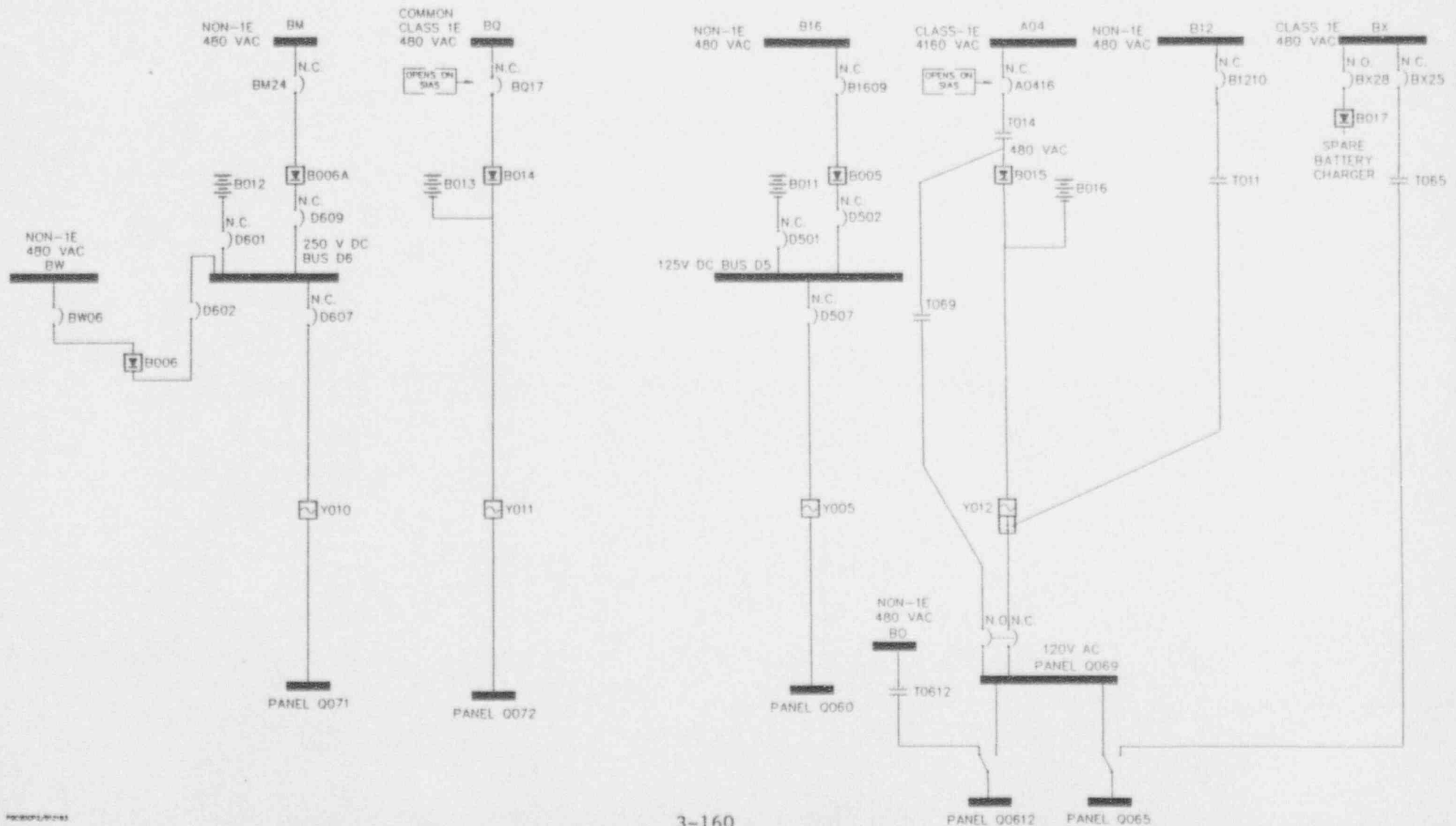


Figure 3.2-20: Non-1E DC Electric Power Simplified P&ID

SAN ONOFRE UNITS 2/3 CLASS NON-1E DC POWER SYSTEM



The PPS receives signals from sensors measuring critical plant parameters. The sensor signals consist of four redundant isolated channels. A single parameter must indicate an unsafe condition on at least two of the four like sensor channels before the protective response is initiated. With one sensor channel bypassed (for test or maintenance), a two-out-of-three coincidence logic will initiate the protective response.

Each of these input parameters is transmitted to an input device, which is either a bistable comparator card, a differential bistable comparator card, or an auxiliary relay card. This device is known as a trip unit. In the trip unit, each input parameter (voltage) is compared to the preset trip setpoint level. If the input is recognized as a trip, it is directed to three-out-of-six relay matrices, depending on the receiving channel(s). These matrices are designed to account for every possible combination of the monitoring channels. If the same parameter trips on more than one channel, the trip is transmitted to trip path relays. These relays force initiation of system response. A manual trip actuation also initiates system response. It should be noted that most of the PPS equipment includes dual auctioneered power supplies so that the system is not affected by single local power supply failures. Loss of the vital bus or the 125 VDC bus, however, will cause a trip to be generated in the affected circuits.

The RPS protects the reactor core and the Reactor Coolant System by forcing a reactor shutdown if a measured parameter indicates an unsafe level. An RPS actuation is generated from High Linear Power Level, High Logarithmic Power Level, High Local Power Density, Low Departure from Nucleate Boiling Ratio (DNBR), High Pressurizer Pressure, Low Pressurizer Pressure, Low Steam Generator Water Level, High Steam Generator Water Level, Low Steam Generator Pressure, High Containment Pressure, Low Reactor Coolant Flow, and High Seismic Acceleration.

Upon receipt of a trip signal from two-out-of-four like input parameter channels, the RPS logic matrix signals the reactor to trip.

The RPS trip paths differ from the generic trip path previously described. The four RPS trip paths consist of under-voltage (UV) trip coils and shut trip coils. These trip coils are actuated by the logic matrices, or a manual trip signal. Trip coils actuate eight reactor trip circuit breakers (TCB'S). TCB's one and five are controlled by trip path one; two and six are controlled by trip path two; three and seven are controlled by trip path three; four and eight are controlled by trip path four. A ninth TCB ties the two motor generator buses together. TCB's one, two, seven and eight can interrupt one Control Element Drive

Mechanism (CEDM) power supply. TCB's three, four, five, and six can interrupt the other CEDM power supply. A successful reactor trip requires that at least one of the breakers in each of the pairs listed below trip in order to fully interrupt electric power to the control element assembly holding coils:

- breakers 1 and 2
- breakers 3 and 4
- breakers 5 and 6
- breakers 7 and 8

The UV trip coils actuate upon a loss of power, but the shunt trip coils require 125 VDC power in order to actuate a trip.

When the TCBs interrupt the CEDM power supply, the Control Element Assemblies drop into the core. A trip signal is also sent to the turbine controls and the feedwater control/steam bypass system.

The SIAS actuates the Safety Injection System components necessary to inject borated water into the RCS. The SI System provides cooling to limit core damage and assure adequate shutdown margin, regardless of temperature, during a LOCA, steam line break accident, or steam generator tube rupture.

The SIAS input parameters which detect these accidents are low pressurizer pressure at 1740 psia (combined with no pressurizer pressure bypass) or high containment pressure at 3.4 psig. The SIAS initiation logic (trip paths) differ from the generic trip path in that the SIAS initiation relays are mechanical, not solid state.

Upon receipt of a signal from two-out-of-four like input parameter channels, the SIAS actuates the following components:

- HPSI system pumps
- HPSI discharge isolation valves to the RCS cold legs
- LPSI system pumps
- LPSI discharge isolation valves to the RCS cold legs
- CS system pumps
- Charging pumps

The RAS initiates recirculation of borated water from the containment sump by switching containment spray and HPSI pump suction from the refueling water storage tank (RWST) to the containment sump. This change allows continuous long term post-accident core cooling using HPSI, following a LOCA. The RAS must be initiated to prevent draining the RWST and losing suction to the SI pumps. The RAS input parameter is low RWST water level at 18.5%. Main Control Board manual trip pushbuttons are not provided for the RAS signal (all other signals have control room manual initiation pushbuttons). Manual pushbuttons are available, however, on the auxiliary relay cabinets.

Upon receipt of signals from two-out-of-four of the channels for low RWST level, the RAS signals the following:

- Opens containment sump valves to HPSI pumps and CS pumps
- Stops LPSI pumps
- Closes ECCS pump mini-flow valves (concurrent with a high containment sump level signal).

The CCAS initiates the emergency fan cooling units inside containment under accident conditions. The fan coolers work in conjunction with the CS system to remove heat from the containment to ensure long-term core cooling.

The CCAS input parameters are identical to the SIAS parameters, low pressurizer pressure (combined with no pressurizer bypass) or high-high containment pressure. Upon receipt of a signal from two of four like input parameter channels, the CCAS actuates the following components:

- Containment emergency fan coolers
- Dome air circulating fans
- CCW isolation valves to the containment fan coolers

The CIAS initiates isolation of process lines penetrating the containment. Isolation prevents the potential release of radioactive material during a LOCA or a steam line break accident. The CIAS input parameter is high containment pressure at 3.4 psig. The CIAS initiation paths differ from the generic trip path in that CIAS initiation relays are mechanical, not solid state.

Upon receipt of signals from two-out-of-four of the channels for high containment pressure, the CIAS signals containment isolation valves to close.

The CSAS initiates spraying of cool, borated water through containment atmosphere. The spray removes heat and iodine from the containment area. Containment heat removal is required to maintain temperature and pressure below design values during and following a LOCA or steam line break accident. The CSAS input parameter is (high-high) containment pressure coincident with SIAS.

Upon receipt of SIAS (taken from each logic matrix) and signals from two-out-of-four of the channels for (high-high) containment pressure, the CSAS signals the containment spray discharge valves to open (containment spray pumps start on SIAS).

The MSIS initiates isolation of both steam generators. This isolation ensures termination of blowdown, feedwater flow and main steam flow in the event of a steam/feed line break or a steam generator tube rupture. The MSIS input parameter is low steam generator pressure at 741 psia.

Upon receipt (from one of the two steam generators) of signals from two-out-of-four of the channels for low steam generator pressure, the MSIS closes the main steam line isolation valves, steam generator AFW isolation valves (if open), steam generator blowdown isolation valves, and feedwater isolation valves for both steam generators.

It should be noted that if an EFAS is also present, then the EFAS signal will override the valve closure signals sent to the AFW isolation valves.

The EFAS initiates the emergency mode of the AFW system to the intact steam generator(s) following a steam line break or loss of feedwater accident. The AFW system provides the intact steam generator(s) with sufficient feedwater for cooling during and following a steam line break accident, or loss of main feedwater.

The EFAS input parameters are:

- Low steam generator water level, (E-088 or E-089)
- Low steam generator pressure, (E-088 or E-089)
- E-088 pressure greater than E-089
- E-089 pressure greater than E-088

The following combinations of input trip parameters actuate EFAS:

- Low E-089 level and not low E-089 pressure actuates EFAS-1.
- Low E-089 level and E-089 pressure greater than E-088 actuates EFAS-1.
- Low E-088 level and not low E-088 pressure actuates EFAS-2.
- Low E-088 level and E-088 pressure greater than E-089 actuates EFAS-2.

In addition to the actuation relays typical to each of the ESFAS subsystems, the EFAS logic also includes cycling relays. These relays override MSIS valve closure signals sent to the AFW isolation valves and cycle the flow control valve(s) to maintain steam generator water level.

The instrumentation for each steam generator remains independent. Upon receipt of the appropriate combination of signals, EFAS starts the AFW pumps and opens flow control and isolation valves to the appropriate steam generator(s).

The EFAS logic consists of two separate initiation circuits; EFAS-1 and EFAS-2. EFAS-1 automatically actuates AFW system pumps and valves that feed steam generator No. 1 (E089) while EFAS-2 automatically actuates AFW system pumps and valves that feed steam generator No. 2 (E088). Each EFAS signal and the AFW system component associated with each signal are in turn composed of two redundant trains; Train A and Train B.

EFAS-1 Train A is designed to initiate the motor-driven AFW pump P-141 with associated valves while Train B initiates the turbine-driven AFW pump P-140 with associated valves. EFAS-2 Train A initiates P-140 with valves, while Train B initiates a separate motor-driven pump P-504.

The LOVS is not actually a portion of the PPS. However, it serves an important safety function that is similar to those of the PPS signals. The LOV signal provides a start signal to the EDG connected to the safety bus that experiences a loss of electric power. The LOV signal also initiates the load sequencing actions that restore power to safety loads once the EDG has started.

One LOV signal is generated for each bus. Upon the detection of an undervoltage condition, the LOV generates signals to trip the

bus feeder breakers, to start the EDG, and to initiate load sequencing.

The PPS subsystems are designed so as to generate appropriate trip signals upon loss of its sensor inputs or various power supplies. As such, the PPS is independent of all support systems for generating a trip signal. However, the PPS relies on several support systems during normal (i.e., non-tripped) operation.

Power for the PPS instrumentation is provided by a number of instrument power supplies that are fed from the four 120 VAC vital instrument busses. One vital bus powers all of the circuitry in a PPS channel. The sensor inputs to the PPS channels are provided by various instruments located in other systems or structures in the plant, including the RCS, the steam generators, the containment, the Nuclear Instrumentation system, and the CEDM Control System.

The only support system required for the PPS system is electric power. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the Plant Protection System is presented in Figures 3.2-21 through 3.2-24.

Figure 3.2-21: ESTAS Functional Block Diagram

SONGS 2/3
ENGINEERED SAFETY FEATURES ACTUATION SYSTEM FUNCTIONAL BLOCK DIAGRAM

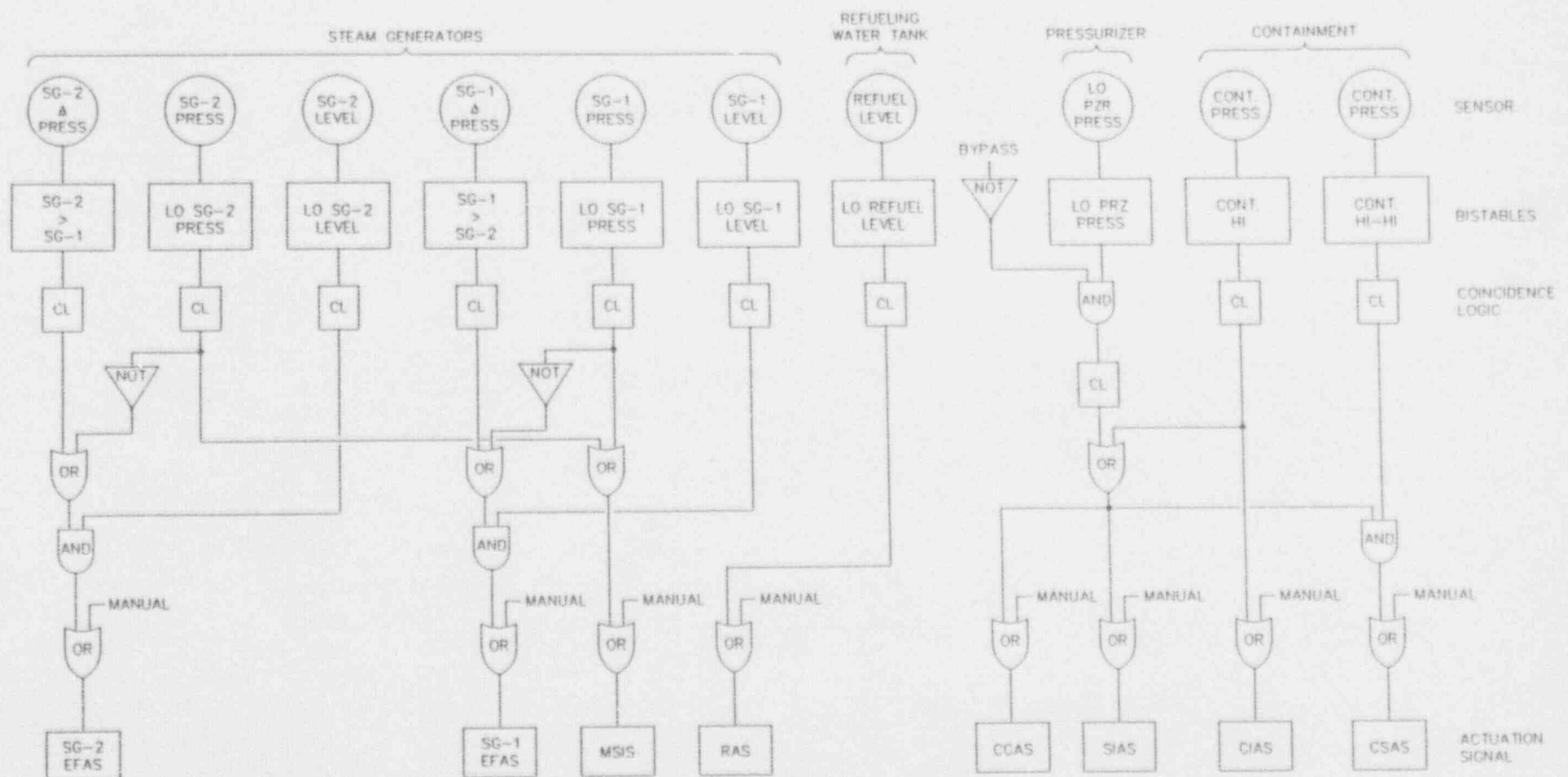


Figure 3.2-22: ESFAS Primary Block Diagram

SONGS UNITS 2/3 PLANT PROTECTION SYSTEM PRIMARY BLOCK DIAGRAM FOR ESFAS

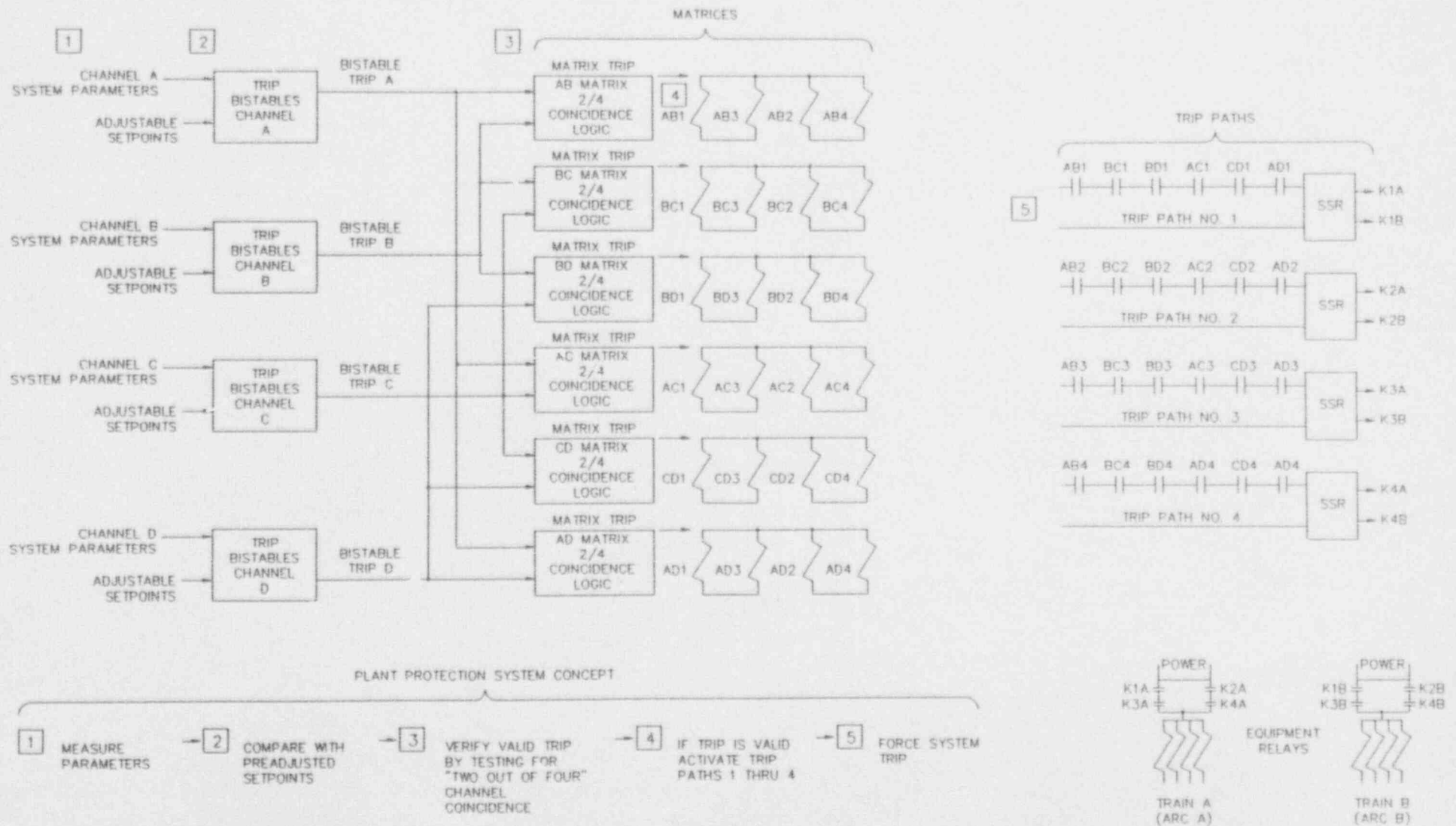


Figure 3.2-23: RPS Functional Block Diagram

SONGS 2/3
REACTOR PROTECTION SYSTEM FUNCTIONAL BLOCK DIAGRAM

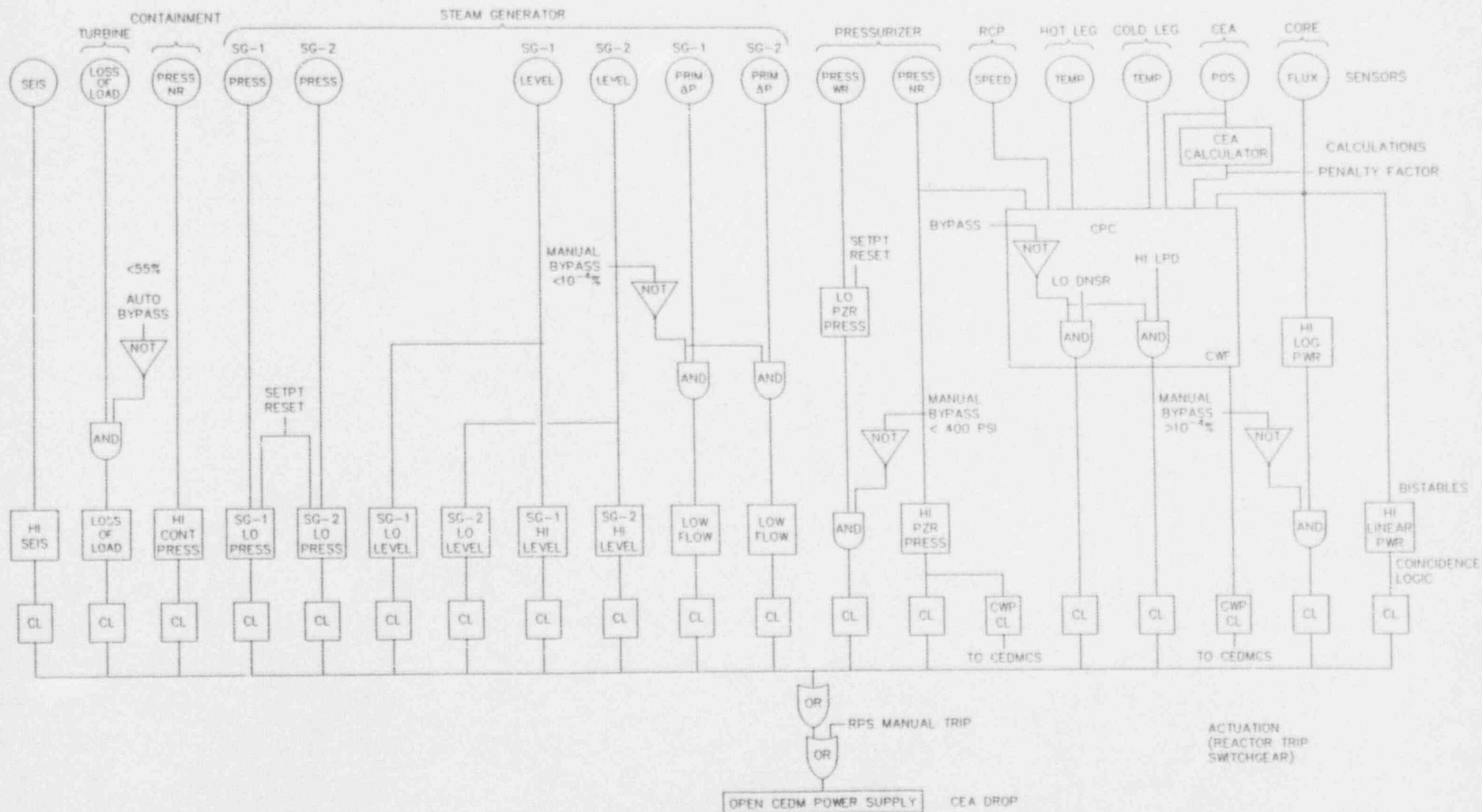
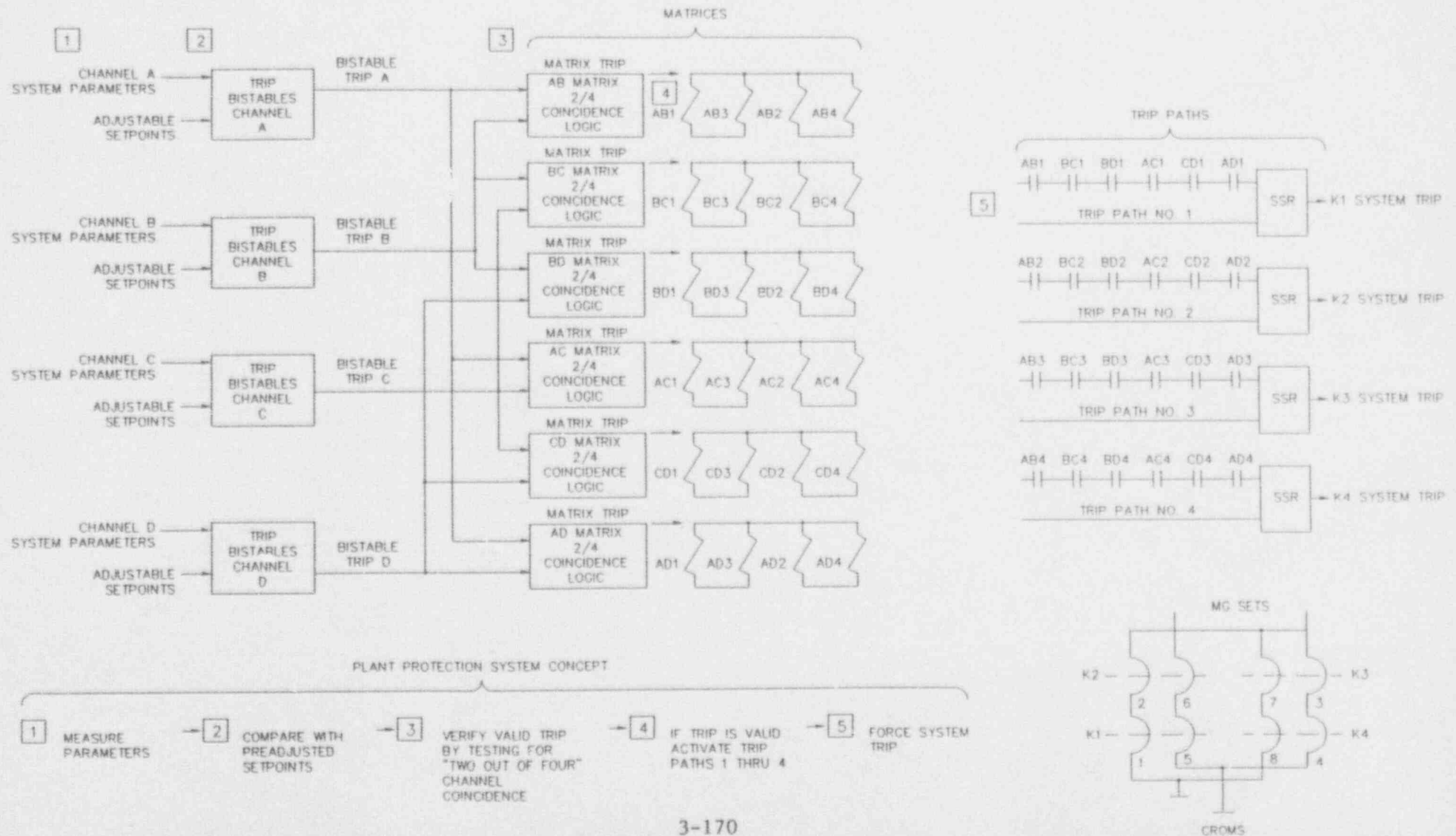


Figure 3.2-24: RPS Primary Block Diagram

SONGS UNITS 2/3

PLANT PROTECTION SYSTEM PRIMARY BLOCK DIAGRAM FOR RPS



3.2.16 Containment Isolation

The function of the Containment Isolation System modeled in the IPE is to isolate containment boundary to prevent or limit the escape of fission products that may result from postulated accidents.

The CIS consists of two redundant trains, Train A and Train B. The instrumentation and controls of the valves in Train A are physically and electrically separate and independent of the instrumentation and controls of the valves in Train B.

The redundant containment isolation valves are provided with diverse valve actuators to avoid common mode failures. In general, isolation valves that are outside containment and are not required to function during post-LOCA conditions are designed to fail in the safe position. These valves are provided with air operators and a spring return to the safe (closed) position. Isolation valves located inside the containment are generally motor-operated valves. These valves with a normally open valve position, fail as-is upon loss of actuating power. This design is based upon the consideration of valve position that ensure the greatest plant safety. All motor-operated containment isolation valves have manual handwheel operators, so that they may be closed or opened on loss of primary motive power. All the valves receiving automatic actuation signals are also provided with remote manual controls in the control room.

Exceptions to the rule of diverse valve actuators for redundant isolation valves include: (1) Small (1 in. or smaller) lines that have solenoid-operated valves both inside and outside the containment. These penetrations are numbered 16A, 16B, 16C, 27C, 30A, and 30B and (2) The penetration (number 9) for shutdown has four motor-operated valves, two inside and two outside the containment. The penetrations (numbers 54 and 55) for containment sump recirculation each have one motor-operated valve inside and outside the containment. All these valves are powered from the Class 1E electric power system as they are required to operate under post-accident conditions.

The CIS actuation system continuously monitors the containment pressure via four independent process instrument channels, (A, B, C, and D), and performs actuation logic to initiate safeguards when two-out-of-four high containment pressure (≥ 3.4 psig) signals are received. The SIS actuates CIS components when either two-out-of-four high containment pressure (≥ 3.4 psig) or two-out-of-four low pressurizer pressure (≤ 1740 psia) signals are received. The loss of electrical power to two of the four like channels in the measurement channels or initiating logic, or to the selective two-out-of-four actuating logic would also

actuate the CIS. In addition, manual initiation of the CIS is provided in the control room.

The CIS is automatically actuated by a CIAS from the ESPAS by two-out-of-four containment high pressure signals, manual operation, or loss of electrical power. To provide diversity in the parameters sensed for initiation, a SIAS will also actuate the CIS components with the exception of the MSIVs, MFIVs and the CCW containment isolation valves. In addition, the containment purge supply and exhaust isolation valves are closed by CPIS.

When CIAS has initiated, all Containment Isolation valves shown on Table 3.2-2 will close. Although the actuation of the CIS is automatic and does not require operator action, sufficient information is provided in the control room to allow the operator to monitor the operation of the CIS and related systems during normal operating and post-accident conditions and to take any anticipatory action that may be desirable.

The support systems required for the CIS include AC power, DC power, and Instrument Air. The system dependencies are tabulated in Table 3.2-1. A simplified P&ID of the CIS is presented in Figure 3.2-25.

Table 3.2-2
CONTAINMENT ISOLATION VALVES THAT CLOSE ON CIAS

Valve Number	Description	Location	Fluid [†]	Open to Contmt?	Comments
HV8204	Main Steam Line	Outside	SS	N	Normally open.
HV8205	Main Steam Line	Outside	SS	N	Normally open.
HV4052	Steam Generator Feedwater	Outside	SC	N	Normally open.
HV4048	Steam Generator Feedwater	Outside	SC	N	Normally open.
HV6211	CCW Inlet	Outside	DW	N	Normally open.
HV6223	CCW Inlet	Inside	DW	N	Normally open.
HV6236	CCW Outlet	Inside	DW	N	Normally open.
HV6216	CCW Outlet	Outside	DW	N	Normally open.
HV9821	Cont Mini-Purge Inlet	Outside	CA	Y	Normally open.
HV9823	Cont Mini-Purge Inlet	Inside	CA	Y	Normally open.
HV9825	Cont Mini-Purge Outlet	Outside	CA	Y	Normally open.
HV9824	Cont Mini-Purge Outlet	Inside	CA	Y	Normally open.
HV9920	Cont Norm A/C Inlet	Outside	DW	N	Normally open.
HV9900	Cont Norm A/C Inlet	Inside	DW	N	Normally open.
HV9971	Cont Norm A/C Outlet	Inside	DW	N	Normally open.
HV9921	Cont Norm A/C Outlet	Outside	DW	N	Normally open.
HV7911	Demin Water to Stations & Sumps	Outside	DW	N	Normally open.
HV5803	Cont Sump Pump Discharge	Inside	SD	N	Normally open.
HV5804	Cont Sump Pump Discharge	Outside	SD	N	Normally open.
HV7259	Cont Waste Gas Vent Header	Outside	WG	N	Normally open.
HV7258	Cont Waste Gas Vent Header	Inside	WG	N	Normally open.
TV9267	Letdown Line to Letdown HX	Inside	PC	N	Normally open.
HV9205	Letdown Line to Letdown HX	Outside	PC	N	Normally open.
HV5388	Instrument Air Supply Line	Outside	A	N	Normally open.
HV9218	RCP Seal Bleed Off	Outside	PC	N	Normally open.
HV9217	RCP Seal Bleed Off	Inside	PC	N	Normally open.
HV7805	Cont Air Rad Mon Outlet	Inside	CA	Y	Normally open.
HV7810	Cont Air Rad Mon Outlet	Outside	CA	Y	Normally open.

Table 3.2-2

CONTAINMENT ISOLATION VALVES THAT CLOSE ON CIAS
(continued)

Valve Number	Description	Location	Fluid ¹	Open to Contmt?	Comments
HV5437	N ₂ Supply to Quench Tank	Outside	N ₂	N	Normally open.
HV7811	Cont Air Rad Mon Inlet	Outside	CA	Y	Normally open.
HV7806	Cont Air Rad Mon Inlet	Inside	CA	Y	Normally open.
HV7802	Cont Air Rad Mon Outlet	Inside	CA	Y	Normally open.
HV7803	Cont Air Rad Mon Outlet	Outside	CA	Y	Normally open.
HV7816	Cont Air Rad Mon Inlet	Outside	CA	Y	Normally open.
HV7801	Cont Air Rad Mon Inlet	Inside	CA	Y	Normally open.
HV7800	Cont Air Rad Mon Inlet	Outside	CA	Y	Normally open.

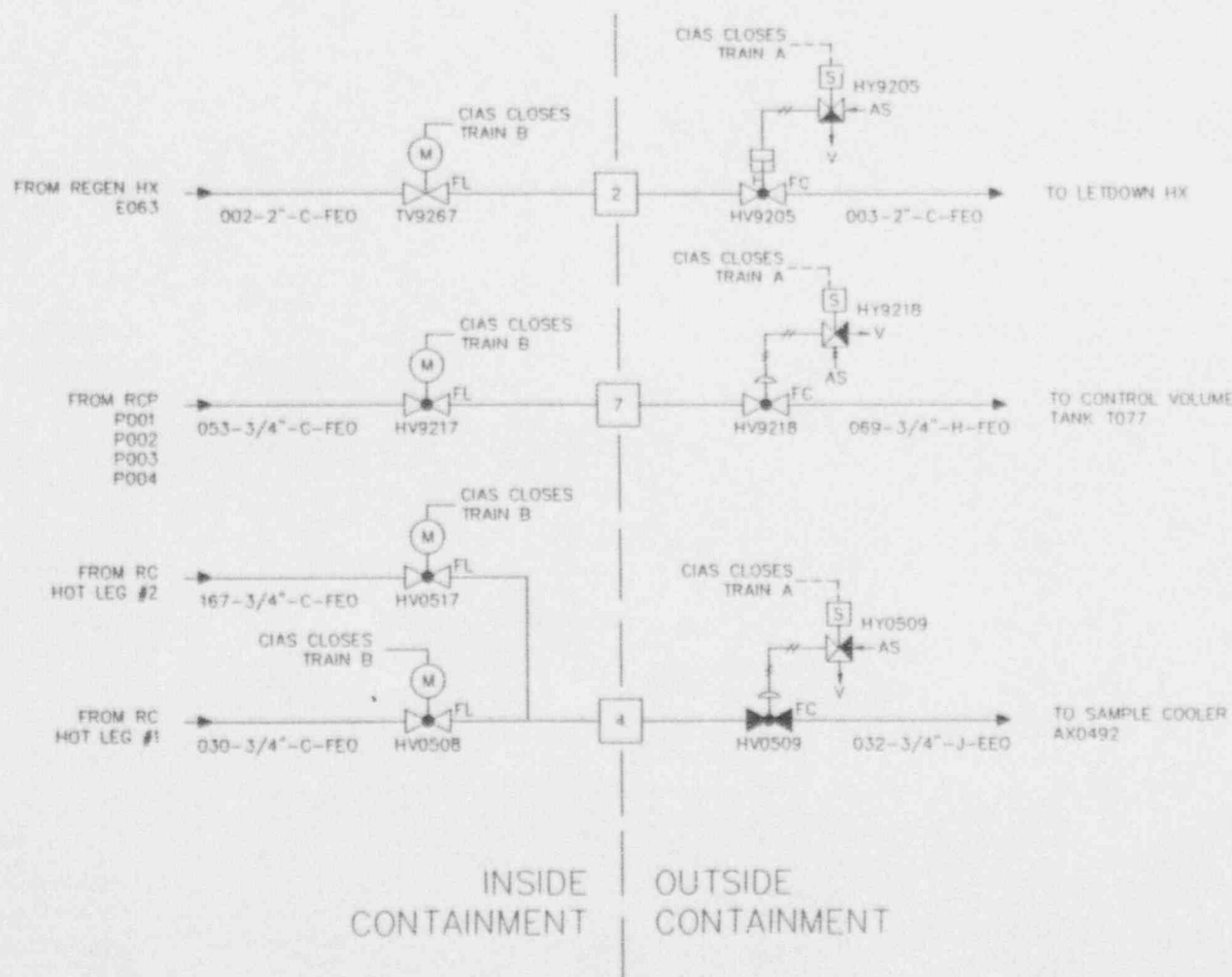
SS - Secondary Steam
 SC - Secondary Coolant
 PC - Primary Coolant
 A - Compressed Air
 N₂ - Nitrogen Gas

SD - Sump Drains
 WG - Waste Gas
 DW - Demineralized Water
 CA - Containment Atmosphere

Figure 3.2-25: Containment Isolation Simplified P&ID

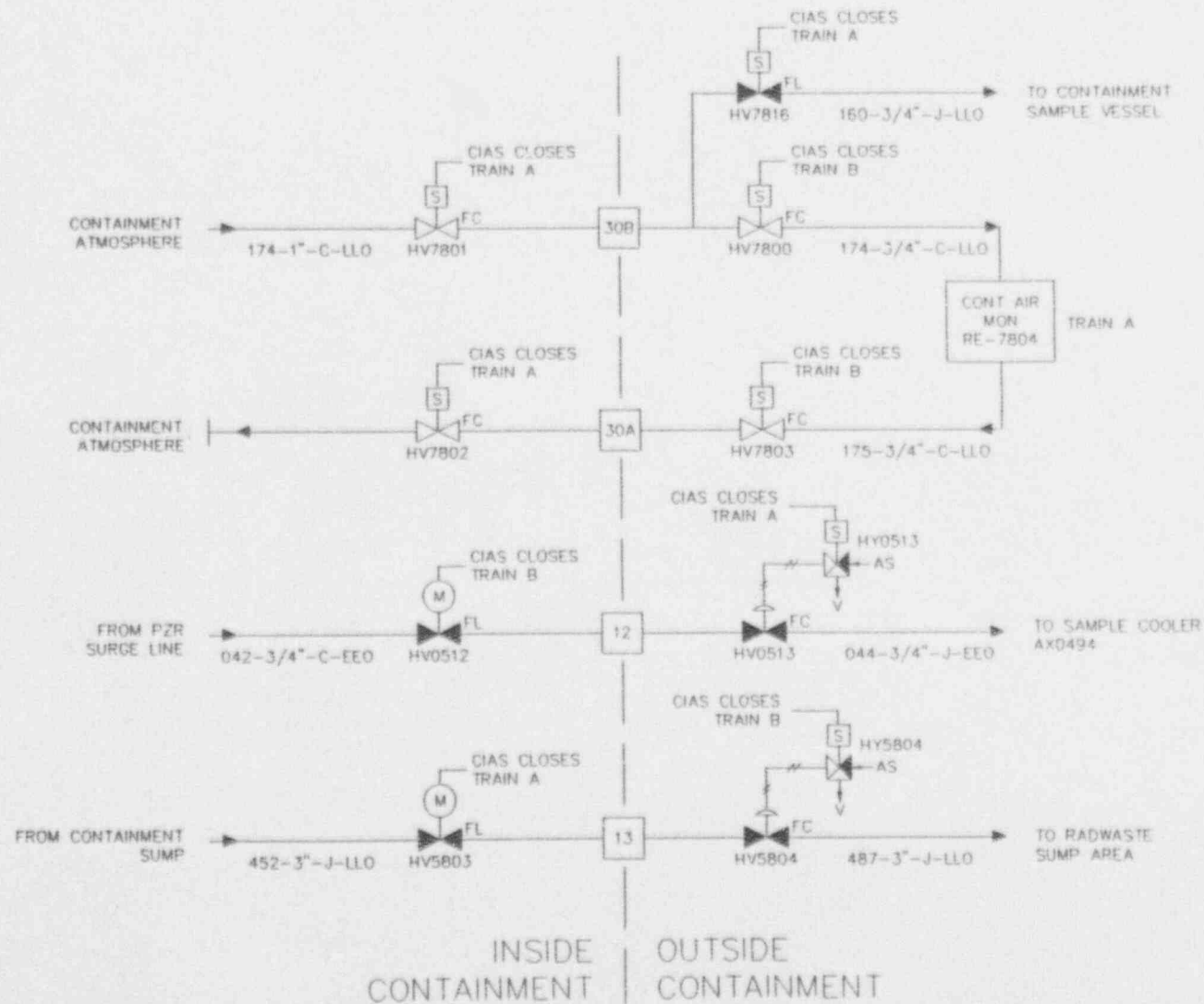
SONGS 2/3 CONTAINMENT ISOLATION

(PAGE 1 OF 4)

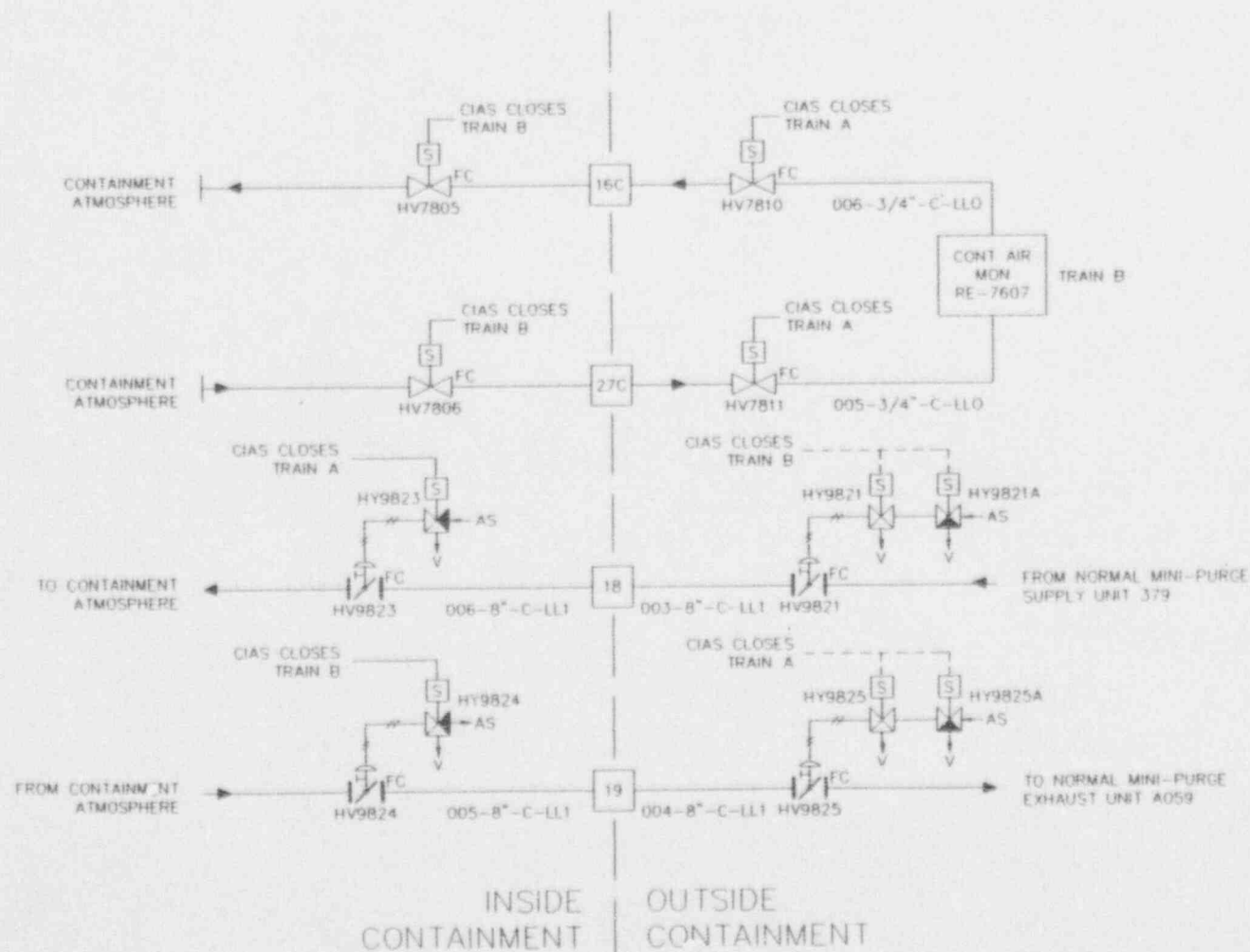


SONGS 2/3 CONTAINMENT ISOLATION

(PAGE 2 OF 4)

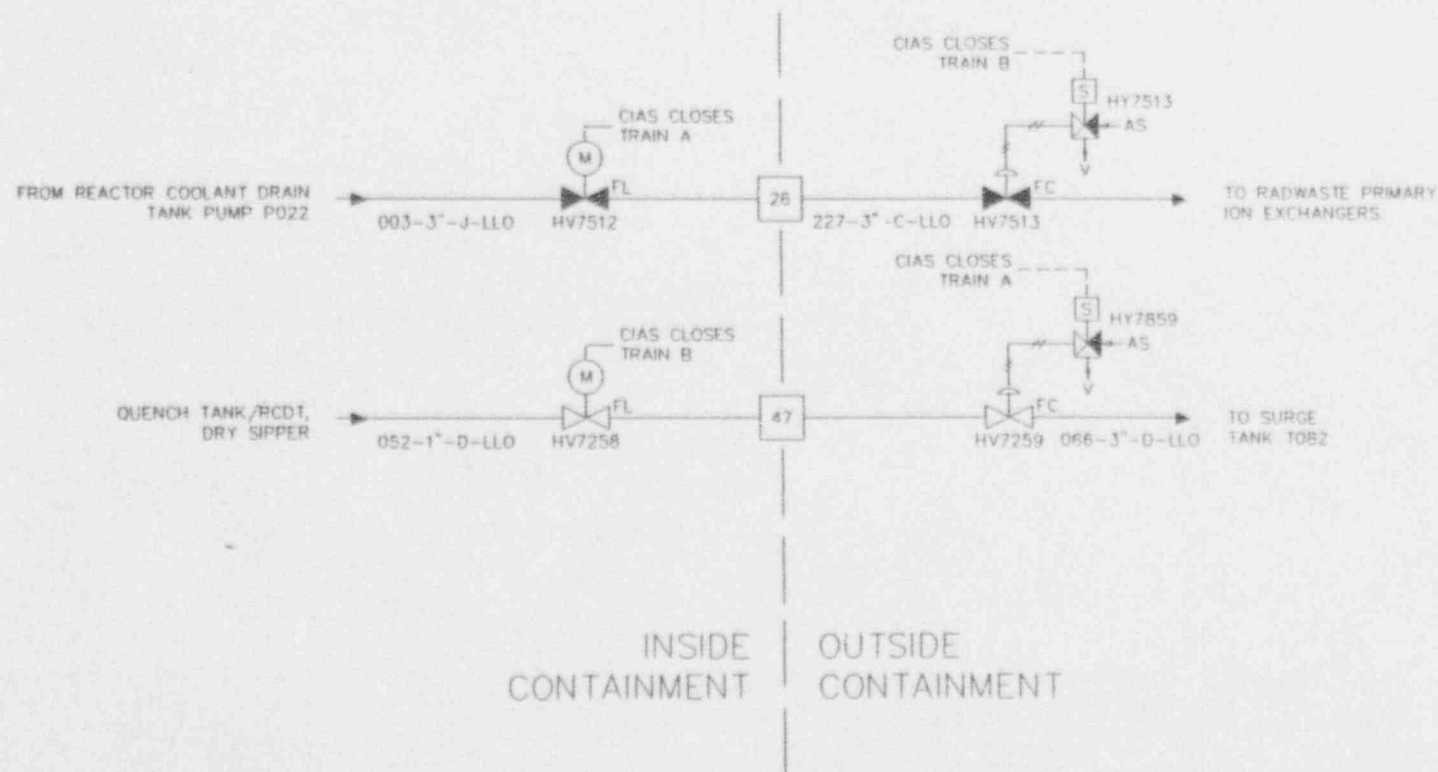


SONGS 2/3 CONTAINMENT ISOLATION (PAGE 3 OF 4)



SONGS 2/3 CONTAINMENT ISOLATION

(PAGE 4 OF 4)



3.3 Sequence Quantification

This section describes the data inputs and methods used in the sequence quantification process. In general, data inputs are required for initiating events and basic events. Sections 3.3.1 through 3.3.4 document generic data, plant-specific data, human failure data and common cause data inputs used for basic events in the plant risk model. Initiating event data inputs are described elsewhere in the report (Sections 3.1.1).

Sections 3.3.5 through 3.3.7 document the methodology used to quantify the plant risk model. Section 3.3.8 summarizes the evaluation of internal floods at SONGS 2/3 and its contribution to plant risk.

3.3.1 Generic Data Analysis

The majority of the basic events contained in the plant risk model represent random failures of equipment. These random failures result from failures of components to operate when demanded (due to failure of the component itself to operate or unavailability of the component due to test or maintenance) or failure of equipment to operate for the duration of its required operation (mission time). Use of plant-specific data based on the availability and reliability of components as experienced at SONGS Units 2 and 3 would provide the most accurate assessment of plant reliability. However, based on the limited operating experience of components and the quality of data (e.g., data not directly suitable for reliability data development), generic data is often used to provide a best estimate of component availability and reliability.

The application of generic data in probabilistic risk assessment is common and its implementation in the SONGS 2/3 IPE is comparable. Generic data represents a large population of components and is therefore more statistically significant than comparable data developed using plant-specific information. Over the last ten years a significant amount of research has been performed developing generic or industry failure rate databases. Nine of the sources were selected for application to the SONGS 2/3 IPE. These data were prioritized based on importance and relevance of the source to SONGS 2/3, applicability of the component type and failure mode, applicability of data to PWRs and consistency with other data sources.

Generic Letter 88-20 (Reference 3.3-1) specifically references the PSA Procedure Guide (NUREG/CR-2815) (Reference 3.3-2) as a viable source of component failure data for use in the IPE. The methodology reference of NUREG/CR-4550, Revision 1, (Reference 3.3-3) also provides a recommended list of generic failure rate data for the IPE. These sources received the highest priority in

the data selection process subject to meeting the applicability and consistency criteria previously cited.

A comprehensive generic data base was developed, including component types and failure modes identified in the fault tree development process. Components identified for plant-specific evaluation were also included in the generic data set. Generic data for components identified for plant-specific evaluation were subsequently updated using Bayesian methods assuming the generic data represented the prior distribution.

Generic data used in the plant risk model is presented in Table 3.3-1. The values listed are based on mean values of the underlying probability distributions. Failures are assumed to occur at a constant rate (e.g., wear-in and wear-out failures associated with beginning and end of life component operation are not considered). Each failure rate is reported with its distribution, error factor and reference.

3.3.2 Plant Specific Data and Analysis

3.3.2.1 Introduction

Past PRAs have shown that plant-specific component performance can have a substantial influence on the calculated core damage risk. Therefore, in order to effectively evaluate the SONGS 2/3 core damage frequency as part of the IPE, component performance data was collected and evaluated. A simplified description of the overall process used to collect and evaluate SONGS 2/3 plant-specific component reliability data is shown in Figure 3.3-1. A period of eight years of component data (1984-1991) was used as the basis for component reliability data selection. SONGS 2 began commercial operation in 1983, and SONGS 3 started commercial operation in 1984. Therefore, the component data gathered includes virtually the entire plant history. This is conservative, because the initial component "wear-in" may be included in this data. However, the failures which occurred during "wear-in" are only included for the initial screening process. For those components which were determined to require detailed plant-specific data analysis, these failures were excluded prior to quantification.

The first step involves the identification of components for plant-specific evaluation. Past industry and NRC PRAs were reviewed to identify components requiring plant-specific evaluation. As a result of these reviews, the component types and specific components identified in Table 3.3-2 were selected. Some components which have a history of weakness in the nuclear industry, such as relief valves, were not selected for plant-specific analysis despite their acknowledged weaknesses. Insufficient SONGS specific operating data and failure data is

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST

COMPONENT	MODE	DESCRIPTION	TYPE	RATE	DISTRIBUTION	REFERENCE	ERROR FACTOR
AC	D	ACCUMULATOR & LEAK/RUPTURE	Hourly	5.0E-06	Lognormal	NUCLARR(3)	10
AM	H	AMPLIFIER HIGH OUTPUT	Hourly	5.0E-06	Lognormal	NUCLARR(3)	10
AM	I	AMPLIFIER LOW/NO OUTPUT	Hourly	5.0E-06	Lognormal	NUCLARR(3)	10
AN	K	ANNUNCIATOR FAILS TO OPERATE	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10
AN	L	ANNUNCIATOR ACTUATES/DE-ACTUATES SPURIOUSLY	Hourly	3.0E-06	Lognormal	NUCLARR(3)	10
AV	M	AIR-OPERATED VALVE OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	8.0E-04	Lognormal	NUREG/CR-4550(2)	10
AV	N	AIR-OPERATED VALVE FAILS TO CLOSE ON DEMAND	Demand	2.0E-03	Lognormal	NUREG/CR-4550(2)	3
AV	O	AIR-OPERATED VALVE FAILS TO REMAIN CLOSED	Hourly	6.0E-07	Lognormal	NUREG/CR-4550(2)	10
AV	P	AIR-OPERATED VALVE FAILS TO OPEN ON DEMAND	Demand	2.0E-03	Lognormal	NUREG/CR-4550(2)	3
AV	Q	AIR-OPERATED VALVE FAILS TO REMAIN OPEN	Hourly	1.0E-07	Lognormal	NUREG/CR-4550(2)	3
AX	J	AUTOMATIC SWITCH FAILS TO ACTUATES/DE-ACTUATES ON DEMAND	Demand	1.0E-03	Lognormal	NUREG/CR-4550(2)	3
B1	M	> 4160V BUS OUT OF SERVICE FOR MAINTENANCE/TEST	Hourly	5.0E-06	Lognormal	NUREG/CR-4550(2)	10
B1	R	> 4160V BUS FAILS TO OPERATE	Hourly	3.0E-08	Lognormal	PSA GUIDE(1)	10
B2	M	4160V BUS OUT OF SERVICE FOR MAINTENANCE/TEST	Hourly	8.0E-06	Lognormal	NUREG/CR-4550(2)	10
B2	R	4160V BUS FAILS TO OPERATE	Hourly	3.0E-08	Lognormal	PSA GUIDE(1)	10
B3	M	480V BUS OUT OF SERVICE FOR MAINTENANCE/TEST	Hourly	8.0E-06	Lognormal	NUREG/CR-4550(2)	10
B3	R	480V BUS FAILS TO OPERATE	Hourly	3.0E-08	Lognormal	PSA GUIDE(1)	10
B4	M	< = 120V BUS OUT OF SERVICE FOR MAINTENANCE/TEST	Hourly	8.0E-06	Lognormal	NUREG/CR-4550(2)	10
B4	R	< = 120V BUS FAILS TO OPERATE	Hourly	3.0E-08	Lognormal	PSA GUIDE(1)	10
BC	M	BATTERY CHARGER OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	3.0E-04	Lognormal	NUREG/CR-4550(2)	10
BC	R	BATTERY CHARGER FAILS TO OPERATE	Hourly	6.0E-07	Lognormal	PSA GUIDE(1)	10
BD	M	125VDC BUS OUT OF SERVICE FOR MAINTENANCE/TEST	Hourly	8.0E-06	Lognormal	NUREG/CR-4550(2)	6
BD	R	125VDC BUS FAILS TO OPERATE	Hourly	1.0E-07	Lognormal	NUREG/CR-4550(2)	6
BI	J	BISTABLE FAILS TO ACTUATES/DE-ACTUATES ON DEMAND	Demand	7.0E-07	Lognormal	NUCLARR(3)	10
BY	M	BATTERY OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	1.0E-03	Lognormal	NUREG/CR-4550(2)	10
BY	R	BATTERY FAILS TO OPERATE	Hourly	2.0E-06	Lognormal	PSA GUIDE(1)	10
BY	S	BATTERY UNAVAILABLE ON DEMAND	Demand	4.0E-04	Lognormal	NUCLARR(3)	3
C1	N	BREAKER (CNTL) > 4160V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4550(2)	10
C1	O	BREAKER (CNTL) > 4160V FAILS TO REMAIN CLOSED	Hourly	1.0E-06	Lognormal	NUREG/CR-4550(2)	10
C1	P	BREAKER (CNTL) > 4160V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4550(2)	10
C1	Q	BREAKER (CNTL) > 4160V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
C2	N	BREAKER (CNTL) 4160V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4550(2)	10

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST
(continued)

COMPONENT	MODE	DESCRIPTION	TYPE	RATE	DISTRIBUTION	REFERENCE	ERROR FACTOR
C2	O	BREAKER (CNTL) 4160V FAILS TO REMAIN CLOSED	Hourly	1.0E-06	Lognormal	NUREG/CR-4660 (2)	10
C2	P	BREAKER (CNTL) 4160V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C2	Q	BREAKER (CNTL) 4160V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
C3	N	BREAKER (CNTL) 480V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C3	O	BREAKER (CNTL) 480V FAILS TO REMAIN CLOSED	Hourly	1.0E-06	Lognormal	NUREG/CR-4660 (2)	10
C3	P	BREAKER (CNTL) 480V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C3	Q	BREAKER (CNTL) 480V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
C4	N	BREAKER (CNTL) < = 120V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C4	O	BREAKER (CNTL) < = 120V FAILS TO REMAIN CLOSED	Hourly	1.0E-06	Lognormal	NUREG/CR-4660 (2)	10
C4	P	BREAKER (CNTL) < = 120V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C4	Q	BREAKER (CNTL) < = 120V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
C5	N	BREAKER (PROT) > 4160V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C5	O	BREAKER (PROT) > 4160V FAILS TO REMAIN CLOSED	Hourly	3.0E-06	Lognormal	PSA GUIDE(1)	10
C5	P	BREAKER (PROT) > 4160V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C5	Q	BREAKER (PROT) > 4160V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
C6	N	BREAKER (PROT) 4160V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C6	O	BREAKER (PROT) 4160V FAILS TO REMAIN CLOSED	Hourly	3.0E-06	Lognormal	PSA GUIDE(1)	10
C6	P	BREAKER (PROT) 4160V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C6	Q	BREAKER (PROT) 4160V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
C7	N	BREAKER (PROT) 480V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C7	O	BREAKER (PROT) 480V FAILS TO REMAIN CLOSED	Hourly	3.0E-06	Lognormal	PSA GUIDE(1)	10
C7	P	BREAKER (PROT) 480V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C7	Q	BREAKER (PROT) 480V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
C8	N	BREAKER (PROT) < = 120V FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C8	O	BREAKER (PROT) < = 120V FAILS TO REMAIN CLOSED	Hourly	3.0E-06	Lognormal	PSA GUIDE(1)	10
C8	P	BREAKER (PROT) < = 120V FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4660(2)	10
C8	Q	BREAKER (PROT) < = 120V FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
CH	R	CHILLER FAILS TO RUN	Hourly	4.0E-06	Lognormal	IEEE 600(6)	10

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST
(continued)

COMPONENT	MODE	DESCRIPTION	TYPE	RATE	DISTRIBUTION	REFERENCE	ERROR FACTOR
CH	S	CHILLER FAILS TO START ON DEMAND	Demand	8.1E-03	Lognormal	ALWR(9)	10
CM	M	COMPRESSOR OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	2.0E-03	Lognormal	NUREG/CR-4650(2)	10
CM	R	COMPRESSOR FAILS TO RUN	Hourly	2.0E-04	Lognormal	NUREG/CR-4650(2)	10
CM	S	COMPRESSOR FAILS TO START ON DEMAND	Demand	5.0E-03	Lognormal	NUCLARR(3)	5
CN	R	CONDENSER FAILS TO OPERATE	Hourly	1.4E-06	Lognormal	IEEE 600(6)	10
CV	C	CHECK VALVE PLUGGED/FOULED	Hourly	5.0E-09	Lognormal	NUCLARR(3)	10
CV	N	CHECK VALVE FAILS TO CLOSE ON DEMAND	Demand	1.0E-03	Lognormal	NUREG/CR-4650(2)	3
CV	O	CHECK VALVE FAILS TO REMAIN CLOSED	Hourly	1.0E-07	Lognormal	PSA GUIDE(1)	10
CV	P	CHECK VALVE FAILS TO OPEN ON DEMAND	Demand	1.0E-04	Lognormal	NUREG/CR-4650(2)	3
CV	Q	CHECK VALVE FAILS TO REMAIN OPEN	Hourly	2.3E-07	Lognormal	OCCONEE(5)	10
DG	M	DIESEL GENERATOR OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	6.0E-03	Lognormal	NUREG/CR-4650(2)	10
DG	R	DIESEL GENERATOR FAILS TO RUN	Hourly	3.0E-03	Lognormal	PSA GUIDE(1)	10
DG	S	DIESEL GENERATOR FAILS TO START ON DEMAND	Demand	3.0E-02	Lognormal	NUREG/CR-4650(2)	3
DP	N	DAMPER FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4650(2)	10
DP	O	DAMPER FAILS TO REMAIN CLOSED	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
DP	P	DAMPER FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4650(2)	10
DP	Q	DAMPER FAILS TO REMAIN OPEN	Hourly	3.0E-07	Lognormal	NUCLARR(3)	10
DY	R	DRYER FAILS TO OPERATE	Hourly	5.0E-06	Lognormal	NUCLARR(3)	10
EV	M	ELECTRO-HYDRAULIC VALVE OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	5.0E-04	Lognormal	NUREG/CR-4650(2)	10
EV	N	ELECTRO-HYDRAULIC VALVE FAILS TO CLOSE ON DEMAND	Demand	2.0E-03	Lognormal	NUREG/CR-4650(2)	3
EV	O	ELECTRO-HYDRAULIC VALVE FAILS TO REMAIN CLOSED	Hourly	1.1E-06	Lognormal	IEEE 600(6)	10
EV	P	ELECTRO-HYDRAULIC VALVE FAILS TO OPEN ON DEMAND	Demand	2.0E-03	Lognormal	NUREG/CR-4650(2)	3
EV	Q	ELECTRO-HYDRAULIC VALVE FAILS TO REMAIN OPEN	Hourly	1.1E-06	Lognormal	IEEE 600(6)	10
FC	H	FLOW CONTROLLER HIGH OUTPUT	Hourly	4.2E-06	Lognormal	NUCLARR(3)	10
FC	I	FLOW CONTROLLER LOW/NO OUTPUT	Hourly	4.2E-06	Lognormal	NUCLARR(3)	10
FL	C	FILTER PLUGGED/FOULED	Hourly	3.0E-06	Lognormal	PSA GUIDE(1)	10
FN	M	FAN OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	2.0E-03	Lognormal	NUREG/CR-4650(2)	10
FN	R	FAN FAILS TO RUN	Hourly	1.0E-06	Lognormal	NUREG/CR-4650(2)	3
FN	S	FAN FAILS TO START ON DEMAND	Demand	3.0E-04	Lognormal	NUREG/CR-4650(2)	3
FS	H	FLOW SENSOR HIGH OUTPUT	Hourly	1.8E-07	Lognormal	OCCONEE(5)	10
FS	I	FLOW SENSOR LOW/NO OUTPUT	Hourly	2.7E-07	Lognormal	OCCONEE(5)	10
FT	H	FLOW XMTR HIGH OUTPUT	Hourly	1.3E-06	Lognormal	OCCONEE(5)	10
FT	I	FLOW XMTR LOW/NO OUTPUT	Hourly	5.4E-07	Lognormal	OCCONEE(5)	10
FU	L	FUSE FAILS TO MAINTAIN CIRCUIT	Hourly	3.0E-08	Lognormal	PSA GUIDE (1)	10
FU	P	FUSE FAILS OPEN CIRCUIT ON DEMAND	Demand	1.0E-06	Lognormal	NUCLARR(3)	10

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST
(continued)

COMPONENT	MODE	DESCRIPTION	TYPE	RATE	DISTRIBUTION	REFERENCE	ERROR FACTOR
FX	J	FLOW SWITCH FAILS TO ACTUATES/DE-ACTUATES ON DEMAND	Demand	3.0E-07	Lognormal	NUCLARR(3)	10
GB	D	GAS BOTTLE LEAKAGE/RUPTURE	Hourly	6.0E-07	Lognormal	IEEE 600(B)	10
HR	R	HEATER FAILS TO OPERATE	Hourly	5.0E-06	Lognormal	NUCLARR(3)	10
HT	C	HEAT EXCHANGER (TUBE) PLUGGED/FOULED	Hourly	5.7E-06	Lognormal	NUREG/CR-4550(2)	10
HT	D	HEAT EXCHANGER (TUBE) LEAK/RUPTURE	Hourly	3.0E-06	Lognormal	PSA GUIDE(1)	10
HT	M	HEAT EXCHANGER (TUBE) OUT OF SERVICE FOR MAINTENANCE	Hourly	3.0E-06	Lognormal	NUREG/CR-4550(2)	10
HV	M	HYDRAULIC VALVE OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	8.0E-04	Lognormal	NUREG/CR-4550(2)	10
HV	N	HYDRAULIC VALVE FAILS TO CLOSE ON DEMAND	Demand	2.0E-03	Lognormal	NUREG/CR-4550(2)	3
HV	O	HYDRAULIC VALVE FAILS TO REMAIN CLOSED	Hourly	1.1E-06	Lognormal	IEEE 600(B)	10
HV	P	HYDRAULIC VALVE FAILS TO OPEN ON DEMAND	Demand	2.0E-03	Lognormal	NUREG/CR-4550(2)	3
HV	Q	HYDRAULIC VALVE FAILS TO REMAIN OPEN	Hourly	1.1E-06	Lognormal	IEEE 600(B)	10
IN	K	INDICATOR/METER FAILS TO OPERATE	Hourly	4.6E-06	Lognormal	IEEE 600(B)	10
IR	M	INVERTER OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	1.0E-03	Lognormal	NUREG/CR-4550(2)	10
IR	R	INVERTER FAILS TO OPERATE	Hourly	6.0E-06	Lognormal	PSA GUIDE(1)	10
IV	N	RELIEF VALVE (PILOT-OPERATED) FAILS TO CLOSE ON DEMAND	Demand	1.8E-02	Lognormal	NUREG/CR-4550(2)	10
IV	O	RELIEF VALVE (PILOT-OPERATED) FAILS TO REMAIN CLOSED	Hourly	3.8E-06	Lognormal	SHOREHAM(4)	10
IV	P	RELIEF VALVE (PILOT-OPERATED) FAILS TO OPEN ON DEMAND	Demand	1.0E-06	Lognormal	NUREG/CR-4550(2)	10
IV	Q	RELIEF VALVE (PILOT-OPERATED) FAILS TO REMAIN OPEN	Hourly	3.8E-06	Lognormal	SHOREHAM(4)	10
LC	H	LEVEL CONTROLLER HIGH OUTPUT	Hourly	1.0E-06	Lognormal	IEEE 600(B)	10
LC	I	LEVEL CONTROLLER LOW/NO OUTPUT	Hourly	1.0E-06	Lognormal	IEEE 600(B)	10
LS	H	LEVEL SENSOR HIGH OUTPUT	Hourly	3.0E-06	Lognormal	NUREG/CR-4550(2)	10
LS	I	LEVEL SENSOR LOW/NO OUTPUT	Hourly	3.0E-06	Lognormal	NUREG/CR-4550(2)	10
LT	H	LEVEL TRANSMITTER HIGH OUTPUT SIGNAL	Hourly	6.1E-07	Lognormal	O'CONNOR(5)	10
LT	I	LEVEL TRANSMITTER LOW/NO OUTPUT SIGNAL	Hourly	7.1E-07	Lognormal	O'CONNOR(5)	10
LX	J	LEVEL SWITCH FAILS TO ACTUATES/DE-ACTUATES ON DEMAND	Demand	3.0E-07	Lognormal	NUCLARR(3)	10
MP	M	MOTOR-DRIVEN PUMP OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	2.0E-03	Lognormal	NUREG/CR-4550(2)	10
MP	R	MOTOR-DRIVEN PUMP FAILS TO RUN	Hourly	1.0E-04	Lognormal	PSA GUIDE(1)	10
MP	S	MOTOR-DRIVEN PUMP FAILS TO START ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4550(2)	10
MS	N	MOTOR STARTER FAILS TO CLOSE ON DEMAND	Demand	3.0E-04	Lognormal	NUCLARR(3)	10

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST
(continued)

COMPONENT	MODE	DESCRIPTION	TYPE	RATE	DISTRIBUTION	REFERENCE	ERROR FACTOR
MS	O	MOTOR STARTER FAILS TO REMAIN CLOSED	Hourly	6.0E-07	Lognormal	NUCLARR(3)	10
MS	P	MOTOR STARTER FAILS TO OPEN ON DEMAND	Demand	3.0E-04	Lognormal	NUCLARR(3)	10
MS	O	MOTOR STARTER FAILS TO REMAIN OPEN	Hourly	6.0E-07	Lognormal	NUCLARR(3)	10
MV	C	MOTOR-OPERATED VALVE PLUGGED/FOULED	Hourly	1.0E-07	Lognormal	NUREG/CR-4650(2)	3
MV	M	MOTOR-OPERATED VALVE OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	8.0E-04	Lognormal	NUREG/CR-4650(2)	10
MV	N	MOTOR-OPERATED VALVE FAILS TO CLOSE ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4650(2)	10
MV	O	MOTOR-OPERATED VALVE FAILS TO REMAIN CLOSED	Hourly	1.0E-07	Lognormal	PSA GUIDE(1)	10
MV	P	MOTOR-OPERATED VALVE FAILS TO OPEN ON DEMAND	Demand	3.0E-03	Lognormal	NUREG/CR-4650(2)	10
MV	O	MOTOR-OPERATED VALVE FAILS TO REMAIN OPEN	Hourly	2.0E-07	Lognormal	PSA GUIDE(1)	10
MX	J	MANUAL SWITCH FAILS TO ACTUATE/DE-ACTUATES ON DEMAND	Demand	1.3E-06	Lognormal	SHOREHAM(4)	3
NV	N	PNEUMATIC VALVE FAILS TO CLOSE ON DEMAND	Demand	1.0E-03	Lognormal	NUCLARR(3)	10
NV	O	PNEUMATIC VALVE FAILS TO REMAIN CLOSED	Hourly	3.8E-07	Lognormal	IEEE 500(6)	10
NV	P	PNEUMATIC VALVE FAILS TO OPEN ON DEMAND	Demand	1.0E-03	Lognormal	NUCLARR(3)	10
NV	O	PNEUMATIC VALVE FAILS TO REMAIN OPEN	Hourly	1.0E-07	Lognormal	NUREG/CR-4650(2)	3
OR	C	ORIFICE PLUGGED/FOULED	Demand	3.0E-04	Lognormal	NUREG/CR-4650(2)	3
PC	H	PRESSURE CONTROLLER HIGH OUTPUT	Hourly	1.3E-06	Lognormal	IEEE 500(6)	10
PC	L	PRESSURE CONTROLLER LOW/NO OUTPUT	Hourly	1.3E-06	Lognormal	IEEE 500(6)	10
PK	H	I/P CONVERTER HIGH OUTPUT	Hourly	6.6E-07	Lognormal	OCONEE(5)	10
PK	L	I/P CONVERTER LOW/NO OUTPUT	Hourly	4.2E-07	Lognormal	OCONEE(5)	10
PR	K	PRESS REGULATOR FAILS TO OPERATE	Hourly	2.4E-06	Lognormal	IEEE 500(6)	10
PS	H	PRESSURE SENSOR HIGH OUTPUT	Hourly	3.0E-06	Lognormal	NUREG/CR-4650(2)	10
PS	L	PRESSURE SENSOR LOW/NO OUTPUT	Hourly	3.0E-06	Lognormal	NUREG/CR-4650(2)	10
PT	H	PRESS TRANSMITTER HIGH OUTPUT	Hourly	6.7E-07	Lognormal	OCONEE(5)	10
PT	L	PRESS TRANSMITTER LOW/NO OUTPUT	Hourly	2.7E-07	Lognormal	OCONEE(5)	10
PV	N	PWR-OP RELIEF VALVE FAILS TO CLOSE ON DEMAND	Demand	2.0E-03	Lognormal	NUREG/CR-4650(2)	3
PV	O	PWR-OP RELIEF VALVE FAILS TO REMAIN CLOSED	Hourly	3.9E-06	Lognormal	NUREG/CR-4650(2)	10
PV	P	PWR-OP RELIEF VALVE FAILS TO OPEN ON DEMAND	Demand	3.0E-04	Lognormal	NUREG/CR-4650(2)	10
PV	O	PWR-OP RELIEF VALVE FAILS TO REMAIN OPEN	Hourly	3.9E-06	Lognormal	NUREG/CR-4650(2)	10
PW	R	PWR SUPPLY < 120V FAILS TO OPERATE	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST
(continued)

COMPONENT	MODE	DESCRIPTION	TYPE	RATE	DISTRIBUTION	REFERENCE	ERROR FACTOR
PX	J	PRESS SWITCH FAILS TO ACTUATES/DE-ACTUATES ON DEMAND	Demand	3.0E-07	Lognormal	NUCLARR(3)	10
RE	J	RELAY FAILS TO ACTUATES/DE-ACTUATES ON DEMAND	Demand	3.0E-04	Lognormal	NUCLARR(3)	10
RE	L	RELAY ACTUATES/DE-ACTUATES SPURIOUSLY	Hourly	6.0E-07	Lognormal	NUCLARR(3)	10
RM	M	ROOM COOLER OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	2.0E-03	Lognormal	NUREG/CR-4660(2)	10
RM	R	ROOM COOLER FAILS TO RUN FOR	Hourly	1.0E-06	Lognormal	NUREG/CR-4660(2)	3
RM	S	ROOM COOLER FAILS TO START ON DEMAND	Demand	3.0E-04	Lognormal	NUREG/CR-4660(2)	3
RV	N	RELIEF VALVE SPRING LOAD FAILS TO CLOSE ON DEM	Demand	3.0E-03	Lognormal	NUCLARR(3)	6
RV	O	RELIEF VALVE SPRING LOAD FAILS TO REMAIN CLOSED	Hourly	3.8E-06	Lognormal	NUREG/CR-4660(2)	10
RV	P	RELIEF VALVE SPRING LOAD FAILS TO OPEN ON DEM	Demand	3.0E-03	Lognormal	NUCLARR(3)	6
RV	O	RELIEF VALVE SPRING LOAD FAILS TO REMAIN OPEN	Hourly	3.8E-06	Lognormal	NUREG/CR-4660(2)	10
SC	H	SPEED CONTROLLER HIGH OUTPUT	Hourly	9.3E-07	Lognormal	IEEE 600(6)	10
SC	I	SPEED CONTROLLER LOW/NO OUTPUT	Hourly	1.4E-06	Lognormal	IEEE 600(6)	10
SR	C	STRAINER PLUGGED/FOULED	Hourly	3.0E-06	Lognormal	PSA GUIDE(1)	10
SS	H	SPEED SENSOR HIGH OUTPUT	Hourly	9.3E-07	Lognormal	IEEE 600(6)	10
SS	I	SPEED SENSOR LOW/NO OUTPUT	Hourly	1.4E-06	Lognormal	IEEE 600(6)	10
SV	J	SOLENOID VALVE FAILS TO ACTUATES/DE-ACTUATES ON DEM	Demand	2.0E-03	Lognormal	NUREG/CR-4660(2)	3
SV	L	SOLENOID VALVE ACTUATES/DE-ACTUATES SPURIOUSLY	Hourly	6.0E-07	Lognormal	NUCLARR(3)	10
SV	M	SOLENOID VALVE OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	8.0E-04	Lognormal	NUREG/CR-4660(2)	10
SK	J	SPEED SWITCH FAILS TO ACTUATES/DE-ACTUATES	Hourly	3.0E-06	Lognormal	NUREG/CR-4660(2)	10
T1	M	>4160V TRANSFORMER OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	3.0E-04	Lognormal	NUCLARR(3)	10
T1	R	>4160V TRANSFORMER FAILS TO OPERATE	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10
T2	M	4160-480V TRANSFORMER OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	3.0E-04	Lognormal	NUCLARR(3)	10
T2	R	4160V-480V TRANSFORMER FAILS TO OPERATE	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10
T3	M	480V-120V TRANSFORMER OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	3.0E-04	Lognormal	NUCLARR(3)	10
T3	R	480V-120V XMFR FAILS TO OPERATE	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10
T4	M	<120V TRANSFORMER OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	3.0E-04	Lognormal	NUCLARR(3)	10
T4	R	<120V TRANSFORMER FAILS TO OPERATE	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10
TC	H	TEMPTR CONTROLLER HIGH OUTPUT	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10
TC	I	TEMPTR CONTROLLER LOW/NO OUTPUT	Hourly	1.0E-06	Lognormal	NUCLARR(3)	10

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST
(continued)

COMPONENT	MODE	DESCRIPTION	TYPE	RATE	DISTRIBUTION	REFERENCE	ERROR FACTOR
TI	J	TIMER FAILS TO ACTUATES/DE ACTUATES ON DEMAND	Demand	3.0E-04	Lognormal	CALVERT CLIFFS(7)	10
TI	L	TIMER ACTUATES/DE-ACTUATES SPURIOUSLY	Hourly	6.0E-06	Lognormal	CALVERT CLIFFS(7)	10
TK	D	TANK LEAK/RUPTURE	Hourly	6.0E-07	Lognormal	NUCLARR(3)	10
TP	M	TURBINE-DRIVEN PUMP OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	1.0E-02	Lognormal	NUREG/CR-4660(2)	10
TP	R	TURBINE DRIVEN PUMP FAILS TO RUN	Hourly	1.0E-04	Lognormal	NUCLARR(3) AND OCONEE(6)	10
TP	S	TURBINE-DRIVEN PUMP FAILS TO START ON DEMAND	Demand	3.0E-02	Lognormal	NUREG/CR-4660(2)	10
TS	H	TEMPERATURE SENSOR HIGH OUTPUT	Hourly	3.0E-06	Lognormal	NUREG/CR-4660(2)	10
TS	I	TEMPERATURE SENSOR LOW/NO OUTPUT	Hourly	3.0E-06	Lognormal	NUREG/CR-4660(2)	10
TT	H	TEMPERATURE TRANSMITTER HIGH OUTPUT	Hourly	7.6E-07	Lognormal	OCONEE(6)	10
TT	I	TEMPERATURE TRANSMITTER LOW/NO OUTPUT	Hourly	8.3E-07	Lognormal	OCONEE(6)	10
TX	J	TEMPERATURE SWITCH FAILS TO ACTUATES/DE-ACTUATES ON DEMAND	Demand	1.0E-04	Lognormal	NUREG/CR-4660(2)	3
VK	H	I/V CONVERTER HIGH OUTPUT	Hourly	4.2E-08	Lognormal	SHOREHAM(4)	10
VK	I	I/V CONVERTER LOW/NO OUTPUT	Hourly	4.2E-08	Lognormal	SHOREHAM(4)	10
VR	R	VOLTAGE REGULATING TRANSFORMER FAILS TO OPERATE	Hourly	7.1E-06	Lognormal	IEEE-600(6)	10
XC	H	POSITION CONTROLLER HIGH OUTPUT	Hourly	2.7E-06	Lognormal	SHOREHAM(4)	10
XC	I	POSITION CONTROLLER LOW/NO OUTPUT	Hourly	2.7E-06	Lognormal	SHOREHAM(4)	10
XS	H	POSITION SENSOR HIGH OUTPUT	Hourly	2.7E-06	Lognormal	SHOREHAM(4)	10
XS	I	POSITION SENSOR LOW/NO OUTPUT	Hourly	2.7E-06	Lognormal	SHOREHAM(4)	10
XV	C	MANUAL VALVE PLUGGED/FOULED	Hourly	1.0E-07	Lognormal	NUREG/CR-4660(2)	3
XV	M	MANUAL VALVE OUT OF SERVICE FOR MAINTENANCE/TEST	Demand	6.0E-04	Lognormal	NUREG/CR-4660(2)	10
XV	N	MANUAL VALVE FAILS TO CLOSE ON DEMAND	Demand	6.0E-04	Lognormal	NUCLARR(3)	10
XV	O	MANUAL VALVE FAILS TO REMAIN CLOSED	Hourly	2.3E-08	Lognormal	IEEE-600(6)	3
XV	P	MANUAL VALVE FAILS TO OPEN ON DEMAND	Demand	1.0E-04	Lognormal	NUREG/CR-4660(2)	3
XV	Q	MANUAL VALVE FAILS TO REMAIN OPEN	Hourly	3.4E-06	Lognormal	OCONEE(6)	10

(1) NUREG/CR-2815, "Probabilistic Safety Analysis Procedure Guide," dated August 1985. (Reference 3.3-2)

(2) NUREG/CR-4660, "Analysis of Core Damage Frequency: Internal Event Methodology" Volume 1, Revision 1, dated April 1980. (Reference 3.3-3)

(3) EGG-659E-8876, "Generic Component Data base for Light Water and Sodium Reactor PFAs (NUCLARR)," dated February 1980. (Reference 3.3-4)

(4) Shoreham Nuclear Power Station Probabilistic Risk Assessment, dated June 1983. (Reference 3.3-5)

Table 3.3-1

SONGS 2/3 GENERIC DATA LIST
(continued)

- (5) NRC/60, "Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3," dated June 1984. (Reference 3.3-6)
- (6) IEEE Std. 500-1984, "IEEE Guide to the Collection and Presentation of Electrical, Electronic Sensing Component, and Mechanical Equipment Reliability Data For Nuclear Power Generating Stations," dated December 1983. (Reference 3.3-7)
- (7) NUREG/CR-3611, "Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant," dated March 1984. (Reference 3.3-8)
- (8) Oak Ridge National Laboratory In-Plant Reliability Data Systems for Pumps, Valves and Electrical Equipment (NUREG/CR-2886, NUREG/CR-3164, NUREG/CR-3831). (Reference 3.3-9)
- (9) Reliability Data Base for ALWR PRA's, Annex D. (Reference 3.3-10)
- (10) NUREG/CR-4772, "Accident Sequence Evaluation Program Human Reliability Analysis Procedure," dated February 1987. (Reference 3.3-17)

Figure 3.3-1
PLANT-SPECIFIC DATA COLLECTION
AND EVALUATION PROCESS

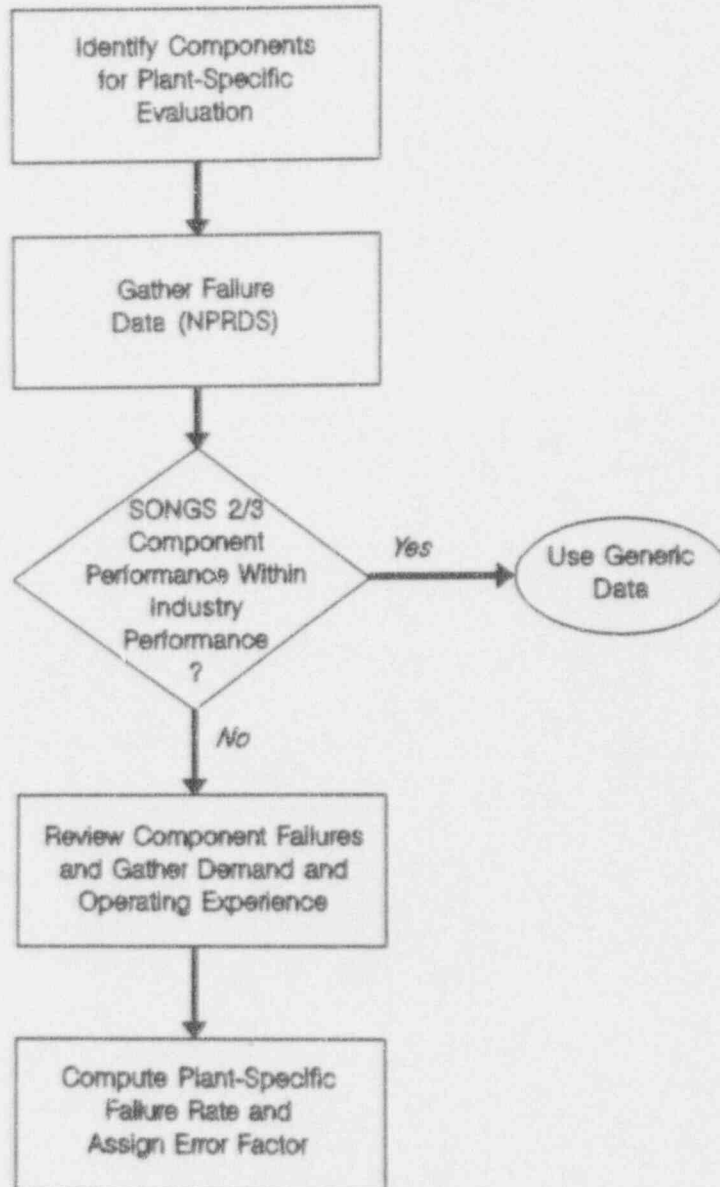


Table 3.3-2

COMPONENTS IDENTIFIED FOR SONGS 2/3
PLANT-SPECIFIC EVALUATION

PUMPS

- Auxiliary Feedwater (AFW) Pumps
- Component Cooling Water (CCW) Pumps
- Containment Spray (CS) Pumps
- Emergency Chilled Water (ECW) Pumps
- High Pressure Safety Injection (HPSI) Pumps
- Low Pressure Safety Injection (LPSI) Pumps
- Saltwater Cooling (SWC) Pumps

VALVES

- Atmospheric Dump Valves (ADVs), Main Steam Isolation Valves (MSIVs), Turbine Bypass Valves
- AFW Valves
- Check Valves - AFW, CCW, HPSI, LPSI, SWC
- Containment Isolation Valves
- Containment Spray Valves
- Chemical & Volume Control System (CVCS) Valves
- HPSI Valves
- LPSI Valves
- SWC Valves

ELECTRICAL COMPONENTS

- Batteries
- Battery Chargers
- Emergency Diesel Generators
- Inverters

OTHER COMPONENTS

- CCW Heat Exchangers
- Emergency Chillers
- Shutdown Cooling Heat Exchangers

available for these components, therefore, generic data will be used.

The Nuclear Plant Reliability Data System (NPRDS) (Reference 3.3-11) was used to prepare component failure analysis reports (CFARs) for all of the components identified. For each component, the CFARs provide a listing of the number of failures, number of components, number of component hours, and failure rate on a plant-specific basis, as well as the same information on an industry-wide basis.

Failures which occurred during the initial component "wear-in" period were included for this initial screening process. While the NPRDS failure rate calculations are not directly applicable to PRA analysis, they provide a consistent basis by which plant-specific performance can be compared to industry average (or generic) performance. In cases where SONGS 2/3 performance was found to be within expected bounds of industry performance, the plant-specific data analysis of that component was terminated and generic data was used to represent component reliability.

For components which were identified by NPRDS as outside the expected range of industry performance, further data was collected. This data consisted of the number of operating hours and number of demands each component experienced during the previous seven years (January 1985 to December 1991). In addition, detailed information was collected on the specific failures in order to classify the failure as demand-related or operation-related. Operating hours and failures prior to 1985 were specifically excluded from consideration to eliminate "wear-in" failures.

Based on the data collected, component-specific failure rates were calculated. This process grouped components with like design and similar operating conditions in order to enhance the accuracy of the calculated failure rates, unless some evidence existed which indicated particularly poor component-specific performance. These plant-specific values were then assigned error factors based on the following methodology from NUREG/CR-4550, Volume 1 (Reference 3.3-3). Once the plant-specific failure rates have been calculated, the chi-square upper confidence limit is determined at 95%. From this value and the plant-specific failure rate, which is assumed to be the mean value, the error factor is determined from the following equation from NUREG/CR-4550:

where: $\lambda_{.95}$ = 95th percentile (upper bound)
 μ = mean value (plant-specific value)
EF = error factor

$$\frac{\lambda_{.95}}{\mu} = \frac{EF}{\text{EXP} \left[\frac{\left(\frac{\ln(EF)}{1.645} \right)^2}{2} \right]}$$

The remainder of this section describes the evaluation performed for SONGS 2/3. Section 3.3.2.2 describes the collection and evaluation of SONGS 2/3 component performance relative to industry performance. Section 3.3.2.3 describes the plant-specific data collection process and results for those components requiring further plant-specific evaluation. Section 3.3.2.4 describes the results of the plant-specific failure rate evaluation.

3.3.2.2 Comparison to Industry Performance

NPRDS data for San Onofre Units 2/3 was used to identify the SONGS 2/3 components to be evaluated for plant-specific failure data. The NPRDS database tracks failure data for components and can be used to compare the SONGS 2/3 component performance with generic industry performance.

NPRDS tracks the manufacturer and model number for the SONGS 2/3 components and calculates a specific failure rate for each component. This failure rate is meaningless as a reliability value, but it does provide a basis by which SONGS 2/3 component performance can be compared to industry, or "generic" values. The SONGS 2/3 component failure rate is dispositioned relative to industry experience using a "Z-value". The Z-value is the number of standard deviations from the industry average failure rate for a given failure rate. A Z-value of 1.645 corresponds to the 95th percentile, assuming a lognormal distribution. This indicates with 95% confidence that the generic failure rate is representative of the plant-specific failure rate for a particular component. Z-values greater than 1.645 indicate that there is less than 95% confidence that the plant-specific failure rate may be adequately represented by the generic failure rate distribution. A confidence level less than 95% is unlikely to exist purely by chance and consequently can be used to identify SONGS 2/3 equipment performance outliers.

The Z-value is based on the Normal Distribution, and is defined in (Reference 3.3-11) as follows:

$$Z = \frac{P_1 - P_2}{\sqrt{P_3 (1 - P_3) \left[\frac{1}{H_{C_1}} + \frac{1}{H_{C_2}} \right]}}$$

where:

$P_1 = \frac{N_{F_1}}{H_{C_1}}$	SONGS 2/3 Failure Rate
$P_2 = \frac{N_{F_2}}{H_{C_2}}$	Industry Failure Rate
$P_3 = \frac{N_{F_1} + N_{F_2}}{H_{C_1} + H_{C_2}}$	Total Failure Rate
$N_{F_1} =$	Number of SONGS 2/3 Failures
$N_{F_2} =$	Number of Industry Failures
$H_{C_1} =$	Number of SONGS 2/3 Component Hours
$H_{C_2} =$	Number of Industry Component Hours

A different significance criterion is used by NPRDS if the total number of failures (SONGS 2/3 plus industry failures) is less than five. In this case, the component is identified as having a significantly higher failure rate if the probability of occurrence, when compared to the industry, is less than five percent (0.05). This probability of occurrence is called the "P-value".

The P-value is based on the Binomial Distribution, and is calculated by NPRDS as follows:

$$P = 1 - \sum_{i=0}^{N_{F_1}-1} \frac{(H_{C_1})!}{i!(H_{C_1}-i)!} (P_3)^i (1 - P_3)^{H_{C_1}-i}$$

where N_{F_1} , H_{C_1} , and P_3 are defined as before.

Table 3.3-3 lists the SONGS 2/3 components in the IPE model which were reviewed using the NPRDS database. Included in the table is a determination of whether the component is considered an outlier

and identification of whether generic or plant-specific data will be used for the component(s). Components with a NPRDS Z-value greater than 1.645 or with a P-value less than 0.05 are considered outliers as discussed above.

It is assumed SONGS 2/3 components with zero failures are not outliers and are not evaluated further. Components without adequate industry failure data are also evaluated further. The review of NPRDS data identified the following components requiring further plant-specific evaluations:

- AFW Valves - HV-4705, HV-4706, HV-4715, HV-4716, HV-4730
- CCW Heat Exchangers
- CCW Pumps
- CVCS Valves - HV-9201, HV-9235, HV-9240, HV-9247
- Diesel Generators
- ECW Pumps
- Emergency Chillers
- HPSI Pumps
- LPSI Pumps
- MSIVs
- MSS Turbine Bypass Valves
- MSS ADVs
- Motor-Driven AFW Pumps
- SWC Pumps
- Turbine-Driven AFW Pump

It should be noted that plant-specific evaluations were performed for those components for which one subcomponent satisfied the generic data criterion and another subcomponent did not. For example, the pump subcomponents of the LPSI pumps were found to be outliers as described above, while the pump motors were found to be adequately represented by generic failure data. In this case, a plant-specific evaluation is performed for both the LPSI pumps and motors.

3.3.2.3 . Compilation of Component Operating Experience

If a component is found to be an outlier as discussed in Section 3.3.2.2, further plant-specific evaluation is necessary. Additionally, components for which no industry data is available for comparison in NPRDS were selected for further analysis.

An estimate of the number of start demands and operating hours for each component was obtained in order to calculate the plant-specific failure rates.

For components which are operated during various modes of plant operation, the modes in which the Plant operated and the

Table 3.3-3
NUCLEAR PLANT RELIABILITY
DATA SYSTEM SUMMARY

SYSTEM	COMPONENT	IS COMPONENT AN OUTLIER?	DISPOSITION
AFW	System Check Valves	NO	GENERIC
AFW	HV-4705 - Valve	NO	GENERIC
AFW	HV-4705 - Valve Operator	YES	PLANT-SPECIFIC
AFW	HV-4706 - Valve	NO	GENERIC
AFW	HV-4706 - Valve Operator	YES	PLANT-SPECIFIC
AFW	HV-4712 - Valve	NO	GENERIC
AFW	HV-4712 - Valve Operator	NO	GENERIC
AFW	HV-4713 - Valve	NO	GENERIC
AFW	HV-4713 - Valve Operator	NO	GENERIC
AFW	HV-4714 - Valve	NO	GENERIC
AFW	HV-4714 - Valve Operator	NO	GENERIC
AFW	HV-4715 - Valve	NO	PLANT-SPECIFIC NOTE 6
AFW	HV-4715 - Valve Operator	NO	PLANT-SPECIFIC NOTE 6
AFW	HV-4716 - Valve	YES	PLANT-SPECIFIC
AFW	HV-4716 - Valve Operator	YES	PLANT-SPECIFIC
AFW	HV-4730 - Valve	NO	GENERIC
AFW	HV-4730 - Valve Operator	YES	PLANT-SPECIFIC
AFW	HV-4731 - Valve	NO	GENERIC
AFW	HV-4731 - Valve Operator	NO	GENERIC
AFW	HV-4762 - Valve	NO	GENERIC
AFW	HV-4762 - Valve Operator	NO	GENERIC
AFW	HV-4763 - Valve	NO	GENERIC
AFW	HV-4763 - Valve Operator	NO	GENERIC
AFW	HV-8200 - Valve	NOTE 1	GENERIC
AFW	HV-8200 - Valve Operator	NO	GENERIC
AFW	HV-8201 - Valve	NOTE 1	GENERIC
AFW	HV-8201 - Valve Operator	NO	GENERIC
AFW	P-140/P-141/P-504TDAFP/MDAFP - Pumps	NOTE 3	PLANT-SPECIFIC
AFW	P-141/P-504 - Motor	NO DATA	PLANT-SPECIFIC
AFW	SV-4700	NO	GENERIC
CCW	System Check Valves	NO	GENERIC

Table 3.3-3

NUCLEAR PLANT RELIABILITY
DATA SYSTEM SUMMARY
(continued)

SYSTEM	COMPONENT	IS COMPONENT AN OUTLIER?	DISPOSITION
CCW	Heat Exchanger - HX	YES	PLANT-SPECIFIC
CCW	P-024/P-025/P-026 - Motor	NO	GENERIC
CCW	P-024/P-025/P-026 - Pump	YES	PLANT-SPECIFIC
CI	HV-7800 - Valve	NO	GENERIC
CI	HV-7800 - Valve Operator	NO	GENERIC
CI	HV-7801 - Valve	NO	GENERIC
CI	HV-7801 - Valve Operator	NO	GENERIC
CI	HV-7802 - Valve	NO	GENERIC
CI	HV-7802 - Valve Operator	NO	GENERIC
CI	HV-7803 - Valve	NO	GENERIC
CI	HV-7803 - Valve Operator	NO	GENERIC
CI	HV-7805 - Valve	NO	GENERIC
CI	HV-7805 - Valve Operator	NO	GENERIC
CI	HV-7806 - Valve	NO	GENERIC
CI	HV-7806 - Valve Operator	NO	GENERIC
CI	HV-7810 - Valve	NO	GENERIC
CI	HV-7810 - Valve Operator	NO	GENERIC
CI	HV-7811 - Valve	NO	GENERIC
CI	HV-7811 - Valve Operator	NO	GENERIC
CS/CEFC	E-399/400/401/402 Emergency Air Coolers - Motor	NOTE 1	GENERIC
CS/CEFC	E-399/400/401/402 Emerg. Air Coolers - H/X	NOTE 4	GENERIC
CS/CEFC	E-399/400/401/402 Emerg. Air Coolers - Blower	NOTE 1	GENERIC
CS/CEFC	HV-6367 - Valve	NO	GENERIC
CS/CEFC	HV-6367 - Valve Operator	NO	GENERIC
CS/CEFC	HV-6369 - Valve	NO	GENERIC
CS/CEFC	HV-6369 - Valve Operator	NO	GENERIC
CS/CEFC	HV-6371 - Valve	NO	GENERIC
CS/CEFC	HV-6371 - Valve Operator	NO	GENERIC

Table 3.3-3

NUCLEAR PLANT RELIABILITY
DATA SYSTEM SUMMARY
(continued)

SYSTEM	COMPONENT	IS COMPONENT AN OUTLIER?	DISPOSITION
CS/CEFC	HV-6373 - Valve	NO	GENERIC
CS/CEFC	HV-6373 - Valve Operator	NO	GENERIC
CS/CEFC	HV-6500 - Valve	NOTE 1	GENERIC
CS/CEFC	HV-6500 - Valve Operator	NOTE 1	GENERIC
CS/CEFC	HV-6501 - Valve	NOTE 1	GENERIC
CS/CEFC	HV-6501 - Valve Operator	NOTE 1	GENERIC
CS/CEFC	HV-8150/8151 - Valve	NOTE 2	GENERIC
CS/CEFC	HV-8150/8151 - Valve Operator	NOTE 1	GENERIC
CS/CEFC	HV-9367/9368 - Valve	NOTE 2	GENERIC
CS/CEFC	HV-9367/9368 Valves - Valve Operator	NO	GENERIC
CS/CEFC	P-012/P-013 - Motor	NOTE 1	GENERIC
CS/CEFC	P-012/P-013 - Pump	NO	GENERIC
CS/CEFC	SDC HX - IX	NOTE 1	GENERIC
CVCS	System Check Valves	NO	GENERIC
CVCS	HV-9201 - Valve & Valve Operator	YES	PLANT-SPECIFIC
CVCS	HV-9235 - Valve & Valve Operator	NO DATA	PLANT-SPECIFIC
CVCS	HV-9240 - Valve & Valve Operator	NO DATA	PLANT-SPECIFIC
CVCS	HV-9247 - Valve & Valve Operator	NO DATA	PLANT-SPECIFIC
CVCS	LV-0227B - Valve	NO	GENERIC
CVCS	LV-0227B - Valve Operator	NO	GENERIC
CVCS	LV-0227C - Valve	NO	GENERIC
CVCS	LV-0227C - Valve Operator	NO	GENERIC
ECW	E-335 - Emergency Chiller	NO DATA	PLANT-SPECIFIC
ECW	E-336 - Emergency Chiller	NO DATA	PLANT-SPECIFIC
ECW	P-160 - Emergency Chilled Water Pump	NO DATA	PLANT-SPECIFIC
ECW	P-162 - Emergency Chilled Water Pump	NO DATA	PLANT-SPECIFIC
EP	Batteries B007 and B008	NOTE 1	GENERIC
EP	Batteries B009 and B010	NOTE 1	GENERIC
EP	Battery Chargers B001 to B004	NO	GENERIC
EP	Diesel Generators - General	NO	PLANT-SPECIFIC

Table 3.3-3

NUCLEAR PLANT RELIABILITY
DATA SYSTEM SUMMARY
(continued)

SYSTEM	COMPONENT	IS COMPONENT AN OUTLIER?	DISPOSITION
EP	Diesel Generators - Engine	YES	PLANT-SPECIFIC
EP	Inverters - General	NO	GENERIC
HPSI	System Check Valves	YES	NOTE 5
HPSI	HV-9300 - Valve	NO	GENERIC
HPSI	HV-9300 - Valve Operator	NO	GENERIC
HPSI	HV-9301 - Valve	NO	GENERIC
HPSI	HV-9301 - Valve Operator	NO	GENERIC
HPSI	HV-9302 - Valve	NO	GENERIC
HPSI	HV-9302 - Valve Operator	NO	GENERIC
HPSI	HV-9303 - Valve	NO	GENERIC
HPSI	HV-9303 - Valve Operator	NO	GENERIC
HPSI	HV-9304 - Valve	NO	GENERIC
HPSI	HV-9304 - Valve Operator	NO	GENERIC
HPSI	HV-9305 - Valve	NO	GENERIC
HPSI	HV-9305 - Valve Operator	NO	GENERIC
HPSI	HV-9306 - Valve	NO	GENERIC
HPSI	HV-9306 - Valve Operator	NO	GENERIC
HPSI	HV-9307 - Valve	NO	GENERIC
HPSI	HV-9307 - Valve Operator	NO	GENERIC
HPSI	HV-9323 - Valve	NO	GENERIC
HPSI	HV-9323 - Valve Operator	NO	GENERIC
HPSI	HV-9324 - Valve	NO	GENERIC
HPSI	HV-9324 - Valve Operator	NO	GENERIC
HPSI	HV-9325 - Valve	NO	GENERIC
HPSI	HV-9325 - Valve Operator	NO	GENERIC
HPSI	HV-9326 - Valve	NO	GENERIC
HPSI	HV-9326 - Valve Operator	NO	GENERIC
HPSI	HV-9327 - Valve	NO	GENERIC
HPSI	HV-9327 - Valve Operator	NO	GENERIC
HPSI	HV-9328 - Valve	NO	GENERIC

Table 3.3-3

NUCLEAR PLANT RELIABILITY
DATA SYSTEM SUMMARY
(continued)

SYSTEM	COMPONENT	IS COMPONENT AN OUTLIER?	DISPOSITION
HPSI	HV-9328 - Valve Operator	NO	GENERIC
HPSI	HV-9329 - Valve	NO	GENERIC
HPSI	HV-9329 - Valve Operator	NO	GENERIC
HPSI	HV-9330 - Valve	NO	GENERIC
HPSI	HV-9330 - Valve Operator	NO	GENERIC
HPSI	HV-9331 - Valve	NO	GENERIC
HPSI	HV-9331 - Valve Operator	NO	GENERIC
HPSI	HV-9332 - Valve	NO	GENERIC
HPSI	HV-9332 - Valve Operator	NO	GENERIC
HPSI	HV-9333 - Valve	NO	GENERIC
HPSI	HV-9333 - Valve Operator	NO	GENERIC
HPSI	HV-9347 - Valve	NO	GENERIC
HPSI	HV-9347 - Valve Operator	NO	GENERIC
HPSI	HV-9348 - Valve	NO	GENERIC
HPSI	HV-9348 - Valve Operator	NO	GENERIC
HPSI	HV-9420 - Valve	NO	GENERIC
HPSI	HV-9420 - Valve Operator	NO	GENERIC
HPSI	HV-9434 - Valve	NO	GENERIC
HPSI	HV-9434 - Valve Operator	NO	GENERIC
HPSI	P-017/P-018/P-019 - Pump	NO, NOTE 3	PLANT-SPECIFIC
HPSI	P-017/P-018/P-019 - Motor	NOTE 1, NOTE 3	PLANT-SPECIFIC
LPSI	System Check Valves	NO	GENERIC
LPSI	HV-0396/8160 - Valve Operator	NOTE 1	GENERIC
LPSI	HV-0396/8160 - Valve	NOTE 1	GENERIC
LPSI	HV-8161 - Valve	NO	GENERIC
LPSI	HV-8161 - Valve Operator	NOTE 1	GENERIC
LPSI	HV-9322/9325/9328/9331 - Valve	NOTE 1	GENERIC
LPSI	HV-9322/9325/9328/9331 - Valve Operator	NO	GENERIC
LPSI	P015/P016 - Motor	NO	PLANT-SPECIFIC

Table 3.3-3

NUCLEAR PLANT RELIABILITY
DATA SYSTEM SUMMARY
(continued)

SYSTEM	COMPONENT	IS COMPONENT AN OUTLIER?	DISPOSITION
LPSI	P015/P016 - Pump	YES	PLANT-SPECIFIC
MSS	ADVs (HV-8419, 8421) - Valve Operator	YES	PLANT-SPECIFIC
MSS	ADVs (HV-8419, 8421) - Valve	YES	PLANT-SPECIFIC
MSS	MSIVs (HV-8204,5) - Valve Operator	NO DATA	PLANT-SPECIFIC
MSS	MSIVs (HV-8204,5) - Valve	NO DATA	PLANT-SPECIFIC
MSS	Turbine Bypass Valves - Valve	NO DATA	PLANT-SPECIFIC
MSS	Turbine Bypass Valves - Valve Operator	YES	PLANT-SPECIFIC
SWC	System Check Valves	NO	GENERIC
SWC	HV-6200 - Valve	NO	GENERIC
SWC	HV-6200 - Valve Operator	NO	GENERIC
SWC	HV-6201 - Valve	NO	GENERIC
SWC	HV-6201 - Valve Operator	NO	GENERIC
SWC	HV-6202 - Valve	NO	GENERIC
SWC	HV-6202 - Valve Operator	NO	GENERIC
SWC	HV-6203 - Valve	NO	GENERIC
SWC	HV-6203 - Valve Operator	NO	GENERIC
SWC	P-112/P-113/P-114/P-307 - Motor	NO DATA	PLANT-SPECIFIC
SWC	P-112/P-113/P-114/P-307 - Pump	NO DATA	PLANT-SPECIFIC

NOTE 1: SONGS component has experienced no failures. Therefore, generic failure data is considered conservative and will be used.

NOTE 2: A SONGS failure rate of $4.1\text{E-}6$ is given in NPRDS for these components. The generic failure rate for these valves failing to open is $3.0\text{E-}3$. Because the SONGS components have experienced negligible failures and no industry data is available for comparison, generic failure data will be used.

NOTE 3: SONGS component is not identified as an outlier, however, due to critical safety function of component, plant specific data will be obtained.

NOTE 4: A SONGS failure rate of $2.0\text{E-}6$ is given in NPRDS for this component. The generic failure rate for this component is $5.7\text{E-}6$. Because these values are comparable and no industry data is available in NPRDS for comparison, generic data will be used.

Table 3.3-3

NUCLEAR PLANT RELIABILITY
DATA SYSTEM SUMMARY
(continued)

- NOTE 5: Only 3 of the 24 HPSI system check valve failures involved "failure to open". "Failures to close" and "failures to remain closed" are numerically insignificant for the HPSI system due to the number of redundant valves available to prevent backflow. The SONGS failure rate for "failure to open" is significantly less than the industry failure rate for HPSI check valves. Therefore, generic failure data can be used.
- NOTE 6: This component is not identified as an outlier, however, valve HV-4715 has the same design and function as HV-4730, therefore, plant specific failure history will be reviewed.

corresponding number of mode operating hours were obtained from the SONGS 2/3 Quarterly Performance Reports (QPR).

3.3.2.4 Results

The number of SONGS 2/3 component failures was determined from both NPRDS and the San Onofre Maintenance Management System (SOMMS). A SOMMS listing of corrective maintenance orders (CMOs) and Non Conformance Reports (NCRs) was obtained for each component identified for further analysis. A cursory review of the CMO descriptions and the NPRDS failure narratives was performed. As required, the specific maintenance orders and/or NCRs were retrieved for additional insight into the event. The SOMMS data was compared to the NPRDS reports to ensure all failures were accounted for. From the NPRDS and SOMMS narratives, each failure was categorized as a failure to run, failure to start or failure to load, as appropriate.

The failures which involve a component failure to start or a mechanical condition which would have precluded the component from starting are included in the "Start" failure column. Failures which occurred while the component was operating or which would have resulted in a failure during operation are included in the "Run" failure column. Failures which occurred during the initial component "wear-in" period, failures during maintenance, and failures which have a negligible effect were not included in this calculation of plant-specific failure rates.

For each component, the plant-specific failure data was Bayesian updated with generic failure data. The generic data was obtained from the component type database described in Section 3.3.1. The Bayesian updated failure rates and error factors are listed in Table 3.3-4, along with generic data for comparison.

3.3.2.5 Component Unavailability Data

This section documents the quantification of plant-specific component and system unavailability for use in the quantification of the SONGS 2/3 IPE fault trees. This data was incorporated into the fault trees as maintenance unavailability basic events.

For the SONGS 2/3 IPE, it is assumed that all initiators occur when the plant is operating at full power. Therefore, only system and component unavailabilities during Mode 1 operations are considered. For the purpose of this quantification, Mode 1 is considered to be power operation with some measurable power level. To incorporate this plant-specific unavailability data into the SONGS 2/3 IPE, a database is developed to document Mode 1 component and system unavailability data gathered. Unavailability data prior to 1984 is excluded from this analysis. The summary database is presented as Table 3.3-5.

Table 3.3-4
PLANT-SPECIFIC DATA SUMMARY

Component Description (Unit 2 & 3)	Bayesian Failure Rate	Bayesian Error Factor	Generic Value & EF (/demand or /hour)
AFW HV-4705 (FT Open)	6.2E-3	2.7	3.0E-3 (10)
AFW HV-4706 (FT Open)	1.3E-2	2.1	3.0E-3 (10)
AFW HV-4716 (FT Open)	9.9E-3	2.3	3.0E-3 (10)
AFW VALVES HV 4715 HV 4730 (FT Open)	1.2E-2	1.8	3.0E-3 (10)
AFW P140 (Turbine Driven)	3.0E-2	1.9	3.0E-2 (10)
	3.1E-4	2.4	2.0E-5 (10)
Motor Driven AFW Pumps P141 P504	4.7E-3	2.7	3.0E-3 (10)
	5.3E-4	2.4	1.0E-4 (10)
CCW Pumps P024 P025 P026	1.2E-2	3.6	3.0E-3 (10)
	8.2E-5	1.5	1.0E-4 (10)
CCW Heat Exchangers	9.6E-5	1.5	5.8E-6 (10)
CVCS HV-9201	2.3E-2	2.7	3.0E-3 (10)
CVCS HV-9235	1.1E-2	3.6	3.0E-3 (10)
CVCS HV-9240	1.1E-2	3.6	3.0E-3 (10)
CVCS HV-9247	1.3E-3	10	3.0E-3 (10)
Emergency Chilled Water Pumps P160 P162	3.8E-3	3.6	3.0E-3 (10)
	3.4E-4	3.7	1.0E-4 (10)

Table 3.3-4

PLANT-SPECIFIC DATA SUMMARY
(continued)

Component Description (Unit 2 & 3)	Bayesian Failure Rate	Bayesian Error Factor	Generic Value & EF (/demand or /hour)
Emergency Chillers	4.3E-3	3.7	8.1E-3 (10)
E335			
E336	5.1E-5	2.8	4.0E-6 (10)
HPSI Pumps	4.8E-3	3.6	3.0E-3 (10)
P017			
P018	6.0E-4	3.7	1.0E-4 (10)
P019			
LPSI Pumps	7.6E-4	10	3.0E-3 (10)
P015			
P016	2.8E-4	1.8	1.0E-4 (10)
MSS ADVs (FT Open or Close)	7.7E-3	1.7	2.0E-3 (3)
MSS Turbine Bypass Valves	1.1E-2	1.5	1.0E-3 (10)
MSS MSIVs (FT Close)	6.6E-3	1.8	2.0E-3 (3)
SWC Pumps	6.1E-3	2.7	3.0E-3 (10)
P112			
P113			
P114	1.3E-4	1.4	1.0E-4 (10)
P307			
DG-Start	1.7E-2	1.7	3.0E-2 (3)
DG002			
DG003			
DG-Load			
DG002			
DG003			
DG-Run	9.6E-3	1.6	3.0E-3 (10)
DG002			
DG003			

Table 3.3-5
PLANT-SPECIFIC COMPONENT UNAVAILABILITIES

SYSTEM	COMPONENT GROUP	COMPONENTS	UNAVAIL.
AFW	Motor Driven AFW Pump	P-141, P-504	0.0076
	Turbine Driven AFW Pump	P-140	0.022
	Turbine Driven AFW Pump Flow Control Valves	HV-4705, -4706	0.0036
	Motor Driven AFW Pump Flow Control Valves	HV-4712, -4713	0.0015
	AFW Isolation Bypass Valves	HV-4714, -4731	0.0018
	Turbine Driven AFW Pump Stop Valves	HV-4716	0.0010
	AFW Isolation Valves	HV-4730, -4715	0.0018
	AFW Flow Control Bypass Valves	HV-4762, -4763	0.041
HPSI	HPSI Pumps	P-17, P-18, P-19	0.05
	Containment Sump Valves	HV-9302, -9303	0.001
	HPSI Injection Valves	HV-9323, -9324, -9326, -9327, -9329, -9330, -9332, -9333	0.0015
LPSI	LPSI Pumps	P-15, P-16	0.0072
	LPSI Injection Valves	HV-9322, -9325, -9328, -9331	0.0014
CS/CEC	Containment Spray Pumps	P-12, P-13	0.0055
	Containment Spray Isolation Valves	HV-9367, -9368	0.0003
	Containment Emergency Fan Coolers	E-399, -400, -401, -402	0.0022
SWC	SWC Heat Exchangers	E-001, -002	0.0065
	SWC Heat Exchangers In Heat Treatment	E-001, -002	0.0030
EP	Emergency Diesel Generators	G002, G003	0.011

3.3.3 Human Failure Data

3.3.3.1 General Methodology

The Human Reliability Analysis (HRA) for SONGS 2/3 is based primarily on NUREG/CR-4772, Accident Sequence Evaluation Program (ASEP): Human Reliability Analysis Procedure (Reference 3.3-12). The ASEP procedure is a shortened, conservative version of the procedure, models, and data for human reliability analysis which are presented in the Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications (NUREG/CR-1278) (Reference 3.3-13). The analysis was separated into pre-initiator (Type A) and post-initiator (Type C) analyses. Operator actions which resulted in a plant trip or other initiating event (Type B) were not modeled in the HRA but are accounted for in the initiator event frequency analysis.

The ASEP methodology was used to model both pre- and post-initiator operator actions. Pre-initiating event human actions include restoration of system components and flow paths following testing and maintenance activities. These actions typically consist of opening or closing of manual or motor operated valves. These tasks are generally performed routinely and repetitively. These actions are modeled as potential failure mechanisms in the system fault trees. With respect to quantification, only the nominal ASEP analysis was used. Calculation worksheets which are based on the ASEP step-by-step procedure were developed for all pre-initiator operator actions. The major factors considered in quantification of the errors included the availability of valve alignment checklists, control room position indication and annunciation, periodic walkdowns of system alignments, availability of an independent checker during system restoration, etc.. The pre-initiator analysis methodology is discussed in more detail in Section 3.3.3.2. The results of the pre-initiator HRA analysis are documented in Section 3.3.3.3.

Post-initiator actions are actions in response to a specific initiating event. These actions typically include tasks specified in the emergency operating instructions, and alarm response procedures. The tasks may require diagnosis, control and alignment of emergency safety systems, local in-plant component restoration, etc.. For quantification of post-initiator operator actions, a simpler, more conservative screening analysis was used in lieu of the ASEP screening analysis. The purpose of the screening analysis was to reduce the effort expended on actions which do not have significant impact on plant risk. The nominal ASEP approach was used for those operator actions which were not screened out and required further analysis.

Operator action summary sheets which fully describe the operator action and the surrounding circumstances were developed for actions which were not screened out. Also, calculation worksheets, which are based on the nominal ASEP analysis procedure, were developed. In instances where the simplistic and conservative methods of ASEP could not be directly applied, NUREG/CR-1278 was used. The post-initiator analysis methodology is discussed in more detail in Section 3.3.3.4. The results of the post-initiator HRA analysis are documented in Section 3.3.3.5.

3.3.3.1.1 Plant Walkdowns, Operator Interviews, Simulator Observations

As an integral part of the analysis, escorted plant walkdowns, operator interviews, and formal IPE simulator observations were utilized to aid in the understanding of key operator actions.

Plant walkdowns of in-plant post-initiator operator actions were performed by a member of the IPE team and a senior reactor operator and/or a shift technical advisor. Walkdowns were performed as closely as possible to the path and speed an actual demand would follow. The travel time to the desired location from the control room was measured and an estimate based on the operator's expertise was used to determine the component restoration or manipulation time. Information obtained from the walkdown included the feasibility of actions based on logistics, time availability, and ease of completion.

Primarily used in the post-initiator human actions portion of the analysis, the intent of the simulator observations was to either support or modify the assumptions used to calculate the human error probabilities (HEP) calculated from NUREG/CR-4772. The simulator observations were performed after an adequate number of important operator actions were identified. These actions were identified during the initial phase of event tree quantification. These actions were combined into four accident sequences which could be run on the SONGS 2 simulator. During different sessions, two complete and separate crews of varying experience and qualifications were asked to respond to each of four accident sequences. After each of the scenarios, each of the crew members were polled independently to privately assess the events and circumstances surrounding the scenario. The crew members were polled independently to reduce the dependency between crew members when polled as a team. The resulting observations were incorporated into the analysis.

3.3.3.2 HRA Methodology for Pre-Initiator Tasks

The methods used to assess pre-initiator operator actions are consistent with NUREG/CR-4772 and the NUREG/CR-4550 studies.

Pre-initiator operator actions which were modeled were reduced to restoration or miscalibration errors. All valves for each standby system were evaluated to determine whether restoration error would result in partial or total failure of the system to perform its required function. The identified valves were further evaluated based on the guidelines listed in Table 3.3-6. These guidelines are consistent with those used in the Sequoyah Unit 1 PRA (NUREG/CR-4550).

All calculations were documented on "Pre-Initiator Human Error Probability Calculation Worksheets." A sample of the worksheet is given in Figure 3.3-2.

3.3.3.3 Pre-initiator HRA Results

The results of the pre-initiator HRA analysis are given in Table 3.3-7.

3.3.3.4 HRA Methodology for Post-Initiator Tasks

The HRA process for post-initiator operator actions was a 4 step process. The process is in accordance with NUREG/CR-4772. The ASEP procedure formally uses a screening approach and a nominal analysis. A simplified and more conservative screening approach was substituted for the ASEP screening approach. This approach is discussed further.

1. Identify the operator action to be modeled. For each initiating event, key operator actions which may impact the consequences of the event were identified. Plant emergency and abnormal operating instructions (EOIs and AOIs) and annunciator response procedures were used to identify the human actions for recovery of accident sequences, or cutsets.
2. Screening of the key operator actions. The plant model was quantified with all operator actions initialized with a failure probability of 1.0. Operator actions which only appeared in cutsets lower than $1\text{E-}7/\text{yr}$ or less were left in the fault tree models but not evaluated further. Operator actions which appeared in cutsets greater than $1\text{E-}7/\text{yr}$ were evaluated further using nominal estimates. And sequences with no operator action modeled and whose probability were greater than $1\text{E-}7$ were examined to identify any potential recovery actions.
3. Quantification of the remaining HRA events. The events not screened out were quantified in accordance to NUREG/CR-4772. The ASEP method uses a single HEP number for a "merged human

Table 3.3-6
QUANTIFICATION OF PRE-INITIATOR HUMAN ACTIONS

1. Assess an HEP of 0.0 if any of the following conditions apply:
 - a. Valve position is annunciated in the control room.
 - b. Valve receives signal to respond when required.
 - c. Valve misposition would result in unexpected flow or lack of flow which would be immediately apparent in the control room.
 - d. Post-maintenance/test valve position is the same as that during the test. Misposition during test would result in inability to perform test.
2. Assess a basic error rate of 0.03 if none of the conditions in step 1 apply.
3. Determine if the recovery factors are available:
 - a) a compelling signal, such as an annunciator, will signal an error
 - b) a post-maintenance/test can locate an error
 - c) a second checker w/ written sign-offs is available to verify correct restoration actions
 - d) a daily or weekly check of status is available
- 4) Apply appropriate recovery factor probabilities from NUREG/CR-4772 to the basic error rate of 0.03.

NOTE: Per Item 4 of Table 5-2 of NUREG/CR-4772 and Chapter 19 of NUREG/CR-1278 (THERP), Table 15-3 of NUREG/CR-1278 was used to assess recovery based on shiftly, daily or monthly status checks using written checkoff lists. Per Chapter 19, the verification checks are considered "active inspections."
- 5) Determine level of with-in person dependence.
 - a) If a series system, assign zero dependence.
 - b) If a parallel system, assign complete dependence if actions are close in time & within 4 feet of each other, high dependence if actions are close in time, are in the same general area and no written check-off list is available. Assign zero dependence if none of the above apply.
6. Modify human error probability per NUREG/CR-4772 rules if non-zero dependence is assigned.
7. Convert median HEP ($F_{T-\text{median}}$) to a mean value (F_T) and apply to the corresponding basic event in the appropriate system fault tree.

Figure 3.3-2

PRE-INITIATOR HUMAN ERROR PROBABILITY CALCULATION WORKSHEET

BASIC EVENT NAME: --- SAMPLE ---	HUMAN ACTION DESCRIPTION:															
BASIC HUMAN ERROR PROBABILITY (BHEP) DETERMINATION: Assign the initial basic human error probability (BHEP) based on steps 1 through 3 and 5 in Table 5-1*. BHEP = 0.03 List Applicable Procedures:																
RECOVERY FACTOR DETERMINATION: Assign recovery factor basic and optimum conditions in accordance with steps 4 and 7 of Table 5-1. Use Table 5-2 and circle the appropriate condition numbers below. <table style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <thead> <tr> <th></th> <th style="text-align: center; border-bottom: 1px solid black;">BASIC</th> <th style="text-align: center; border-bottom: 1px solid black;">OPTIMUM</th> </tr> </thead> <tbody> <tr> <td>Compelling Signals:</td> <td style="text-align: center;">1</td> <td style="text-align: center;">1</td> </tr> <tr> <td>PM or PC Tests:</td> <td style="text-align: center;">2</td> <td style="text-align: center;">2</td> </tr> <tr> <td>Written Standard Check of Specific Action:</td> <td style="text-align: center;">3</td> <td style="text-align: center;">3</td> </tr> <tr> <td>Written Daily/Shiftly Checks of Status:</td> <td style="text-align: center;">4</td> <td style="text-align: center;">4</td> </tr> </tbody> </table> Determine the initial total failure probability ($BHEP \cdot F_{RF}$) in accordance with step 8 of Table 5-1. Use Table 5-3. $BHEP \cdot F_{RF} =$ _____ Assumptions:			BASIC	OPTIMUM	Compelling Signals:	1	1	PM or PC Tests:	2	2	Written Standard Check of Specific Action:	3	3	Written Daily/Shiftly Checks of Status:	4	4
	BASIC	OPTIMUM														
Compelling Signals:	1	1														
PM or PC Tests:	2	2														
Written Standard Check of Specific Action:	3	3														
Written Daily/Shiftly Checks of Status:	4	4														
ACTION DEPENDENCE DETERMINATION: In accordance with step 9 of Table 5-1, assess human action dependence below. Circle the system type below that best describes the context of the human action being evaluated. System Type: Series/Parallel Using Table 5-4, assess the level of dependence associated with this human action, and circle the appropriate level of dependence below. Level of Dependence: Zero/High/Complete (Zero, if System Type is Series) Assumptions:																
MEAN TOTAL FAILURE PROBABILITY (F_T) DETERMINATION: Using Table 5-5, determine the median total failure probability ($F_{T-median}$) and associated error factor (EF) in accordance with step 10 of Table 5-1. $F_{T-median} =$ _____ $EF =$ _____ $F_T =$ _____																

Prepared by: _____

Checked By: _____

Date: _____

Date: _____

*NOTE: For all tables and figures, refer to NUREG/CR-4772.

Table 3.3-7
RESULTS OF PRE-INITIATOR ANALYSIS

System: Low Pressure Safety Injection			
Basic Event	Mean	EF	Description
A-HACV024--X	5E-4	10	LPSI P-015 Stop Check Valve 024 Misaligned
A-HACV025--X	5E-4	10	LPSI P-016 Stop Check Valve 025 Misaligned
A-HAMV0396-X	4E-5	16	LPSI/SDC MOV-0396 Misaligned
A-HAMV8150-X	4E-5	16	LPSI/SDC MOV-8150 Misaligned
A-HAMV8151-X	4E-5	16	LPSI/SDC MOV-8151 Misaligned
A-HAMV8152-X	4E-5	16	LPSI/SDC MOV-8152 Misaligned
A-HAMV8153-X	4E-5	16	LPSI/SDC MOV-8153 Misaligned
A-HAMV8160-X	4E-5	16	LPSI/SDC MOV-8160 Misaligned
A-HAMV8161-X	4E-5	16	LPSI/SDC MOV-8161 Misaligned
A-HAMV9353-X	4E-5	16	LPSI/SDC Warm-up Valve MOV-9353 Misaligned
A-HAMV9359-X	4E-5	16	LPSI/SDC Warm-up Valve MOV-9359 Misaligned
A-HAXV012--X	5E-4	10	LPSI/CCW-P-015 Manual Valve 012 Misaligned
A-HAXV031--X	5E-4	10	LPSI/CCW-P-016 Manual Valve 031 Misaligned
A-HAXV226--X	5E-4	10	LPSI/CCW-P-016 Manual Valve 226 Misaligned
A-HAXV229--X	5E-4	10	LPSI/CCW-P-015 Manual Valve 229 Misaligned

System: Instrument Air System and Nitrogen System			
Basic Event	Mean	EF	Description
B-HAXV054--X	8E-3	10	Instrument Air Manual Valve 054 Misaligned

Table 3.3-7

Results of Pre-Initiator Analysis (continued)

System: Chemical Volume Control System			
Basic Event	Mean	EF	Description
D-HAXV004--X	5E-4	10	CVCS (BAMU Pump Section) Manual Valve 004 Misaligned
D-HAXV005--X	5E-4	10	CVCS (BAMU Pump Section) Manual Valve 005 Misaligned
D-HAXV006--X	5E-4	10	CVCS (BAMU Pump Section) Manual Valve 006 Misaligned
D-HAXV007--X	5E-4	10	CVCS (BAMU Pump Section) Manual Valve 007 Misaligned
D-HAXV016--X	5E-4	10	CVCS (Charging Pump P-192 Suction) Manual Valve 016 Misaligned
D-HAXV018--X	5E-4	10	CVCS (Charging Pump P-192 Discharge) Manual Valve 018 Misaligned
D-HAXV034--X	5E-4	10	CVCS (BAMU Pump Discharge) Manual Valve 034 Misaligned
D-HAXV036--X	5E-4	10	CVCS (BAMU Pump Discharge) Manual Valve 036 Misaligned
D-HAXV054--X	5E-4	10	CVCS (RWST to Charging Pumps) Manual Valve 054 Misaligned
D-HAXV063--X	5E-4	10	CVCS (Charging Pump P-191 Suction) Manual Valve 063 Misaligned
D-HAXV067--X	5E-4	10	CVCS (RWST to Charging PPs) Manual Valve 067 Misaligned
D-HAXV070--X	5E-4	10	CVCS (Charging Pump P-191 Discharge) Manual Valve 070 Misaligned
D-HAXV128--X	8E-3	10	CVCS (Alt. Aux. Spray) Manual Valve 128 Misaligned

System: Component Cooling Water System			
Basic Event	Mean	EF	Description
E-HAECUTRNAX	5E-4	10	CCW Throttle Valve Train A Misaligned
E-HAECUTRNBX	5E-4	10	CCW Throttle Valve Train B Misaligned
E-HAP24VENTU	1E-4	16	CCW Pump Casing Vent Misaligned
E-HAXV172--X	5E-4	10	CCW (Cooling for P-024) Manual Valve 172 Misaligned

Table 3.3-7

Results of Pre-Initiator Analysis (continued)

E-HAXV173--X	5E-4	10	CCW (Cooling for P-024) Manual Valve 173 Misaligned
E-HAXV6507-X	5E-4	10	CCW (Pump P-024 Discharge) Manual Valve 6507 Misaligned
E-HAXV6520-X	5E-4	10	CCW (Pump P-024 Discharge) Manual Valve 6520 Misaligned

System: Main Feedwater System			
Basic Event	Mean	EF	Description
F-IAXV3231-X	8E-3	10	MFW Manual Valve 3231 Misaligned

System: High Pressure Safety Injection			
Basic Event	Mean	EF	Description
H-HACV012--X	5E-4	10	HPSI P-017 Stop Check Valve 012 Misaligned
H-HACV015--X	5E-4	10	HPSI P-019 Stop Check Valve 015 Misaligned
H-HACV016--X	5E-4	10	HPSI P-018 Stop Check Valve 016 Misaligned
H-HADEBRIS-X	5E-5	10	HPSI Containment Drain Misaligned
H-HARFCNL--X	4E-5	7	HPSI Refueling Canal Drain Misaligned
H-HASMPLT--X	1E-4	16	HPSI Emergency Sump Latch Misaligned
H-HAXV013--X	5E-4	10	HPSI Locked Open Manual Discharge Valve 013 Misaligned
H-HAXV014--X	5E-4	10	HPSI Locked Closed Manual Discharge Valve 014 Misaligned
H-HAXV066--X	5E-4	10	HPSI Hot Leg Injection Manual Valve 066 Misaligned
H-HAXV067--X	5E-4	10	HPSI Hot Leg Injection Manual Valve 067 Misaligned
H-HAXV184--X	5E-4	10	HPSI (Mini-Flow Test) Manual Valve 184 Misaligned
H-HAXV185--X	5E-4	10	HPSI (Mini-Flow Test) Manual Valve 185 Misaligned
H-HAXV186--X	5E-4	10	HPSI (Mini-Flow Test) Manual Valve 186 Misaligned
H-HAXV7766-X	5E-4	10	HPSI RWST Cross-connect Manual Valve 7766 Misaligned

Table 3.3-7

Results of Pre-Initiator Analysis (continued)

System: High Pressure Safety Injection			
Basic Event	Mean	EF	Description
H-HAXV7767-X	5E-4	10	HPSI RWST Cross-connect Manual Valve 7767 Misaligned

System: Auxiliary Feedwater System			
Basic Event	Mean	EF	Description
L-HAXV122--X	5E-4	10	AFW (P-140 Discharge) Manual Valve 122 Misaligned
L-HAXV123--X	5E-4	10	AFW (P-140 Discharge - Train "A") Manual Valve 123 Misaligned
L-HAXV125--X	5E-4	10	AFW (P-140 Discharge - Train "A") Manual Valve 125 Misaligned
L-HAXV127--X	5E-4	10	AFW (P-141 Discharge) Manual Valve 127 Misaligned
L-HAXV128--X	5E-4	10	AFW (P-504 Discharge) Manual Valve 128 Misaligned
L-HAXV130--X	5E-4	10	AFW (P-504 Discharge) Manual Valve 130 Misaligned
L-HAXV131--X	5E-4	10	AFW (P-141 Discharge) Manual Valve 131 Misaligned
L-HAXV133--X	5E-4	10	AFW (P-141 Discharge) Manual Valve 133 Misaligned
L-HAXV134--X	5E-4	10	AFW (P-140 Discharge - Train "B") Manual Valve 134 Misaligned
L-HAXV136--X	5E-4	10	AFW (P-140 Discharge - Train "B") Manual Valve 136 Misaligned
L-HAXV152--X	5E-4	10	AFW (P-504 Discharge Bypass) Manual Valve 152 Misaligned
L-HAXV153--X	5E-4	10	AFW (P-141 Discharge Bypass) Manual Valve 153 Misaligned
L-HAXV154--X	5E-4	10	AFW (P-141 Discharge Bypass) Manual Valve 154 Misaligned
L-HAXV214--X	8E-3	10	AFW (Demineralized Water Tank T268) Manual Valve 214 Misaligned
L-HAXV218--X	8E-3	10	AFW (Demineralized Water Tank T266) Manual Valve 218 Misaligned
L-HAXV219--X	8E-3	10	AFW (Demineralized Water Tank T267) Manual Valve 219 Misaligned

Table 3.3-7

Results of Pre-Initiator Analysis (continued)

System: Auxiliary Feedwater System			
Basic Event	Mean	EF	Description
L-HAXV533--X	5E-4	10	APW Manual Valve 533 Misaligned
L-HAXV553--X	5E-4	10	APW Manual Valve 553 Misaligned

System: Heating, Ventilation and Air Conditioning			
Basic Event	Mean	EF	Description
M-HADM255--X	8E-3	10	Inlet Damper for Chiller E255 Misaligned
M-HADP257--X	8E-3	10	Inlet Damper for Chiller E275 Misaligned
M-HADM430--X	8E-3	10	Inlet Damper for Chiller E430 Misaligned
M-HAE255---X	5E-4	10	3 Emergency Chilled Water Valves for E255 Misaligned
M-HAE257---X	5E-4	10	3 Emergency Chilled Water Valves for E257 Misaligned
M-HAE335---X	5E-4	10	6 Emergency Chilled Water Valves for E335 Misaligned
M-HAE335CCWX	5E-4	10	4 CCW Valves to Chiller E335 Misaligned
M-HAE336---X	5E-4	10	6 Emergency Chilled Water Valves for Chiller E336 Misaligned
M-HAE336CCWX	5E-4	10	4 CCW Valves to Chiller E336 Misaligned

System: Containment Spray System			
Basic Event	Mean	EF	Description
N-HACV004--X	1E-3	16	CSS (Train A Spray Header) Stop Check Valve 004 Misaligned
N-HACV006--X	1E-3	16	CSS (Train B Spray Header) Stop Check Valve 006 Misaligned
N-HACV012--X	5E-4	10	CSS (P-012 Discharge) Stop Check Valve 012 Misaligned
N-HACV014--X	5E-4	10	CSS (P-014 Discharge) Stop Check Valve 014 Misaligned
N-HAFLTRNA-X	1E-3	16	CSS Spectacle Flange to Spray Header #1 Misaligned

Table 3.3-7

Results of Pre-Initiator Analysis (continued)

System: Containment Spray System			
Basic Event	Mean	EF	Description
N-HAFLTRNB-X	1E-3	16	CSS Spectacle Flange to Spray Header #2 Misaligned
N-HAXV003--X	5E-4	10	CSS (Train A Spray Header) Manual Valve 003 Misaligned
N-HAXV005--X	5E-4	10	CSS (Train B Spray Header) Manual Valve 005 Misaligned
N-HAXV203--X	5E-4	10	CSS/CEFCE-400 Manual Valve 203 Misaligned
N-HAXV204--X	5E-4	10	CSS/CEFCE-400 Manual Valve 204 Misaligned
N-HAXV205--X	5E-4	10	CSS/CEFCE-401 Manual Valve 205 Misaligned
N-HAXV206--X	5E-4	10	CSS/CEFCE-401 Manual Valve 206 Misaligned
N-HAXV207--X	5E-4	10	CSS/CEFCE-399 Manual Valve 207 Misaligned
N-HAXV208--X	5E-4	10	CSS/CEFCE-399 Manual Valve 208 Misaligned
N-HAXV209--X	5E-4	10	CSS/CEFCE-402 Manual Valve 209 Misaligned
N-HAXV210--X	5E-4	10	CSS/CEFCE-402 Manual Valve 210 Misaligned
N-HAXV6547-X	5E-4	10	CSS/CCW Manual Valve 6547 Misaligned
N-HAXV6548-X	5E-4	10	CSS/CCW Manual Valve 6548 Misaligned

System: Salt Water Cooling			
Basic Event	Mean	EF	Description
P-HAXV044--X	8E-3	10	SWC Manual (Vent) Valve 044 Misaligned
P-HAXV045--X	8E-3	10	SWC Manual (Vent) Valve 045 Misaligned
P-HAXV060--X	8E-3	10	SWC Manual (Vent) Valve 060 Misaligned

Table 3.3-7

Results of Pre-Initiator Analysis (continued)

System: Main Steam System			
Basic Event	Mean	EF	Description
T-HAXV001--X	1E-4	10	MSS/ADV Manual Valve 001 Misaligned
T-HAXV002--X	8E-3	10	MSS/ADV Manual Valve 002 Misaligned
T-HAXV021--X	8E-3	10	MSS/ADV Manual Valve 021 Misaligned
T-HAXV231--X	1E-4	10	MSS/ADV Manual Valve 231 Misaligned
T-HAXV1304-X	8E-3	10	MSS/ADV Manual Valve 1304 Misaligned
T-HAXV1305-X	8E-3	10	MSS/ADV Manual Valve 1305 Misaligned
T-HAXV1306-X	8E-3	10	MSS/ADV Manual Valve 1306 Misaligned
T-HAXV1307-X	8E-3	10	MSS/ADV Manual Valve 1307 Misaligned
T-HAXV910--X	1E-4	10	MSS/ADV Manual Valve 910 Misaligned
T-HAXV913--X	1E-4	10	MSS/ADV Manual Valve 913 Misaligned

basic event." The merged basic event is a combination of best estimates for diagnosis errors and post-diagnosis action errors. The diagnosis error is an error in determining the proper course of action in the time available. The post-diagnosis action error is an error in properly carrying out the correct response to a correct diagnosis. The base estimate for diagnosis error is determined from the ASEP nominal diagnosis model (which is dependent on the diagnosis time available) and adjusted according to performance shaping factors that increase or decrease the base HEP. The time available for the operator to respond was determined primarily by thermal hydraulic (RETRAN) and severe accident codes (MAAP). These codes were used to determine the time to steam generator dryout and RCS boil-off down to the top of the hot leg (where natural circulation would be lost).

The estimate of the post-diagnosis action error is based on the type of action (dynamic or step-by-step) and the amount of stress (moderate or extremely high stress). Those operator actions which were proceduralized were considered step-by-step.

For the SONGS 2/3 IPE, if an operator action requires more detailed modeling or the action to be modeled could not be directly modeled using ASEP methods, the Technique for Human Error Rate Prediction (THERP) method of NUREG/CR-1278, which the ASEP methods are based on, was used. For THERP each human failure event is divided into the procedural steps, or subtasks, dictated by the plant procedures, and then quantified for the failure to perform successfully the steps comprising the event. Finally, these subtasks are quantified and merged to form the probability of failing to successfully complete the required human event.

In cases where multiple operator actions appeared in the same cutset, the actions were evaluated as a whole to determine the possible courses of actions that the control room would take. This evaluation included discussions with operators, comparison with emergency operating instructions, and knowledge gained from observing simulator scenarios. The resulting operator action modeled is considered the probability of failure of the most likely actions to be taken. This likely operator action was quantified using nominal analysis methods with the other operator actions treated as dependent events. In all cases, the dependent operator actions were maintained at the screening value of 1.0.

To support the quantification of each post-initiator operator action, "Operator Action Summary Data Sheets" were

developed to document the scenario and circumstances surrounding the operator action (Figure 3.3-3). All calculations were documented on "Post-Initiator Human Error Probability Calculation Worksheets" (Figure 3.3-4).

4. Requantify plant model and evaluate additional operator actions. The event tree models were recalculated using the developed nominal HEPs. Again the plant cutsets were re-ranked by probability. The highest cutsets were again reviewed to identify additional operator actions. These actions were evaluated and quantified. This process of identification, evaluation and re-quantification of plant models was a continuous and iterative process.

3.3.3.5 Post-Initiator HRA Results

Based on the screening methodology described earlier, all basic events were initially given a screening probability of 1.0. All those cutsets which were greater than $1E-7$ /year and could be addressed with available and appropriate operator actions were evaluated further using nominal HRA quantification methods (ASEP, THERP). Per NUREG-1335 (Reference 3.3-14), all post-initiator human actions whose probability is 0.1 or less which results in a cutset dropping below $1E-7$ /year should be reported. Those operator actions are given in Table 3.3-8.

A list of the key operator actions for each of the major initiating events is listed in Table 3.3-9. Discussion of each of the initiators and the key actions are provided in Sections 3.3.3.5.1 - 3.3.3.5.7.

3.3.3.5.1 Anticipated Transient Without Scram

Based on the philosophy that critical safety functions are managed based on their safety priority, the highest priority following a transient is reactivity control. Following a transient, the operators look immediately to verify that all control element assemblies (CEAs) have fully inserted, reactor power is lowering and that the startup rate is negative. In the event that none of these are satisfied the operators are instructed to manually trip the reactor, initiate emergency boration and de-energize the power to the CEA magnets. These steps are immediate, memorized (with procedural backup) by all control room operators.

Based on simulator observations, immediate post-trip actions are performed by control operators (SRO or RO) for the main, secondary and common control room boards under the supervision of the control room supervisor who is a senior reactor operator (SRO). For all transients observed, the immediate steps

Figure 3.3-3

SAMPLE OPERATOR ACTION SUMMARY DATA SHEET

OPERATOR ACTION:

BASIC EVENT/ FAULT TREE:

- I. INTRODUCTION:
 II. ACCIDENT SEQUENCES INVOLVED:
 III. DESCRIPTION OF HUMAN ACTIONS:
 IV. TIME LINE:
 Time to first indication (or annunciation) (T_i):
 Maximum allowable time (T_m):
 Post-diagnosis action time (T_a):
 Diagnosis Time ($T_d = T_m - T_i - T_a$):
 V. COMPETING ACTIONS:
 VI. PRECEDING RELATED ACTIONS:
 VII. CONSEQUENCES OF FAILING TO PERFORM ACTION:
 VIII. CONSEQUENCES OF PERFORMING ACTION:
 IX. CREW TRAINING AND EXPERIENCE:

[Provide ranking of 0 through 5 (0 being none, 1 being poor, 5 being very good)]

	SIMULATOR	CLASSROOM	PLANT EXPER.
IDENTIFY			
DIAGNOSIS			
RESPONSE			

- X. CLARITY OF APPLICABLE PROCEDURES:
 XI. AVAILABILITY OF RELEVANT INDICATIONS:
 Cues For Operator Action:
 Indicators Used:
 Indicator Availability/Adequacy:
 XII. CONSIDERATIONS FOR "LOCAL" ACTIONS:
 • Is required action proceduralized?
 • How accessible is the component from the control room? Considering distance and number of security doors, estimate time to reach component from the control room.
 • Is action considered to be relatively simple or complex?
 • Are any special tools required (keys, wrenches, etc.)? If so, will they be readily accessible during the accident sequence?
 • Will performance of the action require entering a harsh environment where protection clothing or equipment is necessary?
 • Are there any unique aspects of the action which could affect the likelihood of successful completion (i.e., requires more than one person, must be performed concurrent with other actions, requires communication with the control room, etc.)?
 XIII. COMMUNICATIONS AND OPERATOR AVAILABILITY:
 XIV. OPERATOR OVERSIGHT/CHECKING:
 XV. STRESS LEVEL:
 XVI. SPECIFIC QUESTIONS ABOUT ACTION:
 XVII. OTHER INSIGHTS:

Figure 3.3-4
(Sheet 1 of 2)

SAMPLE POST-INITIATOR HUMAN ERROR PROBABILITY CALCULATION WORKSHEET

BASIC EVENT NAME:	HUMAN ACTION DESCRIPTION:
PROCEDURAL SUPPORT DETERMINATION: <u>STEPS 1 & 2:</u> Is the post-initiator human action supported by written procedures? Circle yes or no below. Yes: List Applicable Procedures: No: Assign Total Failure Probability (F_T) = 1.0.	
REQUIRED TIME RELATIONSHIP DETERMINATION: <u>STEP 3:</u> Using Figure 5 and 7, determine maximum allowable time: Maximum Allowable Time (T_m) = _____ Identify method of determining T_m (Judgement, RETRAN): _____ <u>STEPS 4 - 8:</u> Determine the diagnostic time: Post-diagnosis Action Time (T_a) = _____ Identify method of determining T_a (Judgement, walk-through, simulator, etc): _____ Available Diagnosis Time (T_d) = $T_m - T_a$ = _____ Assumptions: _____	
DIAGNOSIS HEP DETERMINATION: <u>STEP 9:</u> 9a) Select the initial diagnosis HEP from Figure 10 or Table 16. $HEP_{initial}$ = _____ 9b) Is more than 1 abnormal event involved as defined in Table 15, Step 9b? Yes No If yes, adjust HEP per Step 9B (Table 15) and Table 16 & 18. $HEP_{adjusted}$ = _____ 9c) Adjust HEP based on Table 17 guidelines: (Circle one) Upper Lower Nominal 9d) Is diagnosis HEP driven by symptom oriented EOI? (Circle one) Yes No If 'yes,' adjust HEP to lower bound (Figure 10). $HEP_{adjusted}$ = _____ 9e) Does HEP involve knowledge of critical RCS/Containment parameters? (Circle one) Yes No If no, go to step 9g. If parameters are committed to memory, use lower bound values in Figure 10 or Table 16. Otherwise use nominal values. Use Table 17 to adjust the new values, as appropriate. $HEP_{adjusted}$ = _____ (Circle one) Lower Nominal 9f) Not applicable. 9g) Is diagnosis error for HEP credible? (Circle one) Yes No If 'yes,' write last adjusted HEP from Steps 9a - 9e as the final diagnosis HEP below and continue to Step 10. If 'no,' assign 'Final Diagnosis HEP' = 0.0 and discuss below. Final Diagnosis HEP = _____ Assumptions: _____	

Figure 3.3-4
(Sheet 2 of 2)

STEP 10: As defined in Step 10 of Table 15, identify type of post-diagnosis task and stress level:

(Circle one) **Dynamic** **Step-by-step**
(Circle one) **Extremely high** **Moderately high**

Based on type of task and stress level, select HEP (s) for post-diagnosis action HEP(s) from Table 19. [Note: If time stress is present or if this task is required as a result of an ineffective initial task, assess applicability of doubling rule (Step 10g, Table 15). If yes, discuss in assumptions below.]

Post-Diagnosis Action HEP(s) = _____ Table 19 - Item # _____

Assumptions: _____

TOTAL FAILURE PROBABILITY (F_T) DETERMINATION:

STEP 11: Perform step 16 of Table 16 :

F_T = Final Diagnosis HEP + Post-Diagnosis Action HEP(s) = _____
[Note: If the calculated value of F_T exceeds 1.0, use 1.0.]

F_{T-MEAN} = _____ Error Factor (EF) = _____

Prepared by: _____

Checked By: _____

Date: _____

Date: _____

*NOTE: For all figures and tables, refer to Project Instruction PI-007 (Reference 3.3-15). "STEPS" refer to Table 15 of PI-007.

Table 3.3-8
POST-INITIATOR HUMAN ERROR PROBABILITY SUMMARY TABLE

BASIC EVENT	DESCRIPTION	MEAN (EF)
D-HCBORATE-U	Operator fails to emergency borate in an ATWS event.	3E-3 (10)
D-HCNOSIAS2U	No operator response to high temperature alarm to charging pump rooms given no SIAS	5E-3 (10)
E-HCP024---U	Operator fails to attempt to start standby CCW pump P024	1E-3 (10)
F-HCDEPRESSU	Operator fails to depressurize SG's w/i 1 hr. & align condensate	4E-2 (5)
FGHCCNDREC-U	Operator fails to recover condensate after loss of PCS w/i 60 min	6E-2 (3)
FGHCMFWREC-U	Operator fails to recover MFW after loss of PCS	4.3E-1 (3)
H-HC9300&01U	Operator fails to close HV-9300 and 9301 per SO23-12-3	5E-3 (5)
H-HCHLRECRUCU	Operator fails to establish hot leg recirculation within four (4) hours	5E-5 (5)
K-HCSCRAM--U	Operator fails to manually SCRAM reactor	3E-3 (10)
L-HCBYPASS-V	Operator fails to open HV-4762 or 4763 w/in 60 min w/ procedure	1E-3 (10)
L-HCCRCNNCTU	Operator fails to cross-connect MDAFWP to opposite SG	7E-3 (5)
L-HCCSTMU--U	Operator fails to provide CST Makeup per procedure	2E-5 (5)
L-HCNSBOMANU	Operator fails to manually control AFW flow valves w/i 2.5 - 8 hrs.	6E-3 (10)
L-HCSBO-MANU	Operator fails to manually operate the TDAFWP w/o DC power w/i 1 hour (SBO event)	6E-3 (5)
L-HCTP146--U	Operator fails to manually operate TDAFW pump (No DC power @ 8 hr; Non-SBO)	6E-3 (5)
L-HCTP1401HU	Operator fails to man open HV-4716 (Stop Valve) w/i 1 hr given Battery 9 fails	1.2E-2 (10)
M-HCE331---U	Operator fails to align chiller E331 to backup E330	5E-2 (10)
M-HCNOSIAS-U	Operator fails to respond to high temperature alarm in the switchgear/distribution room given no SIAS	1.6E-3 (10)
MRHC3E335--U	Operator fails to cross-tie CCW to chiller E335 from other unit given SGTR	3E-03 (5)
MRHC3E336--U	Operator fails to cross-tie CCW to chiller E336 from other unit given SGTR	3E-03 (5)
N-HCCSINJCTU	Operator fails to depressurize below CS Pump shutoff pressure given HPSI failure (Induced LOCA)	0.1 (10)
NBHCCSINJCTU	Operator fails to depressurize below CS Pump shutoff pressure given HPSI failure (Medium LOCA)	1.0
NCHCCSINJCTU	Operator fails to depressurize below CS Pump shutoff pressure given HPSI failure (Small LOCA)	0.5 (10)
T-HCDEPRESEU	Operator fails to depressurize RCS early (SGTR)	1E-3 (5)
T-HCINDLOCAU	Operator fails to depressurize RCS and control ECCS flow - induced LOCA	7.5E-2 (10)
TDHCCSPRAYU	Operator fails to depressurize and cooldown RCS to reduce RCS leak (SSL)	6E-3 (10)
TRHCADV-P-U	Operator fails to manually operate ADV locally given SGTR	3E-03 (10)
U-HCSHED60MU	Operator fails to loadshed within 1 hour	6E-03 (5)

Table 3.3-9

POST-INITIATOR HUMAN ACTIONS

INITIATOR	KEY OPERATOR ACTIONS
ATWS	<ul style="list-style-type: none"> Manual reactor trip Emergency boration
LOCA	<ul style="list-style-type: none"> Depressurization of the RCS to utilize low head safety injection pumps given a loss of HPSI pumps Establishment of hot leg injection
SGTR	<ul style="list-style-type: none"> Depressurization of the RCS to reduce primary to secondary leakage Provide make-up to the condensate storage tank
LOP/SBO	<ul style="list-style-type: none"> Recovery of offsite power Manual operation of the turbine-driven AFW pump without DC power
Loss of PCS	<ul style="list-style-type: none"> Recovery of MFW Recovery of alternative SG make-up via the condensate pumps
Turbine Trip (w/PCS)	<ul style="list-style-type: none"> Restore room cooling to the switchgear, inverter/distribution, and charging pump rooms Manual operation of the turbine-driven AFW pump without DC power Manual operation of the AFW flow control valves
Feed/Steam Line Break	<ul style="list-style-type: none"> Isolate the affected steam generator

performed are identical and carried out expediently. For the ATWS scenario, the crews were observed to complete the immediate recovery actions following an automatic SCRAM failure within a minute. Each of the primary and secondary board operators push redundant manual scram buttons (2 on each panel) with the primary control operator also initiating emergency boration. The de-energization of the control element drive mechanisms is accomplished by the common board control operator. These actions are continuously reinforced through training and practiced in the simulator.

Key insights included:

- All personnel observed within the control room immediately observed the automatic scram failure based on the failure of 'rod bottom' lights to completely illuminate. Multiple operators loudly announced that an ATWS had occurred. This is a good practice and serves to ensure that all personnel within the control room were immediately aware of the situation.
- Although all immediate actions were proceduralized, all personnel completed the ATWS actions completely, accurately and expediently, from memory and later confirmed by procedure.
- In non-ATWS events, it was observed that although the rod bottom lights are all illuminated, the operators by training redundantly push the manual scram buttons. This reduces the reliance on specific plant indications to confirm reactivity control.

3.3.3.5.2 LOCA

Following a LOCA/reactor trip, the SIAS will initiate starting of the low and high pressure safety injection pumps and the CS pumps. As in all events, the operators respond by observing all the immediate alarms and indications as well as immediately verifying reactivity control. The control room supervisor (CRS) initiates the standard post-trip actions (SPTA) (Emergency Operating Instruction SO23-12-1) which, based on the condition of important safety functions and parameters, will lead to a diagnosis of a LOCA. Formal diagnosis via the SPTA may take up to 10-15 minutes. The operator is then directed to the LOCA EOI SO23-12-3. The general flow of the SPTA and LOCA EOI is to ensure and verify that all safety functions are properly operating and meeting their

safety function. This includes verifying that a LOCA is in progress, ensuring a SIAS has been initiated, that all injections pumps are running, and that secondary heat removal is operating properly.

By procedure, after 2 hours following safety injection actuation, if entry into shutdown cooling is not anticipated within 4 hours following SIAS, then simultaneous hot and cold leg injection is initiated to preclude possible boron precipitation in the RCS vessel which may inhibit core cooling.

In a special case of the small or medium LOCA, if the HPSI system is unavailable and the leak is beyond the capacity of the charging pumps, the RCS pressure will be too high to allow the use of lower head injection pumps to preclude further inventory loss and eventual core uncover. The continuous loss of RCS inventory control should be observed by the control room operators but will formally be observed by the Shift Technical Advisor (STA) during his continuous monitoring of the safety function status checks (Attachment 1 of all EOIs). The 'Response Not Obtained' column of the procedure will direct the CRS to Attachment 6 of the "Functional Recovery" procedure (SO23-12-9) under 'Recovery-RCS Inventory Control.' In this attachment, they are guided to reduce pressure below the CS pump shutoff head (approximately 250 psig) to allow injection. If containment spray pumps are also unavailable, then pressure is reduced to the LPSI pump shutoff (approximately 200 psig).

Key insights include:

- During simulator observation of a small LOCA with failure of the HPSI pumps, the operators were able to reduce the pressure below the CS pump shutoff head before core uncover. The key in successful injection recovery is dependent on the speed of RCS pressure reduction. The time line in completing the action includes the time taken for the operators to conclude that RCS inventory control safety function is not being satisfied and the time taken to depressurize the RCS below the pressure of the low head injection pumps. The depressurization time is impacted by the RCS cooldown requirement of 100°F/hour limit. For medium LOCAs, sufficient time may be unavailable.
- In the LOCA simulator scenarios, it was observed that operators, per procedure, verify that the HPSI pumps are running. When the pumps were

unavailable, the operators immediately attempted to start the standby pump. Similarly, when CCW was unavailable (annunciated), the operators immediately attempted to start the available standby CCW pump. The procedures ask the operators to ensure that the mentioned pumps are operating. Although the procedures do not specifically state that the standby pump needs to be started when the automatic pumps fail, the operators demonstrated that doing so is an automatic reflex response.

3.3.3.5.3 Steam Generator Tube Rupture

The general philosophy following a steam generator tube rupture (SGTR) is to use the faulted steam generator to aid in reducing the primary system temperature to below 530°F in order to minimize the possibility of lifting the steam generator safety relief valves on the affected steam generator and to reduce the primary to secondary pressure differential to reduce RCS leakage. Following a SGTR, the operators initiate the SPTA (EOI SO23-12-1). The SPTA will direct the operators to the SGTR procedure (EOI SO23-12-4) where the operators are instructed to ensure and maximize RCS makeup via the charging pumps and safety injection pumps, and then, using both steam generators, reduce the hot leg temperature to below 530°F, isolate the steam generator and bring the RCS pressure to within 50 psi of the affected SG. Continued heat removal over 24 hours via the AFW system will require the operators to locally makeup to the CST. The cue to monitor the CST level is given in the main body and in the floating steps of the EOI.

Key insights:

- Based on operator discussions and simulator observations, the operators understand that the priority response to a SGTR is to reduce the primary system temperature and pressure to reduce primary to secondary leakage in order to conserve RCS inventory and to reduce the spread of radioactivity into the secondary system via an open safety valve.
- The operators will likely determine that the event is a SGTR before entering the SPTA due to the high secondary system radiation monitor alarms off each steam generator. These alarms are located on the

common board near the entrance to the main control room area.

In cases where a slow but increasing primary to secondary leak precedes a full tube rupture, the operators are forewarned by secondary system radiation monitors that a SGTR may be eminent and that a plant shutdown may be required to prevent a complete rupture. If shutdown is required, the operators lower power via emergency boration and eventually trip the reactor manually from a lower power level.

The operators are well trained on the symptoms of an eminent tube rupture, and on the parameters to monitor prior to and following a tube rupture. They are also aware of the required plant and operator response to prevent further plant damage and ensure public safety.

To compound the increase in levels in the affected steam generator during the simulator exercises, the feedwater regulating valves were failed in the open position in order to evaluate the operator's response to a potential overfill event. Although the operator was not immediately aware of the valve failure and the rapidly increasing steam generator level, in all cases, the secondary system board control operator successfully provided manual back-up to the failed automatic reactor trip override system (which runs back the MFW flow to 5%) thus preventing overfill. Manual backup of this MFW flow runback feature is a trained immediate and memorized action.

3.3.3.5.4 Loss of Offsite Power/Station Blackout

The loss of offsite power is immediately observable in the control room. Aside from the loss of normal light levels in the control room, the common board control operator should immediately verify the loss of offsite power based on indication and undervoltage annunciators on the common board. If the EDGs are available, both motor-driven AFW pumps and the turbine-driven AFW pumps should be available to supply steam generator (SG) makeup. If all AC power is unavailable, then only the turbine-driven AFW pump is available for SG makeup. The turbine-driven AFW pump should start automatically following EFAS initiation and continue to run using DC control power for 8 hours. If power is not restored within 90

minutes (assuming the operators do not loadshed), then the control power to the AFW discharge valves is unavailable and must be operated locally. Local operation must be coordinated with the control room where level indication should still be available. Since the rate of decay heat reduction is small, the flow control position requires minimal throttling to prevent SG overfill. Other than trying to restore offsite power and emergency diesel generators, which are generally actions taken by other personnel outside the control room, there should be no other competing actions. Longer term operation with SBO will require the operators to manually control the turbine-driven AFW pump.

Key insights:

- Operations and the Training Department for SCE are particularly sensitive to the importance of the ability to manually operate the turbine-driven AFW pump P-140 without power. Two clear, simple and legible signs have been installed locally near P-140 for the purposes of a) resetting the overspeed trip, and b) operating P-140 without DC power. These serve to remind the operator of the steps needed for recovery. Each action has also been proceduralized with testing given formally through the Job Performance Measures program which is administered by the Training Department. Each of the actions have been performed in the field thus confirming the feasibility of the recovery actions.

3.3.3.5.5 Loss of Power Conversion System (PCS)

The loss of the PCS which includes the turbine/generator, condenser and the MFW system results in a reactor/turbine trip and an eventual demand for AFW. The loss of portions of the PCS has occurred a number of times over the life of SONGS 2/3. In all cases the AFW system was available to provide SG makeup. With AFW available, the operator only needs to verify satisfaction of the critical safety functions per the SPTA. However, should the AFW system become unavailable, the MFW pumps and/or the condensate pumps may be restored to provide make-up. This is dependent, however, on what initially caused the loss of the PCS.

Key insights:

- In the simulator, the operators demonstrated familiarity with using the condensate pumps as an alternate feedwater source. The operators reduced

the secondary system pressure below the condensate pump shutoff head and provided secondary cooling.

3.3.3.5.6 Turbine Trip with PCS Available

In an uncomplicated reactor/turbine trip, all safety functions are satisfied with all secondary makeup sources available including the MFW pumps (at approximately 5% of full power flow). The buses normally powered off the unit's generator are transferred over to offsite power via the reserve auxiliary transformers. However, in particular, the event in which fast transfer of 4kV Bus A08 is not successful, source power to normal HVAC is lost and cooling to the 1-E ESF switchgear, inverter/distribution, and charging pump room is left unavailable. An undervoltage alarm is expected immediately upon fast transfer failure. SG makeup will be supplied by AFW. Also, MFW may trip due to high discharge pressure failure (power to miniflow is eventually lost). Since a SIAS may not occur (which initiates emergency HVAC), the switchgear and the ESF distribution rooms will heat up. Continued heat-up to 122°F in the ESF switchgear room could result in loss of control power to the AFW flow control valves and the MFW regulating system. When the room reaches 95°F, a high temperature annunciator in the control room alarms cuing the operator of the rising temperature. It is expected that the alarm setpoint will be reached within 5 minutes of the fast transfer failure and that 70 minutes would be available following the alarm for the operator to provide cooling. Similar alarms are available for the inverter/distribution, charging pump and battery rooms. The operator response for each of these alarms is found in the associated alarm response procedure which guides the operator to locally verify the high temperature environment, alarm setpoints, and the existence of any fire. The CRS is then guided to consider initiating emergency HVAC.

Key insights include:

- Given that the common board control operator is familiar that all buses transfer to offsite power following a reactor trip, the failure of any bus to transfer should be obvious. The operators may immediately respond and attempt to make the transfer manually assuming that the automatic transfer failed, the breakers may still be manipulated remotely from the control room. Credit is not given in the analysis for this immediate recovery action.

3.3.3.5.7 Feed/Steam Line Break

The most conservative cases evaluated were breaks inside containment. With respect to operator response and long term plant response, the two events are responded to identically by the operators. Immediately¹ following a break, all engineered safety features actuation signals (except the RAS) initiate. The containment sump level alarm will signify leakage in containment. Operators will respond by initiating the SPTA verifying maximum injection flow and isolation of both Sgs. The RCS is rapidly being cooled and depressurized by the blowdown of the affected SG. To prevent potential rapid repressurization of the RCS following dryout of the affected SG, the operators will establish a steaming path on the unaffected SG prior to dryout of the affected SG. At this point, continued heat removal will be through the unaffected SG.

Key insights include:

- In the simulator, the secondary board operators are told to watch level on the affected steam generator. When the blowdown reaches approximately 5% level wide range, the operator is to operate the steam bypass control system or atmospheric dump valve in order to establish steam demand on the unaffected steam generator. This is the major task that the secondary board operator has and is directly focused on this action.
- To compound the scenario in the simulator, auxiliary feedwater to the affected steam generator was rendered unavailable. The operators pursued two paths in order to provide feedwater:
 - 1) reduce SG pressure to allow use of the condensate pumps and 2) cross-tie the AFW pump which normally feeds the opposite SG. The first path (condensate pumps) is indicated in the functional recovery for RCS heat removal. However, the instructed use of the condensate and condensate transfer pumps is precluded by the closure of the MFW isolation valves (CIAS, MSIS). No further guidance is given in the procedures for this case and time may be wasted pursuing the use of the condensate pumps. The second path, cross-tie of the AFW pump, is not proceduralized in the

¹less than 1 minute.

emergency operating instruction but is an evolution which is done during plant startup. Both simulator crews exhibited resourcefulness in pursuing this abnormal alignment which was based on past system knowledge.

3.3.4 Common Cause Failure Data

The effects of failures that subjugate the redundancy and/or diversity in the current design of SONGS 2/3 (referred to as dependent failures) were incorporated using various methods. Common-cause failures, or those failures in which two or more similar components fail due to a shared cause, represent only a subset of the dependent failures considered. Other dependent failures such as support system failures that can fail multiple frontline systems and subtle interactions that are not captured using standard PRA methods were integral in identifying failure modes that could defeat the diversity and redundancy of the SONGS 2/3 design.

3.3.4.1 Explicit Dependencies

The application of event tree/fault tree methodology includes dependent failures through the modeling identification and quantification of the following:

- Functional coupling, i.e. accident sequence dependencies
- Shared system dependencies, e.g. support systems
- Human coupling among systems
- Spatial dependencies
- Intercomponent dependencies

The first four dependent failure causes are treated through explicit modeling techniques. The last dependent failure type is treated using a qualitative evaluation coupled with a parametric quantification method.

Event tree models developed establish the functional coupling among systems for each postulated accident sequence. The event tree models include explicitly the functional dependencies that may cause direct failure of systems. Dependencies between systems in an event tree sequence are captured either from the structure

of the sequence explicitly or the propagation of failures preceding the system in the boolean analysis of the sequence.

Both fault trees and dependency matrices are used together to identify system dependencies. System fault tree analysis includes explicit equipment dependencies within the system and on other systems outside the system boundary (support systems). The dependency matrix provides a simplified formalism for identifying these dependencies. System dependencies arising from the dependence of frontline systems on support systems, such as power or service water, are included in the logic model by including the basic events representing component failure modes associated with failures of these support systems in the frontline system model. Support system equipment failures which fail multiple systems are propagated in the boolean analysis of the model and are therefore modeled and identified explicitly.

The human interface with safety and non-safety systems is a key contributor to system availability. Operator actions are incorporated directly in the fault tree and event tree construction based on procedures, training, and practices where the operator interface may defeat single and multiple components or systems. These failures are propagated through the model in a manner similar to that described for support systems. In some cases multiple operator actions occur in an accident sequence which can influence the likelihood that operator actions will be completed successfully. Details of the human interface dependencies are detailed in Section 3.3.3.

Spatial dependencies pertain to the effects of harsh environments on equipment operability. These are treated explicitly in the logic models with dependencies of system components on room cooling. Spatial dependency effects are also considered in the internal flood evaluation described in Section 3.3.8.

3.3.4.2 Subtle Dependencies

The following potential subtle interactions discussed in NUREG/CR-4550, Vol. 1, Section 6.2, were evaluated for applicability to the SONGS 2/3 IPE effort.

1. DG Load Sequence Failures

Description

NUREG-4550 references four Interim Reliability Evaluation Program studies that identified several single failures in a diesel generator load sequencer system of a BWR. The circuit is designed to strip off loads on the DGs following a Loss of Offsite Power (LOP). The circuit uses redundant trip relays to ensure that this function is accomplished.

The circuit is designed to work in the following manner: (1) a LOP de-energizes the coils associated with contacts 1 through 4; (2) upon de-energization, these normally-open contacts close; (3) given closure of contacts 1 or 2, trip coil A energizes; (4) given closure of contacts 3 or 4, trip coil B energizes; and (5) if either of the trip coils are energized, all loads are stripped off the Dgs and cannot be reloaded. As can be seen, redundancy is employed in this load stripping circuit. The problem with this circuit design is that redundancy is not employed during the subsequent reload.

Applicability to SONGS 2/3

The load sequencing at SONGS 2/3 is not performed by a Load Sequencer. The timing for load addition is provided by individual time delay relays in the control circuits of each loading requiring such. Upon loss of bus voltage, undervoltage relays initiate the trip of loads on the ESF buses. When voltage is restored to the bus, individual timers in the control circuit for each load requiring sequencing are energized.

2. Sneak Circuits Following Power Restoration

Description

Sandia National Laboratories (SNL) recently discovered a potential problem in the Reactor Core Isolation Cooling (RCIC) system circuitry at a particular BWR. The problem occurs following power restoration to the RCIC circuits. This could occur during a LOP and subsequent energization of the circuits by the diesel. Because of the design of the RCIC steam leak detection circuit, it is possible for a sneak circuit to occur and cause an unintended isolation of the RCIC pump.

Fault tree analysis is not a very good tool for identifying such a failure mode because it is caused by a sequencing problem in the

relays. Since fault trees are generally time-independent, they are normally incapable of identifying sequencing failure modes.

It appears there are at least three subtle design aspects which lead to the occurrence of this failure mode: (1) the RCIC system contains an isolation circuit, (2) the isolation circuitry is de-energized given a LOP (i.e., the circuitry is not fed by a non-interruptible, battery-backed vital AC power supply), and (3) the isolation circuit contains a seal-in circuit.

The details of the sneak circuit are discussed in NUREG-4550. In general, the interaction involves a contact race during bus re-energizing that could result in a spurious isolation signal.

Applicability to SONGS 2/3

The only system at SONGS 2/3 where a steam leak detection circuit is potentially applicable is the AFW system. However, this system does not have a leak detection circuit that could cause an inadvertent isolation of the steam supply.

3. Bus Switching Logic Problems

Description

Brookhaven National Laboratory (BNL) recently discovered a problem in the bus switching logic at a PWR. There are at least two subtle aspects to this interaction: (1) a safety-related DC power supply is also being used to perform a bus switching operation in the switchyard and safety-related loads are normally powered from the unit transformer rather than from offsite power; and (2) a safety-related AC bus does not have a diesel directly powering it; it must relay on diesel power from another bus via a breaker which only closes given a LOP.

Applicability to SONGS 2/3

The design of the SONGS 2/3 switchyard is provided with a dedicated DC power supply and therefore, does not rely on plant DC supplies for switching operations.

The safety related buses at SONGS 2/3 are powered by an offsite supply independent of the main transformer with a fast transfer to an alternate offsite supply source if the primary supply is unavailable. Therefore, fast transfer following a plant trip is not normally required to maintain offsite power supply to the safety related buses.

4. Pump Room Cooling

Description

A particular plant design may be such that, given a loss of room cooling, the maximum room temperature remains below the temperature for which a pump and its control circuits are qualified. An analyst may, therefore, conclude that room cooling for this pump is not required. However, upon further investigation, it is found that a room cooler isolation control circuit exists which trips the pump at 200°F; this temperature is reached within 20 minutes following loss of room cooling. Therefore, room cooling is actually required for this pump.

SNL has found room cooler test procedures to be inadequate at two different plants. In both cases it was found that a portion of the actuation circuit was never verified to be functioning properly. These cases are briefly described below:

1. At one plant, it was determined that cooling of the ESF switchgear room was required. The cooling system was safety-grade and was tested monthly. The cooling system was actuated by a wall-mounted thermostat. However, the monthly test required the cooler to be started via a switch which bypassed the thermostat portion of the actuation circuit. The plant has since changed the test procedure so that the availability of the thermostat is verified monthly. The plant now uses a hot air blower to actuate the thermostat.
2. At another plant it was determined that cooling of the Residual Heat Removal (RHR) pump room is required. The room cooler at this plant is actuated from a slave relay following pump start. The RHR pumps are tested monthly. However, the pump test procedure does not require test personnel to verify that the room cooler is functioning properly.

It is becoming a standard practice in PRAs to assign very low non-recovery probabilities to failure of room cooling. The rationale for this is that all the operators have to do is open the door to the room to allow natural circulation cooling to occur. This may not be a plausible recovery method for certain rooms that have doors whose open and close status is under administrative control or governed by technical specifications. For example, certain Emergency Core Cooling System (ECCS) pumps are enclosed behind

water-tight flood doors that are only allowed to be in the open position for a short time. This severely hampers recovery efforts following loss of room cooling.

Applicability to SONGS 2/3

A review of the HVAC dependencies for the various plant equipment was included in the system analysis. Many of the ESF pump motors are water cooled and are modeled with a CCW dependency. Instances where room cooling was required are specifically modeled in the system fault trees. This results in a room cooling dependency primarily for the ESF switchgear rooms, CVCS pump rooms, and BAMU pump rooms.

5. Voltage Drop

Description

PRAs typically assume that a LOP occurs instantaneously. There have been several LOPs in the industry in which it took several minutes for the grid to degrade to the point at which offsite power was totally lost. During these several minutes, the grid voltage or frequency "dropped" out of tolerance. This degraded condition may cause fuses to blow following subsequent power surges and breakers to open within plant systems that are normally powered from the grid. At one plant, breakers apparently opened in some of the normally operating service water pumps. These pumps are also used to supply cooling to the diesels. As a worst case, this event can result in a station blackout if all the service water pumps trip off before the total LOP. In this case, the operators recognized the problem and reset the breakers before the total LOP. Because of events like this, many plants have upgraded the circuits that cut off the grid supply to the plant. Some plants have raised the cutoff set point so that grid separation occurs before significant degradation of the grid.

Applicability to SONGS 2/3

This interaction was not incorporated into the SONGS 2/3 study because sufficient data on the magnitude and length of previous voltage drops are not available. It is therefore, not possible to predict the probability of fuse failure and thus incorporate the interaction into the system models. It was noted, however, that the specific configuration of the SONGS 2/3 switchyard and the degraded voltage protection scheme at the safety related 4 kV buses reduce the likelihood of this interaction occurring.

6. Terminal Block Inside Containment

Description

Recent equipment qualification studies indicate that many types of terminal blocks do not perform adequately in a steam environment. (A terminal block is located in an electrical junction box and is used to connect wire ends within a circuit.) Studies indicate that instrument errors can occur in circuits that contain terminal blocks when exposed to a high temperature ($>100^{\circ}\text{C}$) saturated steam environment. There is a concern that ECCS actuation systems which contain terminal blocks in containment will malfunction following a LOCA and not actuate core cooling in time to prevent core damage.

Applicability to SONGS 2/3

In general, terminal blocks are not used in Safety Related Systems inside containment. There are, however, several instances where terminal blocks internal to specific components inside containment exist. Examples of these are Limitorque limit switches and RTDs. In these cases, the environmental qualification for the component specifically included the qualification of the terminal block.

7. Isolation of All Feedwater Flow

Description

Many PWRs have steam generator isolation control systems that are designed to shut off all feedwater to the generator given low secondary pressure. These systems have caused problems at PWRs in the past. For example, at one plant a power bus failure caused the secondary atmospheric dump valve to open. This resulted in the blowdown of all steam generators. The isolation system actuated and cut off all main and auxiliary feedwater flow to the generators. Following this event, some plants made modifications to the steam generator isolation logic so that simultaneous isolation of all steam generators is prohibited. The fix allows isolation of a subset of the steam generators that are below the low-pressure actuation setpoint, but prohibits isolation of all of them if they are all at low pressure. This ensures that some feedwater can be delivered to at least one of the generators given a common cause event occurs that causes all generators to go below the low-pressure isolation setpoint.

Applicability to SONGS 2/3

The MSIS initiates closure of all MFW and AFW flow control valves to the steam generators. However, the MSIS signal will not affect AFW valves if an EFAS signal is present. In addition, an EFAS signal overrides an existing MSIS signal so that proper AFW component function is preserved. The treatment of this initiation signal and its interaction with the AFW valves is specifically modeled in the AFW fault trees.

8. Alternate Core Cooling Systems

Description

Many published PRAs have only given credit for safety grade core cooling systems. This may be unduly conservative. Many plants have several alternate core cooling modes that are not preferred or safety grade but can be used in an emergency as a "last ditch effort." The following list gives examples of these core cooling modes:

- Using service water to supply makeup to the PWR steam generator or the BWR reactors;
- Aligning a diesel fire pump to supply makeup to the PWR steam generator or the BWR reactor;
- Increasing control rod drive injection system flow in BWRs;
- Blowing down the reactor vessel (BWR) or steam generators (PWR) and allowing the condensate pumps to inject; or
- Aligning the boron injection pumps from a large water source.

These types of alternate core cooling systems should be considered in a PRA analysis if the following conditions are met:

- Use of these systems are described in the emergency procedures;
- A flow rate of at least 200 gpm can be delivered to the PWR steam generators or the BWR reactor; and

- The time required to establish flow from these systems is consistent with cooling requirements.

Applicability to SONGS 2/3

The MFW system is used as a secondary heat removal system for events which do not generate an MSIS where the secondary pressure integrity is maintained and events which do not generate a CIAS. Loss of post-LOCA recirculation cooling can be mitigated by RWST refill. Beyond these no alternate methods are proceduralized or credited in the IPE.

9. Steam Binding of the Auxiliary Feedwater Pumps

Description

Steam binding of AFW pumps has been shown to be a problem at PWRs as reported in AEOD/C404, "Steambinding of Auxiliary Feedwater Pumps", July 1984. Several of the instances reported occurred at the PWRs under investigation in the NUREG/CR-4550 studies.

Applicability to SONGS 2/3

Isolation and flow control valves in the SONGS 2/3 AFW system are maintained normally closed. This alignment insures multiple barriers to steam intrusion that could potentially lead to steam binding of pumps.

10. Air Binding of Cooling Water Systems

Description

There have been several incidents involving the failure or partial failure of the cooling water systems because of air binding caused by leaks in a load being cooled. The plant compressed air systems have both compressor cooling and aftercoolers that are supplied with some form of cooling water. If a leak develops in these coolers, the higher pressure air will enter the cooling system and could result in air binding. This is particularly a problem with closed-cooling systems, but could also be a problem with open systems. This can result in failure of multi-train systems, depending on plant design. Depending on the other loads on the cooling system, this potential common cause failure of the air system and the entire cooling system can be important as a failure or an initiating event.

Applicability to SONGS 2/3

Given the history of this event at SONGS 2/3 for the standby CCW pumps, SCE has implemented procedure and design changes to prevent reoccurrence of such an event.

11. Steam Line Break Isolation CircuitryDescription

There have been several cases of problems involving isolation of steam-driven systems in BWRs. These systems usually have isolation circuitry to protect against steam-line breaks. This circuitry uses temperature readings as an indication of a line break. These temperature readings may include all locations where the steam pipe is routed. Therefore, when assessing the need for room cooling, the cooling requirements of equipment in all areas where isolation temperature readings are taken must be considered. This can be overlooked by just assuming a need for cooling of the room where the pump is located. This problem is further complicated because some plants have the cooling to these other areas as non-essential loads. It should also be noted that this type of event is not limited to BWRs.

Applicability to SONGS 2/3

The only steam driven components are the AFW and MFW turbine-driven pumps. The steam supply valves do not have an automatic line break detection logic which could cause their spurious closure. The valves supplying the AFW steam-driven pump (HV-8200, 8201) automatically close upon receipt of an MSIS signal. Steam supply to the MFW pumps is isolated upon closure of the MSIVs on an MSIS. However, the EFAS signal defeats the MSIS close function and opens the steam valves.

12. Passive Component FailuresDescription

The internal event core-damage frequency in one PWR PRA is dominated by the failure of a manual butterfly valve in the discharge of the nuclear service water system. This valve is in a common line that nearly all of the service water loads discharge to before returning to the lake. Failure of this valve in a manner that blocks flow prevents cooling of most safety loads. In addition, this scenario is difficult to diagnose and even more difficult to recover from. Although passive failures (e.g., stem/disc separation) of valves are rare; these events need to be

considered at pinch points, particularly in common support systems. It is also interesting to note that the plant has experienced this failure mode in a service water valve of the same design and size as the common valve. The valve that did fail is further upstream and only blocked flow from one RHR heat exchanger.

Applicability to SONGS 2/3

Areas where a credible single passive failure results in failure of multiple systems were identified during the individual system analyses and included in the associated fault tree(s) as required. This includes plugging of valves in the Saltwater Cooling System and valves failing to remain open.

13. Isolation of Non-Essential Cooling Water Loads

Description

Sometimes the failure to isolate the non-essential headers of an important cooling water system can result in inadequate cooling of the essential loads because of the potential for pump runout and failure. This means that care should be taken when determining the impact of potential diversion paths from support cooling systems.

Applicability to SONGS 2/3

Flow paths which require isolation in order to assure proper system functioning were considered a flow diversion path and were specifically modeled in the system fault tree(s).

14. Discharge Check Valve Failures for Cross-Tied Pumps

Description

There have been many occurrences of system failure caused by failure (stuck open) of the discharge check valve in one train of a two-train, cross-tied system. Thus, when one pump is turned on with the other pump idle, the flow simply recirculates backward through the idle pump and results in functional failure of the system. The same failure mode occurs if one pump operates and the other fails while its discharge valve is stuck open. Thus, even if the backflow itself is not sufficient to constitute failure of the system, a stuck-open check valve can be important if the normally operating pump fails and the idle pump cannot be actuated, or if the attempted actuation of the idle pump results in system rupture. Sometimes, the check valves in both trains

have been found stuck open at the same time. This failure mode is not normally included in system fault trees, but this review suggests that perhaps it should be.

The importance of this event is determined by the failure probability of the check valve. This failure probability is partially determined by the procedure involving the pump tests. If the pump discharge valve on the idle pump is closed or the trains are isolated during test, the check valve may receive a plant lifetime of demands with no verification that the valve reseats to a closed position preventing backflow. On the other hand, other indications such as loss of water from a water leg fill system could lead to a continuous status check, depending on system configuration.

Applicability to SONGS 2/3

Check valve failure to prevent back-flow and pump-to-pump flow diversion was specifically modeled in the system fault trees in instances where it represented a potential flow diversion path.

15. System Failure Following Station Blackout

Description

In a review of eight PRAs relative to the SBO issue, there is a vast difference in treatment of the failure modes of reactor coolant pump seals following loss of seal cooling (often the result of a total LOP), and in the treatment of battery depletion. These differences introduce a significant degree of uncertainty into the PRA, since they are all based on analyst assumptions and with little or no data.

Applicability to SONGS 2/3

The SONGS 2/3 Station Blackout models include the assessments of RCP seal integrity and battery capacity as a function of blackout duration.

16. Dependent Events Based on Operating Experience

Description

There have been a number of recent activities to better scope out the problem of dependent and common cause events. Probably the best current collection of actual events that are in the nuclear data base are compiled in EPRI NP-3967 (Reference 3.3-16). While there is considerable controversy on how to account for common

cause events, the report clearly demonstrates the inaccuracy of models that do not specifically treat common cause events. While it has been a frequent criticism that quantification of these events leads to numbers but no indication of how to improve plants, a review of the events in EPRI NP-3967 will demonstrate that causes are known for a large percentage of these events.

Applicability to SONGS 2/3

Common cause events were considered in the SONGS 2/3 IPE. The common cause factors were taken from industry references and NUREG-4550. The REBECA computer package used in the IPE substitutes common cause basic events in a post-processor module.

17. Main Feedwater Following Plant Trip

Description

Many PRAs have demonstrated that the availability of MFW after a plant trip is highly plant-specific and that it is, therefore, not correct to make assumptions about MFW availability. For many plants, MFW is not available at all following a reactor trip.

Applicability to SONGS 2/3

MFW is credited for secondary side heat removal for events that do not result in an MSIS or CIAS and where secondary side pressure integrity is maintained.

18. Refill of Dry Steam Generators

Description

Different PWR operators appear to have different concerns relative to refill of a dry steam generator. At some plants it is administratively precluded, but operators say they would use the option; at others, operators say they would not use the option. Another issue is whether the admission of water can lead to damage that makes the sequence more serious (i.e., many broken tubes leading to LOCA and containment bypass).

Applicability to SONGS 2/3

Refill of hot, dry steam generators is assumed successful for the SONGS 2/3 IPE based on design features of the steam generators and the EOIs.

19. Main/Auxiliary Feedwater Commonalities

Description

A PWR PRA identified a number of areas in which failure modes for the MFW system can also affect the emergency (or auxiliary) feedwater system. Although newer plants are likely to have virtually total separation between the two systems, other plants may also exhibit similar problems.

In this case, the Emergency Feedwater (EFW) pumps draw suction from the upper surge tank. When this tank becomes depleted, the operators are instructed to switch suction over to the main condenser hotwell. (As a side note, the two motor-driven EFW pumps can draw only a limited amount of water from the hotwell following the switchover, because of the location of their suction pipe; and then, only if the condenser vacuum is broken. For cooling beyond about two hours, the plant must rely on the turbine-driven EFW pump alone.) The primary purpose of the upper surge tank is to accommodate fluctuations in the condensate inventory during power operation. This leads to several potential problems. For example, if there is a large leak or rupture in the MFW or condensate lines, the operators must take quick action to isolate the break before the upper surge tank inventory is depleted by draining to the condenser as inventory is lost. This can happen in as little as four to five minutes in the case of a large feedwater line break. A more frequent occurrence is the loss of instrument air, which causes loss of main feedwater. It also causes the makeup valve from the upper surge tank to the condenser hotwell to fail open, rapidly draining the upper surge tank. If the loss of air is a consequence of a LOP (the air compressors are all load-shed), the situation is somewhat worse, since the valve the operators must open to supply suction to the turbine-driven pump from the hotwell is motor-operated, and its power supply is also load-shed.

Applicability to SONGS 2/3

The AFW suction supply has no commonalities with the MFW system. The limited interconnection between the AFW and MFW discharge piping is treated in the fault tree as a potential flow diversion path.

20. PORV Block Valve Closure

Description

Many PWRs have trouble with leakage from Power Operated Relief Valves (PORVs) and, as a matter of practice, have a large PORV unavailability because of block valve closure (there are some cases where the valves are closed more than 80% of the time). In many PRAs, it has been assumed that the technical specifications prohibit this, but this is often not the case. The PORV unavailability can lead to a different characterization of plant sequences since a transient-induced LOCA is more likely if the safety valves must lift because the PORVs are unavailable. This topic is also critical to the anticipated transient without scram sequences and the success of feed and bleed.

Applicability to SONGS 2/3

The SONGS 2/3 plants do not have PORVs. Pressurizer safety valves are used to maintain primary pressures within limits. Failure of the safety valve to reclose after an opening demand is specifically modeled in the fault tree.

21. Overfill of Steam Generators

Description

PRAs have been somewhat inconsistent in their treatment of steam generator overfill leading to failure of a turbine-driven feedwater pump. Water carry-over through the steam lines to the turbine can lead to a sequence involving successful initial response followed by a later loss of the turbine-driven feedwater pump.

Applicability to SONGS 2/3

The affects of steam generator overfill are treated explicitly in the steam generator tube rupture event tree. A separate analysis of the steam generator overfill is included in the IPE.

22. Normal Operating Configuration

Description

Various plant-specific PRAs have shown that the normal operating configuration of systems cannot always be inferred from plant P&IDs. For example, the P&ID shows valves as normally closed when, in reality, the plant operates with these valves open. As

another example, the P&ID indicates that a room containing three high-pressure injection pumps has two room coolers, each receiving power and cooling water from a different division. Discussions with the plant revealed that, during normal operation, only one of the two room coolers is normally operating. Further discussion also revealed that it is not prohibited to power the cooler fan from Division 1 and supply the cooling water to the cooler heat exchanger from Division 2. By correctly modeling the normal operating configuration of this system, several single failures of the three high-pressure injection pumps were identified.

Applicability to SONGS 2/3

The normal operating configuration of the SONGS 2/3 plant systems was used in the analysis. This configuration was established based on reviews of the normal operating procedures and discussions with plant operations personnel.

23. Locked Door Dependencies

Description

During a station blackout, the security system at some plants locks the powered security restrictive and key-locked doors, that is, they do not fail open, thereby, potentially restricting accident response actions. The plant configuration is not always obvious during special types of accidents such as a station blackout.

Applicability to SONGS 2/3

The consequences of loss of power to plant security devices and its impact on equipment access is addressed in the existing SONGS 2/3 SBO procedures. Discussions with plant personnel determined that loss of power to key-locked doors and other powered security restrictive measures did not compromise operator access to equipment.

3.3.4.3 Common Cause Dependencies

A common cause event is defined as an event leading to the failure or unavailable state of more than one component at the same time and due to the same shared cause. Common cause events require the existence of some cause-effect relationship that links the failures of a set of components to a single shared root cause. This is commonly a result of shared attributes such as component type, location, component function, manufacturer, internal design

envelope, external design envelope, operational states and modes, testing and maintenance practices.

The initial logic model includes basic events that are considered independent. Dependencies among component failures related to human interaction, environment, spatial relationship are generally not accounted for explicitly in the logic model, although the basic events are not, in fact, independent. The common cause dependency between components is accomplished by substitution of component failures with a common cause basic event which includes the failure contribution of a second or higher order component failing given one or more failures has already occurred. These events represent the class of residual dependent failures whose root causes are not explicitly modeled.

The greatest sources of uncertainty in common cause analysis lie in the areas of data collection and interpretation. Due to the rarity of common cause events and the limited experience of individual utilities, the amount of plant-specific data for common cause analysis is very limited. To identify the potential for common cause failure of key components, components identified for plant-specific evaluation were screened to identify the occurrence of similar failure modes between components within a mean time between tests. Based on this screening, no components were identified for plant-specific common cause evaluation. Therefore, data from generic sources was used to make statistical inferences about the frequencies of the common cause events.

The intercomponent dependent analysis used is based on the information contained in NRC report NUREG/CR-4780 [8-2] documented in NUREG-4550, Volume 1. The Beta Factor method was used to estimate the common cause contributions to system unavailability. The beta factor model is a single parameter model; that is, it uses one parameter in addition to the total component failure probability to calculate the common cause failure probabilities.

Table 3.3-10 provides a summary of the common cause failures considered and the associated Beta factors used.

Table 3.3-10

COMMON CAUSE BETA FACTORS

Common Cause Failure	Beta Factor (2/3/4 Failures)
Diesel Generators Fail to Start	.038/.018/.013
Battery Fails to Operate	.004
LPSI Pumps Fail to Start	.15
HPSI Pumps Fail to Start	.21/.10
CVCS Pumps Fail to Start	.056
Containment Spray Pumps Fail to Start	.11
SWC/CCW Pumps Fail to Start	.026/.014/.0096
CVCS/LPSI/HPSI MOVs Fail to Open	.088/.057/.054
APW Motor-Driven Pumps Fail to Start	.056
APW MOVs Fail to Open	.088/.057
ADVs Fail to Open	.10
Emergency Chillers Fail to Start	.056
Pressurizer Safety Valves Fail to Open	.07
Air Operated Valves Fail to Open/Close	.10
MOVs Fail to Open/Close	.088/.057/.054
Main Steam Isolation Valves	.088

3.3.5 Quantification of Unavailability of Systems and Functions

System failure frequencies are quantified using the ERIN Engineering REBECA software package. REBECA is a self-contained, safety related reliability and risk analysis software program which supports fault tree construction and analysis, as well as event tree construction and analysis.

The SONGS 2/3 includes a number of systems and features that are designed to respond to an abnormal plant condition or initiating event by automatically shutting down the plant and initiating appropriate system operation. There are several critical safety functions including reactivity control, pressure control, temperature control, and inventory control. For each critical safety function, there are several systems which can function to adequately provide the requisite response.

The event trees described in Section 3.1.2.4, 3.1.2.5, 3.1.2.6 and 3.1.2.7 depict the functions required for each initiating event analyzed. Front-line systems are those systems required to perform the primary function for each event tree node. Each such front-line system relies upon a set of "support systems" which provide power, cooling, or other support functions.

The approach for modeling fault trees includes both front-line system fault trees and separate support system fault trees. The dependency of front-line systems on support systems is incorporated by logic links. This method has greater clarity of model depiction and allows easier review and future use. By developing models in this way it is possible to see the importance of each support system directly.

The fault tree models are constructed to account for explicit equipment and their dependencies, operator actions, common cause events, and mutually exclusive events. The system fault trees basically consist of all the active components that are required to successfully perform the required function. Added to these are the support systems dependencies necessary to support the active function.

In addition to active components, passive components such as manual valves (or manual switches) are included in the fault tree models. These are included when it is considered possible that the component could be mispositioned following maintenance or testing, thus disabling the function. This is evaluated as part of the HRA which not only evaluates test and maintenance actions, but also operator actions in response to initiating events. Human reliability is known to be a significant factor influencing overall system performance and reliability, and, therefore, significant effort is necessary to account for operator and test and maintenance actions.

As part of the fault tree development, there are times when the system operation is other than the "normal." For example, the running pumps in the service water system are alternated. To account for these system operation differences, special events (diamond) are inserted into the fault trees to include risk contributions due to these off-normal periods. Also, diamond events are used when data is unavailable or when further definition of the model is inconsequential.

The effects of dependent and multiple failures are also incorporated into the analysis. The REBECA computer code includes a post-processor module that does this analysis for intercomponent dependencies (common cause) rather than explicit modeling in the

system/event trees. The module includes the ability to specify sets of common components that may be susceptible to common cause failure and to interrogate all cutsets to identify common component failure sets. The common cause failure probabilities are then substituted for the random failure probabilities. Components considered susceptible to common cause failures are identified in the common cause beta factor table in Section 3.3.4.

Another part of the REBECA post-processor module eliminates mutually exclusive events. Mutually exclusive events are basic events which, for operational or other reasons, cannot occur in the same failure set (cutset). In most instances, mutually exclusive events involve maintenance of components which, by technical specification or maintenance practices, cannot be out of service at the same time. Failure to eliminate mutually exclusive events introduces system failures which are not realistic. The mutually exclusive database includes a list of combinations of events by basic event name that cannot occur simultaneously. The REBECA post-processor then removes pairwise mutually exclusive events in the cutset results.

3.3.6 Generation of Support System States and Quantification of Their Probabilities

The SONGS 2/3 IPE Level I PRA uses the REBECA computer code package. REBECA uses a linked fault tree approach and considers cutset results files in the solution of the Level I event trees. Thus, as explained in greater detail in Section 3.3.7, there are no quantified support system states.

3.3.7 Quantification of System Frequencies

3.3.7.1 Quantification Approach

The system fault tree models are quantified using the REBECA computer code package. The system models are quantified using flag sets with the house event flag settings appropriate to the event or post-trip condition appropriate for the event being analyzed. The frontline systems or logic in the frontline system's fault trees are analyzed to produce cutset files for processing in REBECA's SEQPRO event tree analysis module. System analyses for input into SEQPRO are processed without common cause substitution, as the REBECA POST-PROCESSOR module performs the common cause basic event substitution as part of the SEQPRO post-processing. In this way the common cause analysis is captured in the event tree analysis.

3.3.7.2 SONGS IPE Model Analysis

The initiating event groups presented in Section 3.1.1 were analyzed using event trees, each of which included as many as 11 key functional requirements. The total number of potential sequences associated with combinations of functional failures could total several hundred sequences per event tree. By analyzing only those sequences which contribute directly to the core damage risk associated with each initiating event, this number is reduced to a manageable level.

The event tree analyses are completed using a nominal culling limit of $1.0E-10$. Although there are cutsets with values below this limit, the exclusion of these cutsets, given the overall quantified core damage frequency on the order of $1.0E-5$, does not significantly affect the results. This method of analyses is judged to capture >95 percent of the actual plant risk and is therefore acceptable. The frequency of serious plant damage (i.e., core melt) due to each initiator is determined by adding the frequencies due to each scenario. The overall likelihood of core damage is obtained by adding the total frequency for each initiator.

The SONGS IPE event tree quantification involved two steps:

- 1) Accident sequence cutset generation, and
- 2) Review of results.

Accident Sequence Analysis

Each event tree is analyzed using the REBECA computer code package. The event trees described in Section 3.1.2.4 through 3.1.2.7 have fault tree results files or point estimates defined for each node. The SEQPRO module in REBECA builds sequence files for each sequence by considering the nodes to be merged logically by an "and" logic operator and eliminating those failures that have caused failures in nodes earlier in the event tree time phase. Each accident sequence is processed to find the minimal cutsets in that sequence.

The cutset results are processed in a POSTPROCESSOR that substitutes common cause (CC) basic events and eliminates cutsets containing previously assigned mutually exclusive (MEX) events. The CC substitution uses common cause data files generated by the fault tree analyst based on component similarity of design function, component environment, and other factors. The MEX elimination removes cutsets containing events the analyst has determined cannot occur at the same time. This usually is applied

to events that imply Technical Specification violation such as both pumps of a two train system out of service (maintenance unavailability). However, it is also applied to conditional logic as well, as in the case of the support system initiator basic events imbedded in the fault tree models.

Sequence Cutset Review

The significant sequences are reviewed for consistency with event tree success criteria and assumptions. Special attention is paid to review for expected common cause events. Checks are performed to ensure the dominant cutsets for each sequence are logical and, in fact, minimal. This check serves to validate the structure of the fault tree models and their time-phased analyses in the event trees. The quantified results are discussed in Section 3.3.10.

3.3.8 Internal Flooding Analysis

3.3.8.1 Introduction

NRC GL 88-20 requires, in part, that internal plant flood events be analyzed as part of the IPE process. In GL 88-20 the NRC refers to guidance for the performance of IPE evaluations. NUREG-1335 provides a brief synopsis of the internal flood initiators to be evaluated as part of the IPE. Specifically, NUREG-1335 requires evaluation of:

"Internal flooding initiators such as overfilling of water tanks, hose and pipe ruptures, and pump seal leaks along with their frequencies and resulting damage to important plant equipment, including water intrusion. Include the result of the quantification of the flooding sequences that lead to core damage."

The purpose of this section is to describe the methodology applied in the internal flooding analysis of the IPE for SONGS 2/3. The objective of the internal flood analysis is to quantify the impact that internal flooding has on the risk of core damage for SONGS 2/3. To accomplish this, the internal flooding analysis team identified locations at SONGS 2/3 that are both susceptible to flooding and contain equipment modeled in the IPE. Then, based on flood hazard sources and equipment vulnerability, the potential flooding scenarios were defined and assessed with regard to the impact of each scenario on core damage frequency.

Internal flooding has been carefully considered in the design of SONGS 2/3. The SONGS 2/3 UFSAR (Reference 3.3-17) documents in Section 3.4 and 10.4.5 the flood protection design for the

probable maximum precipitation (pmp) and probable maximum flood (pmf) (external flood sources), as well as flood protection from component failures (outside containment) (internal flood sources). The IPE limits the review to impacts from internal flood sources.

Section 3.3.8.2 presents the methodology used in the SONGS 2/3 IPE internal flood analysis. Section 3.3.8.3 presents the flood zone and scenario descriptions. Section 3.3.8.4 summarizes the walkdown insights gained. Section 3.3.8.5 presents the results and conclusions, with overall insights.

3.3.8.2 SONGS 2/3 Internal Flood Methodology

3.3.8.2.1 Overview

In order for SONGS 2/3 to have a plant risk contribution from internal floods, all of the following conditions must occur:

- Unexpected, uncontrolled release of water or other liquid in the plant;
- Plant trip, transient, or other off-normal condition that could result in a challenge to core integrity; and
- Consequential impact or failure of IPE equipment due to flooding or other causes that degrades the plant's capability to reach a safe shutdown condition following a flooding event.

The IPE internal flood study addressed each of these conditions for all flood scenarios, as well as limited consideration of recovery of necessary plant functions prior to core damage.

All plant areas except containment were included within the scope of the flood analysis. Flooding in containment has been thoroughly analyzed in previous safety studies (e.g., loss of coolant accident analyses) and is, therefore, not included in the IPE flood study.

The scope of the IPE flood analysis includes flood hazards from all plant liquid (primarily water) sources that could affect IPE equipment. Internal flood hazard sources include all installed, fixed liquid systems and temporary (e.g. hose or tubing) liquid systems that are used on a repetitive, routine basis. Potential temporary hose or tubing systems that would be used for one-time maintenance or repair applications are outside the scope of the analysis. Damage associated with internal flood hazards includes

only short-term (less than 24 hour) liquid inundation effects on IPE equipment. Associated hazards such as pipe whip, steam impingement, and water spray are outside the scope of the analysis.

Also, the effects of liquid jets and sprays are only included implicitly to the extent that they are included in historical plant-specific and generic internal flooding data. While the IPE internal flood analysis provides a strong basis for detailed geometric force of impingement studies, these specific scenario analyses are outside the scope of the current IPE work.

3.3.8.2.1.1 Analysis Steps

Analysis of the internal flooding impact on overall plant risk includes the following general steps:

- Preliminary flood scenario development
- Plant walkdown
- Initial flood scenario frequency screening
- Refinement of analysis bases and assumptions
- Final flood scenario frequency screening (if necessary)

The final two steps above were performed iteratively until each scenario was determined to be below the established screening frequency or until the scenario frequency was as low as reasonably achievable using the screening methods of this study.

3.3.8.2.1.1.1 Step 1- Preliminary Flood Scenario Development

In this step, the internal flooding analysis team developed preliminary flood scenario tables for the plant. These tables are used as a basis for flood scenario definition and analysis in subsequent steps.

In this step the information collected during other project tasks and information from SONGS design information was carefully reviewed to support the following subtasks:

- Component - location cross reference development
- Hazard source - location cross reference development

- Mitigating/Isolation features - location cross reference development
- Flood propagation path analysis
- Preliminary flood scenario table documentation

Consideration of IPE equipment cable terminal points (e.g., junction boxes) was included in this analysis to the maximum extent possible using the SONGS 2/3 Electrical Elementary Wiring Diagrams.

3.3.8.2.1.1.2 Step 2 - Plant Walkdown

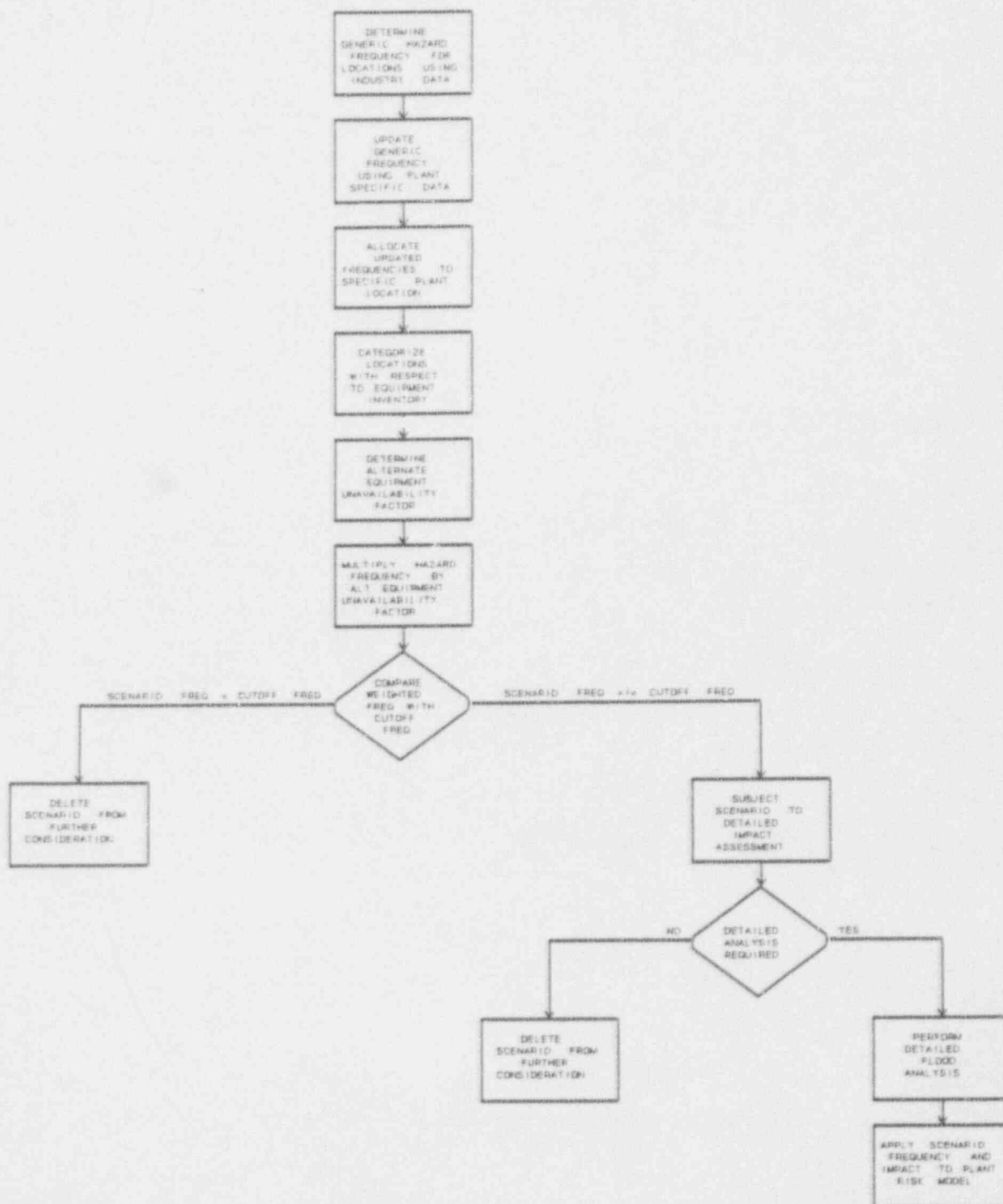
In this step, the internal flooding analysis team physically inspected the plant to refine and verify the preliminary flood scenario tables so that they may be used to accurately define potential flood scenarios in the flood scenario importance screening in Step 3.

3.3.8.2.1.1.3 Step 3 - Initial Flood Scenario Frequency Screening

In this step, the internal flooding analysis team refined the preliminary internal flood scenario tables based on the results of Step 2 and developed quantitative screening criteria for flood scenario risk importance. The team then proceeded to develop and record flood scenario screening frequencies for each flood scenario documented in the internal flood scenario tables. The team then performed two levels of flood scenario importance screening, the first based on maximum conservative scenario impact and the second based on assessed scenario impact. The conceptual flow of a sample screening process is presented in Figure 3.3-5.

In order to screen internal flood scenarios at SONGS 2/3, it was first necessary to estimate an annual frequency of flooding in each flood zone defined in the analysis. The internal flooding analysis team found no significant plant specific flooding data at SONGS 2/3. Therefore, industry data was used to develop flood zone flood initiation screening frequencies in this analysis. This was accomplished by taking the total internal flood frequency for a specific plant building and "spreading" it throughout the flood zones defined within that building. Reference 3.3-18 provides a documented source for annual flood frequencies in nuclear power plant buildings. Reference 3.3-18 compiled industry

Figure 3.3-5
SAMPLE SCREENING PROCESS



data through 1987. The data was compiled for events that could only occur during power operations, shutdown operations and those that could occur in either plant configuration. The Reference 3.3-18 data shown in Table 3.3-11 is the total for power operations and those floods that could occur in either plant configuration.

Table 3.3-11
MAIN CHARACTERISTICS OF TOTAL FLOOD
FREQUENCY DISTRIBUTIONS

System	Flood Size	5th Percentile	Median	95th Percentile	Mean
Auxiliary Building	≥ Small	5.4E-03	2.1E-02	8.0E-02	3.1E-02
	≥ Medium	1.4E-03	8.5E-03	4.9E-02	1.5E-02
	≥ Large	4.5E-04	3.4E-03	2.4E-02	7.5E-03
Turbine Building	≥ Small	1.2E-03	7.8E-03	5.0E-02	1.5E-02
	≥ Medium	1.2E-03	6.2E-03	3.3E-02	1.1E-02
	≥ Large	6.2E-04	3.9E-03	2.1E-02	7.1E-03
Circulating Water	≥ Small	5.0E-04	3.5E-03	2.3E-02	7.2E-03
	≥ Medium	5.0E-04	3.5E-03	2.3E-02	7.2E-03
	≥ Large	3.8E-04	3.2E-03	2.3E-02	6.2E-03
	Extra Large	1.9E-04	1.4E-03	9.6E-03	3.1E-03
Service Water	≥ Small	7.7E-04	6.8E-03	4.9E-02	1.4E-02
	≥ Medium	4.0E-04	3.9E-03	4.5E-02	1.0E-02
	≥ Large	5.2E-04	3.9E-03	2.9E-02	7.9E-03

Using the Level I PRA risk quantification results and the screening criteria set forth in NUREG-1335, the internal flooding analysis team developed cutoff criteria of $1.0E-6/\text{yr}$ for further scenario analysis. The scenario screening was performed in two phases. In the first screening phase, the conservative flood zone screening frequencies and maximum equipment impact were considered. After the first screening phase, a second screening phase was performed. This was done by performing a more realistic assessment of the scenario impact on PRA equipment and scenario frequency. This screening process provides analysis completeness and closure.

3.3.8.2.2.1.4 Step 4 - Refinement of Analysis Bases and Assumptions

In this step the analysis bases and assumptions were refined and documented for each of the flood scenarios that passed through the importance screening process and required detailed quantitative analysis. The internal flooding analysis team carefully reviewed

the remaining scenarios and consulted previous studies and specific references on fluid mechanics and dynamics to properly characterize the bases and assumptions to be used in the quantification process of Step 5. The internal flooding analysis team documented all analysis bases and assumptions for the detailed quantification of important flood scenarios performed in Step 5.

The key bases and assumptions applied in the initial screening analysis are presented as follows:

1. Cable termination points for power, control, or instrumentation cables supporting components modeled in the Level I PRA were considered susceptible to flooding unless their qualification for liquid submergence was documented.
2. During the initial screening of flood scenarios, all Level I PRA components in flood-affected areas were conservatively considered to fail from submergence, liquid jets, or spray.
3. In the screening analysis, all outside control room human actions were conservatively assumed to be failed, and the in-control room human actions for only those flood scenarios that started in or propagated through the control room were assumed to be failed. No cutset recovery factors were considered.
4. The flood scenario core damage frequency used as the limit for additional analysis applied during screening was $1.0E-6/\text{yr}$.
5. Flood scenario initiation frequencies were calculated using historical flood data which included flood events resulting from human error during operation and maintenance as well as pipe break events. Therefore, flood events induced by human error were accounted for in the initial flood frequencies assigned to the flood zones in this analysis.
6. In the screening analysis, liquid propagation in the vertical direction (i.e., to flood zones below the flood initiation zone) was assumed to be infinite in zones containing infinite flood sources (e.g., circulating water). That is, it would drain to the associated building sump and fill all susceptible flood zones below grade until liquid flowed out of the building through doorways

or other openings above grade. In zones containing only finite flood sources liquid propagation in the vertical direction was assumed to fill only the lowest level susceptible flood zones below grade.

7. Liquid propagation in the horizontal direction was assumed to effectively pass through two concentric doors on the same elevation as the flood initiation zone if the flood source was infinite (e.g., circulating water). If the flood source was finite, liquid propagation in the horizontal direction was assumed to effectively pass through one door on the same elevation as the flood initiation zone.
8. Liquid propagating to zones above grade would accumulate to an effective level of one foot above the zone floor elevation.
9. Scenarios involving the failure of any system modeled in the PRA due to loss of liquid inventory above (i.e., no associated failure of that system's flood susceptible equipment) is assumed to be analyzed in the special initiator category of the IPE and is not considered as part of this analysis.

In this task, the analysis bases and assumptions were refined for each of the flood scenarios that passed through the initial screening process (i.e., core damage frequency impact predicted to be greater than $1.0E-6/\text{yr}$) and required a more detailed quantitative screening analysis. The general bases and assumptions revised and applied in the detailed flood scenario analysis are presented as follows:

10. In order to establish a more realistic propagation path for more likely flood scenarios, spread of the flood is limited to those locations reached within 20 minutes.
11. Large floods are floods with rates greater than 10,000 gpm. All other floods are classified as small/medium floods. When appropriate, separate propagations for large and for small/medium floods are considered.
12. The flood drain system in the flood initiation zone will sufficiently accommodate flood liquid drainoff for small/medium floods (<1,000 gpm), so that horizontal flood

propagation outside the flood initiation zone is insignificant in terms of equipment damage.

13. A general flood recovery human error rate of $1.0E-02$ applies to all large floods. This accounts for operator action to stop a large flood during the 0 to 20 minute time frame after flood initiation but before a critical set (minimal cutset) of equipment is failed leading to core damage.
14. The impact in flood propagation zones was selectively revised to account for equipment failure only below calculated or assumed maximum liquid heights. Also, equipment was not failed if its spatial relationship to the source precluded impact.
15. The PRA model human actions were reviewed to take credit for selected human actions that would not be affected by the flood, since all outside control room human actions were initially assumed to be failed by the flood.
16. Additional flood-specific recovery was applied where appropriate.

3.3.8.2.1.1.5 Step 5 - Final Flood Scenario Frequency Screening

Based on the results of steps 3 and 4, the internal flood analysis team performed more detailed analysis on the selected scenarios which exceeded the screening criteria of $1.0E-6/\text{yr}$ and calculated more realistic core damage frequencies.

Based on the results of Steps 3 and 4, the internal flood analysis team performed detailed analysis on selected scenarios and calculated more realistic flood scenario frequencies using the following equation:

$$S_y = B_i (f_{x,i} + F_{x,i}) f_{Gx,j} f_{Sx,j}$$

where: S_y = annual frequency of flooding hazard scenario y ,

B_i = total annual frequency of a flooding hazard of any severity in building i ,

- $f_{x,i}$ = probability of a hazard occurring in an area x associated with scenario y , building i , given that the hazard has occurred in building i ,
- $F_{x,i}$ = probability of a hazard occurring in an area other than area x in building i propagating to area x given that the hazard has occurred in building i ,
- $f_{G,x,j}$ = probability of a hazard occurring at the location j , where equipment associated with scenario y could possibly be affected, given that the hazard has occurred in area x , and
- $f_{S,x,j}$ = probability of a hazard that has occurred at location j is of sufficient severity to cause equipment failure.

This equation was used in quantifying the scenarios, starting from the data sources of the annual frequency of a hazard occurring in a particular building in SONGS 2/3, then considering the fraction of that hazard that may occur in the postulated area and conditional factors such as spatial correlation, the severity of the hazard, and the possibility of propagation to or from another flood zone. In this equation the $f_{G,x,j}$ values are often called geometric factors, and the $f_{S,x,j}$ values are called severity factors. These values were conservatively taken as 1.0 in the screening process in Step 3. In this step, geometric and severity factors were carefully evaluated for all scenarios requiring additional analysis as determined in Step 3. The result of this step is a list of updated frequencies for those flood scenarios significant to plant risk.

Modified flood scenarios were then requantified. Those with core damage frequencies remaining above $1.0E-06/\text{yr}$ were subjected to the steps described in this paragraph until predicted core damage frequency went below $1.0E-6/\text{yr}$ or until all reasonable scenario modification and recovery factors within the scope of the methodology described herein were implemented.

3.3.8.2.3 SONGS 2/3 Flood Susceptibility Overview

3.3.8.2.3.1 Flood Design Aspects

The SONGS 2/3 containment itself is designed to accommodate flooding associated with major components containing water within the containment. Therefore, as previously stated, this flooding zone was excluded from this analysis and is considered treated by the analysis of loss of coolant accident and the associated flooding included in the internal event IPE study.

The major sources of flooding considered in the study included the following:

- Miscellaneous Tanks,
 - Refueling water storage tanks,
 - Primary plant makeup storage tank,
 - Turbine plant cooling water makeup tank,
 - Condensate storage tanks,
 - Radwaste storage tanks,
 - Chemical storage tanks,
- Circulating water pumps,
- Component cooling water surge tanks, pumps, and piping,
- Salt water cooling pumps and piping,
- Screen wash pumps and piping,
- Condenser boxes,
- Condensate pumps and piping,
- Main feedwater pumps and piping,
- Spent fuel storage pool, and
- Charging system piping.

The methodology employed in this analysis included an evaluation of critical areas within the plant to determine their susceptibility to flooding and subsequent effects. A thorough understanding of the plant layout was essential to the evaluation of the flooding scenarios.

SONGS 2/3 is a modern plant design with equipment, tanks, and piping located at multiple elevations. The bulk of the pumps and piping is located, for NPSH reasons, below plant grade level. A review of the flood protection design as described in the SONGS 2/3 UFSAR Section 3.4 indicated that floods originating in pump or tank rooms should be limited to those rooms. This limits the floods that can propagate from one room or hallway to other redundant components. Given this design consideration, the initial flood zones generally corresponded to plant buildings.

There are also tanks located outside the plant structure at grade level. Due to their locations and plant grade considerations, these tanks were judged to be incapable of flooding any buildings through catastrophic tank failure and are screened from further

consideration. Examples in this category are: the turbine plant cooling water and fire water storage tanks.

This initial review indicated that the turbine building itself should be investigated for flood sources (primarily the circulating water system) housed within the turbine building. This zone is of particular concern since a flood propagates to both SONGS 2 and 3 buildings. Thus, resulting in a potential challenge to both plants simultaneously. To facilitate this, an evaluation of the structure has been performed to identify flood zones. The zones that have been selected are described in Section 3.3.8.3.

The design of SONGS 2/3 with regard to post-trip decay heat removal shows a significant dependency on feedwater for secondary heat removal and for decay heat removal. Due to a lack of pressurizer PORVs in the C-E NSSS design, the decay heat removal options, beyond successful feedwater addition, are limited. As such, one of the primary concerns in the flooding evaluation of SONGS 2/3 will be the impact on main feedwater and condensate, and auxiliary feedwater systems. Another concern is maintaining RCS integrity to support decay heat removal using secondary systems. As an initial screening, the following questions were asked:

1. Does the flood cause a plant transient?
2. Is post-trip RCS integrity impacted?
3. Does the flood impact both MFW and AFW or related support systems?
4. Can the flood be mitigated prior to MFW and AFW failure?

The initial investigation of each flooding zone involved an assessment of the degree to which the zone represents a closed area which can contain a flood and impact the MFW and AFW systems or RCS integrity. Any area which cannot be flooded (i.e., retain sufficient water so as to be a hazard) or results in no impact to these systems was screened from further consideration.

Those areas which could be flooded then receive detailed analysis to determine flood sources and equipment affected by postulated floods. This analysis is documented in the following sections.

3.3.8.2.3.2 Flood Procedural Aspects

This section addresses actions that can be taken by an operator in the unlikely event of a flood at SONGS 2/3. Section 3.3.8.5 of this report clearly indicates that the chance of core damage at SONGS 2/3 in all nine flood scenarios is less than 10^{-6} /year, but additional measures are in place that serve to prevent and/or mitigate possible flood damage.

Control room annunciation of sump pump operation may indicate possible flood in particular areas or systems. A number of plant procedures provide explicit direction on the response to flooding indication. Therefore, the SONGS 2/3 operator(s) have an opportunity to diagnose the condition and perform the necessary actions to remedy the situation.

3.3.8.3 Flood Zone Determination and Screening

3.3.8.3.1 Flood Zone Description

Based upon the layout of SONGS 2/3 and considering the flood protection design, a series of flood zones have been selected. These zones are designated in Table 3.3-12.

A brief discussion of the flood scenarios and effects on components located within these flood zones is presented in the following.

Zone 1 - Plant Grade Outside of Plant Structures

There are a number of tanks and fluid systems located in the yard outside of the plant structure. The major flood sources include the fire water tanks (T-102 and T-103), the demineralized water storage tanks (DWSTs), and the turbine plant cooling water (TPCW) pumps and heat exchangers. These tanks are located a sufficient distance from plant structures and the grade area allows sufficient spread of any flood that they were judged not to be a hazard.

Table 3.3-12
SONGS 2/3 FLOOD ZONES

Zone	Area
1	Grade Elevation (El. 30ft)
2	Plant Intake Structure
3	Turbine Building Condenser and Main Feedwater Pump Area (El. 7ft)
4	Control Building (El. 9ft, 30ft, 50ft, & 70 ft)
5	Safety Equipment Building (El. -15ft, -5ft, 9ft)
6	AFW Pump Room and Penetration Doghouse
7	Auxiliary Building (Radwaste Area)
8	Fuel Handling Building
9	Diesel Generator Building

Zone 2 - Intake Structure

This zone includes the circulating water pumps (P-115, 116, 117 and 118), salt water cooling pumps (P-112, 113, 114 and 307), screen wash pumps (P-126 and 127) and associated components. This flood is extensively reviewed in the flood analysis in the SONGS 2/3 UFSAR Section 10.4.5. Given that the pumps in this zone represent an infinite flood source, it can be postulated that failure of one of the lines or the pumps in this area could easily flood this zone. This could generate a plant trip and potentially cause loss of the ultimate heat sink. A flood in this zone propagates into the turbine building 7ft elevation (Flood Zone 3) and saltwater cooling pump piping tunnel. This flood challenges the availability of the power conversion systems (PCS) (e.g. could cause loss of main feedwater). It is possible to achieve safe plant shutdown by using the auxiliary feedwater pumps located in Flood Zone 6 and saltwater cooling could still be maintained by the continued operation or startup of pumps in the unaffected Unit 3 intake structure. Operation of these pumps will provide access to the ultimate heat sink. Alternatively, it is possible to achieve this safe shutdown via use of secondary cooling and primary plant makeup. In this scenario steam generator cooling is achieved by the auxiliary feedwater system with atmospheric dump valve operation to remove heat. Adequate makeup to RCS inventory is available from the charging pumps and RWST to operate in this mode for a sustained period.

For this scenario to result in core damage, the following must occur:

- The Unit 2 intake structure must become flooded due to an accident.
- Saltwater cooling pumps in the Unit 3 intake structure must fail to operate.
- Auxiliary feedwater system or atmospheric dump valve system and main steam safety valves must fail to remove reactor decay heat.
- The charging system must fail to provide RCS makeup.

Using a frequency of service water flood (Reference 3.3-18) of $1.4\text{E-}02/\text{yr}$, an unreliability of $1.9\text{E-}3$ for the saltwater cooling pumps operation in the Unit 3 intake structure, and a non-AC dependent unreliability of $1.5\text{E-}2$ for the auxiliary feedwater and charging systems, this results in a screening value of $4.0\text{E-}7/\text{yr}$. Based on this analysis, this flood scenario is screened from further consideration.

Zone 3 - Turbine Building Condenser and Main Feedwater Area

Zone 3 encompasses the entire turbine building and contains the condensers, the condensate pumps, vacuum pumps, steam jet air ejectors, and associated auxiliaries and the main feedwater pumps. In the event of a postulated flood in this area, it can be envisioned that the condenser vacuum pump could be lost and low condenser vacuum would occur due to either the break itself or the loss of vacuum pump operation. A flood in this zone can also result in loss of the condensate or main feedwater pumps or associated components (i.e. MCCs).

It can be postulated that a flood would occur due to failure of the condenser expansion joints, failure of the condenser structure, loss of seals associated with the piping leading to or from the condenser and/or failure of pumping components associated with feedwater flow or heater drains.

It is postulated that upon flooding, loss of condenser vacuum or feedwater flow would occur directly or indirectly leading to a rapid turbine generator trip and plant trip. The turbine generator trip would result in runback of the feedwater pumps, if still operating. The area encompassed by Zone 3 would require in excess of 2 million gallons to be flooded to a height of two (2) feet to affect components in this zone. Each of four (4) circulating water pumps have an approximate capacity of 207,000 gallons per minute. It is anticipated that trip of the turbine and isolation of the pump would occur in a few seconds, limiting the water level to well below the 9 foot elevation.

Given loss of all equipment in this zone, it is still possible to achieve safe shutdown by using the auxiliary feedwater system to remove heat using the atmospheric dump valves. It is assumed that the turbine building drain systems can handle small floods. It is also assumed that insufficient water would collect, during a medium sized flood, to impact the PCS components. Therefore, using the flood frequency for large size floods from Reference 3.3-18, the flood frequency of $7.1\text{E-}03$ per year and an AFW system reliability of $6.7\text{E-}05/\text{demand}$, the initial screening value for this scenario is estimated at $4.8\text{E-}7/\text{yr}$.

Zone 4 - Control Building Area

This flood zone is essentially the entire control building. The significant components/areas of this building are;

- 1) the normal and essential chiller rooms on elevation 9 ft.
- 2) the relay room on elevation 9 ft.

- 3) the control room and control room cabinet area on elevation 30 ft.
- 4) the essential and non-essential power distribution buses on elevation 50 ft.

The 9 ft. elevation is potentially impacted by a flood in the turbine building. However, the maximum postulated elevation for a flood that originates in the turbine building or intake structure is 9 ft. 1 inch (UFSAR Section 10.4.5). This flood assumes an unmitigated circulating water system flood for twenty (20) minutes. This is consistent with Assumption No. 10 in Section 3.3.8.2.2.1.4. In addition, the turbine building (Zone 3) is the only flood zone that can propagate into the control building. One (1) inch of water in the control building lower elevation will not adversely impact any of the equipment located there or any of the control devices or terminations in the relay cabinets. Therefore, floods originating outside Zone 4 cannot adversely impact any of the equipment located in the control building.

The individual elevations within the control building impact various flood sources. A flood originating in the 9 ft. elevation could involve only fire suppression, CCW, and chiller water lines. A rupture of any of these lines within a room is postulated to disable only the equipment within the room. As noted in Section 3.3.8.3.2, a flood anywhere in the 9 ft. elevation except for the relay room does not impact any of the plant system functions credited for shutdown following a internal flood. The relay room itself does not have a flood source that could disable the relay cabinets and/or the wiring within them. Since a postulated flood does not disable any systems credited for shutdown following a flood, elevation 9 ft. of Flood Zone 4 was screened from further evaluation.

A flood originating at the 30 ft. elevation could adversely impact the control room and/or the control room cabinets. This area of the control building does not have any significant flood sources. However, if a flood were to occur, the probability that operator action would occur to isolate the source prior to any system failure is very high because the control room is continuously manned. Therefore, the 30 ft. elevation of the control building was screened from further evaluation.

The 50 ft. elevation of the control building contains all of the essential AC and DC power distribution equipment. The distribution equipment are located within closed rooms. There are no significant flood sources located within any of the rooms. The only credible flood sources are the normal and emergency chilled water lines and the fire suppression lines that are located in the hallway. A rupture of any one of these lines is expected to result in a flood that deposits water onto the floor. Given the

observed gap under doors at this level, the water will propagate under various doors into the distribution equipment rooms. However, the water will also propagate under the doors into stairways.

For this flood scenario, the flood is expected to result in less than 4 inches of water on the floor of the 50 ft. elevation. This area, if filled to a depth of four (4) inches, represents a volume of 3,778 ft.³ or 28,250 gallons. This depth will not impact the operability of the AC and DC power components at this level. Given the maximum flow rates of 1420 gpm, 640 gpm and 1,000 gpm for the normal and emergency chilled water and fire water sources at this elevation, no impact is expected and this zone was screened from further consideration.

The higher elevations of the control building do not contain any equipment required for plant shutdown following an internal flood. In addition, the propagation path for any flood on those elevations do not result in consequences that have not already been evaluated as part of the evaluation of the lower elevations in this building. Therefore, the 70 ft. and 85 ft. elevations of the control building were also screened out from further evaluation.

Zone 5 - Safety Equipment Building (SEB)

The SEB (Flood Zone 5) generally contains the following ESF equipment:

- High pressure safety injection (HPSI)
- Low pressure safety injection (LPSI)
- Containment spray (CS)
- Component cooling water (CCW)

These systems are primarily required as part of the plant response to the entire spectrum of loss of coolant accidents (LOCAs). The CCW system also supports the normal and emergency chilled water system for ESF switchgear coolers. However, as detailed below, flooding in the SEB does not have a significant impact on plant safety.

Based on the information in the flooding scenario table and the walkdown checklist floods in the SEB are screened out based on the following:

- 1) Limited challenge to AFW/MFW post-trip reliability
 - The emergency chilled water (ECHW) supply may be lost to the ESF switchgear rooms, but if the opposite unit's CCW/SWC is intact, ECHW may be maintained. Additionally, the normal chilled

water supply, cooled by turbine plant cooling water (TPCW), will be available.

- 2) The CCW pumps are located in separate water-tight rooms. Thus, a spill/flood in any one room does not propagate to another and a CCW initiated flood can be mitigated by startup of an inactive loop. Plant response to loss of CCW is modeled as a special initiator. Considering assumption No. 9 of Section 3.3.8.2.2.1.4, loss of CCW is not evaluated in the IPE internal flood analysis.
- 3) If the rupture is the RWST suction line, the flood should be limited to the ECCS pump room in which the break occurs. This event does not challenge plant systems and only requires an orderly shutdown in response.
- 4) Ruptures of the CCW surge tanks are limited to the room and, thus, only affect one CCW train.
- 5) The SEB sumps and level alarms provide the operator with an opportunity to diagnose and respond to the most probable occurrences (i.e., large leaks).

In summary, floods in the SEB require plant shutdown, but do not significantly affect secondary heat removal systems (i.e., AFW or MFW). Floods in the SEB do not result in a transient and, thus, orderly plant shutdown should consequently occur. Based on these considerations, this flood zone was screened from further evaluation.

Zone 6 - AFW Pump Room and Penetration Doghouse

Flood Zone 6 includes the auxiliary feedwater (AFW) pump room and piping tunnels to the AFW containment penetrations and SEB pump rooms.

The AFW pump room contains the three (3) AFW pumps (P-140, 141 and 504), as well as associated flow control valves, and pump related instrumentation. As previously introduced, the AFW system is essential to non-LOCA post-transient response at SONGS 2/3. The principal flood hazard sources are the condensate storage tank (CST) suction line to the AFW pumps, the refueling water storage tank (RWST) suction to the ECCS pumps in the SEB, and fire water headers in the room itself. An additional source in the AFW penetration doghouse is the steam generator blowdown lines from E-088/089. The flood from these sources was screened out for the following reasons:

- 1) The flood of this zone does not cause or require immediate plant trip. Thus, there should be no transient challenge.
- 2) An orderly plant shutdown following this flood can be performed using the main feedwater (MFW) system.
- 3) A flood in this zone does not directly affect or propagate to zones that would affect MFW reliability.
- 4) The most likely floods, leaks or large leaks, will propagate to the piping tunnels to the SEB and containment prior to affecting the AFW components in the room. Thus, except for the assumed potential for loss of one (1) electric AFW pump due to water spray, a degraded AFW system may be available to assist in plant shutdown.

Considering the lack of impact on MFW and the potential for AFW recovery, the estimated core damage frequency is estimated to be significantly less than $1.0E-6/\text{yr}$. Therefore, this flood zone is screened from further evaluation.

Zone 7 - Auxiliary Building (Radwaste Area)

The Radwaste building is located adjacent to the control building. The only system important to safety in this building is the chemical volume and control system (CVCS). Impact to the CVCS can cause plant trip and provides post-trip RCS makeup. However, any CVCS impact would only come from a flood in an individual charging pump room. As stated in the initial basis for this flood analysis, if RCS integrity is maintained, no RCS makeup is required. However, it was reviewed for completeness.

Zone 8 - Fuel Handling Building (FHB)

The FHB is an adjunct to the east side of the radwaste building. The spent fuel pool is not a flood source that can propagate to any other flood zone. As such, a flood in this zone will not affect any critical components. Accordingly, Flood Zone 8 was screened from further consideration.

Zone 9 - Diesel Generator (DG) Building

The DG building contains two lower rooms containing the two emergency diesel generators G-002 and G-003. The upper level of the building contains the engine exhaust, combustion air intake and engine cooling support systems. The only flood sources in each of the lower rooms is a TPSW line and fire suppression lines.

As these lines are of a small bore, and the rooms are equipped with drain systems to a sump outside the building, no flood buildup that could propagate to the other DG room or up to the level of DG components is postulated. Additionally, flood of this zone does not require an immediate plant trip, offsite power should be available, and orderly plant shutdown should occur. Accordingly, Flood Zone 9 was screened from further consideration.

3.3.8.3.2 Electrical Evaluation

In order to implement the screening basis introduced in Section 3.3.8.2.3, certain AFW/MFW and RCS integrity functions must be ensured for evaluation with regard to each flood zone. Therefore, the SONGS 2/3 internal flooding evaluation included the assessment of electrical power and control function vulnerabilities associated with the AFW/MFW and RCS functions described in Section 3.3.8.2.3.

The review for RCS integrity began with a review of the containment isolation valves listed in Table 6.2-35 of the UFSAR and the list of potential ISLOCA paths from the SONGS 2/3 ISLOCA report (Reference 3.3-19). This list was reviewed to screen out those valves (leakage paths) whose failure would not represent a notable challenge to RCS integrity. The following criteria was used to screen potential RCS leakage paths for this internal flooding evaluation.

1. 0.75 inch or smaller lines
2. Lines where a check valve is available
3. Lines which do not directly connect to the RCS

Leakage paths that satisfied at least one of these criteria were deleted from further evaluation. The only remaining lines after this screening were the letdown and shutdown cooling lines. However, the valves in the shutdown cooling lines are normally closed with power removed during normal power operations. Therefore, it is not possible for flood induced failures to cause the shutdown cooling line valves to spuriously open. Therefore, this line was excluded from further evaluation. The letdown line was evaluated for potential flood induced failures. The other plant system functions that were evaluated for potential flood induced failure were the auxiliary feedwater (AFW), main feedwater (MFW), and main feedwater isolation functions. AFW and MFW are credited for decay heat removal while MFW isolation is required to prevent steam generator overfill.

The analysis assumed that all junction and terminal boxes as well as power distribution equipment were susceptible to flood induced failure unless they were NEMA rated for water spray and/or underwater use, or the specific area where they were located was protected against internal flooding. A piece of equipment is

considered to be protected against floods if the postulated flood does not submerge the component or expose it to direct spray.

The SONGS 2/3 system descriptions were used to identify the applicable electrical drawings while the location codes used on the drawings provided the physical plant locations. A portion of the wiring for all of the system components have terminal end(s) in the control room and/or the relay room.

In summary, this evaluation concluded that no flood of any intermediate cable terminations could cause an unplanned interaction with any IPE safety system. Several flood interactions were noted, but they were dispositioned on the basis of component location and flood location arguments. Therefore, no special consideration of these terminations is necessary in the internal flood analysis.

3.3.8.4 Plant Walkdown Results

As part of the IPE internal flood analysis, a walkdown was performed with the following objectives:

- Verification of postulated flood sources and identification of any additional sources.
- Verification of propagation paths and characterization of their credibility.
- Verification and identification of components that can cause a plant trip and/or challenge the ability to safely shutdown the plant.

The raw data obtained in these walkdowns is provided in Appendix C of Reference 3.3-20. The following is a compilation of the insights gained from the walkdown activity.

Walkdown Insights

The following observations are noted:

- Floods at plant grade, external to the plant structures, do not challenge the plant, either in terms of a transient impact or challenge to systems necessary to achieve safe shutdown.
- A flood in the SONGS 2 plant intake structure does not propagate to the SONGS 3 intake structure and vice versa. Therefore, providing that the affected plant's saltwater cooling pumps in the

unaffected intake structure are operating or operable, a flood in this structure does not significantly challenge plant safety.

- A flood in the turbine building of either unit propagates to the opposite unit's turbine building via a common floor area at the 7 ft. elevation. Thus, a flood in this area results in a trip and consequent challenge to both SONGS 2 and SONGS 3 simultaneously. This is not a specific problem unless the Level 1 model includes modeling of the opposite unit's capability for the shared chilled water system, CCW cross-connect or AC power cross-connect. This was previously stated not to be the case.
- A flood in the turbine building will affect the instrument air system and AC/DC support systems for main feedwater and condensate systems. Thus, non-recoverable loss of PCS was assumed for floods in this area.
- Floods in the control building are limited to small-bore piping associated with the chilled water systems and fire water. A sizeable CCW supply to the chillers was noted at the 9 ft. elevation. However, the loss of chilled water systems do not immediately challenge plant systems and should not result in a need for plant trip.
- The Safety Equipment Building (SEB) contains many systems required for LOCA response. A flood in the lower elevations of this building will result in a technical specification required plant shutdown, but will not significantly challenge plant safety.
- A flood that originates from or impacts the CCW system will be limited to a selected train of components by the flood door design of the SEB. Common cause, non-recoverable loss of CCW function due to flood induced impacts is not postulated.
- All floods originating in the piping penetration area propagate to the lowest level (elevation 9 ft.). The sump pumps (P-285 & 286) are normally aligned for manual starting. Sump level alarms should alert operators of flood conditions in this area.

- A flood in the AFW pump room should propagate into the piping tunnel to the SEB and AFW penetration doghouse prior to impacting AFW components in the room. A barrier was installed in the piping tunnel to prevent the steam from a steam line break in the AFW pump room from propagating to the doghouse or electrical vault areas. This flood would be detected by plant personnel, either directly or by RWST/CST level instrumentation, and controlled shutdown using MPW initiated.
- Floods in the Auxiliary Building (Radwaste area), Fuel Handling Building or Diesel Generator Building do not result in a plant trip or consequent challenge to safety systems. The CVCS components in the Auxiliary Building are protected by watertight flood door design and, thus should not be impacted by floods.

These observations are further detailed in the scenario descriptions presented in Section 3.3.8.3.1.

3.3.8.5 Results/Conclusions

Because of the conservative assumptions used in most aspects of the study and the limited application of recovery and flood isolation probabilities, the results are generally considered to be conservative for all scenarios. These conservatisms include:

- Flood propagation is generally representative of the largest possible flood in its size category. Most floods within a category would have less extensive propagation.
- The effort to apply all applicable recoveries is prohibitive because extensive study of flood impact on each recovery would be required. Therefore, only selected recoveries adequate to reduce the core damage frequency below the screening value have been credited.
- All impacted equipment is assumed to fail in the most unfavorable way. Only selected failure modes were reviewed in detail and determined to be unlikely as a result of flooding.

As summarized in Table 3.3-13 all flood zone/scenarios were screened from further analysis or consideration based on a screening analysis or detailed analysis. The core damage values from this screening study have not been added to the functional

accident sequence core damage frequencies for internal events in the IPE. This decision is based on the following considerations:

- Results are judged to be much more conservative than results for internal events in the IPE.
- The level of detail is sufficient to conclude that the core damage frequency is low and to identify the areas with the highest sensitivity to internal flood events.
- This decision is compatible with the intent of the Severe Accident Policy Statement and the philosophy which has been developed for the Internal Fires IPEEE (Reference 3.3-2).

Table 3.3-13
SONGS 2/3
IPE INTERNAL FLOOD ANALYSIS
SUMMARY RESULTS

Flood Zone	Description	Detailed Analysis	Final Screening
1	Plant Grade-Outside of Structures	N	<1.0E-06
2	Plant Intake Structures	Y	<1.0E-06
3	Turbine Building	Y	<1.0E-06
4	Control Building	N	<1.0E-06
5	Safety Equipment Building (ECCS Components)	N	<1.0E-06
6	APW Pump Room	N	<1.0E-06
7	Auxiliary Building (Radwaste)	N	<1.0E-06
8	Fuel Handling Building	N	<1.0E-06
9	Diesel Generator Building	N	<1.0E-06

3.3.9 Interfacing System LOCA (ISLOCA) Analysis

3.3.2.1 Introduction

The evaluation of public risk at nuclear power plants has generally found the risk to be very low. Part of the reason for the low assessed risk can be attributed to the "defense in depth" philosophy of nuclear power plants. This defense in depth includes multiple barriers to prevent the release of radionuclides

to the environment. Nevertheless, there have been postulated accident scenarios which might compromise the defense in depth by causing all of the following: damage to the fuel, bypass of the RCS boundary, and bypass of the containment boundary. One such accident type is referred to as the interfacing system LOCA (ISLOCA). This type of sequence involves the loss of isolation between the high pressure RCS and a low pressure system that penetrates the containment. This condition could lead to the loss of reactor coolant outside containment and, if it involves low pressure ECCS, simultaneously disable ECCS injection capability. Such an ISLOCA scenario could lead to core damage and have substantially higher consequences than other postulated severe accidents because the containment is also bypassed. This section presents an evaluation of SONGS 2/3 potential susceptibility to ISLOCA related core damage.

As part of the first full scale nuclear power plant probabilistic risk assessment, WASH-1400 (Reference 3.3-22), the possibility of an ISLOCA was identified and the frequency of such an event was quantified. WASH-1400 identified a specific accident sequence associated with a unique PWR system configuration in which two check valves acted as the pressure isolation boundary and whose failure could cause a LOCA outside containment, thereby bypassing the containment function. The WASH-1400 evaluation found a relatively high frequency of an ISLOCA for that particular system and valve configuration, depending on the testing of the interfacing valves. For example, there may be an undetected failure of one of the isolation check valves and an ISLOCA occurs if there is failure of the other check valve, with consequent failure of low pressure piping.

PRAs of nuclear power plants have identified the possibility of ISLOCA related accident sequences that can result in core damage and core melt progression in a rapid fashion and simultaneously cause the bypass of the containment. An ISLOCA accident scenario can be of concern because:

- It bypasses the defense-in-depth function of the containment.
- It minimizes the opportunity for accident management actions to mitigate the accident.
- It minimizes the opportunity for effective emergency plan implementation.
- It results in potentially large radionuclide releases that may impact the surrounding population, that is, may result in higher consequences.

These postulated ISLOCA accident scenarios have been estimated to occur at low frequencies. Nevertheless, there have been precursors or related events that indicate that the frequencies may not be very low for all plants. It is for this reason that NUREG-1335 suggests a review of ISLOCA susceptibility for nuclear power plants as part of the IPE performed in response to GL 88-20.

3.3.9.1.1 Objective

This section presents an evaluation to determine the frequency of ISLOCA occurrence at SONGS 2/3. The investigation of ISLOCA events at SONGS 2/3 is motivated by several factors. These factors include the following:

- The potential for adverse impact on public safety due to inducing a core damage event and bypassing containment;
- personnel safety associated with injury from contact with steam or contaminated water; and
- the effect on plant availability associated with the cleanup and analysis that may be required before a restart can be justified.

3.3.9.1.2 Scope

The scope of SONGS 2/3 ISLOCA evaluation is defined by the following.

Systems

Only the interfaces with the potential for overpressurizing low pressure systems outside containment which are connected directly to the RCS are being investigated in this evaluation. Other issues related to flow diversion during cold shutdown are not within the scope of Generic Letter No. 88-20 and are, therefore, not addressed.

LOCA Type

The assessment of public risk associated with nuclear power plant operations involves a number of possible events. In the past (e.g., WASH-1400), experts have identified that the principal contributors to public risk arise from operation at power and the potential release of radionuclides from the core. Based upon these insights, the SONGS 2/3 ISLOCA assessment is limited to plant operating Modes 1 and 2, consistent with NUREG-1335 "Individual Plant Examination: Submittal Guidance."

Mode of Plant Operation

The investigation of SONGS 2/3 interfacing system LOCA events which can lead to core damage and potentially large radionuclide releases will include power operation events only. Shutdown events are not explicitly evaluated since investigation of shutdown events are not within the scope of GL 88-20. Other bases for not evaluating shutdown ISLOCA events include:

- Events which occur during shutdown provide insights into the possibility of failures that can occur at power. However, there are substantially different system alignments and testing occurring during non-power operation which are not appropriate to consider in the evaluation of SONGS 2/3 ISLOCA events. Therefore, the events considered are those occurring during power operation.
- These events are judged to be negligible contributors to overpressurization core damage events during shutdown.
- There is no comparable PRA evaluation or methodology currently developed to allow the relative investigation of shutdown events.

Line Size

The scope of this analysis is to consider those lines which have the potential to create a substantial hazard for safe shutdown of the plant. Estimates of the blowdown rates for lines in the 1 inch diameter range for water breaks and 2 inch diameter range for steam breaks indicate that such flow rates can be easily coped with by the operator using either ECCS or alternative injection methods. Therefore lines smaller than these diameters are excluded from consideration. This is consistent with previous industry operating experience and PRA practice.

Small diameter interfacing line breaks are not explicitly investigated (e.g., instrument lines, nitrogen lines) because these events would not substantially affect multiple systems outside containment nor cause a substantial additional demand on primary system make up or shutdown capabilities.

External Event Effects

External event effects have not been incorporated in the analysis to calculate the frequency of challenge to the ISLOCA initiating event frequency.

High Temperature

The failure of high pressure interfaces that result in high temperature primary fluid flowing in low pressure/low temperature rated systems outside containment have been observed in some plants. However, the limited data on pipe tests is only related to finite length cylinders with internal pressure loading. No test results are available for effects such as thermal strains in pipes. Therefore, the thermal stresses induced by such events are not considered threats to system rupture and, consequently, ISLOCAs at SONGS 2/3.

3.3.9.2 Evaluation of Potential ISLCCA Pathways

An ISLOCA involves failure of the RCS pressure isolation valves (PIVs) to maintain pressure boundary integrity between high and low pressure piping with consequential pipe rupture in a low pressure system connected to the RCS. This condition causes loss of reactor coolant, can disable ECCS, and creates a radionuclide release pathway bypassing containment.

The evaluation of ISLOCA begins with the identification of potential ISLOCA pathways. The following ISLOCA attributes determine potential ISLOCA pathways:

- the pathway must be connected to the RCS,
- the interfacing system must have a design pressure significantly lower than that of the RCS,
- the lower pressure interfacing system must extend outside containment,
- the interfacing lines should have a diameter of at least 1 inch for water breaks and at least 2 inches for steam breaks (lines with smaller diameters are considered to have a negligible contribution to core damage),
- the high to low pressure interface in the pathway must have less than four normally closed pressure isolation valves upstream of the interface,
- the path could be overpressurized by introduction of primary system pressure due to inadvertent valve opening or valve failures from any cause,
- the path, if so pressurized, could produce a leakage rate of primary system coolant of sufficient magnitude to cause collateral damage to other systems needed for safe shutdown, and

- the overpressurization event must be possible during power operation.

It can be discerned from these ISLOCA attributes that all possible ISLOCA pathways are included in a subset of all pathways penetrating the containment structure. A complete list of SONGS 2/3 containment penetrations is available in Chapter 6.2 of the SONGS 2/3 UFSAR. The penetrations listed in Table 6.2-35 of the UFSAR represent the initial group of pathways considered in the ISLOCA evaluation.

Initially, 94 pathways that act as containment isolation barriers are considered. From these 94 pathways which penetrate containment, potential ISLOCA pathways are selected by comparing characteristics of these pathways to those attributes that satisfy the ISLOCA screening criteria. An explanation of each of these ISLOCA criteria is summarized below.

- Criteria 1: Connected to the RCS - The line must connect directly to the RCS to be a potential ISLOCA pathway. By definition, an ISLOCA involves a loss of RCS inventory outside of containment.
- Criteria 2: Pipes Greater than Minimum Size - ISLOCA pathways of concern in the ISLOCA evaluation are those which present a significant risk of core damage relative to other types of accident scenarios. The magnitude of risk for core damage is a function of the consequences of an event and the frequency the event is expected to occur. The ISLOCA pathway line size provides a measure of the plant's ability to achieve shutdown. Any interfacing lines smaller than 1 inch for water lines or 2 inches for steam lines were screened out of the ISLOCA analysis.
- Criteria 3: Lower Design Pressure than RCS - The interfacing system LOCA pathway must have a design pressure which is lower than that of the RCS. The high/low design pressure interface represents the mechanism for failure of low pressure piping and components which causes loss of RCS inventory outside of containment. High pressure to low pressure interfaces between systems located within the confines of containment (e.g., accumulators) are not considered because a break at the interface will not directly result in discharge of reactor coolant outside containment.
- Criteria 4: Three or Fewer PIVs - The consequences of core damage due to a RCS leak outside containment considering only attributes of the pathway depend

on the number and types of barriers between the high/low pressure interface on the high pressure side. As such, the pathway must have three or fewer pressure isolation valves upstream of the high/low pressure interface in order to be considered a potential ISLOCA pathway. A greater number of PIVs would reduce the probability of an ISLOCA below a value which is considered insignificant relative to other sequences from common PRA experience.

Criteria 5: Overpressurization Possible While at Power - The overpressurization event must be possible during power operation. Although events which occur during shutdown prove insightful, there are significantly different system alignments and test procedures which are not appropriate to the evaluation of ISLOCA probability. Operations at power is included in the ISLOCA definition and for the purposes of this evaluation, is considered in all aspects of information gathering.

Each penetration was compared to the screening criteria and only systems which meet all selection criteria are considered potential ISLOCA pathways. If an interface did not satisfy a particular criterion it was removed from any further screening or consideration as an ISLOCA pathway.

3.3.9.3 Description of Potential ISLOCA Pathway

Of the initial 94 pathways all except five (5) were eliminated as potential ISLOCA pathways from the analysis based on the ISLOCA screening criteria. A significant number of pathways were eliminated because they either did not directly connect to the RCS (Criteria 1) or had small diameters (Criteria 2), and; therefore, were considered to have negligible contribution to core damage. The pathways that satisfied all ISLOCA screening criteria were judged to be potential ISLOCA pathways, and were retained to be explicitly evaluated to quantify the ISLOCA frequency at SONGS 2/3. These pathways are:

Table 3.3-14
CANDIDATE ISLOCA PATHWAYS

Penetration 9	Shutdown Cooling Return to LPSI Pumps
Penetration 48	LPSI Path to RCS Loop 1A
Penetration 49	LPSI Path to RCS Loop 1B
Penetration 50	LPSI Path to RCS Loop 2A
Penetration 51	LPSI Path to RCS Loop 2B

All of these penetrations share interface with the LPSI system. In the case of penetrations 48, 49, 50 and 51, the path is from the RCS to the LPSI pump discharge. There are three PIVs prior to the high/low pressure interface. However, the design capacity of the piping between HV-9322, 9325, 9328 and 9331 and the LPSI pumps is 615 psi as compared to a nominal RCS design pressure of 2500 psi. This section of piping is equipped with pressure relief protection (PSV-9318) which may preserve pipe integrity, but will still result in the non-recoverable loss of reactor coolant.

In the case of the shutdown cooling return line via penetration 9, there are only two PIVs and the high/low pressure interface is inside containment. The design pressure of the piping between HV-9337, 9377, and HV-9336 outside of containment is 435 psi. The piping between HV-9337 and HV-9339 has a design pressure of 2485 psi and is equipped with a pressure relief valve PSV-9338. The piping between HV-9377 and HV-9378 also has a design pressure of 2485 psi and a relief valve PSV-9363. These shutdown cooling relief valves are rated for 5 gpm relief and exist to relieve any pressure build-up that may accumulate due to leak of the upstream valves (2HV-9339 and 9378).

Figures 3.3-6 and 3.3-7 illustrate the valve configuration at the high to low pressure interface for each of the identified potential ISLOCA pathways. The evaluation of SONGS 2/3 ISLOCA initiator frequency is based on the valve configuration for a single line in each of the potential ISLOCA pathways given in Figures 3.3-6 and 3.3-7.

The following provides information regarding each identified potential ISLOCA pathway required an ISLOCA evaluation including the function of each system pathway, characteristics of the high to low pressure interfacing valves in each pathway (e.g., PIV test and surveillance requirements, PIV position indications), and the characteristics of the low pressure system.

The potential ISLOCA pathways presented in Figures 3.3-6 and 3.3-7 are part of two systems at SONGS 2/3. These systems are as follows:

- Low Pressure Safety Injection System (LPSI)
- Shutdown Cooling (SDC)

Low Pressure Safety Injection System (LPSI)

The LPSI functions to provide low pressure, high volume, borated water to the RCS in large LOCA events. These discharge flow paths, which are shared with other systems (HPSI and SITs), are provided with redundant check valves in series and motor-operated valves for system and containment isolation reasons. The high/low

Figure 3.3-6 Simplified P&ID: Penetrations 48 thru 51

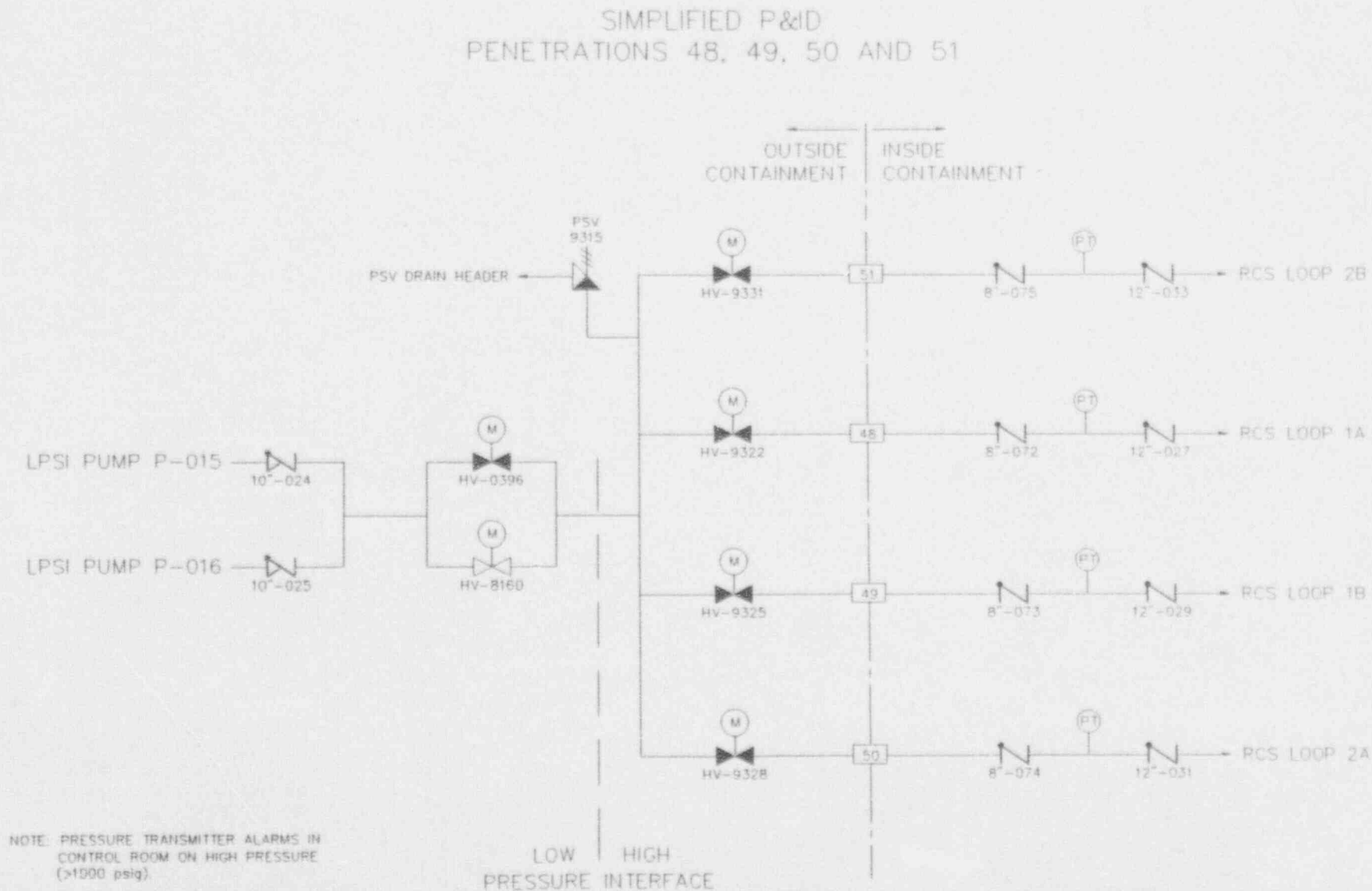
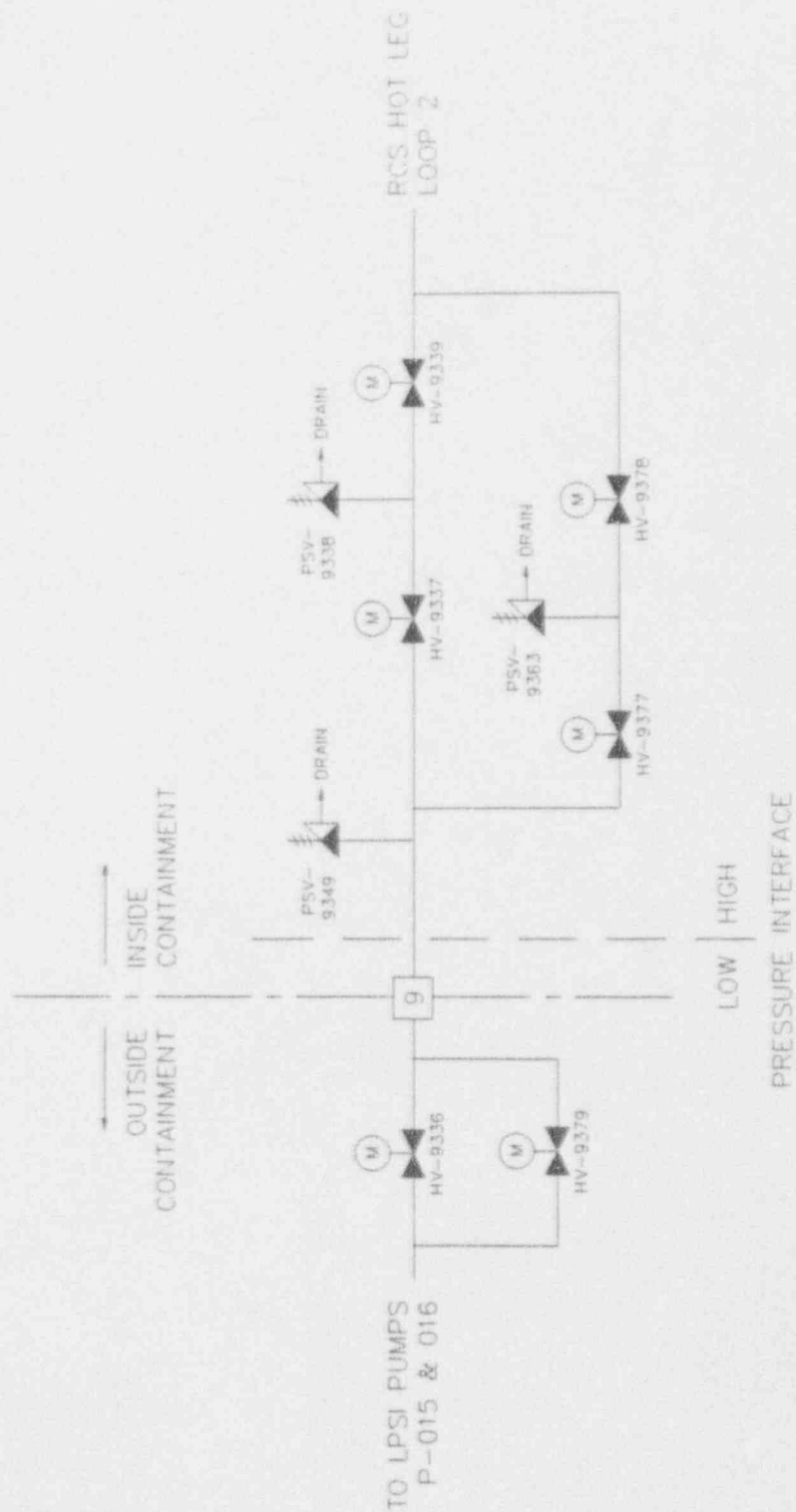


Figure 3.3-7 Simplified P&ID: Penetration 9

SIMPLIFIED P&ID
PENETRATION 9



pressure interface in the LPSI lines is a drop in piping design pressure from 2485 to 615 psi (Reference 3.3-17). However, since there are only three (3) PIVs, the lines are defined as potential ISLOCA pathways.

Shutdown Cooling System (SDC)

The SDC system functions to remove decay heat during periods when the reactor is shutdown. As such, it must interface with the RCS. However, since it is normally operated when RCS pressure is less than or equal to approximately 350 psi (Modes 4, 5 and 6), the SDC has low pressure piping design. The piping upstream of HV-9337, 9339, 9377 and 9378 is designed for 2485 psi (Reference 3.3-17).

3.3.9.4 Analysis of ISLOCA Frequency

NUREG/CR-4550 (Reference 3.3-3) provides, in Volume 2, an expert elicitation on the treatment of ISLOCA in Level I analyses and presents a simplistic method for calculating the ISLOCA frequency. The NUREG/CR-4550 input is presented below.

The ISLOCA issue reviewed in NUREG/CR-4550 involves the quantification of the frequency of an ISLOCA between the high pressure primary system and the low pressure residual heat removal (RHR) system. The primary concern is the reliability of the two check valves placed in series in the RHR discharge path into the primary system. At issue is in what modes and how frequently the check valves could fail to maintain a pressure barrier between the systems.

Three failure scenarios are hypothesized:

1. Random independent rupture (catastrophic leakage) of both valves.
2. Failure of one check valve to reclose upon RCS pressurization followed by random rupture of the other valve.
3. The undetected failure of one valve during operation between test periods followed by the rupture of the other valve. This undetected failure can be caused by opening of the disc, or severe deterioration of the seat. This failure is not detected because the other valve is holding pressure. When the good valve fails, the first valve failure becomes apparent.

The NUREG/CR-4550 compilation of expert elicitation input resulted in the following distribution of ISLOCA frequencies for the two check valve isolation systems considered:

Interfacing Systems LOCA Frequency (yr^{-1}) Per RHR-RCS Pathway

Quartile	Surry	Sequoyah
.05th	1.3E-11	1.2E-11
.50th	1.6E-8	9.5E-9
.95th	1.7E-6	1.2E-6
Mean	3.8E-7	2.7E-7

NUREG/CR-4550 cautions that "...testing intervals, testing procedures, and piping configuration will affect the scenario at any particular plant." As such, prior to using the NUREG/CR-4550 values it is useful to compare the attributes of ISLOCA pathways identified at SONGS 2/3 to that of Surry and Sequoyah.

With regard to piping configuration, NUREG/CR-4550 states:

"The models developed for Sequoyah were slightly different than the models for Surry. The piping configuration at Sequoyah is such that should the low pressure side check valve fail to close after a test or use of the RHR system, the accumulator inventory would drain through it, setting off an alarm. This failure would probably be detected. Thus, the failure-to-close scenario at Surry involves the potential failure to close of either of the two check valves, while at Sequoyah it involves the potential failure to close of only the check valve closest to the high pressure side."

Based on that discussion, SONGS 2/3 is much closer to Sequoyah in that SIT alarms at SONGS 2/3 would alert operators to the same condition. As such, it is most appropriate to use the Sequoyah data for SONGS 2/3. In addition, SONGS 2/3 has an additional feature in the LPSI/HPSI injection header to each RCS cold leg which would indicate the failure of the check valve closest to the RCS. This is a pressure transmitter/indicator which alarms in the control room when the pressure in the header exceeds 1000 psig. Undetected failure of the header check valves closest to the RCS is not probable with proper operation of this pressure detection instrumentation. Therefore, hidden failures of either check valve on the RCS boundary at the HPSI/LPSI header is highly unlikely due to the unique design of SONGS 2/3, and the use of the assumptions and probabilities for failure of these check valves taken from NUREG/CR-4550 is conservative.

With regard to test interval and acceptance criteria, NUREG-0452 (Reference 3.3-23) was reviewed. This NUREG provides the standard technical specifications for Westinghouse pressurized water reactors. Both Surry and Sequoyah are Westinghouse plants. The review of NUREG-0452 against the SONGS 2/3 technical

specifications showed they are identical. Therefore, with regard to test frequency and acceptance criteria, the NUREG/CR-4550 data is considered applicable to SONGS 2/3.

Given the above, the value used in determining ISLOCA pathway frequency is reduced to common cause rupture of two check valves in series. NUREG/CR-4550 addressed this in the following:

"The panel members all considered the fact that no data exist for the first failure scenario (valve rupture), but information from valve specialists from industry and laboratories did suggest to them that the failure mode was possible. Data exist regarding the failure of check valves to reclose, but several experts expressed concern that poor detection of this failure mode places significant uncertainty on any analysis of this data. Several experts also expressed the belief that common cause failure probabilities for check valves are reasonable features to incorporate in the accident models since common cause failures for many other mechanical devices are modeled."

Therefore, it is concluded that it is appropriate to use the NUREG/CR-4550 ISLOCA frequency data in quantifying SONGS 2/3 ISLOCA risk. The NUREG/CR-4550 data considered common cause effects in arriving at the frequency value. Additionally, while the above information indicates that the Sequoyah data is more applicable (and is, in fact, lower), the average of the Surry and Sequoyah mean values will be conservatively used in determining the SONGS 2/3 ISLOCA frequency.

NUREG/CR-4550 cautions that the panel members developed models for a single RHR-RCS interface. The resulting frequency estimates must be multiplied by the number of such systems interfaces to calculate the total plant-specific interfacing systems LOCA frequency.

LPSI ISLOCA Pathways (Penetrations 48, 49, 50 and 51)

In the case of the LPSI pathways there are four lines joining at a common LPSI pump header from P-015 and 016. As illustrated in Figure 3.3-6, the lines each contain two (2) check valves and one motor-operated valve (MOV). The lines to each RCS loop and their respective valves are presented below.

Table 3.3-15
LPSI LINE(S) VALVES

RCS Loop	Check Valves	MOV
1A	12"-027, 8"-072	2HV-9322
2A	12"-031, 8"-074	2HV-9328
1B	12"-029, 8"-073	2HV-9325
2B	12"-033, 8"-075	2HV-9331

The design is such that the check valves closest to the RCS see full RCS operating pressure and the next upstream check valve sees the SIT nominal operating pressure of 625 psia. The SITs are T-007, 008, 009 and 010 for RCS loops 1B, 1A, 2A and 2B, respectively. The SITs are checked for level and pressure on a regular frequency. Therefore, there is significant assurance that the check valves will be properly seated during power operations.

Using the average of the Surry and Sequoyah mean frequencies results in a mean frequency of $3.3\text{E-}7/\text{yr}$ for each of the LPSI ISLOCA pathways. A conservative judgement is made in the case of the LPSI MOVs that they each have a 0.01 probability of misalignment, rupture or other failure. Thus the LPSI ISLOCA frequency is estimated to be $3.3\text{E-}9/\text{yr}$ per pathway or $1.3\text{E-}8$ for all four pathways.

Shutdown Cooling (SDC) ISLOCA Pathways (Penetration 9)

In the case of the SDC pathways there are four (4) MOVs 2HV-9337, 9339, 9377 and 9378 arranged in two trains of two valves each. Thus there are two pathways. During normal power operation, the valves are closed (key switch in closed position and key removed) and power is removed. For valves HV-9337 and HV-9377, the circuit breaker at the starter is also maintained open. During SDC operations, these valves are locked open.

In addition to normal offsite power, four independent emergency power supplies, two from the emergency diesel generators and two from 125 VDC bus inverters, are provided for the isolation valve combination. This arrangement assures that a single failure of an isolation valve or power supply does not preclude availability of the system or preclude positive isolation at the boundary with the RCS. Valves 2HV-9377 and 2HV-9378 are powered from separate DC battery bus inverters.

Since the SDC system is not designed to accommodate full RCS pressure, isolation of the system suction line is assured by interlocks on the four parallel suction line isolation valves inside containment (2HV-9337, 9339, 9377 and 9378). An independent interlock, utilizing pressurizer pressure, is provided for each of the valves. Each interlock is designed to prevent

opening of its associated valve whenever pressurizer pressure is \geq 376 psia. This pressure is the maximum allowable (including margin) SDC initiation pressure which will not result in overpressurization of the LPSI header. An audible alarm sounds in the control room whenever any of the valves is off the full closed position and pressurizer pressure is \geq 383 psia. The interlock also provides automatic closure of the valves when pressurizer pressure \geq 715 psia.

The valves are normally controlled by OPEN/CLOSE key-operated handswitches, with OPEN/CLOSE status lights, at control room panel CR-57. The key is removable in either position. The valves can also be controlled by OPEN/CLOSE spring return-to-center handswitches at evacuation shutdown panel (L-42). Point of control switches (L-42) with LOCAL and CONTROL ROOM position determine controlling location. Valve position inputs to the plant monitoring system and the critical functions monitoring system.

Given all of the independence of power, indication, interlock and alarm, it is judged there is a negligible probability of SDC isolation valve misalignment. Given the failure modes for the check valves discussed in the NUREG/CR-4550 related to random rupture, undetected failure and disk and seat deterioration, it is also judged these results can be applied to the SONGS 2/3 SDC ISLOCA pathways. Therefore the SDC contribution is estimated to be $3.3\text{E-}7/\text{yr}$ per pathway for a total of $6.5\text{E-}7$ for both pathways.

SONGS 2/3 Estimated ISLOCA Frequency

As shown in Table 3.3-16, the SONGS 2/3 ISLOCA initiator frequency is the sum of frequency for each of the identified pathways for a total of $6.6\text{E-}7/\text{yr}$.

Table 3.3-16
ISLOCA FREQUENCY CONTRIBUTORS

ISLOCA Pathway	Contribution to CDF	Aggregate CDF
LPSI Loop 1A	3.3E-9/yr	
LPSI Loop 1B	3.3E-9/yr	
LPSI Loop 2A	3.3E-9/yr	
LPSI Loop 2B	3.3E-9/yr	
Total LPSI Loops		1.3E-8/yr
SDC Loop "A"	3.3E-7/yr	
SDC Loop "B"	3.3E-7/yr	
Total SDC Loops		6.5E-7/yr
Total SONGS 2/3 ISLOCA Frequency		6.6E-7/yr

No mitigation features exist to respond to the ISLOCA path failures analyzed here and, thus the 6.6E-7/yr frequency can be equated to a SONGS 2/3 core damage frequency due to ISLOCA events.

3.3.10 Level I Quantification Results

The primary result of the Level I quantification is the frequency of each individual event tree sequence as comprised of cutsets. The frequency results for the dominant event tree sequences are provided in Table 3.3-17. This table provides a brief description of the event sequence, the functional accident class it is part of, the mean core damage frequency associated with the sequence and the fractional contribution to the total core damage frequency.

Table 3.3-17
DOMINANT SEQUENCES FROM LEVEL I PRA

EVENT TREE	SEQ #	SEQUENCE DESCRIPTION	ACCIDEN. CLASS	CORE DAMAGE FREQ. (/yr)	CONTRIB TO CDF
LOP	11	Loss of Offsite Power Followed By Failure of Secondary Heat Removal and Failure To Recover Offsite Power	IA	5.7E-06	0.194
PCS	5	Loss of Power Conversion System Followed By Failure of Secondary Heat Removal	IA	2.1E-06	0.072
SL	5	Small LOCA Followed By Failure of Cold Leg Recirculation	IIIB	2.0E-06	0.068
ML	5	Medium LOCA Followed By Failure of Cold Leg Recirculation	IIID	2.0E-06	0.068
TT	5	Transient With PCS Initially Available Followed By Failure of Secondary Heat Removal	IA	1.8E-06	0.061
SBO	16	Station Blackout Followed By Failure of the Turbine Driven AFW Pump and Failure To Restore AC Power Within 1 Hour	IC	1.8E-06	0.059
TWS	17	ATWS Followed By Unfavorable MTC Conditions	IV	1.7E-06	0.056
LL	5	Large LOCA Followed By Failure of Cold Leg Recirculation	IIID	1.7E-06	0.056
ML	20	Medium LOCA Followed By Failure of HPSI and Containment Spray In Injection	IIIC	1.4E-06	0.046
LL	11	Large LOCA Followed By Failure of LPSI	IIIC	8.7E-07	0.030
SSL	10	Small-small LOCA Followed By Failure of Secondary Heat Removal	IA	8.2E-07	0.028
SL	22	Small LOCA Followed By Failure of HPSI and Containment Spray In Injection	IIIA	8.1E-07	0.027
VL	3	Interfacing System LOCA	VA	6.6E-07	0.022
PCS	11	Loss of Power Conversion System Followed By Failure of a Pressurizer Safety Valve To Reclose and Failure of HPSI In Recirculation	IIIB	6.4E-07	0.022
ML	3	Medium LOCA Followed By Failure of Hot/Cold Leg Recirculation	IIID	6.1E-07	0.021
SGR	4	Steam Generator Tube Rupture Followed By Failure of HPSI and Charging In Injection (MFW Available)	VB	5.4E-07	0.018
LL	13	Large LOCA Followed By SITs To Inject	IIIC	4.7E-07	0.016
TWS	9	ATWS Followed By Failure of emergency Boration	IV	4.4E-07	0.015
SGR	10	Steam Generator Tube Rupture Followed By Failure of Secondary Heat Removal	VB	4.4E-07	0.015
LL	3	Large LOCA Followed By Failure of Hot/Cold Leg Recirculation	IIID	3.0E-07	0.010
LDC	5	Loss of 125V DC Bus Followed by Failure of Secondary Heat Removal	IA	2.4E-07	8.1E-03
TT	17	Transient With PCS Initially Available Followed by Failure of Pressurizer Safety Valve To Reclose and Failure of HPSI In Recirculation	IIIB	2.3E-07	7.9E-03

Table 3.3-17

DOMINANT SEQUENCES FROM LEVEL I PRA
(continued)

EVENT TREE	SEQ #	SEQUENCE DESCRIPTION	ACCIDENT CLASS	CORE DAMAGE FREQ. (/yr)	CONTRIB TO CDF
SLB	7	Steam Line Break Followed by Failure of Main Steam Isolation (Downstream Break)	IA	2.2E-07	7.6E-03
SBO	5	Station Blackout Followed by Failure To Restore AC Power Within 8 Hours	IC	2.1E-07	7.2E-03
VR	02	Unmitigated Reactor Pressure Vessel Rupture	IIA	2.0E-07	6.8E-03
TWS	13	ATWS Followed by Failure of Pressurizer Safety Valve To Open	IV	1.9E-07	6.4E-03
SSL	4	Small-small LOCA Followed by Failure of HPSI In Injection	IIIA	1.7E-07	5.9E-03
TWS	25	ATWS Followed by Failure of Emergency Boration (Low Power)	IV	1.6E-07	5.6E-03
SGR	20	Steam Generator Tube Rupture Followed by Failure of Operator To Isolate Affected Steam Generator and Failure of AFW	VB	1.5E-07	5.0E-03
CCW	4	Loss of CCW Followed by Failure of the Operator To Trip The RCPs	IIA	1.3E-07	4.3E-03
PCS	29	Loss of Power Conversion System Followed by Failure of a Pressurizer Safety Valve To Reclose and Failure of HPSI and Containment Spray In Injection	IIA	1.1E-07	3.8E-03
SLB	13	Steam Line Break Followed by Failure of Main Steam Isolation (Upstream Break)	IA	9.6E-08	3.3E-03
TWS	15	ATWS Followed by Failure of Turbine To Trip	IV	9.5E-08	3.2E-03
SLB	11	Steam Line Break Followed by Failure of Secondary Heat Removal	IA	8.4E-08	2.8E-03
TWS	29	ATWS Followed by Failure of Pressurizer Safety Valve To Open (Low Power)	IV	7.1E-08	2.4E-03
SL	12	Small LOCA Followed By Failure of Secondary Heat Removal	IA	6.4E-08	2.2E-03
SL	3	Small LOCA Followed By Failure To Control Containment Heat Loads	IIIB	5.9E-08	2.0E-03
ML	9	Medium LOCA Followed By Failure of Containment Heat Removal	IIID	5.1E-08	1.7E-03
SGR	8	Steam Generator Tube Rupture Followed By Failure of HPSI and Charging In Injection (AFW Available)	VB	3.9E-08	1.3E-03
TT	29	Transient With PCS Initially Available Followed By Failure of Pressurizer Safety Valve To Reclose and Failure of HPSI and Containment Spray In Injection	IIA	3.6E-08	1.2E-03
SGR	16	Steam Generator Tube Rupture Followed By Failure of Operator To Depressurize (early or Late)	VB	3.3E-08	1.1E-03

Table 3.3-17

DOMINANT SEQUENCES FROM LEVEL I PRA
(continued)

EVENT TREE	SEQ #	SEQUENCE DESCRIPTION	ACCIDENT CLASS	CORE DAMAGE FREQ. (/yr)	CONTRIB TO CDF
SGR	13	Steam Generator Tube Rupture Followed By Failure of Operator To Depressurize early With Failure of Long-term RCS Makeup	VB	3.0E-08	1.0E-03
TWS	11	ATWS Followed by Failure of AFW	IV	2.3E-08	7.8E-04
PCS	19	Loss of Power Conversion System Followed by Failure of Secondary Heat Removal With A Stuck Open Pressurizer Safety Valve	IA	2.0E-08	6.7E-04
PCS	9	Loss of Power Conversion System Followed by Failure of a Pressurizer Safety Valve To Reclose and Inadequate Containment Heat Management	IIB	1.9E-08	6.4E-04
LDC	23	Loss of 125 VDC Bus Followed by Failure of Automatic Reactor Trip	IIA	1.6E-08	5.5E-04
SBO	8	Station Blackout Followed by Failure To Manually Control AFW Flow and Failure To Restore AC Power Within 5.5 Hours	IC	1.5E-08	5.0E-04
SGR	18	Steam Generator Tube Rupture Followed by Failure of Operator to Isolate Affected Steam Generator and Failure of HPSI in Injection	VB	1.4E-08	4.6E-04
TWS	27	ATWS Followed by Failure of AFW (Low Power)	IV	8.3E-09	2.8E-04
TT	19	Transient With PCS Initially Available Followed by Failure of Secondary Heat Removal (Pressurizer Safety Valve Stuck Open)	IA	7.1E-09	2.4E-04
TT	15	Transient With PCS Initially Available Followed By Failure of Pressurizer Safety Valve To Reclose and Failure To Manage Containment Heat Loads	IIB	6.7E-09	2.3E-04
CCW	8	Loss of CCW Followed By Failure of the RCP High Temperature Alarm System	IIA	6.1E-09	2.1E-04
SL	15	Small LOCA Followed by Failure of HPSI in Injection and Failure of Containment Spray in Recirculation	IIIB	4.6E-09	1.6E-04
LOP	9	Loss of Offsite Power Followed By Failure of A Pressurizer Safety Valve To Reclose and Failure of HPSI in Injection	IIA	3.6E-09	1.2E-04
CCW	10	Loss of CCW Followed by Failure of Automatic Reactor Trip	IIA	2.6E-09	8.7E-05
LDC	29	Loss of 125 VDC Bus Followed by Failure of Pressurizer Safety Valves to Reclose, Failure of HPSI and Containment Spray in Injection	IIA	1.9E-09	6.6E-05
SLB	05	Steam Line Break Followed by Failure to Isolate Both Steam Lines and Failure of Secondary Heat Removal From Intact Steam Generator	IA	1.8E-09	6.1E-05
SBO	11	Station Blackout Followed by Failure to Loadshed Within 30 Minutes and Failure to Restore AC Power Within 8 Hours	IC	1.2E-09	3.9E-05

Table 3.3-17

**DOMINANT SEQUENCES FROM LEVEL I PRA
(continued)**

EVENT TREE	SEQ #	SEQUENCE DESCRIPTION	ACCIDENT CLASS	CORE DAMAGE FREQ. (/yr)	CONTRIB TO CDF
PCS	22	Loss of Power Conversion System Followed by Failure of Pressurizer Safety Valves to Reclose, Failure of HPSI in Injection, and Failure of Containment Spray in Recirculation	IIB	8.5E-10	2.9E-05
LDC	15	Loss of 125 VDC Bus Followed by Failure of Pressurizer Safety Valves to Reclose, Failure of Main Feedwater and Failure of the Operator to Depressurize the RCS	IIB	5.0E-10	1.7E-05
LDC	17	Loss of 125 VDC Bus Followed by Failure of Pressurizer Safety Valves to Reclose, Failure of Main Feedwater, Failure of the Operator to Depressurize the RCS, and Failure of HPSI in Recirculation	IIB	4.5E-10	1.5E-05
ML	07	Medium LOCA Followed by Failure of Containment Heat Removal in Recirculation	IIID	3.4E-10	1.1E-05
LOP	05	Loss of Offsite Power Followed by Failure of a Pressurizer Safety Valve to Reclose and Failure of HPSI in Recirculation	IIB	2.5E-10	8.5E-06
SBO	14	Station Blackout Followed by Failure to Loadshed Within 30 Minutes, Failure to Manually Control AFW Flow, and Failure to Restore AC Power Within 2.5 Hours	IC	2.4E-10	8.1E-06
LL	09	Large LOCA Followed by Failure of Containment Heat Removal in Injection	IIID	2.3E-10	7.7E-06
TT	25	Transient With PCS Initially Available Followed by Failure of Pressurizer Safety Valves to Reclose, Failure of HPSI in Injection, Failure of Main Feedwater, and Failure of Containment Spray in Recirculation	IIB	1.8E-10	6.0E-06
LL	07	Large LOCA Followed by Failure of Containment Heat Removal in Recirculation	IIID	1.7E-10	5.7E-06
TWS	05	ATWS Followed by Failure of Pressurizer Safety Valves to Reclose and Failure of HPSI in Recirculation	IIB	8.9E-11	3.0E-06
LDC	19	Loss of 125 VDC Bus Followed by Failure of Pressurizer Safety Valves to Reclose and Failure of Secondary Heat Removal	IA	4.6E-11	1.6E-06
TWS	07	ATWS Followed by Failure of Pressurizer Safety Valves to Reclose and Failure of HPSI in Injection	IIA	4.2E-11	1.4E-06
TWS	21	ATWS Followed by Failure of Pressurizer Safety Valves to Reclose and Failure of HPSI in Recirculation (Low Power)	IIB	2.1E-11	7.1E-07
TWS	23	ATWS Followed by Failure of Pressure Safety Valves to Reclose and Failure of HPSI in Injection (Low Power)	IIA	1.2E-11	4.0E-07

These same sequences can be regrouped and characterized in terms of functional accident classes described in Section 3.1.2.1. The overall Level I core damage frequency results are characterized in Table 3.3-18 in terms of the core damage frequency and fractional contribution of each functional accident class.

The individual event tree sequences describe the system failures involved in the core damage sequence, but do not identify the specific component contributors to system failures and core damage. In order to understand the results in more detail, it is sometimes useful to review the dominant cutsets from the PRA. Cutsets are the combinations of specific component (or system) failures which lead to core damage. The dominant cutsets for the overall plant model are provided in Table 3.3-19. This table provides the core damage frequency associated with the combination of failures, the basic event values for each failure and the fractional contribution to the total core damage frequency for all cutsets with core damage frequencies greater than $1E-7/\text{yr}$.

3.3.10.1 Importance Measures

The results of the Level I PRA can also be presented in terms of the relative contribution of specific basic events to the core damage frequency. Three mathematical importance measures are presented here: Fussell-Vesely Importance, Risk Reduction Importance, and Risk Increase Importance.

Fussell-Vesely Importance

The primary basic event importance measure developed from the IPE model is the Fussell-Vesely (F-V) basic event importance on a plant level basis. The F-V importance is a ratio of the union of those cutsets containing a specific basic event to the total core damage frequency (CDF). As such, the F-V importance is presented as a fractional value between 0 and 1.0. The plant level F-V basic event importance results are provided in Table 3.3-20. This table presents the F-V importance for basic events with importance values greater than 0.01.

Risk Reduction Importance

The risk reduction importance measure is defined as the core damage frequency reduction which would be observed if the basic event value were reduced to 0.0. The risk reduction importance of a basic event can be obtained by multiplying the basic event F-V importance by the total CDF. Table 3.3-21 provides these results for the same events presented in Table 3.3-20.

Risk Increase Importance

The risk increase importance measure is somewhat the inverse of risk reduction in that it represents the contribution to the increase in CDF if the selected basic event valves were raised to 1.0. This risk measure is not applicable to initiating events per NUREG/CR-4598. The risk increase importance is calculated by the following formula:

$$F_{RiskIncrease} = (FV) \cdot CDF \cdot \left[\frac{1}{BE_{Prob.}} - 1 \right]$$

The formula adds a normalized core damage frequency (the second term) to the remainder of the CDF related to other events. This measure gives insight into those items that the PRA would be sensitive to component unavailability increases. Table 3.3-22 provides the IPE risk increase importance measures for the basic events presented in Tables 3.3-20 and 3.3-21.

Table 3.3-18
FUNCTIONAL ACCIDENT SEQUENCE CONTRIBUTION TO CORE DAMAGE

Functional Accident Class	Definition	CORE DAMAGE FREQ. (1 YR.)	CONTRIB. TO CDF
IA	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Injection Phase	1.2E-05	0.40
IB	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Recirculation Phase	N/A	N/A
IC	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup Due To Station Blackout	2.0E-06	0.067
IIA	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase	5.1E-07	0.017
IIB	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase	9.0E-07	0.030
IIIA	Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase	9.8E-07	0.033
IIIB	Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase	2.1E-06	0.070
IIIC	Accident Sequences Initiated By Medium or Large LOCA With Loss of Primary Coolant Makeup In The Injection Phase	2.7E-06	0.092
IIID	Accident Sequences Initiated By A Medium or Large LOCA With Loss of Primary Coolant Makeup or Adequate Heat Removal In The Recirculation Phase	4.6E-06	0.16
IV	Accident Sequences Involving Failure of Reactivity Control	2.7E-06	0.09
VA	Systems LOCA Outside Containment Leading to Loss of Effective Primary Coolant Inventory Makeup	6.6E-07	0.022
VB	Steam Generator Tube Rupture Leading to Loss of Effective Primary Coolant Inventory Makeup	6.5E-07	0.022

Table 3.3-19

DOMINANT CUTSETS FROM LEVEL I PRA MODEL

FRACTION OF CDF	BASIC EVENT FREQUENCY	IDENTIFIERS	VALUES	BASIC EVENT DESCRIPTIONS
4.808E-02	1.404E-06	FTPE-KMO-TWS FTPE-Z2--TWS INIT-TT--TT K-DOOMECHSCRM NOT--Z1--TWS	1.000E+00 5.000E-02 3.810E+00 1.000E-05 7.370E-01	- MANUAL REACTOR TRIP UNSUCCESSFUL - HIGH MTC CONDITIONS EXIST (UNFAVORABLE) - TRANSIENT WITH PCS INITIALLY AVAILABLE INITIATING EVENT - MECHANICAL FAILURE OF THE RPS TO SCRAM - POWER LEVEL GREATER THAN 20%
1.558E-02	4.551E-07	FTPE-N1--ML H-MPCC0001-S H-Z2017019-K H-Z218T017-K INIT-ML--ML	1.000E+00 4.790E-04 9.500E-01 1.000E+00 1.000E-03	- FAILURE TO DEPRESS RCS AND ALIGN CS FOR RCS INJECTION - COMMON CAUSE FAILURE -MP-S --> 017, 018, AND 019 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - MEDIUM LOCA INITIATING EVENT
1.113E-02	3.250E-07	AEO0H1LOOP2Z FTPE-VLR-VL	3.250E-07 1.000E+00	- INTERFACING SYTEM LOCA VIA SDC HOT LEG LOOP 2 &HV-9337,9339 - NON-RECOVERY FROM ISLOCA
1.113E-02	3.250E-07	AEO0H2LOOP2Z FTPE-VLR-VL	3.250E-07 1.000E+00	- INTERFACING SYTEM LOCA VIA SDC HOT LEG LOOP 2 &HV-9377,9378 - NON-RECOVERY FROM ISLOCA
1.046E-02	3.054E-07	INIT-LOP-LOP L-TP140---M U-DG2G2--8HR U-DG2G3--8HR U-HC3A4A660V U-HC0SPWR60U U-DOGWLOOP-Z	1.070E-01 2.200E-02 7.680E-02 7.680E-02 1.000E+00 1.170E-01 1.880E-01	- LOSS OF OFFSITE POWER INITIATING EVENT - TURBINE-DRIVEN PP 140 DQS FOR MAINTENANCE - DIESEL GENERATOR 2G2 FT RUN - TRAIN A ESF POWER - DIESEL GENERATOR 2G3 FT RUN - TRAIN B ESF POWER - OPER FAILS TO TIE IN BUS 3A04(OR BUS 3A06) W/1 60 MIN (SBO) - NONRECOVERY OF OFFSITE POWER IN 60 MINUTES - LOOP EVENT GRID RELATED LOOP - NO OFFSITE PWR AVAILABL
9.365E-03	2.735E-07	FGHCCNDREC-U FGHCFWREC-U INIT-PCS-PCS L-HCCSTMU--U NOT--T---PCS	6.000E-02 4.300E-01 5.300E-01 2.000E-05 1.000E+00	- NON-RECOVERY OF EMERGENCY CONDENSATE WITHIN 60 MINUTES - NON-RECOVERY OF MAIN FEEDWATER WITHIN 60 MINUTES - LOSS OF POWER CONVERSION SYSTEM INITIATING EVENT - OPERATOR FAILS TO PROVIDE T121 (CST) MAKEUP PER PROCEDURE - SUCCESS OF MAIN STEAM RELIEF
9.041E-03	2.640E-07	H-MVCC0039-P INIT-ML--ML	2.640E-04 1.000E-03	- COMMON CAUSE FAILURE -MV-P --> 9420 AND 9434 - MEDIUM LOCA INITIATING EVENT
8.904E-03	2.600E-07	FTPE-F---SSL INIT-SSL-SSL L-HCCSTMU--U NOT--T---SSL	1.000E+00 1.300E-02 2.000E-05 1.000E+00	- MFW UNAVAILABLE DUE TO CIAS - SMALL-SMALL LOCA INITIATING EVENT - OPERATOR FAILS TO PROVIDE T121 (CST) MAKEUP PER PROCEDURE - SUCCESS OF MAIN STEAM RELIEF
8.589E-03	2.508E-07	H-MVCC0035-P H-Z2017019-K H-Z218T017-K INIT-SL--SL NOT--T---SL	2.640E-04 9.500E-01 1.000E+00 1.000E-03 1.000E+00	- COMMON CAUSE FAILURE -MV-P --> 9302 AND 9305 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - SMALL LOCA INITIATING EVENT - SUCCESS OF MAIN STEAM RELIEF
8.589E-03	2.508E-07	H-MVCC0035-P H-Z2017019-K H-Z218T017-K INIT-ML-ML	2.640E-04 9.500E-01 1.000E+00 1.000E-03	- COMMON CAUSE FAILURE -MV-P --> 9302 AND 9305 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - MEDIUM LOCA INITIATING EVENT
8.589E-03	2.508E-07	H-MVCC0038-P H-Z2017019-K H-Z218T017-K INIT-ML--ML	2.640E-04 9.500E-01 1.000E+00 1.000E-03	- COMMON CAUSE FAILURE -MV-P --> 9304 AND 9305 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - MEDIUM LOCA INITIATING EVENT
8.589E-03	2.508E-07	H-MVCC0038-P H-Z2017019-K H-Z218T017-K INIT-SL--SL NOT--T---SL	2.640E-04 9.500E-01 1.000E+00 1.000E-03 1.000E+00	- COMMON CAUSE FAILURE -MV-P --> 9304 AND 9305 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - SMALL LOCA INITIATING EVENT - SUCCESS OF MAIN STEAM RELIEF

Table 3.3-19

DOMINANT CUTSETS FROM LEVEL 1 PRA MODEL
(continued)

FRACTION OF CDF	BASIC EVENT FREQUENCY	IDENTIFIERS	VALUES	BASIC EVENT DESCRIPTIONS
8.589E-03	2.508E-07	H-MVCC0033-P H-ZZ017019-K H-ZZ18T017-K INIT-SL--SL NOT--T---SL	2.640E-04 9.500E-01 1.000E+00 1.000E-03 1.000E+00	- COMMON CAUSE FAILURE -MV-P --> 9302 AND 9303 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - SMALL LOCA INITIATING EVENT - SUCCESS OF MAIN STEAM RELIEF
8.589E-03	2.508E-07	H-MVCC0033-P H-ZZ017019-K H-ZZ18T017-K INIT-ML--ML	2.640E-04 9.500E-01 1.000E+00 1.000E-03	- COMMON CAUSE FAILURE -MV-P --> 9302 AND 9303 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - MEDIUM LOCA INITIATING EVENT
8.589E-03	2.508E-07	H-MVCC0036-P H-ZZ017019-K H-ZZ18T017-K INIT-SL--SL NOT--T---SL	2.640E-04 9.500E-01 1.000E+00 1.000E-03 1.000E+00	- COMMON CAUSE FAILURE -MV-P --> 9303 AND 9304 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - SMALL LOCA INITIATING EVENT - SUCCESS OF MAIN STEAM RELIEF
8.589E-03	2.508E-07	H-MVCC0036-P H-ZZ017019-K H-ZZ18T017-K INIT-ML--ML	2.640E-04 9.500E-01 1.000E+00 1.000E-03	- COMMON CAUSE FAILURE -MV-P --> 9303 AND 9304 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - MEDIUM LOCA INITIATING EVENT
7.792E-03	2.275E-07	H-MPCC0001-S H-ZZ017019-K H-ZZ18T017-K INIT-LL--LL	4.790E-04 9.500E-01 1.000E+00 5.000E-04	- COMMON CAUSE FAILURE -MP-S --> 017, 018, AND 019 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - LARGE LOCA INITIATING EVENT
7.792E-03	2.275E-07	H-MPCC0001-S H-ZZ017019-K H-ZZ18T017-K INIT-SL--SL NCHCCSINJCTU NOT--T---SL	4.790E-04 9.500E-01 1.000E+00 1.000E-03 5.000E-01 1.000E+00	- COMMON CAUSE FAILURE -MP-S --> 017, 018, AND 019 - HPSI PUMPS 017 AND 019 AVAILABLE - P018 NOT ALIGNED TO TRAIN B - SMALL LOCA INITIATING EVENT - OP FAILS TO DEPRESS RCS AND ALIGN CS FOR INJECTION (SL) - SUCCESS OF MAIN STEAM RELIEF
6.849E-03	2.000E-07	FTPE-X---VR INIT-VL--VR	1.000E+00 2.000E-07	- NON-RECOVERY FROM REACTOR VESSEL RUPTURE - PRESSURE VESSEL RUPTURE INITIATOR
6.688E-03	1.953E-07	FTPE-KMD-TWS FTPE-ZZ--TWS INIT-PCS-PCS K-DOMECHSCRM NOT--Z1--TWS	1.000E+00 5.000E-02 5.300E-01 1.000E-05 7.370E-01	- MANUAL REACTOR TRIP UNSUCCESSFUL - HIGH MTC CONDITIONS EXIST (UNFAVORABLE) - LOSS OF POWER CONVERSION SYSTEM INITIATING EVENT - MECHANICAL FAILURE OF THE RPS TO SCRAM - POWER LEVEL GREATER THAN 20%
6.244E-03	1.823E-07	F-HCDEPRESSU FGHCFWREC-U INIT-PCS-PCS L-HCCSTMU--U NOT--T---PCS	4.000E-02 4.300E-01 5.300E-01 2.000E-05 1.000E+00	- OP FAILS TO DEPRESS SG's W/I 1 HR AND ALIGN CONDENSATE - NON-RECOVERY OF MAIN FEEDWATER WITHIN 60 MINUTES - LOSS OF POWER CONVERSION SYSTEM INITIATING EVENT - OPERATOR FAILS TO PROVIDE T121 (CST) MAKEUP PER PROCEDURE - SUCCESS OF MAIN STEAM RELIEF
4.733E-03	1.382E-07	INIT-LOP-LOP L-TP140---S L-TP140NR--S U-DG2G2--8HR U-DG2G3--8HR U-HC3A4A660V U-HC0SPWR60U U-DOGWLOOP-Z	1.070E-01 2.990E-02 3.330E-01 7.680E-02 7.680E-02 1.000E+00 1.170E-01 1.880E-01	- LOSS OF OFFSITE POWER INITIATING EVENT - TURBINE-DRIVEN PP 140 FT START ON DEMAND - FAILURE OF P140 TO START IS NOT RECOVERABLE - DIESEL GENERATOR 2G2 FT RUN - TRAIN A ESF POWER - DIESEL GENERATOR 2G3 FT RUN - TRAIN B ESF POWER - OPER FAILS TO TIE IN BUS 3A04 (OR BUS 3A06) W/I 60 MIN (SBO) - NONRECOVERY OF OFFSITE POWER IN 60 MINUTES - LOOP EVENT GRID RELATED LOOP - NO OFFSITE PWR AVAILABL

Table 3.3-19

DOMINANT CUTSETS FROM LEVEL 1 PRA MODEL
(continued)

FRACTION OF CDF	BASIC EVENT FREQUENCY	IDENTIFIERS	VALUES	BASIC EVENT DESCRIPTIONS
4.716E-03	1.377E-07	INIT-LOP-LOP	1.070E-01	- LOSS OF OFFSITE POWER INITIATING EVENT
		L-TP140---M	2.200E-02	- TURBINE-DRIVEN PP 140 OOS FOR MAINTENANCE
		M-HCBCBFAILU	5.000E-01	- OPER FT RESPOND TO BATT CHRG B2 FAILURE GIVEN PREV RESP FAIL
		M-HCNOSIAS-U	1.000E-03	- NO OPRT RESPONSE TO HIGH TEMPERATURE ALARM-ESF SWGR/DIST
		NOT--T---LOP	1.000E+00	- SUCCESS OF MAIN STEAM RELIEF
		U-HCOSPWR60U	1.170E-01	- NONRECOVERY OF OFFSITE POWER IN 60 MINUTES
4.702E-03	1.373E-07	INIT-LOP-LOP	1.070E-01	- LOSS OF OFFSITE POWER INITIATING EVENT
		L-HCHV4716PU	1.000E+00	- OPERATOR FAILS TO MANUALLY OPEN HV4716 LOCALLY AFTER FAULT
		L-MV4716---P	9.890E-03	- MTR-OPERATED VLV 4716 FT OPEN ON DEMAND
		U-DG2G2--BHR	7.680E-02	- DIESEL GENERATOR 2G2 FT RUN - TRAIN A ESF POWER
		U-DG2G3--BHR	7.680E-02	- DIESEL GENERATOR 2G3 FT RUN - TRAIN B ESF POWER
		U-HC3A4A660V	1.000E+00	- OPER FAILS TO TIE IN BUS 3A04(OR BUS 3A06) W/1 60 MIN (SBO)
		U-HCOSPWR60U	1.170E-01	- NONRECOVERY OF OFFSITE POWER IN 60 MINUTES
		U-DGWL00P-Z	1.880E-01	- LOOP EVENT GRID RELATED LOOP - NO OFFSITE PWR AVAILABL
4.520E-03	1.320E-07	H-MVCC0039-P	2.640E-04	- COMMON CAUSE FAILURE -MV-P --> 9420 AND 9434
		INIT-LL--LL	5.000E-04	- LARGE LOCA INITIATING EVENT
4.349E-03	1.270E-07	FTPE-W---CCW	1.000E+00	- RCP SEAL FAIL GIVEN LOSS OF CCW TO RUNNING RCP
		FTPE-Z---CCW	5.000E-04	- OPERATOR FAILS TO TRIP RCP GIVEN ANNUNCIATOR SIGNAL
		INIT-CCW-CCW	2.540E-04	- LOSS OF COMPONENT COOLING WATER
		NOT--Y---CCW	1.000E+00	- LOSS OF CCW ANNUNCIATES IN THE CONTROL ROOM
4.294E-03	1.254E-07	H-MVCC0038-P	2.640E-04	- COMMON CAUSE FAILURE -MV-P --> 9304 AND 9305
		H-ZZ017019-K	9.500E-01	- HPSI PUMPS 017 AND 019 AVAILABLE
		H-ZZ18T017-K	1.000E+00	- P018 NOT ALIGNED TO TRAIN B
		INIT-LL--LL	5.000E-04	- LARGE LOCA INITIATING EVENT
4.294E-03	1.254E-07	H-MVCC0036-P	2.640E-04	- COMMON CAUSE FAILURE -MV-P --> 9303 AND 9304
		H-ZZ017019-K	9.500E-01	- HPSI PUMPS 017 AND 019 AVAILABLE
		H-ZZ18T017-K	1.000E+00	- P018 NOT ALIGNED TO TRAIN B
		INIT-LL--LL	5.000E-04	- LARGE LOCA INITIATING EVENT
4.294E-03	1.254E-07	H-MVCC0035-P	2.640E-04	- COMMON CAUSE FAILURE -MV-P --> 9302 AND 9305
		H-ZZ017019-K	9.500E-01	- HPSI PUMPS 017 AND 019 AVAILABLE
		H-ZZ18T017-K	1.000E+00	- P018 NOT ALIGNED TO TRAIN B
		INIT-LL--LL	5.000E-04	- LARGE LOCA INITIATING EVENT
4.294E-03	1.254E-07	H-MVCC0033-P	2.640E-04	- COMMON CAUSE FAILURE -MV-P --> 9302 AND 9303
		H-ZZ017019-K	9.500E-01	- HPSI PUMPS 017 AND 019 AVAILABLE
		H-ZZ18T017-K	1.000E+00	- P018 NOT ALIGNED TO TRAIN B
		INIT-LL--LL	5.000E-04	- LARGE LOCA INITIATING EVENT
4.018E-03	1.173E-07	INIT-LOP-LOP	1.070E-01	- LOSS OF OFFSITE POWER INITIATING EVENT
		L-TP140---M	2.200E-02	- TURBINE-DRIVEN PP 140 OOS FOR MAINTENANCE
		M-HC00001-S	4.260E-04	- COMMON CAUSE FAILURE -CH-S-->E-335,E-336
		NOT--T---LOP	1.000E+00	- SUCCESS OF MAIN STEAM RELIEF
		U-HCOSPWR60U	1.170E-01	- NONRECOVERY OF OFFSITE POWER IN 60 MINUTES
3.774E-03	1.102E-07	INIT-SLB-SLB	5.420E-04	- STEAM LINE BREAK AND FEEDWATER LINE BREAK INITIATING EVENT
		NOT--TDS-SLB	7.000E-01	- STEAM LINE BREAK DOWNSTREAM OF MSIVS
		T-HVCC0001-N	5.810E-04	- COMMON CAUSE FAILURE -HV-N --> 8204 AND 8205
		T-00E-089--Z	5.000E-01	- S/G E-089 AFFECTED BY INITIATING EVENT (FAULTED S/G)
3.774E-03	1.102E-07	INIT-SLB-SLB	5.420E-04	- STEAM LINE BREAK AND FEEDWATER LINE BREAK INITIATING EVENT
		NOT--TDL SLB	7.000E-01	- STEAM LINE BREAK DOWNSTREAM OF MSIVS
		T-HVCC0001-N	5.810E-04	- COMMON CAUSE FAILURE -HV-N --> 8204 AND 8205
		T-00E-088--Z	5.000E-01	- S/G E-088 AFFECTED BY INITIATING EVENT (FAULTED S/G)

Table 3.3-19

DOMINANT CUTSETS FROM LEVEL 1 PRA MODEL
(continued)

<u>FRACTION OF CDF</u>	<u>BASIC EVENT FREQUENCY</u>	<u>IDENTIFIERS</u>	<u>VALUES</u>	<u>BASIC EVENT DESCRIPTIONS</u>
3.758E-03	1.097E-07	INIT-TT--TT	3.810E+00	- TRANSIENT WITH PCS INITIALLY AVAILABLE INITIATING EVENT
		L-HCCSTMU--U	2.000E-05	- OPERATOR FAILS TO PROVIDE T121 (CST) MAKEUP PER PROCEDURE
		NOT--T---TT	1.000E+00	- SUCCESS OF MAIN STEAM RELIEF
		U-HC2Q065--U	1.000E+00	- OPERATOR FAILS TO XFER Q065 TO MCC BX VIA KIRK-KEY INTLK
		U-IRY012-1DR	1.440E-03	- INVERTER Y012 FT OPERATE W/1 24 H

TABLE 3.3-20

FUSSELL-VESELY IMPORTANCE MEASURES FOR TOP BASIC EVENTS

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	FUSSELL-VESELY IMPORTANCE
INIT-LOP-LOP	LOSS OF OFFSITE POWER INITIATING EVENT	0.11	0.27
U-HCOSPWR60U	NONRECOVERY OF OFFSITE POWER IN 60 MINUTES	0.12	0.26
L-TP140----M	TURBINE-DRIVEN PP 140 OOS FOR MAINTENANCE	2.2E-02	0.16
INIT-TT--TT	TRANSIENT WITH PCS INITIALLY AVAILABLE INITIATING EVENT	3.8	0.15
INIT-ML--ML	MEDIUM LOCA INITIATING EVENT	1.0E-03	0.14
U-DOGWLOOP-2	LOOP EVENT GRID RELATED LOOP - NO OFFSITE PWR AVAILABLE	0.19	0.13
INIT-LL--LL	LARGE LOCA INITIATING EVENT	5.0E-04	0.11
INIT-PCS-PCS	LOSS OF POWER CONVERSION SYSTEM INITIATING EVENT	0.53	0.11
INIT-SL--SL	SMALL LOCA INITIATING EVENT	1.0E-03	0.10
K-DOMECHSCRM	MECHANICAL FAILURE OF THE RPS TO SCRAM	1.0E-05	9.0E-02
NOT--Z1--TWS	POWER LEVEL GREATER THAN 20%	0.74	8.2E-02
L-TP140NR--S	FAILURE OF P140 TO START IS NOT RECOVERABLE	0.33	8.0E-02
L-TP140----S	TURBINE-DRIVEN PP 140 FT START ON DEMAND	3.0E-02	8.0E-02
L-HCHV4716PU	OPERATOR FAILS TO MANUALLY OPEN HV4716 LOCALLY AFTER FAULT	1.0	7.9E-02
L-MV4716---P	MTR-OPERATED VLV 4716 FT OPEN ON DEMAND	9.9E-03	7.9E-02
L-MP504--1DR	MTR-DRIVEN PP 504 FT RUN FOR 24 HR - TRAIN B	1.3E-02	6.9E-02
U-DG2G2--BHR	DIESEL GENERATOR 2G2 FT RUN - TRAIN A ESF POWER	7.7E-02	6.6E-02
U-DG2G3--BHR	DIESEL GENERATOR 2G3 FT RUN - TRAIN B ESF POWER	7.7E-02	6.4E-02
L-MP141--1DR	MTR-DRIVEN PP 141 FT RUN FOR 24 HR - TRAIN A	1.3E-02	6.3E-02
U-HC3A4A660V	OPER FAILS TO TIE IN BUS 3A04(OR BUS 3A06) W/I 60 MIN (SBO)	1.0	5.9E-02
FTPE-Z2--TWS	HIGH MTC CONDITIONS EXIST (UNFAVORABLE)	5.0E-02	5.7E-02
FGHCFWREC-U	NON-RECOVERY OF MAIN FEEDWATER WITHIN 60 MINUTES	0.43	5.0E-02
FTPE-N1--ML	FAILURE TO DEPRESS RCS AND ALIGN CS FOR RCS INJECTION	1.0	4.7E-02
L-HCCSTMU--U	OPERATOR FAILS TO PROVIDE T121 (CST) MAKEUP PER PROCEDURE	2.0E-05	4.6E-02
H-MP019--1DR	MTR-DRIVEN PP 019 FT RUN FOR 24 HR	1.4E-02	3.8E-02
INIT-SGR-SGR	STEAM GENERATOR TUBE RUPTURE INITIATING EVENT	1.0E-02	3.8E-02
H-MPCC0001-S	COMMON CAUSE FAILURE -MP-S --> 017, 018, AND 019	4.8E-04	3.7E-02
INIT-SSL-SSL	SMALL-SMALL LOCA INITIATING EVENT	1.3E-02	3.4E-02
H-MP017----M	PUMP 017 UNAVAILABLE DUE TO MAINTENANCE / TEST	5.0E-02	3.2E-02
P-HTE001-1DM	HEAT X (TUBE) E001 OOS FOR MAINT W/I 24 H	6.5E-03	3.2E-02
H-MP019----M	PUMP 019 UNAVAILABLE DUE TO MAINTENANCE / TEST	5.0E-02	3.1E-02

TABLE 3.3-20

**Fussell-Vesely Importance Measures for Top Basic Events
(continued)**

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	FUSSELL-VESELY IMPORTANCE
L-MPCC0001-S	COMMON CAUSE FAILURE -MP-S --> 141 AND 504 (AFW MDPS)	2.7E-04	3.1E-02
FGHCCNDREC-U	NON-RECOVERY OF EMERGENCY CONDENSATE WITHIN 60 MINUTES	6.0E-02	3.1E-02
FTPE-F---SSL	MFW UNAVAILABLE DUE TO CIAS	1.0	2.8E-02
H-MVCC0033-P	COMMON CAUSE FAILURE -MV-P --> 9302 AND 9303	2.6E-04	2.8E-02
H-MVCC0035-P	COMMON CAUSE FAILURE -MV-P --> 9302 AND 9305	2.6E-04	2.8E-02
H-MVCC0036-P	COMMON CAUSE FAILURE -MV-P --> 9303 AND 9304	2.6E-04	2.8E-02
H-MVCC0038-P	COMMON CAUSE FAILURE -MV-P --> 9304 AND 9305	2.6E-04	2.8E-02
Y-DOORV-DEM-Z	POST-TRIP PRESSURIZER SAFETY VALVES DEMANDED	0.10	2.6E-02
M-MPP162-1DR	MTR-DRIVEN PP P162 FT RUN FOR 24 HR - LOOP A ESF HVAC E336	8.1E-03	2.6E-02
U-C2A0805--P	BKR (CNTL) 4160V A0805 FT OPEN ON DEMAND	3.0E-03	2.5E-02
U-C2A0807--N	BKR (CNTL) 4160V A0807 FT CLOSE ON DEMAND	3.0E-03	2.5E-02
NOT--Z2--TWS	LOW/MEDIUM MTC CONDITIONS EXIST	0.95	2.5E-02
M-HCBCBFAILU	OPER FT RESPOND TO BATT CHRG B2 FAILURE GIVEN PREV RESP FAIL	0.50	2.5E-02
M-HCNOSIAS-U	NO OPRT RESPONSE TO HIGH TEMPERATURE ALARM-ESF SWGR/DIST	1.0E-03	2.5E-02
M-MPP160-1DR	MTR-DRIVEN PP P160 FT RUN FOR 24 HR - LOOP B ESF HVAC E335	8.1E-03	2.4E-02
F-HCDEPRESSU	OP FAILS TO DEPRESS SG's W/I 1 HR AND ALIGN CONDENSATE	4.0E-02	2.4E-02
M3HC-E336PWJ	OP FT CROSS-TIE POWER TO BUS A04 AND BUS BQ FOR HVAC	1.0	2.4E-02
M3HC-E335PWJ	OP FT CROSS-TIE POWER TO BUS A06 AND BUS BS FOR HVAC	1.0	2.3E-02
FTPE-VLR-VL	NON-RECOVERY FROM ISLOCA	1.0	2.3E-02
H-MP018---M	PUMP 018 UNAVAILABLE DUE TO MAINTENANCE / TEST	5.0E-02	2.3E-02
FTPE-TIL-PCS	OPERATOR FAILS TO DEPRESSURIZE RCS AND CONTROL ECCS FLOW	1.0	2.2E-02
L-MP504----S	MTR-DRIVEN PP 504 FT START ON DEMAND - TRAIN B	4.7E-03	2.1E-02
B-HCFILTR--U	OPERATOR FAILS ALIGN STANDBY FILTER	1.0	2.0E-02
WCHCCSINJCTU	OP FAILS TO DEPRESS RCS AND ALIGN CS FOR INJECTION (SL)	0.50	1.9E-02
L-MP141----S	MTR-DRIVEN PP 141 FT START ON DEMAND - TRAIN A	4.7E-03	1.9E-02
L-MP504----M	MTR-DRIVEN PP 504 OOS FOR MAINTENANCE - TRAIN B	7.6E-03	1.8E-02
Y-RV0200---N	RELIEF VLV SPRING LOAD 0200 FT CLOSE ON DEM	3.0E-03	1.8E-02
Y-RV0201---N	RELIEF VLV SPRING LOAD 0201 FT CLOSE ON DEM	3.0E-03	1.8E-02

TABLE 3.3-20

Fussell-Vesely Importance Measures for Top Basic Events
(continued)

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	FUSSELL-VESELY IMPORTANCE
L-MP141---M	MTR-DRIVEN PP 141 OOS FOR MAINTENANCE - TRAIN A	7.6E-03	1.7E-02
H-HCP17STRU	OPERATOR FAILS TO START STANDBY HPS1 PUMP PD17	0.10	1.6E-02
L-HCTP140--U	OPER FT MANUALLY OPERATE TO AFW PUMP (NO DC PWR @ 8H)	6.0E-03	1.6E-02
M-C3BQ08---W	BKR (CNTL) 480V BQ08 FT CLOSE ON DEMAND	3.0E-03	1.6E-02
F-ZZCONDMU-Z	INADEQUATE CST CONDENSATE MAKEUP TO THE HOT WELL	1.0	1.6E-02
U-HC2Q065--U	OPERATOR FAILS TO XFER Q065 TO MCC BX VIA KIRK-KEY INTLK	1.0	1.6E-02
M-C3BS08---N	BKR (CNTL) 480V BS08 FT CLOSE ON DEMAND	3.0E-03	1.6E-02
M-CHCC0001-S	COMMON CAUSE FAILURE -CH-S-->E-335,E-336	4.3E-04	1.6E-02
H-MPD18--1DR	MTR-DRIVEN PP 018 FT RUN FOR 24 HR	1.4E-02	1.4E-02
P-HTED02-1DM	HEAT X (TUBE) E002 OOS FOR MAINT W/I 24 H	6.5E-03	1.4E-02
L-C2A0603--N	BKR (CNTL) 4160V A0603 FT CLOSE ON DEMAND	3.0E-03	1.4E-02
T-OOE-088--Z	S/G E-088 AFFECTED BY INITIATING EVENT (FAULTED S/G)	0.50	1.4E-02
U-IRY012-1DR	INVERTER Y012 FT OPERATE W/I 24 H	1.4E-03	1.4E-02
H-MVCC0039-P	COMMON CAUSE FAILURE -MV-P --> 9420 AND 9434	2.6E-04	1.4E-02
L-TP140NR1DR	TURBINE DRIVEN PP 140 FT TO RUN IS NOT RECOVERABLE	0.33	1.4E-02
H-MPCC0004-S	COMMON CAUSE FAILURE -MP-S --> 018 AND 019	1.0E-03	1.4E-02
T-OOE-089--Z	S/G E-089 AFFECTED BY INITIATING EVENT (FAULTED S/G)	0.50	1.4E-02
H-MV9303---P	MTR-OPERATED VLV 9303 FT OPEN ON DEMAND	3.0E-03	1.3E-02
H-MV9305---P	MTR-OPERATED VLV 9305 FT OPEN ON DEMAND	3.0E-03	1.3E-02
INIT-SLB-SLB	STEAM LINE BREAK AND FEEDWATER LINE BREAK INITIATING EVENT	5.4E-04	1.3E-02
L-SV4700---J	SOLENOID VALVE 4700 FT ACT/DE-ACT ON DEM	2.0E-03	1.3E-02
L-C2A0404--N	BKR (CNTL) 4160V A0404 FT CLOSE ON DEMAND	3.0E-03	1.3E-02
U-DG2G2----S	DIESEL GENERATOR 2G2 FT START ON DEMAND - TRAIN A ESF POWER	1.7E-02	1.3E-02
U-00PCLOOP-Z	LOOP EVENT PLANT- CENTERED LOOP - NO NON-1E PWR AVAILABLE	0.81	1.3E-02
L-TP140--1DR	TURBINE DRIVEN PP 140 FT RUN FOR 24 H	7.3E-03	1.3E-02
U-DG2G3----S	DIESEL GENERATOR 2G3 FT START ON DEMAND - TRAIN B ESF POWER	1.7E-02	1.3E-02
UFHCFSTXFRU	OPERATOR FAILS TO RECOVER NON-1E FAST TRANSFER FAILURE	0.10	1.3E-02
E-ZZ25T024-K	PUMP PD25 NOT ALIGNED TO TRAIN B	1.0	1.2E-02
H-MP019----S	MTR-DRIVEN PP 019 FT START ON DEMAND	4.8E-03	1.2E-02

TABLE 3.3-20

Fussell-Vesely Importance Measures for Top Basic Events
(continued)

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	FUSSELL-VESELY IMPORTANCE
M-CHE-336--S	CHILLER E-336 FT START ON DEMAND - LOOP A ESF HVAC	4.3E-03	1.2E-02
M-CHE-335--S	CHILLER E-335 FT START ON DEMAND - LOOP B ESF HVAC	4.3E-03	1.1E-02
T-HVCC0001-N	COMMON CAUSE FAILURE -HV-N --> 8204 AND 8205	5.8E-04	1.1E-02
L-HCNSBOMAND	OP FT MAN CTL AFW FLOW VALVES W/I 2.5 TO 8.0 HOURS	6.0E-03	1.1E-02
M-MPP162---S	MTR-DRIVEN PP P162 FT START ON DEMAND - LOOP A ESF HVAC E336	3.8E-03	1.1E-02
H-HASMP1T--X	EMERGENCY SUMP LATCH LEFT OPEN	1.0E-04	1.1E-02
M-MPP160---S	MTR-DRIVEN PP P160 FT START ON DEMAND - LOOP B ESF HVAC E335	3.8E-03	1.0E-02
H-MPD17--1DR	MTR-DRIVEN PP 017 FT RUN FOR 24 HR	1.4E-02	1.0E-02

Table 3.3-21
RISK REDUCTION VALUES FOR BASIC EVENTS

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	RISK REDUCTION VALUE
INIT-LOP-LOP	LOSS OF OFFSITE POWER INITIATING EVENT	0.11	7.8E-06
U-HCOSPWR60U	NONRECOVERY OF OFFSITE POWER IN 60 MINUTES	0.12	7.7E-06
L-TP140---M	TURBINE-DRIVEN PP 140 OOS FOR MAINTENANCE	2.2E-02	4.6E-06
INIT-TT--TT	TRANSIENT WITH PCS INITIALLY AVAILABLE INITIATING EVENT	3.8	4.4E-06
INIT-ML--ML	MEDIUM LOCA INITIATING EVENT	1.0E-03	4.1E-06
U-00GWLOOP-Z	LOOP EVENT GRID RELATED LOOP - NO OFFSITE PWR AVAILABL	0.19	3.9E-06
INIT-LL--LL	LARGE LOCA INITIATING EVENT	5.0E-04	3.3E-06
INIT-PCS-PCS	LOSS OF POWER CONVERSION SYSTEM INITIATING EVENT	0.53	3.3E-06
INIT-SL--SL	SMALL LOCA INITIATING EVENT	1.0E-03	3.0E-06
K-DOMECHSCRM	MECHANICAL FAILURE OF THE RPS TO SCRAM	1.0E-05	2.7E-06
NOT--Z1--TWS	POWER LEVEL GREATER THAN 20%	0.74	2.4E-06
L-TP140NR--S	FAILURE OF P140 TO START IS NOT RECOVERABLE	0.33	2.4E-06
L-TP140---S	TURBINE-DRIVEN PP 140 FT START ON DEMAND	3.0E-02	2.4E-06
L-HCHV4716PU	OPERATOR FAILS TO MANUALLY OPEN HV4716 LOCALLY AFTER FAULT	1.0	2.3E-06
L-MV4716---P	MTR-OPERATED VLV 4716 FT OPEN ON DEMAND	9.9E-03	2.3E-06
L-MP504--1DR	MTR-DRIVEN PP 504 FT RUN FOR 24 HR - TRAIN B	1.3E-02	2.0E-06
U-DG2G2--8HR	DIESEL GENERATOR 2G2 FT RUN - TRAIN A ESF POWER	7.7E-02	1.9E-06
U-DG2G3--8HR	DIESEL GENERATOR 2G3 FT RUN - TRAIN B ESF POWER	7.7E-02	1.9E-06
L-MP141--1DR	MTR-DRIVEN PP 141 FT RUN FOR 24 HR - TRAIN A	1.3E-02	1.9E-06
U-HC3A4A660V	OPER FAILS TO TIE IN BUS 3A04(OR BUS 3A06) W/I 60 MIN (SBO)	1.0	1.8E-06
FTPE-Z2--TWS	HIGH MTC CONDITIONS EXIST (UNFAVORABLE)	5.0E-02	1.7E-06
FGHCFWREC-U	NON-RECOVERY OF MAIN FEEDWATER WITHIN 60 MINUTES	0.43	1.5E-06
FTPE-N1--ML	FAILURE TO DEPRESS RCS AND ALIGN CS FOR RCS INJECTION	1.0	1.4E-06
L-HCSTMU--U	OPERATOR FAILS TO PROVIDE T121 (CST) MAKEUP PER PROCEDURE	2.0E-05	1.4E-06
H-MP019--1DR	MTR-DRIVEN PP 019 FT RUN FOR 24 HR	1.4E-02	1.1E-06
INIT-SGR-SGR	STEAM GENERATOR TUBE RUPTURE INITIATING EVENT	1.0E-02	1.1E-06
H-MPCC0001-S	COMMON CAUSE FAILURE -MP-S --> 017, 018, AND 019	4.8E-04	1.1E-06
INIT-SSL-SSL	SMALL-SMALL LOCA INITIATING EVENT	1.3E-02	9.9E-07
H-MP017---M	PUMP 017 UNAVAILABLE DUE TO MAINTENANCE / TEST	5.0E-02	9.5E-07
P-HTE001-1DM	HEAT X (TUBE) E001 OOS FOR MAINT W/I 24 H	6.5E-03	9.4E-07
H-MP019---M	PUMP 019 UNAVAILABLE DUE TO MAINTENANCE / TEST	5.0E-02	9.3E-07
L-MPCC0001-S	COMMON CAUSE FAILURE -MP-S --> 141 AND 504 (AFW MDPS)	2.7E-04	9.2E-07
FGHCCNDREC-U	NON-RECOVERY OF EMERGENCY CONDENSATE WITHIN 60 MINUTES	6.0E-02	9.1E-07
FTPE-F---SSL	MFV UNAVAILABLE DUE TO CIAS	1.0	8.3E-07
H-MVCC0033-P	COMMON CAUSE FAILURE -MV-P --> 9302 AND 9303	2.6E-04	8.2E-07

Table 3.3-21

RISK REDUCTION VALUES FOR BASIC EVENTS
(continued)

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	RISK REDUCTION VALUE
H-MVCC0035-P	COMMON CAUSE FAILURE -MV-P --> 9302 AND 9305	2.6E-04	8.2E-07
H-MVCC0036-P	COMMON CAUSE FAILURE -MV-P --> 9303 AND 9304	2.6E-04	8.2E-07
H-MVCC0038-P	COMMON CAUSE FAILURE -MV-P --> 9304 AND 9305	2.6E-04	8.2E-07
Y-QORV-DEM-Z	POST-TPIP PRESSURIZER SAFETY VALVES DEMANDED	0.10	7.8E-07
M-MPP162-1DR	MTR-DRIVEN PP P162 FT RUN FOR 24 HR - LOOP A ESF HVAC E336	8.1E-03	7.6E-07
U-C2A0805--P	BKR (CNTL) 4160V A0805 FT OPEN ON DEMAND	3.0E-03	7.5E-07
U-C2A0807--N	BKR (CNTL) 4160V A0807 FT CLOSE ON DEMAND	3.0E-03	7.5E-07
NOT--Z2--TW5	LOW/MEDIUM MTC CONDITIONS EXIST	0.95	7.5E-07
M-HCBCBFAILU	OPER FT RESPOND TO BATT CHRG B2 FAILURE GIVEN PREV RESP FAIL	0.50	7.3E-07
M-HCNOSIAS-U	NO OPRT RESPONSE TO HIGH TEMPERATURE ALARM-ESF SWGR/DIST	1.0E-03	7.3E-07
M-MPP160-1DR	MTR-DRIVEN PP P160 FT RUN FOR 24 HR - LOOP B ESF HVAC E335	8.1E-03	7.2E-07
F-HCDEPRESSU	OP FAILS TO DEPRESS SG's W/I 1 HR AND ALIGN CONDENSATE	4.0E-02	7.2E-07
M3HC-E336PWJ	OP FT CROSS-TIE POWER TO BUS A04 AND BUS B0 FOR HVAC	1.0	7.2E-07
M3HC-E335PWJ	OP FT CROSS-TIE POWER TO BUS A06 AND BUS B5 FOR HVAC	1.0	6.9E-07
FTPE-VLR-VL	NON-RECOVERY FROM ISLOCA	1.0	6.7E-07
H-MP01B----M	PUMP 01B UNAVAILABLE DUE TO MAINTENANCE / TEST	5.0E-02	6.7E-07
FTPE-TIL-PCS	OPERATOR FAILS TO DEPRESSURIZE RCS AND CONTROL ECCS FLOW	1.0	6.5E-07
L-MP504----S	MTR-DRIVEN PP 504 FT START ON DEMAND - TRAIN B	4.7E-03	6.2E-07
B-HCFILTR--U	OPERATOR FAILS ALIGN STANDBY FILTER	1.0	5.8E-07
NCHCCSINJCTU	OP FAILS TO DEPRESS RCS AND ALIGN CS FOR INJECTION (SL)	0.50	5.7E-07
L-MP141----S	MTR-DRIVEN PP 141 FT START ON DEMAND - TRAIN A	4.7E-03	5.6E-07
L-MP504----M	MTR-DRIVEN PP 504 OOS FOR MAINTENANCE - TRAIN B	7.6E-03	5.4E-07
Y-RV0200---N	RELIEF VLV SPRING LOAD 0200 FT CLOSE ON DEM	3.0E-03	5.3E-07
Y-RV0201---N	RELIEF VLV SPRING LOAD 0201 FT CLOSE ON DEM	3.0E-03	5.3E-07
L-MP141----M	MTR-DRIVEN PP 141 OOS FOR MAINTENANCE - TRAIN A	7.6E-03	5.0E-07
H-HCP175STRU	OPERATOR FAILS TO START STANDBY HPSI PUMP P017	0.10	4.8E-07
L-HCTP140--U	OPER FT MANUALLY OPERATE TD AFW PUMP (NO DC PWR @ BH)	6.0E-03	4.8E-07
M-C3B00B---N	BKR (CNTL) 480V B00B FT CLOSE ON DEMAND	3.0E-03	4.8E-07
F-Z2CONDMU-Z	INADEQUATE CST CONDENSATE MAKEUP TO THE HOT WELL	1.0	4.7E-07
U-HC20065--U	OPERATOR FAILS TO XFER Q065 TO MCC BX VIA KIRK-KEY INTLK	1.0	4.6E-07
M-C3B50B---N	BKR (CNTL) 480V B50B FT CLOSE ON DEMAND	3.0E-03	4.6E-07
M-CHCC0001-S	COMMON CAUSE FAILURE -CH-S-->E-335,E-336	4.3E-04	4.6E-07
H-MP01B--1DR	MTR-DRIVEN PP 01B FT RUN FOR 24 HR	1.4E-02	4.2E-07
P-HTE002-1DM	HEAT X (TUBE) E002 OOS FOR MAINT W/I 24 H	6.5E-03	4.2E-07

Table 3.3-21

RISK REDUCTION VALUES FOR BASIC EVENTS
(continued)

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	RISK REDUCTION VALUE
L-C2A0603--N	BKR (CNTL) 4160V A0603 FT CLOSE ON DEMAND	3.0E-03	4.2E-07
T-DOE-088--Z	S/G E-088 AFFECTED BY INITIATING EVENT (FAULTED S/G)	0.50	4.1E-07
U-IRY012-1DR	INVERTER Y012 FT OPERATE W/I 24 H	1.4E-03	4.0E-07
H-MVCC0039-P	COMMON CAUSE FAILURE -MV-P --> 9420 AND 9434	2.6E-04	4.0E-07
L-TP140NR1DR	TURBINE DRIVEN PP 140 FT TO RUN IS NOT RECOVERABLE	0.33	4.0E-07
H-MPCC0004-S	COMMON CAUSE FAILURE -MP-S --> 018 AND 019	1.0E-03	4.0E-07
T-DOE-089--Z	S/G E-089 AFFECTED BY INITIATING EVENT (FAULTED S/G)	0.50	4.0E-07
H-MV9303---P	MTR-OPERATED VLV 9303 FT OPEN ON DEMAND	3.0E-03	4.0E-07
H-MV9305---P	MTR-OPERATED VLV 9305 FT OPEN ON DEMAND	3.0E-03	4.0E-07
INIT-SLB-SLB	STEAM LINE BREAK AND FEEDWATER LINE BREAK INITIATING EVENT	5.4E-04	4.0E-07
L-SV4700---J	SOLENOID VALVE 4700 FT ACT/DE-ACT ON DEM	2.0E-03	3.9E-07
L-C2A0404--N	BKR (CNTL) 4160V A0404 FT CLOSE ON DEMAND	3.0E-03	3.8E-07
U-DG2G2----S	DIESEL GENERATOR 2G2 FT START ON DEMAND - TRAIN A ESF POWER	1.7E-02	3.8E-07
U-DOOCL00P-Z	LOOP EVENT PLANT- CENTERED LOOP - NO NON-1E PWR AVAILABLE	0.81	3.8E-07
L-TP140--1DR	TURBINE DRIVEN PP 140 FT RUN FOR 24 H	7.3E-03	3.7E-07
U-DG2G3----S	DIESEL GENERATOR 2G3 FT START ON DEMAND - TRAIN B ESF POWER	1.7E-02	3.7E-07
UFHCFASXFRU	OPERATOR FAILS TO RECOVER NON-1E FAST TRANSFER FAILURE	0.10	3.7E-07
E-ZZ257024-K	PUMP P025 NOT ALIGNED TO TRAIN B	1.0	3.5E-07
H-MP019----S	MTR-DRIVEN PP 019 FT START ON DEMAND	4.8E-03	3.4E-07
M-CHE-336--S	CHILLER E 336 FT START ON DEMAND - LOOP A ESF HVAC	4.3E-03	3.4E-07
M-CHE-335--S	CHILLER E-335 FT START ON DEMAND - LOOP B ESF HVAC	4.3E-03	3.3E-07
T-HVCC0001-N	COMMON CAUSE FAILURE -HV-N --> 8204 AND 8205	5.8E-04	3.3E-07
L-HCNSBOMANU	OP FT MAN CTL AFW FLOW VALVES W/I 2.5 TO 8.0 HOURS	6.0E-03	3.2E-07
M-MPP162---S	MTR-DRIVEN PP P162 FT START ON DEMAND - LOOP A ESF HVAC E336	3.8E-03	3.1E-07
H-HASMLT--X	EMERGENCY SUMP LATCH LEFT OPEN	1.0E-04	3.1E-07
M-MPP160---S	MTR-DRIVEN PP P160 FT START ON DEMAND - LOOP B ESF HVAC E335	3.8E-03	3.0E-07
H-MP017--1DR	MTR-DRIVEN PP 017 FT RUN FOR 24 HR	1.4E-02	3.0E-07

Table 3.3-22

RISK INCREASE VALUES FOR BASIC EVENTS

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	RISK INCREASE VALUE
K-DOOMECHSCRM	MECHANICAL FAILURE OF THE RPS TO SCRAM	1.0E-05	2.6E-01
L-TK121----D	CONDENSATE STORAGE TANK UNAVAILABLE	1.3E-06	7.6E-02
L-HCCSTMJ--U	OPERATOR FAILS TO PROVIDE T121 (CST) MAKEUP PER PROCEDURE	2.0E-05	6.7E-02
K-DOSIAS-CCZ	FAILURE OF COMMON CIRCUITRY FOR SIAS TRAINS A & B	8.5E-06	1.3E-02
U-T24X---1DR	4160V-480V XFMR 4X FT OPERATE 24 H	2.4E-05	5.9E-03
U-T26X---1DR	4160V-480V XFMR 6X FT OPERATE 24 H	2.4E-05	5.1E-03
U-BCB1---1DR	BATTERY CHARGER B1 FT OPERATE 24 H	1.4E-05	3.6E-03
U-BCB2---1DR	BATTERY CHARGER B2 FT OPERATE 24 H	1.4E-05	3.5E-03
L-MPCCD001-S	COMMON CAUSE FAILURE -MP-S --> 141 AND 504 (AFW MDPS)	2.7E-04	3.4E-03
H-TK005--1DD	RWST TANK 005 UNAVAILABLE	2.7E-06	3.3E-03
H-TK006--1DD	RWST TANK 006 UNAVAILABLE	2.7E-06	3.3E-03
H-HARFCNL--X	REFUELING CANAL DRAIN LEFT CLOSED (LIQ. HOLDUP)	4.0E-05	3.1E-03
H-HADEBRIS-X	EXCESSIVE DEBRIS IN CONTAINMENT DRAIN (SUMP PLUGS)	5.0E-05	3.1E-03
H-MVCC0033-P	COMMON CAUSE FAILURE -MV-P --> 9302 AND 9303	2.6E-04	3.1E-03
H-MVCC0035-P	COMMON CAUSE FAILURE -MV-P --> 9302 AND 9305	2.6E-04	3.1E-03
H-MVCC0036-P	COMMON CAUSE FAILURE -MV-P --> 9303 AND 9304	2.6E-04	3.1E-03
H-MVCC0038-P	COMMON CAUSE FAILURE -MV-P --> 9304 AND 9305	2.6E-04	3.1E-03
H-HASMLT--X	EMERGENCY SUMP LATCH LEFT OPEN	1.0E-04	3.1E-03
K-DORAS-CC-2	FAILURE OF COMMON CIRCUITRY FOR RAS TRAINS A & B	8.5E-06	3.1E-03
H-MPCCD001-S	COMMON CAUSE FAILURE -MP-S --> 017, 018, AND 019	4.8E-04	2.2E-03
H-HCHLRECRU	OP FT ESTABLISH HOT LEG RECIRC. INJ W/I 4 HRS	5.0E-05	1.5E-03
H-MVCC0039-P	COMMON CAUSE FAILURE -MV-P --> 9420 AND 9434	2.6E-04	1.5E-03
M-CHCC0001-S	COMMON CAUSE FAILURE -CH-S-->E-335,E-336	4.3E-04	1.1E-03
K-DOCCRPSS	COMMON CAUSE FAILURE OF RPS AND DSS TO SCRAM REACTOR	2.5E-05	7.4E-04
H-HCNOSIAS-U	NO DPRT RESPONSE TO HIGH TEMPERATURE ALARM-ESF SWGR/DIST	1.0E-03	7.2E-04
T-HVCC0001-N	COMMON CAUSE FAILURE -HV-N --> 8204 AND 8205	5.8E-04	5.5E-04
K-DOMSISCC-Z	FAILURE OF COMMON CIRCUITRY FOR MSIS TRAINS A & B	8.5E-06	5.4E-04
H-HAXV7766-X	MANUAL VALVE HV-7766 MISALIGNED - RWST CROSS CONNECT	5.0E-04	5.0E-04
H-HAXV7767-X	MANUAL VALVE HV-7767 MISALIGNED - RWST CROSS CONEECT	5.0E-04	5.0E-04
A-MVB160-1HQ	MTR-OPERATED VLV 8160 FT REM OPEN 1 H	2.0E-07	5.0E-04
A-MVB161-1HQ	MTR-OPERATED VLV 8161 FT REM OPEN 1 H	2.0E-07	5.0E-04
A-HAMV0396-X	MOV HV-0396 MISALIGNED - OTHER CS SDC HX BYPASS	4.0E-05	5.0E-04

Table 3.3-22

RISK INCREASE VALUES FOR BASIC EVENTS
(continued)

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	RISK INCREASE VALUE
A-HAMVB160-X	MOV HV-B160 MISALIGNED - CS SDC HX BYPASS	4.0E-05	5.0E-04
A-HAMVB161-X	MOV HV-B161 MISALIGNED - CS SDC HX BYPASS	4.0E-05	5.0E-04
A-MPCC0001-S	COMMON CAUSE FAILURE -MP-S --> 015 AND 016	1.1E-04	5.0E-04
A-MV0396-1D0	MTR-OPERATED VLV 0396 FT REM CLOSED 1 H	1.0E-07	5.0E-04
H-MPCC0004-S	COMMON CAUSE FAILURE -MP-S --> 018 AND 019	1.0E-03	3.9E-04
W-TK007---2D	TANK 007 LEAK/RUPTURE W/I 1 H	5.0E-07	3.8E-04
W-TK008---2D	TANK 008 LEAK/RUPTURE W/I 1 H	5.0E-07	3.8E-04
W-TK009---2D	TANK 009 LEAK/RUPTURE W/I 1 H	5.0E-07	3.8E-04
W-TK010---2D	TANK 010 LEAK/RUPTURE W/I 1 H	5.0E-07	3.8E-04
W-TK007---M	SIT TANK 007 UNAVAILABLE DUE TO MAINTENANCE	1.1E-04	3.8E-04
W-TK008---M	SIT TANK 008 UNAVAILABLE DUE TO MAINTENANCE	1.1E-04	3.8E-04
W-TK009---M	SIT TANK 009 UNAVAILABLE DUE TO MAINTENANCE	1.1E-04	3.8E-04
W-TK010---M	SIT TANK 010 UNAVAILABLE DUE TO MAINTENANCE	1.1E-04	3.8E-04
H-CV027---P	CHECK VLV 027 FT OPEN ON DEMAND	1.0E-04	3.8E-04
H-CV029---P	CHECK VLV 029 FT OPEN ON DEMAND	1.0E-04	3.8E-04
H-CV031---P	CHECK VLV 031 FT OPEN ON DEMAND	1.0E-04	3.8E-04
H-CV033---P	CHECK VLV 033 FT OPEN ON DEMAND	1.0E-04	3.8E-04
W-CV040---P	CHECK VLV 040 FT OPEN ON DEMAND	1.0E-04	3.8E-04
W-CV041---P	CHECK VLV 041 FT OPEN ON DEMAND	1.0E-04	3.8E-04
W-CV042---P	CHECK VLV 042 FT OPEN ON DEMAND	1.0E-04	3.8E-04
W-CV043---P	CHECK VLV 043 FT OPEN ON DEMAND	1.0E-04	3.8E-04
L-CV448---P	CHECK VLV 448 FT OPEN ON DEMAND	1.0E-04	3.5E-04
L-CV124---P	CHECK VLV 124 FT OPEN ON DEMAND	1.0E-04	3.4E-04
U-IRY012-1DR	INVERTER Y012 FT OPERATE W/I 24 H	1.4E-03	2.8E-04
B-FL003--1DC	FILTER 003 PLUGGED/FOULED W/I 24 H	7.2E-04	2.7E-04
B-FL004--1DC	FILTER 004 PLUGGED/FOULED W/I 24 H	7.2E-04	2.7E-04
B-FL005--1DC	FILTER 005 PLUGGED/FOULED W/I 24 H	7.2E-04	2.7E-04
FTPE-Y---CCW	LOSS OF CCW ANNUNCIATOR FAILS TO OPERATE	2.4E-05	2.5E-04
FTPE-Z---CCW	OPERATOR FAILS TO TRIP RCP GIVEN ANNUNCIATOR SIGNAL	5.0E-04	2.5E-04
A-MVCC0005-P	COMMON CAUSE FAILURE -MV-P --> 9322 AND 9325	2.6E-04	2.5E-04
A-MVCC0006-P	COMMON CAUSE FAILURE -MV-P --> 9322 AND 9328	2.6E-04	2.5E-04

Table 3.3-22

RISK INCREASE VALUES FOR BASIC EVENTS
(continued)

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	RISK INCREASE VALUE
A-MVCC0007-P	COMMON CAUSE FAILURE -MV-P --> 9322 AND 9331	2.6E-04	2.5E-04
A-MVCC0008-P	COMMON CAUSE FAILURE -MV-P --> 9325 AND 9328	2.6E-04	2.5E-04
A-MVCC0009-P	COMMON CAUSE FAILURE -MV-P --> 9325 AND 9331	2.6E-04	2.5E-04
A-MVCC0010-P	COMMON CAUSE FAILURE -MV-P --> 9328 AND 9331	2.6E-04	2.5E-04
U-B2A04--1DR	4160V BUS A04 FT OPERATE 24 H	7.2E-07	2.5E-04
U-B2A06--1DR	4160V BUS A06 FT OPERATE 24 H	7.2E-07	2.5E-04
U-B3B04--1DR	480V BUS B04 FT OPERATE 24 H	7.2E-07	2.5E-04
U-B3B06--1DR	480V BUS B06 FT OPERATE 24 H	7.2E-07	2.5E-04
U-B3BE---1DR	480V BUS BE FT OPERATE 24 H	7.2E-07	2.5E-04
U-B3BJ---1DR	480V BUS BJ FT OPERATE 24 H	7.2E-07	2.5E-04
K-OOSIAS-A-Z	SIAS A INDEPENDENT SIGNAL FAILURE	1.0E-06	2.5E-04
K-OOSIAS-B-Z	SIAS B INDEPENDENT SIGNAL FAILURE	1.0E-06	2.5E-04
U-C2A0805--P	BKR (CNTL) 4160V A0805 FT OPEN ON DEMAND	3.0E-03	2.5E-04
U-C2A0807--N	BKR (CNTL) 4160V A0807 FT CLOSE ON DEMAND	3.0E-03	2.5E-04
L-MV4716---P	MTR-OPERATED VLV 4716 FT OPEN ON DEMAND	9.9E-03	2.3E-04
L-TP140---M	TURBINE-DRIVEN PP 140 OOS FOR MAINTENANCE	2.2E-02	2.0E-04
L-SV4700---J	SOLENOID VALVE 4700 FT ACT/DE-ACT ON DEM	2.0E-03	1.9E-04
Y-RV0200---N	RELIEF VLV SPRING LOAD 0200 FT CLOSE ON DEM	3.0E-03	1.7E-04
Y-RV0201---N	RELIEF VLV SPRING LOAD 0201 FT CLOSE ON DEM	3.0E-03	1.7E-04
H-MPCC0002-S	COMMON CAUSE FAILURE -MP-S --> 017 AND 018	1.0E-03	1.7E-04
L-FLP140-1DC	FILTER P140 PLUGGED/FOULED W/I 24 H	7.2E-04	1.6E-04
F-ZZCONDLMSZ	LOSS OF VACUUM	4.9E-05	1.6E-04
L-MV4716---M	MTR-OPTD VLV 4716 OOS FOR MAINTENANCE	9.6E-04	1.6E-04
M-C3B008---N	BKR (CNTL) 480V B008 FT CLOSE ON DEMAND	3.0E-03	1.6E-04
P-HTE001-1DC	HEAT X (TUBE) E001 PLUGGED/FOULED W/I 24 H	1.4E-04	1.6E-04
L-MP504--1DR	MTR-DRIVEN PP 504 FT RUN FOR 24 HR - TRAIN B	1.3E-02	1.6E-04
M-C3B508---N	BKR (CNTL) 480V B508 FT CLOSE ON DEMAND	3.0E-03	1.5E-04
H-MPCC0003-S	COMMON CAUSE FAILURE -MP-S --> 017 AND 019	1.0E-03	1.5E-04
L-HAXV122--X	MANUAL VALVE 122 MISALIGNED - P140 DISCHARGE	5.0E-04	1.5E-04
L-MP141--1DR	MTR-DRIVEN PP 141 FT RUN FOR 24 HR - TRAIN A	1.3E-02	1.4E-04
P-HTE001-1DM	HEAT X (TUBE) E001 OOS FOR MAINT W/I 24 H	6.5E-03	1.4E-04

Table 3.3-22

RISK INCREASE VALUES FOR BASIC EVENTS
(continued)

BASIC EVENT NAME	BASIC EVENT DESCRIPTION	BASIC EVENT VALUE	RISK INCREASE VALUE
L-C2A0603--N	BKR (CNTL) 4160V A0603 FT CLOSE ON DEMAND	3.0E-03	1.4E-04
H-MSBE35---N	MTR STARTER BE35 FT CLOSE ON DEMAND	3.0E-04	1.4E-04
H-MSBY28---N	MTR STARTER BY28 FT CLOSE ON DEMAND	3.0E-04	1.4E-04
U-DGCC0006-S	COMMON CAUSE FAILURE -DG-S --> 2G2 AND 2G3	6.6E-04	1.3E-04
U-MPCC0006-S	COMMON CAUSE FAILURE -MP-S --> 2P093 AND 2P094	3.0E-04	1.3E-04
H-MV9303---P	MTR-OPERATED VLV 9303 FT OPEN ON DEMAND	3.0E-03	1.3E-04
H-MV9305---P	MTR-OPERATED VLV 9305 FT OPEN ON DEMAND	3.0E-03	1.3E-04
T-AVCC0001-P	COMMON CAUSE FAILURE -AV-P --> B419 AND B421	2.0E-04	1.3E-04
U-T12XR1-1DR	>4160V XFMR 2XR1 FT OPERATE W/1 24 H	2.4E-05	1.3E-04
U-T216X--1DR	4160V-480V XFMR 16X FT OPERATE 24 H	2.4E-05	1.3E-04
L-MP504----S	MTR-DRIVEN PP 504 FT START ON DEMAND - TRAIN B	4.7E-03	1.3E-04
L-C2A0404--N	BKR (CNTL) 4160V A0404 FT CLOSE ON DEMAND	3.0E-03	1.3E-04
H-MV9303---M	MTR-OPTD VLV 9303 DOS FOR MAINTENANCE	1.0E-03	1.2E-04
H-MV9305---M	MTR-OPTD VLV 9305 DOS FOR MAINTENANCE	1.0E-03	1.2E-04
M-FNA-165--S	FAN A-165 FT START ON DEMAND	3.0E-04	1.2E-04
M-FNE-430--S	FAN E-430 FT START ON DEMAND	3.0E-04	1.2E-04
M-DR9557-1DC	ORIFICE 9557 PLUGGED/FOULED	3.0E-04	1.2E-04
L-MP141----S	MTR-DRIVEN PP 141 FT START ON DEMAND - TRAIN A	4.7E-03	1.2E-04
H-CV003----P	CHECK VLV 003 FT OPEN ON DEMAND	1.0E-04	1.2E-04
L-FLP504-1DC	FILTER P504 PLUGGED/FOULED W/1 24 H	7.2E-04	1.1E-04
M-FNA-1651DR	FAN A-165 FT RUN FOR 24 H	2.4E-04	1.1E-04
M-FNE-4301DR	FAN E-430 FT RUN FOR 24 H	2.4E-04	1.1E-04
L-HAXV533--X	MANUAL VALVE 533 MISALIGNED - P504 DISCHARGE	5.0E-04	1.1E-04
L-FLP141-1DC	FILTER P141 PLUGGED/FOULED W/1 24 H	7.2E-04	1.0E-04
E-MP026--1DR	MTR-DRIVEN PP 026 FT RUN FOR 24 HR	2.0E-03	1.0E-04
U-BCB5---1DR	BATTERY CHARGER B5 FT OPERATE 24 H	1.4E-05	1.0E-04

3.4 Results and Screening Process

3.4.1 Application of Generic Letter Screening Criteria

As part of the IPE process the NRC has requested in Appendix 2 of the GL 88-20 (Reference 3.4-1) that each utility provide certain minimum reporting requirements relative to the results. These reporting requirements are easily derived from the IPE and include the following:

- (1) Functional sequences that contribute $1E-6$ or more per reactor year to core damage.
- (2) Functional sequences that contribute 5 percent or more to the total core damage frequency.
- (3) Functional sequences that have core damage frequencies greater than or equal to $1E-6$ per reactor year and that lead to containment failure which can result in a radioactive release magnitude greater than or equal to the BWR-3 or PWR-4 release categories of WASH-1400.
- (4) Functional sequences that contribute to a containment bypass frequency in excess of $1E-7$ /reactor year.
- (5) Any unique functional sequences which are important contributors to core damage frequency.

Appendix 2 of GL 88-20 uses a functional sequence approach based on faulted components or actions in establishing the selection criteria. The NUREG-1335 (Reference 3.4-2) guidelines use a system fault approach as an alternative selection criterion. The options presented in Appendix 2 of GL 88-20 (functional sequence-based) were selected over the alternative offered in NUREG-1335.

In addition to the reporting of these results, the NRC has also requested in Section 2.1.6 of NUREG-1335, the following additional elaborations:

- (1) A discussion of the screened sequences.
- (2) A list of the major contributors to those sequences.
- (3) A thorough discussion of the evaluation of the applicable decay heat removal function.

3.4.1.1 Functional Sequences Meeting the Screening Criteria

The core damage frequency results for the functional accident classes defined in Section 3.1 are the basis for screening the

SONGS 2/3 IPE results. Table 3.4-1 presents a comparison of the functional accident class results to the NRC screening criteria.

3.4.1.2 Description of Sequences Meeting Screening Criteria

The following section provides a brief summary of the major contributors to each of the functional accident sequences meeting the screening criteria.

Class IA - 1.2E-5 (40%)

This class of sequences involves loss of RCS heat removal. This is typically due to a transient event with loss of main feedwater, condensate, and auxiliary feedwater. The dominant contributors to this class involve sequences initiated by loss of offsite power (49%) or loss of the power conversion system (18%). These initiators lead to loss of main feedwater and condensate and result in a demand on the auxiliary feedwater system. There are many contributors which lead to failure of auxiliary feedwater, with no single failure dominating these sequences. However, the largest single contributor to AFW failure involves random failures of AFW pumps (~24%), followed by loss of room cooling to the ESF power distribution rooms which, in turn leads to loss of AFW flow control. Because the turbine-driven AFW pump can be operated even without ESF AC power, failure of the turbine-driven pump is also a substantial contributor. One additional contributor to AFW failure involves failure to replenish the CST from one of the many sources (~11%). Transients with feedwater initially available (TT) also contribute (15%) when the fast transfer of the BOP 4kV buses fails, leading to loss of MFW and condensate. LOCA events and steamline breaks also contribute (7% and 3%, respectively) due to the generation of a CIAS (and/or MSIS) which isolates MFW.

Although SONGS 2/3 do not have bleed and feed capability, the relative independence of the main feedwater and auxiliary feedwater systems result in a relatively low core damage frequency for this class of sequences.

Class IC - 2.0E-6 (7%)

This class of sequences involves Station Blackout sequences with loss of auxiliary feedwater. The dominant contributor to this class is a station blackout followed by failure of the turbine-driven auxiliary feedwater pump (88%). The dominant contributors to turbine-driven auxiliary feedwater pump unavailability for these sequences are unavailability due to maintenance (38%),

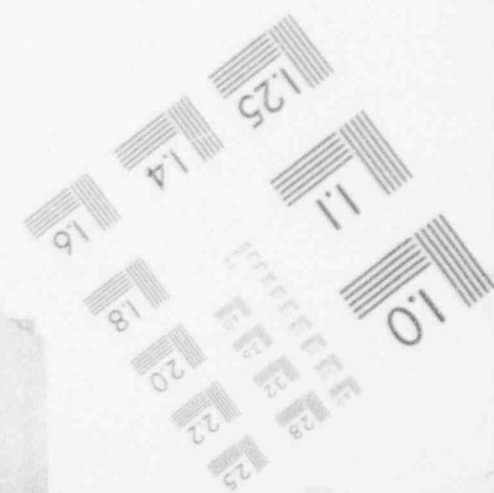
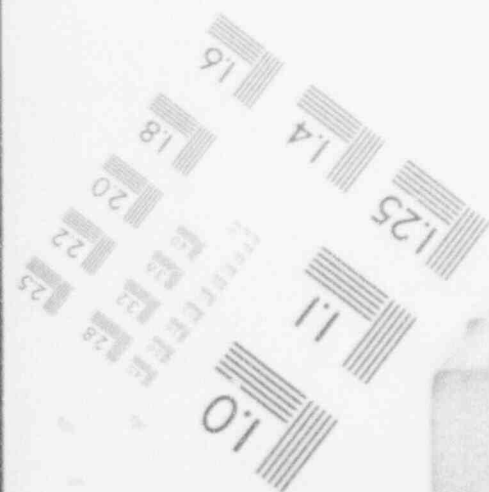
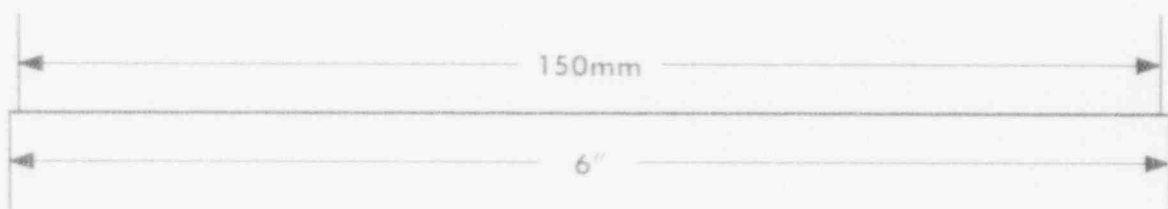
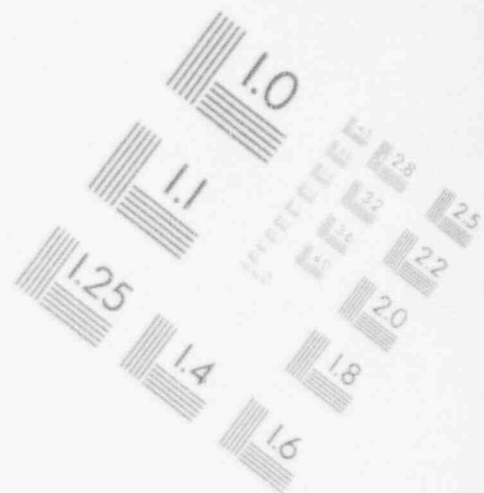
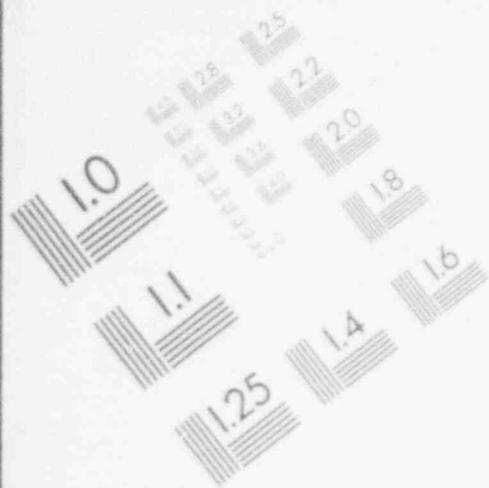
Table 3.4-1

COMPARISON OF FUNCTIONAL ACCIDENT SEQUENCES
TO NRC SCREENING CRITERIA

Class	Definition	CDF	% of CDF	MEETS CRITERIA?				
				1	2	3	4 ¹	5
IA	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Injection Phase	1.2E-5	40%	Y	Y	Y	N	N
IC	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup Due To Station Blackout	2.0E-6	7%	Y	Y	Y	N	N
IIA	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase	5.1E-7	2%	N	N	N	N	N
IIB	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase	9.0E-7	3%	N	N	N	N	N
IIIA	Accident Sequences Initiated By A Small LOCAs With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase	9.8E-7	3%	Y ²	N	Y ²	N	N
IIIB	Accident Sequences Initiated By A Small LOCAs With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase	2.1E-6	7%	Y	Y	Y	N	N
IIIC	Accident Sequences Initiated By Medium or Large LOCA With Loss of Primary Coolant Makeup In The Injection Phase	2.7E-6	9%	Y	Y	Y	N	N
IIID	Accident Sequences Initiated By A Medium or Large LOCAs With Loss of Primary Coolant Makeup or Adequate Heat Removal In The Recirculation Phase	4.6E-6	16%	Y	Y	Y	N	N

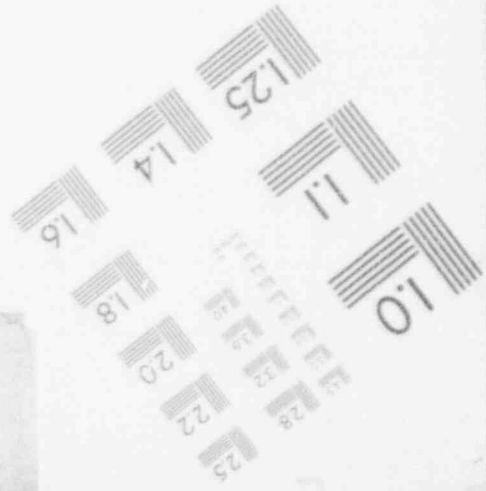
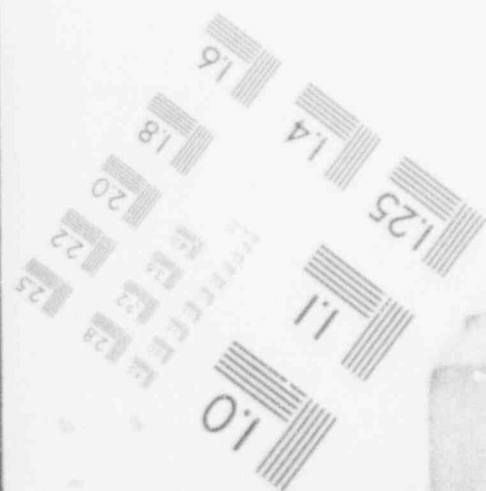
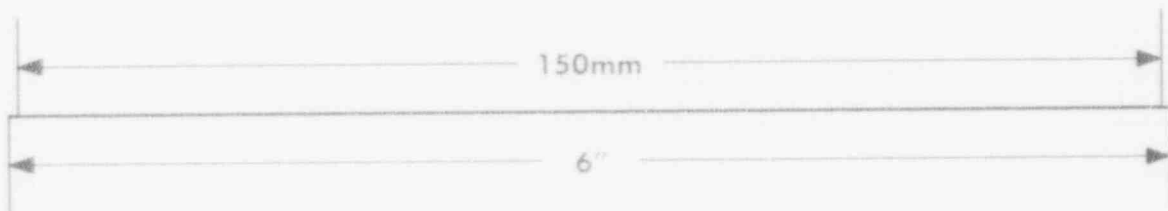
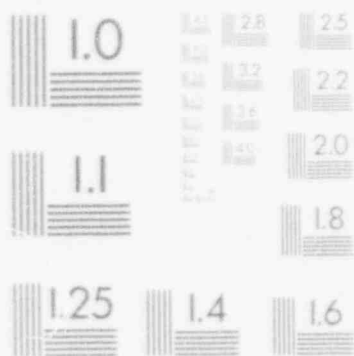
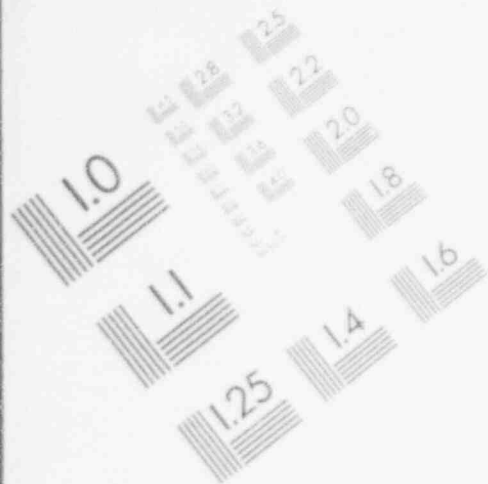
1

IMAGE EVALUATION TEST TARGET (MT-3)



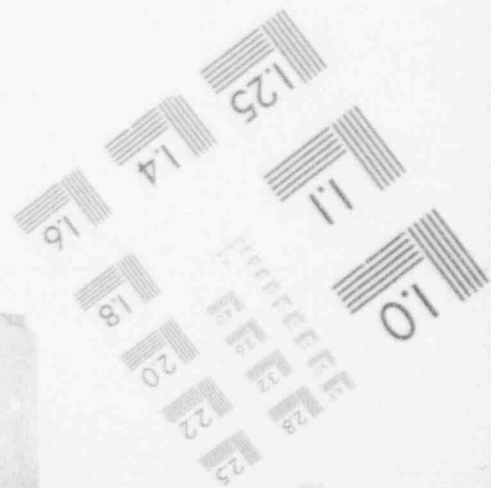
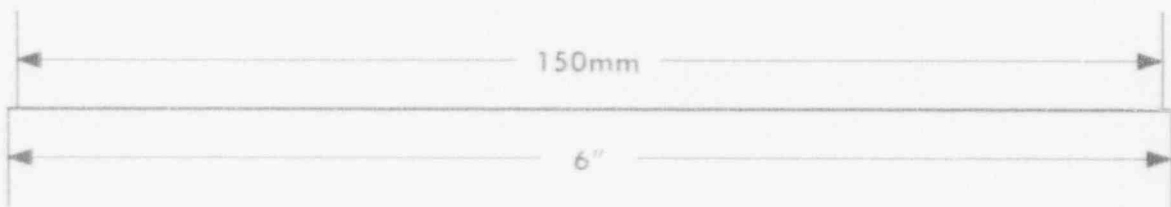
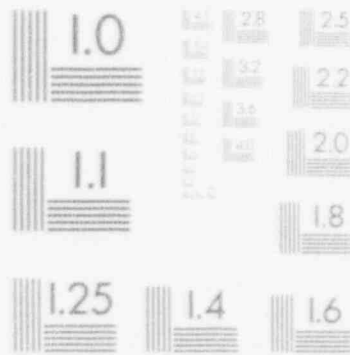
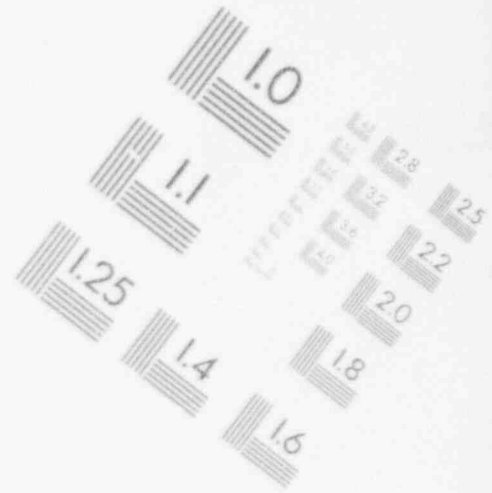
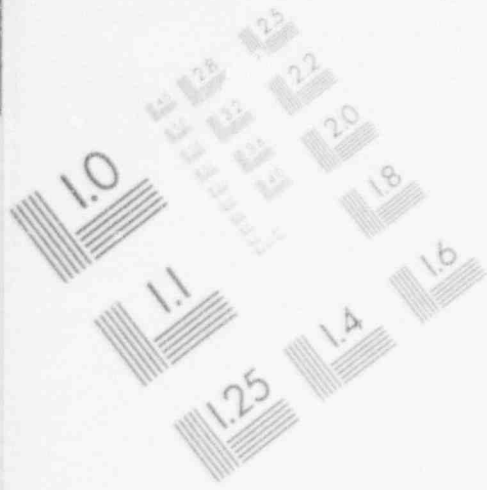
1

IMAGE EVALUATION TEST TARGET (MT-3)



1

IMAGE EVALUATION
TEST TARGET (MT-3)



1

IMAGE EVALUATION TEST TARGET (MT-3)

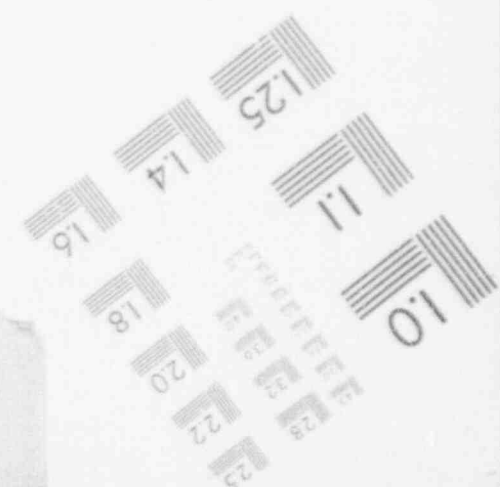
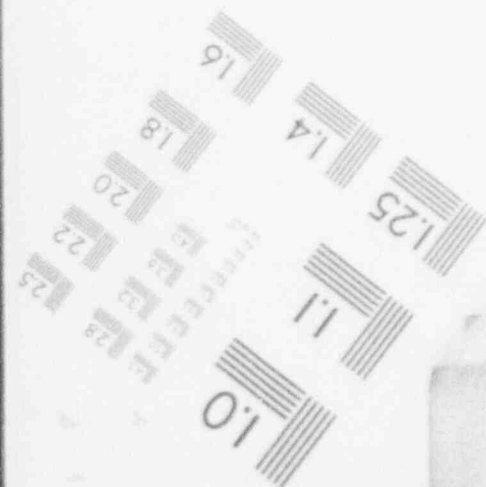
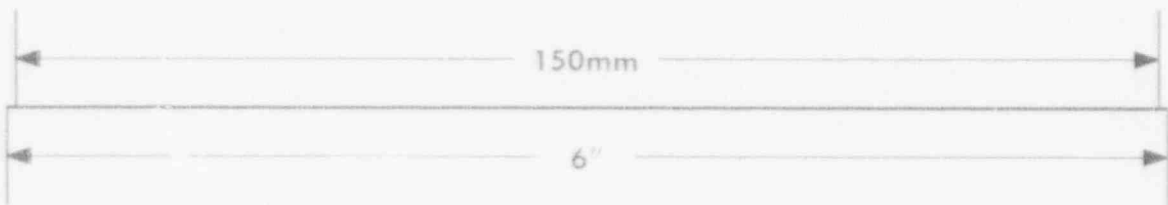
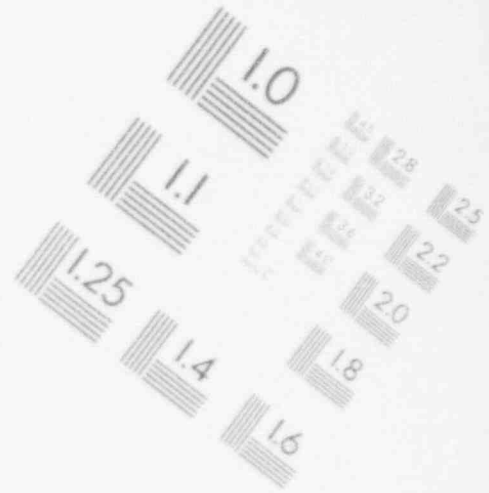
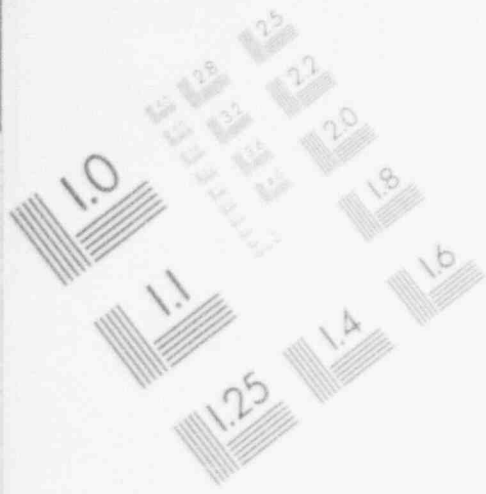


Table 3.4-1

COMPARISON OF FUNCTIONAL ACCIDENT SEQUENCES
TO NRC SCREENING CRITERIA
(continued)

Class	Definition	CDF	% of CDF	MEETS CRITERIA?				
				1	2	3	4 ¹	5
IV	Accident Sequences Involving Failure of Reactivity Control	2.7E-6	9%	Y	Y	Y	N	N
VA	Systems LOCA Outside Containment Leading to Loss of Effective Primary Coolant Inventory Makeup	6.6E-7	2%	N	N	N	Y	N
VB	Steam Generator Tube Rupture Leading to Loss of Effective Primary Coolant Inventory Makeup	6.5E-7	2%	N	N	N	Y	N
	Total CDF	3.0E-5						

1. For the purposes of the screening, it is assumed that all functional core damage sequences with frequencies greater than 1E-6 per reactor year could, with some probability, lead to a release exceeding the criteria.
2. For the purpose of screening, the value of 9.8E-7/yr is considered equivalent to 1E-6/yr.

failure to start and run (19%) and failure of the steam block valve to the turbine-driven AFW pump (19%). Long term station blackout sequences contribute relatively less (~12%) due to the extended battery life at SONGS (8 hours with load shedding) and the ability to manually control the turbine-driven auxiliary feedwater pump flow without control power.

Class IIIA - 9.8E-7 (3%)

This class of sequences includes small and small-small LOCA events with loss of adequate coolant makeup during injection. Small LOCA events dominate this class, contributing 82% to the class with small-small LOCA contributing the other 18%. These sequences are dominated by common cause failure of all three HPSI pumps to start (23%), common cause failure of two HPSI pumps with random unavailability of the other (~15%), support system failures (e.g., CCW [-19%] and HVAC [5%]) which lead to failure of the reactor coolant makeup systems (e.g. HPSI and/or charging).

Class IIIB - 2.1E-6 (7%)

This class of sequences includes small LOCA events with loss of adequate coolant makeup during recirculation. Essentially all the core damage frequency for this class comes from small LOCA events. These events are dominated by common cause failure of the containment ECCS recirculation sump valves to open (~54%). In the SONGS 2/3 design, each ECCS train is supplied during recirculation via a separate suction line from the sump. Each suction line has two normally closed MOVs which must open in order to establish flow. Other contributors include common sump problems such as emergency sump latch mispositioning, debris in sump, and refueling canal drain mispositioning (~10%), and insufficient RWST injection due to improper valve alignments (~8%).

Class IIIC - 2.7E-6 (9%)

This class of sequences includes medium and large LOCA events with loss of adequate coolant makeup during injection. The event sequences in this class were evenly split between large LOCA (50%) and medium LOCA (50%). The dominant contributors to the medium LOCA sequences are common cause failures of the HPSI pumps (28% of total), and support system failures related to CCW cooling (7% of total). The dominant contributors to large LOCA sequences are common cause failures of the injection valves (17% of total), common cause failure of LPSI pumps (2% of total) and SIT tank failures (6% of total).

Class IIID - 4.6E-6 (16%)

This class of sequences includes medium and large LOCA events with loss of adequate coolant makeup during recirculation. The event sequences are roughly split between medium LOCA (58%) and large LOCA (42%). These events are dominated by common cause failure of the containment ECCS recirculation sump valves to open (~40%). As described above, in the SONGS 2/3 design, each ECCS train is supplied during recirculation via a separate suction line from the sump. Each suction line has two normally closed MOVs which must open in order to establish flow. Other contributors include failures of hot leg recirculation valves (8%), common sump problems such as emergency sump latch mispositioning, debris in sump, and refueling canal drain mispositioning (7%), and insufficient RWST injection due to improper valve alignments (6%).

Class IV - 2.7E-6 (9%)

This class of sequences includes all anticipated transients without scram (ATWS) sequences. The event sequences which contribute to this class are dominated by the more frequent transients such as transients with feedwater available (85%), transients with feedwater unavailable (12%), and loss of offsite power (2%). The dominant contributor to the failure to scram in these sequences is mechanical faults in the scram system (>99%). The dominant contributor to core damage in these ATWS events is unfavorable MTC (~63%). Based on plant specific analyses, this unfavorable MTC was estimated to be roughly 5% of the fuel cycle. In addition, failure to manually trip the turbine was a substantial contributor (~25%). Other sequences contributing to this class include failure of emergency boration (~5%) and inadequate RCS pressure relief due to pressurizer safety valves failing to lift at their proper relief pressure (~10%).

Class VA - 6.6E-7 (2%)

This class of sequences involves interfacing system LOCAs. As described in Section 3.3.9, the dominant contributors to this class are failures of the two shutdown cooling hot leg loops.

Class VB - 6.5E-7 (2%)

This class of sequences involves steam generator tube rupture sequences leading to core damage. The dominant contributors to this class are failure of RCS makeup long term due to failure of HPSI and charging injection (~82%). The dominant contributors to HPSI failure are common cause failure of the three pumps (21% of total), common cause failure of two HPSI pumps with random failure of the standby pump (17% of total) and SIAS failure (14%

of total). Dominant contributors to charging failure are failure of a standby charging pump to start (12% of total) or run (15% of total) and SIAS failure (14% of total).

3.4.2 Vulnerability Screening

As part of the IPE process the NRC has requested that each utility provide the definition of vulnerability to be used in the evaluation of the IPE results. NUREG-1335, states that the reporting guidelines not only include the reporting of a wide variety of accident sequences uncovered in the IPE process but also the identification of the following:

"A list of any vulnerabilities identified by the review process, a concise discussion of the criteria used by the utility to define vulnerabilities, and the fundamental causes of each vulnerability. Vulnerabilities associated with the decay heat removal function should be specifically highlighted."

The definition of severe accident vulnerability used in evaluating the results of the SONGS 2/3 IPE is as follows:

A vulnerability in a PWR is a plant feature which contributes a disproportionately large percentage to either core damage or significant release probabilities which are in turn significantly higher than those of an average PWR.

Based on this definition of vulnerability, the total core damage frequency of 3.0×10^{-5} per reactor year, and the containment performance described in Section 4, no severe accident vulnerability exists at SONGS 2/3.

3.4.3 Decay Heat Removal (DHR) Evaluation

3.4.3.1 Introduction

This section provides a discussion of the adequacy of the SONGS shutdown decay heat removal (DHR) systems as evaluated in the SONGS 2/3 IPE. This section summarizes the effort to satisfy the GL 88-20 requirement for a plant specific evaluation of Unresolved Safety Issue (USI) A-45 (Reference 3.4-3).

3.4.3.2 Historical Perspective

The generic issue of decay heat removal capability was approved as an unresolved safety issue by the NRC in 1980. Prior to becoming a USI, Task A-45, as it was referred to, focused on the adequacy of steam generator auxiliary feedwater systems and

alternative means of decay heat removal at PWRs. When the issue was approved as a USI (such an approval indicates that resources will be provided to resolve the issue), USI A-45 was broadened to also investigate the need and possible design requirement for improving reliability of decay heat removal systems for BWRs.

In NUREG-1289 (Reference 3.4-4), which is the NRC staff resolution of USI A-45, the staff defines the systems related to the decay heat removal function as those components and systems required to maintain primary and secondary coolant inventory control and to transfer heat from the reactor coolant system to an ultimate heat sink following shutdown of the reactor for normal events or abnormal transients, such as loss of main feedwater, loss of offsite power, and small-break loss-of-coolant accidents (SBLOCAs). The USI A-45 program was not concerned with anticipated transients without scram, interfacing system loss-of-coolant accidents, or those emergency core cooling systems that are required only during the reflood phase to maintain coolant inventory and dissipate heat for a short period following either a medium or a large LOCA. The USI A-45 program did consider supporting systems, such as the component cooling water system, essential service water system, and emergency onsite AC and DC power systems that are required for various modes of decay heat removal. The reliability of the reactor protection system was not addressed, and successful shutdown of the reactor is assumed.

Six case studies have been performed with the purpose of identifying vulnerabilities of decay heat removal systems and recommending possible modifications (References 3.4-5, 3.4-6, 3.4-7, 3.4-8, 3.4-9, 3.4-10). A primary conclusion from these studies is that the issues of vulnerabilities and possible modifications tend to be plant specific. As such, the resolution of USI A-45 recommended by the NRC in both the IPE GL 88-20 and NUREG-1289 is to incorporate USI A-45 into the IPE process. The IPEs, therefore, are expected to lead to resolution of the generic USI A-45 issue on a plant-by-plant basis.

The NRC staff request in GL 88-20 is as follows:

"...Unresolved Safety Issue (USI) A-45 entitled "Shutdown Decay Heat Removal Requirements" had as its objective the determination of whether the decay heat removal function at operating plants is adequate and if cost-beneficial improvements could be identified. We concluded that a generic resolution to the issue (e.g., a dedicated decay heat removal system for all plants) is not cost effective and that resolution could only be achieved on a plant-specific basis. To implement a plant-specific resolution would require each plant to do an examination of its decay heat removal system to identify vulnerabilities. In the

IPE, each plant will do an examination of both its decay heat removal system and those systems used for the other safety functions for the purpose of identifying severe accident vulnerabilities. Therefore, we have concluded that the most efficient way to resolve A-45 is to subsume it in the IPE.

You should ensure that your IPE particularly identifies decay heat removal vulnerabilities. To achieve this assurance, we have extracted insights gained from the six case studies performed for the USI A-45 program. These insights are discussed in Appendix 5 to this letter and should be considered as you conduct your IPE..."

3.4.3.3 Definitions

The staff definition of DHR in USI A-45 is an expanded version of the functional definition of decay heat removal in a PWR. This expansion results in the inclusion of inventory makeup systems in addition to the function of decay heat removal. Therefore, in discussions of contributors to the core damage frequency in the SONGS 2/3 IPE, it is important to ensure that the definition of DHR being used is that of the NRC in USI A-45 rather than the definition traditionally assigned to DHR function in PRAs.

In this context, the following functional classes from the SONGS 2/3 IPE are considered as part of the USI A-45 definition of DHR:

- IA Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Injection Phase
- IB Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Recirculation Phase
- IC Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup Due To Station Blackout
- IIA Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase
- IIB Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase
- IIIA Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase

- IIIB Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase
- IIID Accident Sequences Initiated By A Medium or Large LOCA With Loss of Primary Coolant Makeup or Adequate Heat Removal In The Recirculation Phase

3.4.3.4 NRC Staff Criteria/Objectives (NUREG-1289)

The purpose of USI A-45 regarding Shutdown Decay Heat Removal Requirements is to evaluate the adequacy of current designs to ensure that Light Water Reactors (LWRs) do not pose unacceptable risk as a result of DHR system failures. The primary objectives of the USI A-45 program are to evaluate the safety adequacy of DHR systems in existing LWR power plants and to assess the value and impact (or benefit-cost) of alternative measures for improving the overall reliability of the DHR function.

At the time the USI A-45 program commenced, the NRC also started to develop a set of qualitative safety goals and quantitative design objectives (QDO). To aid the progress of the USI A-45 program, some interim QDOs were defined with the knowledge that these might have to be changed later in the program to conform with the final decisions of the Commission. The principal quantitative design objective selected for USI A-45 is the frequency of core damage due to failure of the DHR function, designated by $p(\text{cm})_{\text{DHR}}$. An interim value of $1\text{E-}5$ per reactor year for examining the DHR-related risk at individual plants was recommended by the NRC staff in NUREG-1289 (P. 4-14).

NUREG-1289 states: "(a) limited scope plant specific PRA could demonstrate the adequacy of the existing decay heat removal function by documenting that its contribution to core damage frequency was relatively low, on the order of $1\text{E-}5$ per reactor year or less."

The decay heat removal criteria, as can be seen, is structured such that at least the initial screening is based solely on the core damage frequency as the figure of merit. This is based on the NRC's conclusion that if this screening value is met, then little, if any, cost beneficial modifications would be possible.

The experience gained from application of PRAs to U.S. LWRs in the USI A-45 and other programs suggests that, when the systematic examinations for severe accident vulnerabilities (IPEs and IPEEs) have been completed, the existing plants will fall into three broad categories as far as the quantifiable adequacy of their DHR function is concerned. Pending further guidance from the Commission, the following quantitative values (expressed as means) have been used by the staff as a basis for categorization of these events:

Category	Classification of Level of DHR Vulnerability	Criterion
1	Frequency of core damage due to failures of DHR function ($p(cm)_{DHR}$) acceptably small or reducible to an acceptable level by simple improvements.	$p(cm)_{DHR}$ less than 3×10^{-5} per reactor-year
2	DHR performance characteristics intermediate between Categories 1 and 3.	$p(cm)_{DHR}$ less than 3×10^{-4} per reactor-year but greater than 3×10^{-5}
3	Frequency of core damage so large that prompt action to reduce $p(cm)_{DHR}$ to an acceptable level is necessary.	$p(cm)_{DHR}$ greater than 3×10^{-4} per reactor-year

These action levels and quantitative design objectives are used in the SONGS 2/3 IPE process to provide the NRC staff a consistent comparison basis for categorizing SONGS 2/3 and allowing a management decision on whether further effort on plant modification is necessary.

3.4.3.5 Comparison of SONGS 2/3 IPE Results With NRC Staff Criteria

The following table summarizes the functional accident classes contributing to the NRC staff definition of DHR sequences:

FUNCTIONAL ACCIDENT SEQUENCES CONTRIBUTING TO DHR

Class	Definition	Contribution To CDF
IA	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup In The Injection Phase	1.2E-5
IC	Accident Sequences Involving Loss of Both Primary and Secondary Coolant Makeup Due To Station Blackout	2.0E-6
IIA	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase	5.1E-7
IIB	Accident Sequences Involving an Induced Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase	9.0E-7
IIIA	Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Injection Phase	9.8E-7
IIIB	Accident Sequences Initiated By A Small LOCA With Loss of Primary Coolant Makeup or Loss of Adequate Heat Removal In The Recirculation Phase	2.1E-6
IIID	Accident Sequences Initiated By A Medium or Large LOCA With Loss of Primary Coolant Makeup or Adequate Heat Removal In The Recirculation Phase	4.6E-6
TOTAL CDF CONTRIBUTION FROM DHR SEQUENCES		2.3E-5

3.4.3.6 USI A-45 Conclusion for SONGS 2/3

The assessment of the adequacy of SONGS 2/3 decay heat removal systems was performed as part of the SONGS 2/3 IPE. The IPE used both the NRC quantitative design objectives and qualitative insights from past USI A-45 studies (References 3.4-11 through 3.4-21) as input for the analysis. The SONGS 2/3 IPE evaluation supports the conclusion that no vulnerabilities exist at SONGS 2/3 to adversely affect the operators' ability to accomplish the DHR function during an accident. As can be seen from the table above, the frequency of core damage associated with DHR failures is approximately $2.3\text{E-}5$ per reactor year using the NRC definition of DHR related sequences in USI A-45 (i.e., accident sequences that result in core damage due to the loss of coolant inventory control or decay heat removal capability). This is roughly equivalent to the screening criteria of $3\text{E-}5$ CDF per reactor year set by the NRC staff in NUREG-1289. This comparatively low core damage frequency results in the determination that no plant modifications at SONGS 2/3 are judged to be cost beneficial.

With respect to externally initiated events, a separate SONGS 2/3 PRA analysis will be undertaken in the future to address the requirements of the IPEEE. However, presently there are no known system dependencies that could significantly contribute to the failure of decay heat removal due to spatial interactions.

3.4.4 Steam Generator Overfill Evaluation

3.4.4.1 Introduction

The evaluation of SONGS 2/3 steam generator overfill has been performed in response to Generic Letter (GL) 89-19, "Safety Implication of Control Systems in LWR Nuclear Power Plants" (Reference 3.4-22). As a result of the technical resolution of Unresolved Safety Issue (USI) A-47, "Safety Implications of Control Systems in LWR Nuclear Power Plants" (Reference 3.4-23), the NRC recommended that all PWR plants provide automatic steam generator overfill protection (GL 89-19). This conclusion was based on safety assessments by NRC contractors. The results of these studies are summarized in NUREG/CR-1217, "Evaluation of Safety Implications of Control Systems in LWR Nuclear Power Plants" (Reference 3.4-24).

The purpose of this evaluation is to calculate the probability of core damage and significant offsite release as a result of a steam generator overfill event at SONGS 2/3.

3.4.4.2 Analysis Methodology for Steam Generator Overfill

NRC GL 89-19 recommends that all PWR plants install automatic steam generator overfill protection to resolve USI A-47. SCE has

undertaken an effort to (1) determine the applicability of the results of the GL 89-19 and its supporting NRC contractor analyses, and (2) perform a SONGS 2/3 plant-specific evaluation. The latter is documented in Section 3.4.4.3

To assess the applicability of GL 89-19 related analyses, the following steps were taken:

- Review GL 89-19, USI A-47, NUREG/CR-3958, NUREG 1217 (Reference 3.4-25), and NUREG 1218 (Reference 3.4-26) for applicability to SONGS 2/3.
- Review the underlying assumptions in the NRC analyses.
- Review the major steps in the analysis presented in NRC and CE Owners' Group efforts.
- Determine the relevance of the above underlying assumptions and major analysis steps to the SONGS 2/3 plant design.
- Develop an analysis approach as required to reflect the SONGS 2/3 plant design.
- Document the results of the SONGS 2/3 evaluation.

Based on a review of the NRC analyses, the general approach used in NUREG/CR-3958 is appropriate and applicable for a plant-specific evaluation of SONGS 2/3. However, several plant design differences were incorporated in this evaluation. These differences are discussed in Section 3.4.4.4.

3.4.4.3 Evaluation of Steam Generator Overfill

The following documents were reviewed and are used as reference documents for this study:

- Unresolved Safety Issue A-47, "Safety Implications of Control Systems in LWR Power Plants."
- Generic Letter 89-19, Request For Action Related to Resolution of Unresolved Safety Issue A-47 "Safety Implications of Control Systems in LWR Power Plants" Pursuant to 10 CFR 50.54 (f), Sept. 20, 1989.
- NUREG/CR-1217, "Evaluation of Safety Implications of Control Systems in LWR Power Plants" - Technical Findings Related to USI A-47, November 1988, Final Report.

- NUREG-1218, Regulatory Analysis For Resolution of USI A-47, "Safety Implications of Control Systems in LWR Power Plants," November 1988, Final Report.
- NUREG/CR-3958, "Effects of Control System Failures on Transients, Accidents and Core Melt Frequencies at a Combustion Engineering Pressurized Water Reactor," March 1986.

Based on a review of the above documents, the general approach used in NUREG/CR-3958 is appropriate and applicable for a plant-specific evaluation of SONGS 2/3. However, there are several plant design differences that were incorporated in this evaluation.

3.4.4.4 Steam Generator Overfill Event Tree Description

The steam generator overfill event tree for SONGS 2/3 is shown in Figure 3.4-1. The following sections describe the analysis and bases for the values used for each event tree node.

Steam Generator Overfill Event

In the 13 years of plant operation, a steam generator overfill has never occurred at SONGS 2/3. A steam generator high level trip protects SONGS 2/3 from steam generator overfill events. However, several events have occurred which required the high steam generator level reactor trip to actuate. The reactor trip, in turn, closed the feedwater regulating valve. Based on NUREG/CR-3958, the frequency of steam generator overfill events for plants like SONGS 2/3 is conservatively estimated to be 0.1 per reactor year.

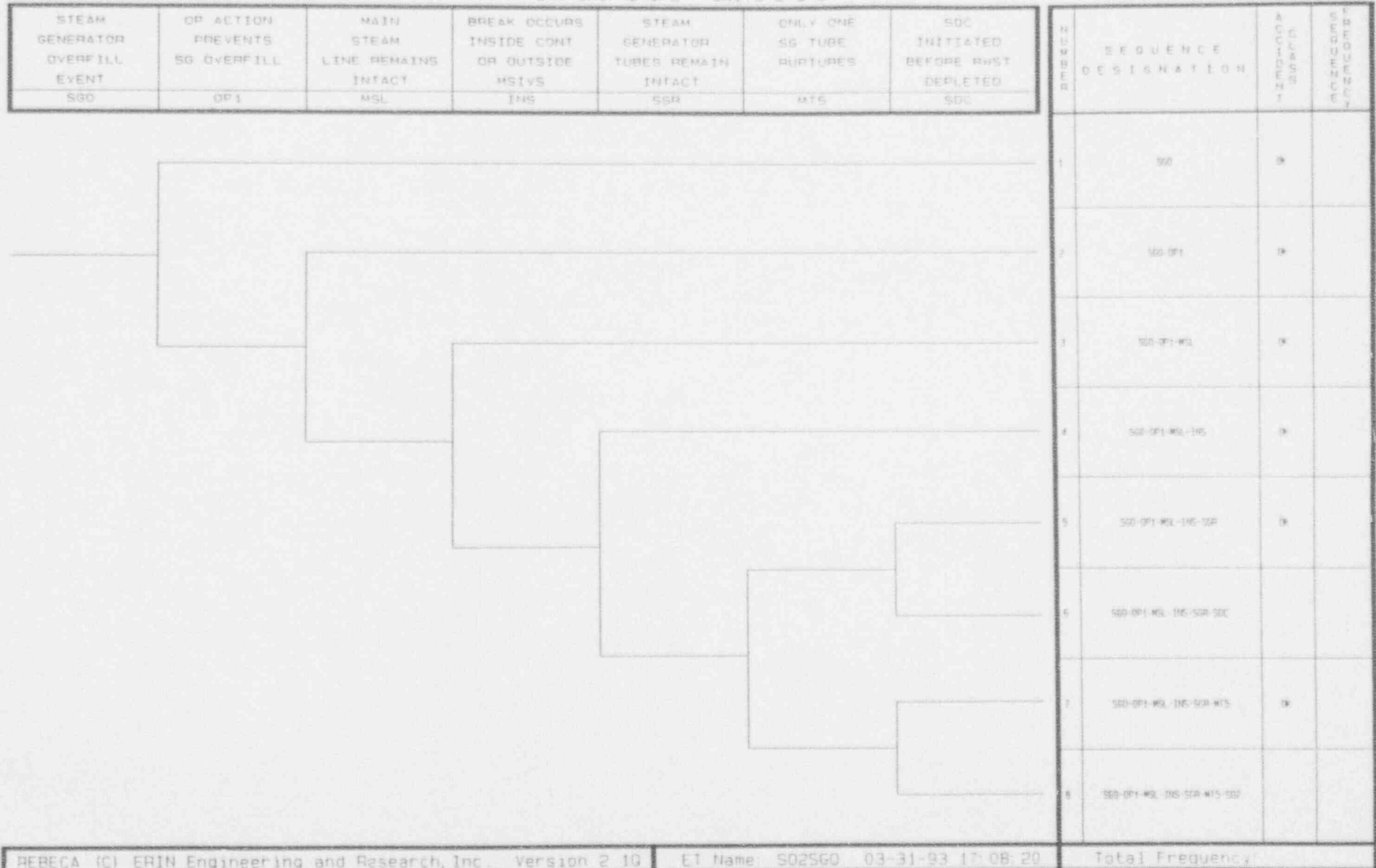
The SONGS 2/3 design makes it unlikely that a random failure could lead to overfill. The most likely scenario for overfill is a failure of a feedwater regulating valve in the open position. Assuming 4 transients per year and a feedwater regulating valve 'failure to close' probability of $3E-3$ per demand, the SG overfill frequency is approximately 0.024/year.¹ Although this calculation would support the use of a smaller initiating event frequency, the conservative NUREG/CR-3958 value of 0.1 per year is used in the analysis.

¹ 4 events/year * 2 valves * $3E-3$ /demand = 0.024 year

Figure 3.4-1: Steam Generator Overfill Event Tree

STEAM GENERATOR OVERFILL EVENT TREE

SAN ONOFRE IPE - UNITS 2 & 3



Operator Action Prevents SG Overfill

This event tree node represents the likelihood of an operator preventing excessive low quality steam from spilling over the top of the steam generator into the main steam line. Should SG overfill occur, the potential exists to cause a break in the main steam lines. The SONGS 2/3 Emergency Operating Instructions (EOIs) call for operator action to close the feedwater block valves upon reactor trip. This action directly mitigates the dominant overfill scenario at SONGS 2/3. Closure of the feedwater block valves isolates the feedwater regulating valves, but allows flow through the lower capacity feedwater bypass valves.

The closure of the feedwater block valves is a memorized, immediate standard post-trip action. The operators are emphatically trained on this action in both classroom training and in the simulator.

Simulator exercises developed and observed by the IPE human reliability analysis team found that the operating crews immediately isolate the block valve. In scenarios designed to cause a potential overfill, each crew rapidly closed the block valve. Based on NUREG/CR-4772 and the simulator observations, the probability of an operator failing to complete an immediate memorized skill-based action which is backed up by procedure is 0.01.² The CEOG analyses on this topic (Reference 3.4-27) also supports a value of 0.01 for this action.

Main Steam Line Remains Intact

This node represents the potential for SG overfill to lead to a rupture of a main steam line. This event is subject to large uncertainty. In some of the early steam generator overfill analyses, NRC contractors used a highly conservative estimate for this value (0.5). Another NRC analysis on steam generator tube integrity (Reference 3.4-28) estimates the likelihood of steam line break to be very low (on the order of 0.001). The likelihood of multiple steam generator tube rupture was said to be dominated by random steam line breaks and not overfill events. Nevertheless, a conservative estimate for the likelihood of steam line break given overfill of 0.13 is assumed based on Appendix B of NUREG-1218. This reference cites a total of 15 known overfill type events. Damage was known to have occurred in only 2 of the 15 events.

² From NUREG/CR-4772 (Table 8-5, Item 10), an operator error probability of 0.001 is applicable if the action is for a reactor vessel/containment critical parameter and is 1) committed to memory, 2) a skill based action, and 3) backed up by written procedure. In this case, although, it is not a reactor vessel/containment critical parameter, the act of preventing overfill (closure of the feedwater block valve) is the only active, physical action that the secondary board operator must do following a trip. Other than visual verification of system status indicators, this active step is continuously and actively emphasized during training. Although a probability of 0.001 would be appropriate, a conservative value of 0.01 is used.

Break Occurs Inside Containment or Outside MSIVs

Assuming the steam lines fail upon SG overfill, it is necessary to determine whether the break of the steam line occurs in a location that can be easily mitigated. For this analysis, the SONGS 2/3 main steam system is divided into three general regions: inside containment, outside containment/downstream of the MSIVs, and between the containment wall and the MSIV. Should a break occur inside the containment, and the steam generator tubes rupture, the sequence of events is similar to a LOCA with ECCS recirculation available for long term RCS makeup. Should a break occur downstream of the MSIVs, the main steam isolation system would isolate the break before sufficient differential pressure across the steam generator tubes could develop, thus avoiding potential SG tube rupture. Based on IPE analyses, the unreliability of each MSIV is estimated to be less than 0.01. Due to this high reliability, it is not necessary to consider the case of main steam line break downstream of the MSIVs.

The remaining case, a main steam line break occurring in the short segment between the outside containment wall and the MSIV, cannot be isolated by closure of the MSIV. This length of pipe is approximately 15 feet and is considered in the design basis as 'super pipe' (i.e., it is not susceptible to random failures due to the design and inspection requirements placed on the piping).

The CEOG conservatively estimated that the conditional probability of steam line break in such a section to be approximately 0.16 based on the ratio of main steam piping between the containment and MSIVs to the total main steam piping upstream of MSIVs (Reference 3.4-27). This conservative value is used to represent the conditional likelihood of a full guillotine break of the main steam line.

Steam Generator Tubes Remain Intact

This node represents the likelihood of steam generator tubes rupturing due to high primary to secondary differential pressures following a guillotine break of the main steam line. The location of the break analyzed (between the containment wall and the MSIV) is downstream of the flow restrictor (which is designed to limit the rate of steam generator depressurization). Nevertheless, given the high differential pressures potentially present following a steam line break, there is some potential for rupture of the steam generator tubes. Based on the analysis presented in Reference 3.4-28, it is estimated that the conditional probabilities for tube ruptures are as follows:

# of Tubes Ruptured	Conditional Probability
1	0.025
2 or more	0.0255
Total	0.0505

Thus, a value of 0.0505 is used to represent the overall likelihood that the steam generator tubes do not remain intact following a main steam line break.

Only One SG Tube Ruptures

This node represents the likelihood that only one tube ruptures, given a main steam line break. Based on the table above, the likelihood of more than one tube rupturing is 0.05 (0.0255/0.0505).

SDC Initiated Before RWST Depleted

This node represents the potential to avoid core damage by initiating shutdown cooling (SDC) prior to depletion of the RWST inventory. With two simultaneous events diagnosed, a main steam line break and a steam generator tube rupture, the operators would be transferred by the Standard Post Trip Action procedure to the Functional Recovery procedure for further direction. The occurrence of these two events is evident to the operators by the available control room alarms. Low pressure in a single steam generator initiates a main steam isolation signal and alarm indicating a steam line break. High secondary plant radioactivity (as measured by a detector in the steam line just outside the containment and upstream of the break) initiates a corresponding alarm suggesting a possible steam generator tube rupture.

Given these symptoms, the EOIs direct the operators to immediately begin cooldown and depressurization of the RCS to minimize flow out of the broken SG tubes. Subsequent isolation of the faulted SG is initiated when T_H is reduced to below 530°F. For cases with only a single steam generator tube ruptured, SONGS 2/3 thermal hydraulic analysis indicates that many hours (~10 hours) are available for the operators to cooldown and depressurize the RCS to the shutdown cooling limits prior to depleting the RCS makeup source (i.e., RWST). Based on a conservative human reliability analysis, the human error rate for this case is assumed to be 0.05.

For multiple tube ruptures, the minimum time to RWST depletion is approximately 3.7 hours. This is based on the runout flow of the HPSI pumps.³ Based on a procedurally controlled cooldown rate of 100°F per hour, 3.7 hours is sufficient time to reach the shutdown cooling initiation limits. Therefore, a conservative estimate of the human error rate of 0.2 is used for the multiple tube rupture case.

3.4.4.5 Results

The steam generator overfill event tree has two sequences that could lead to core damage: Sequence 6 and Sequence 8. Based on the quantitative bases provided above, the core damage frequency has been conservatively estimated:

Event Tree Sequence	Description	Estimated Core Damage Frequency
6	Steam Generator Overfill With MSLB and Rupture of One Steam Generator Tube	2.6E-8/yr
8	Steam Generator Overfill With MSLB and Rupture of More Than One Steam Generator Tube	1.1E-7/yr
Total Estimated CDF Due to Overfill		1.3E-7/yr

3.4.4.6 Conclusions

The results of the SONGS 2/3 steam generator overfill analysis indicate that a conservative estimate of the total core damage frequency due to overfill events is 1.3E-7/year. This is a very small contributor (~0.4%) to the total core damage frequency of 3.0E-5/year. A more realistic analysis using rigorously developed point estimates would be expected to reduce this frequency to less than 1E-7/yr. Also, the likelihood of a potential significant offsite release through a break in the main steam line (1.3E-7/yr) is a small contributor (~ 3%) to the total significant offsite release frequency for SONGS 2/3 (5E-6/yr) calculated in the IPE. Based on these results, no further plant improvements will be considered.

³ assuming the HPSI pumps are not stopped nor throttled

3.5 References

References for Section 3.1

- 3.1-1 NUREG/CR-4550, Volume 1, "Analysis of Core Damage Frequency: Internal Events Methodology," Revision 1, January 1990.
- 3.1-2 NUREG-1032, "Evaluation of Station Blackout Accidents at Nuclear Power Plants", June 1988.
- 3.1-3 NUREG/CR-4407, "Pipe Break Frequency Estimation for Nuclear Power Plants", May 1987.
- 3.1-4 WASH-1400, "Reactor Safety Study, An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," USAEC, August 1974.
- 3.1-5 ERIN Engineering and Research, Inc., "Severe Accident Issue Closure Guidelines," NUMARC 91-04, January 1992.
- 3.1-6 CEN-152, Combustion Engineering Emergency Procedure Guidelines, Revision 3.
- 3.1-7 Combustion Engineering, "An Evaluation of the RCP Seal Integrity Issue GI-23," NPSD-537, September 1989.
- 3.1-8 Updated Final Safety Analysis Report, San Onofre Nuclear Generating Station, Unit 2, Revision 8.
- 3.1-9 NUREG/CR-4483, "Reactor Vessel Rupture Failure Probability Following Through-Wall Cracks Due to Pressurized Thermal Shock," April 1988.
- 3.1-10 NUREG/CR-3958, " Effects of Control System Failures on Transients, Accidents and Core Melt Frequencies at a Combustion Engineering Pressurized Water Reactor," March 1986.
- 3.1-11 EPRI-6992-L, "A Study of Pipe Failures in U.S. Commercial Nuclear Power Plants", February 1990.
- 3.1-12 Letter from R.M. Rosenblum (SCE) to U.S. NRC, "Reactor Coolant Pump Seals, Requested Information, San Onofre Nuclear Power Generating Station Units 2 and 3," 27 December 1989.
- 3.1-13 NUREG/CR-2815, "Probabilistic Safety Analysis Procedure Guide," dated August 1985.

References for Section 3.3

- 3.3-1 USNRC Generic Letter No. 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR§50.54(f)," dated November 23, 1988.
- 3.3-2 NUREG/CR-2518, "Probabilistic Safety Analysis Procedure Guide," dated August 1985.
- 3.3-3 NUREG/CR-4550, Volumes 1 and 2, "Analysis of Core Damage Frequency: Internal Events Methodology", Revision 1, January 1990.
- 3.3-4 EGG-SSRE-8875, "Generic Component Data Base for Light Water and Sodium Reactor PRAs (NUCLARR)," dated February 1990.
- 3.3-5 Shoreham Nuclear Power Station Probabilistic Risk Assessment, dated June 1983.
- 3.3-6 NSAC/60, "Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3," dated June 1984.
- 3.3-7 IEEE Std. 500-1984, "IEEE Guide to the Collection and Presentation of Electrical, Electronic Sensing Component, and Mechanical Equipment Reliability Data For Nuclear Power Generating Stations," dated December 1983.
- 3.3-8 NUREG/CR-3511, "Interim Reliability Evaluation Program: Analysis of the Calvert Cliffs Unit 1 Nuclear Power Plant," dated March 1984.
- 3.3-9 Oak Ridge National Laboratory In-Plant Reliability data Systems for Pumps, Valves and Electrical Equipment (NUREG/CR-2886, NUREG/CR-3154, NUREG/CR-3831).
- 3.3-10 Reliability Data Base for ALWR PRAs, Annex D.
- 3.3-11 NPRDS Component Failure Analysis Report Training Manual.
- 3.3-12 NUREG/CR-4772, "Accident Sequence Evaluation Program (ASEP): Human Reliability Analysis Procedure," February 1987.
- 3.3-13 NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," August 1983.
- 3.3-14 NUREG-1335, "Individual Plant Examination: Submittal Guidance, Final Report," dated August 1989.

- 3.3-15 SONGS 2/3 IPE Project Instruction PI-007, "Human Reliability Analysis," April 1991.
- 3.3-16 EPRI NP-3967, "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," June 1985.
- 3.3-17 Sections 3.4 and 10.4.5, SONGS 2/3 Updated Final Safety Analysis Report (UFSAR), Revision 8.
- 3.3-18 "Internal Flood Frequencies during Shutdown and Operation for Nuclear Power Plants," N. O. Siu, et al., prepared for Public Service of New Hampshire, Pickard, Lowe and Garrick, Inc., PLG-0624, May 1988.
- 3.3-19 "San Onofre Units 2 and 3, Evaluation of Interfacing System Loss of Coolant Accident (ISLOCA)", Revision 0, June 1992.
- 3.3-20 "San Onofre Units 2 and 3, IPE Internal Flood Analysis," Revision A, July 1992.
- 3.3-21 NUREG-1407, "Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, Final Report," dated June 1991.
- 3.3-22 Reactor Safety Study: An Assessment of Accident Risks on U.S. Commercial Nuclear Power Plants, U.S. Nuclear Regulatory Commission, NUREG 75/014, WASH-1400, October 1975.
- 3.3-23 NUREG-0452, "Standard Technical Specifications for Westinghouse Pressurized Water Reactors," Revision 4, Fall 1981.

References for Section 3.4

- 3.4-1 USNRC Generic Letter No. 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities - 10 CFR§50.54(f)," dated November 23, 1988.
- 3.4-2 NUREG-1335, "Individual Plant Examination: Submittal Guidance, Final Report," dated August 1989.
- 3.4-3 U.S. Nuclear Regulatory Commission, Unresolved Safety Issues Summary, "Aqua Book", NUREG-0606, Vol. 7, No. 3, August 16, 1985.

- 3.4-4 "Regulatory and Backfit Analysis: Unresolved Safety Issue A-45, Shutdown Decay Heat Removal and Requirements", Nuclear Regulatory Commission, NUREG-1289, September 1988.
- 3.4-5 "Shutdown Decay Heat Removal Analysis of a Westinghouse 2-Loop Pressurized Water Reactor. Case Study," NUREG/CR-4458, SAND86-2496, Sandia National Laboratories, March 1987.
- 3.4-6 "Shutdown Decay Heat Removal Analysis of a Westinghouse 3-Loop Pressurized Water Reactor. Case Study," NUREG/CR-4762, SAND86-2377, Sandia National Laboratories, March 1987.
- 3.4-7 "Shutdown Decay Heat Removal Analysis of a Babcock and Wilcox Pressurized Water Reactor. Case Study," NUREG/CR-4713, SAND86-1832, Sandia National Laboratories, March 1987.
- 3.4-8 "Shutdown Decay Heat Removal Analysis of a Combustion Engineering 2-Loop Pressurized Water Reactor. Case Study," NUREG/CR-4710, SAND86-1797, Sandia National Laboratories, July 1987.
- 3.4-9 "Shutdown Decay Heat Removal Analysis of a General Electric BWR3/Mark I, Case Study," NUREG/CR-4448, SAND85-2373, Sandia National Laboratories, March 1987.
- 3.4-10 "Shutdown Decay Heat Removal Analysis of a General Electric BWR/4 Mark I Case Study," NUREG/CR-4767, SAND86-2419, Sandia National Laboratories, July 1987.
- 3.4-11 "BWR Decay Heat Removal System Appraisal", EPRI NP-0861, Science Applications International Company, August 1978.
- 3.4-12 "Brunswick Decay Heat Removal Probabilistic Safety Study", NSAC-083, Nuclear Safety Analysis Center, October 1985.
- 3.4-13 NUREG/CR-1556, "Study of Alternate Decay Heat Removal Concepts for Light Water Reactors - Current Systems and Proposed Options", Sandia National Laboratories, April 1981.
- 3.4-14 NUREG/CR-2883, "Study of the Value and Impact of Alternative Decay Heat Removal Concepts for Light Water Reactors", Sandia National Laboratories, Vol. 1, June 1983.

- 3.4-15 NUREG/CR-2883, "Study of the Value and Impact of Alternative Decay Heat Removal Concepts for Light Water Reactors", Sandia National Laboratories, Vol. 2, June 1983.
- 3.4-16 NUREG/CR-2883, "Study of the Value and Impact of Alternative Decay Heat Removal Concepts for Light Water Reactors", Sandia National Laboratories, Vol. 3, June 1983.
- 3.4-17 NUREG/CR-3713, "Grouping of Light Water Reactors for Evaluation of Decay Heat Removal Capability", Brookhaven National Laboratories, June 1984.
- 3.4-18 NUREG/CR-2182, "Loss of DHR Sequences at Browns Ferry Unit One - Accident Sequence Analysis", Oakridge National Laboratory, Vol. 1, November 1981.
- 3.4-19 NUREG/CR-2973, "Loss of DHR Sequences at Browns Ferry Unit One - Accident Sequence Analysis", Oakridge National Laboratory, April 14, 1983.
- 3.4-20 NSAC-088, "Residual Heat Removal Experience Review and Safety Analysis BWR," Nuclear Safety Analysis Center, July 1985.
- 3.4-21 NSAC-157, "Residual Heat Removal Experience Review and Safety Analysis - 1984-1989 - Boiling Water Reactors", Nuclear Safety Analysis Center, January 1991.
- 3.4-22 Generic Letter 89-19, Request For Action Related to Resolution of Unresolved Safety Issue A-47 "Safety Implications of Control Systems in LWR Power Plants" Pursuant to 10 CFR 50.54 (f), Sept. 20, 1989.
- 3.4-23 Unresolved Safety Issue A-47, "Safety Implications of Control Systems in LWR Power Plants."
- 3.4-24 NUREG/CR-1217, "Evaluation of Safety Implications of Control Systems in LWR Power Plants" - Technical Findings Related to USI A-47, November 1988, Final Report.
- 3.4-25 NUREG/CR-3958, "Effects of Control System Failures on Transients, Accidents and Core Melt Frequencies at a Combustion Engineering Pressurized Water Reactor," March 1986.
- 3.4-26 NUREG/CR-1218, Regulatory Analysis For Resolution of USI A-47, "Safety Implications of Control Systems in LWR Power Plants," November 1988, Final Report.

- 3.4-27 Letter from P.W. Richardson, Jr. (Assistant Project Manager - CEOG/ABB) to CEOG/Severe Accident Working Group, "CEOG/NRC Meeting on S/E Overfill Protection (GL89-19); November 20, Forwarding of Summary," November 27, 1990.
- 3.4-28 NUREG-0844, "NRC Integrated Program for the Resolution of Unresolved Safety Issues A-3, A-4, and A-5 Regarding Steam Generator Tube Integrity," September 1988, Final Report.

4.0 BACK-END ANALYSIS

The main objective of performing the SONGS 2/3 Back-end analysis, as described in NUREG-1335, was to provide a framework for understanding containment failure modes, the impact of controlling phenomena, key plant systems and features, and important operator actions that affect containment performance, and to identify specific vulnerabilities, if any, to severe accidents associated with the containment and containment mitigating systems.

The Front-end analysis identified the dominant sequences that contribute to core damage. The Back-end analysis involves analyzing representative sequences to determine the timing and nature of any radionuclide releases to the environment. This task requires gathering information relative to the SONGS 2/3 containment design, modeling the response of the containment systems, assessing the potential controlling phenomena, and modeling the physical processes that control the transport of fission products to the environment.

Because SONGS Units 2 and 3 are essentially identical, the Front-end analysis resulted in a single core damage quantification that applies to both units. Similarly, there are no differences between SONGS Units 2 and 3 that would impact the Back-end results. The source term analysis is based on the Front-end results and is valid for both SONGS units.

Although the IPE mission time is 24 hours, the Back-end analysis simulated accident sequences over 48 hours to provide greater understanding of containment performance during the later stages of a scenario. It should be recognized that the Front-end modeling assumptions do not apply beyond 24 hours since sufficient time would be available for additional recovery actions that are not credited in the current IPE. This is consistent with other industry PRAs.

4.1 Plant Data and Plant Description

The SONGS 2/3 containment structure, along with those containment systems important to the containment and source term analysis, are described below. Detailed plant-specific data are used to model containment features in order to realistically evaluate the containment response to a core damage accident. A review of plant drawings was supplemented by an extensive containment walkdown performed during a refueling outage.

4.1.1 Containment Structure

SONGS 2/3 employs a large, dry containment design. Figures 4.1-1 and 4.1-2 illustrate two vertical sections of the containment as adapted from the General Arrangement drawings. The containment structure is a horizontally and vertically prestressed, post-

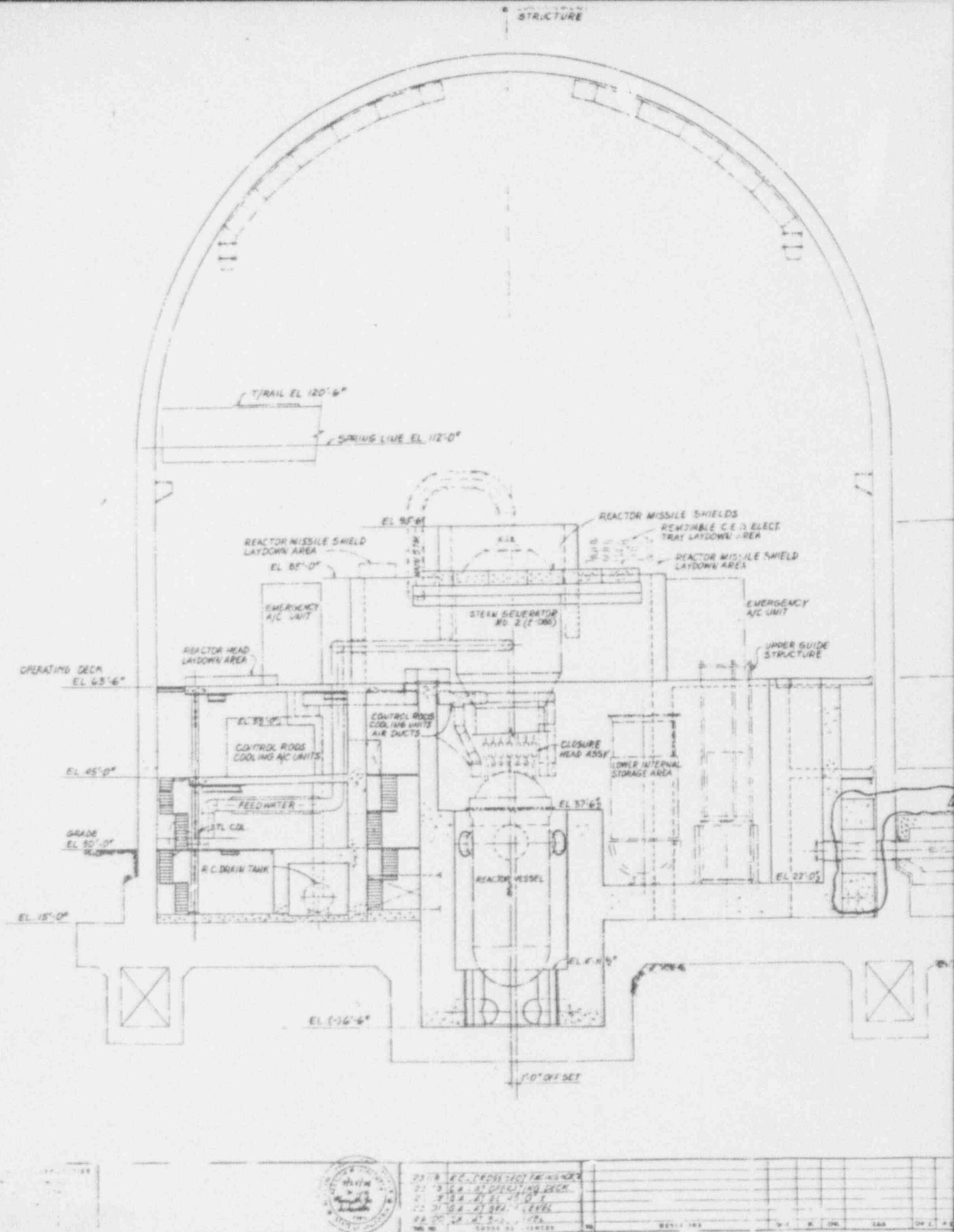
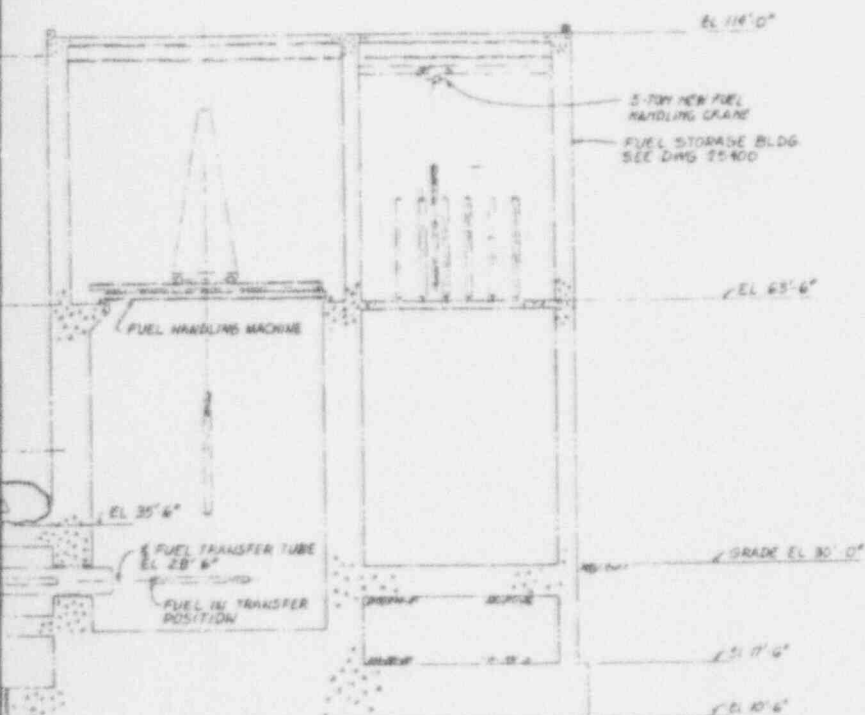


Figure 4.1-2 Containment, vertical section facing north (adapted from Bechtel drawing 23105-3).

Also Available On
Aperture Card



08-1

[illegible]

23109-2

9305040247-02

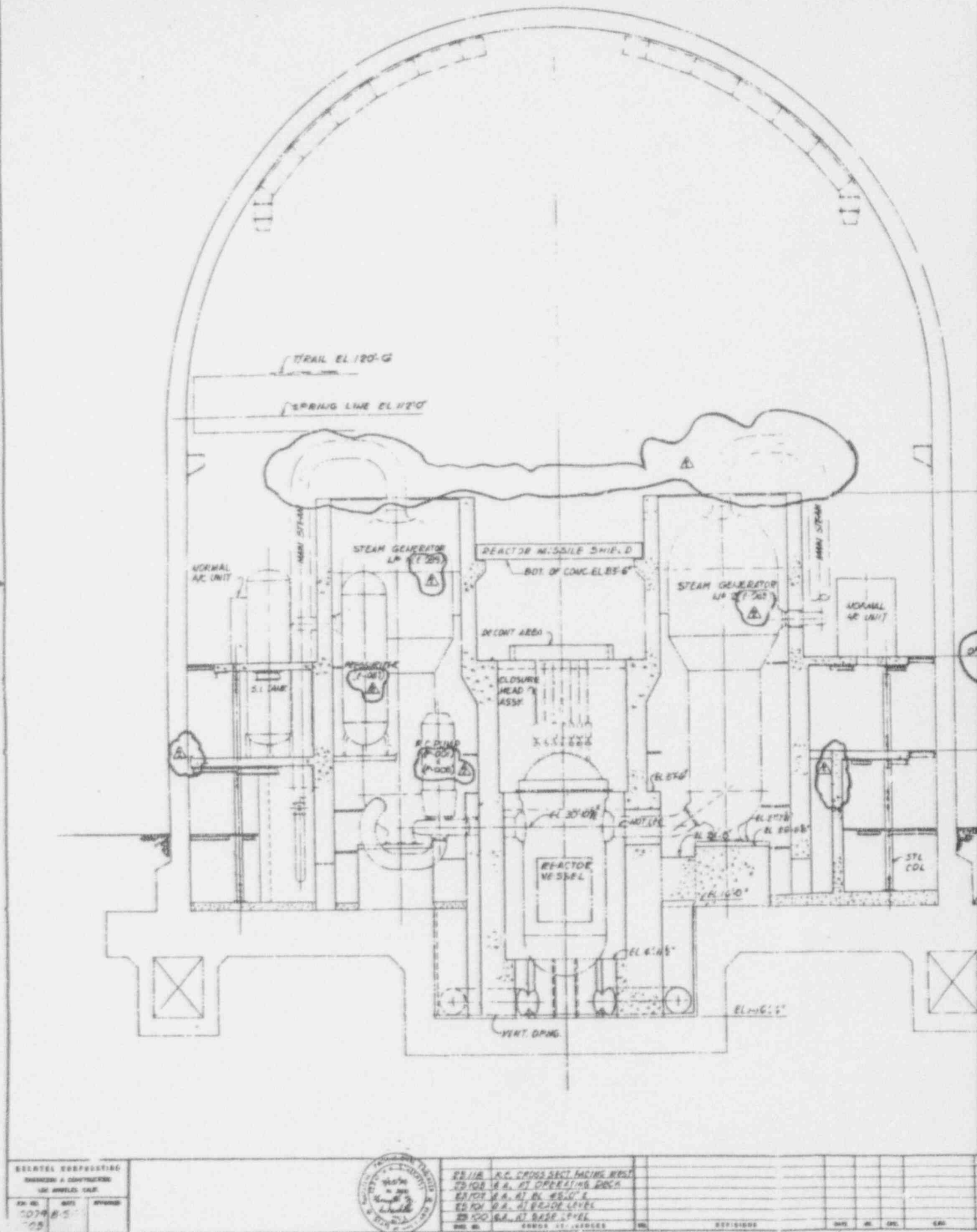


Figure 4.1-1 Containment, vertical section facing west (adapted from Bechtel drawing 23104-2).

SI APERTURE CARD

Also Available On
Aperture Card

WALL EL 95'-0"

ATING DECK EL 95'-0"

LOOR EL 48'-0"

RADE EL 30'-0"

CONC EL 15'-0"

UNIT-2

REVISIONS										SAR PHOTO NUCLEAR GENERATING STATION									
1	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
3	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
4	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
5	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
6	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
7	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
8	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
9	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
10	REVISED CONC WALL ON AIR DUCT	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

CONTAINMENT INTERIOR STRUCT.
GENERAL ARRANGEMENT
CROSS SECTION FACING WEST
SOUTHERN CALIFORNIA Edison COMPANY
SCALE 1/8" = 1'-0"

23204-2

9305040247-03

tensioned concrete cylinder resting on top of a reinforced concrete slab and closed at the top by a prestressed, post-tensioned concrete dome. The containment free volume is approximately 2.3×10^6 ft³. The interior of the containment is lined with a 1/4 in. carbon steel liner plate. The reactor pressure vessel (RPV) is located so that the bottom of the vessel (elevation 1 ft 11 in.) is below the lowest floor of the containment (elevation 15 ft 0 in). Principal nominal dimensions of the containment building are shown in Table 4.1-1.

The MAAP code (Reference 4.1-1) is used in the SONGS 2/3 IPE to model the core damage phenomena and containment response. In MAAP terminology, the large containment volume above the operating deck (at the 63 ft 6 in elevation), is referred to as the "upper compartment." The "lower compartment" is that portion of the containment, between the containment floor (15 ft 0 in elevation) and the operating deck, which is inside the secondary shield wall but outside the reactor shield wall (that is, the primary shield wall). The "annular compartment" is the part of containment below the operating deck but outside the secondary shield wall.

The open design and significant venting areas for the subcompartments within the SONGS 2/3 containment help ensure a well-mixed atmosphere, a feature which inhibits combustible gas pocketing. Steel grating around the periphery of the operating deck provides a flow path between the annular and upper compartments. The "lower and upper compartments" communicate through large openings around the steam generators and above the reactor coolant pumps. The "lower and annular compartments" communicate through four manways on the 15 ft 0 in. elevation (containment floor level). Other manways at elevations 30 ft 0 in. and 45 ft 0 in. provide additional communication between the "lower and annular compartments".

The SONGS 2/3 containment is laid out such that the two primary system loops are located inside the secondary shield wall near the bottom of the lower compartment. Each of these primary loops contains 2 cold leg pipes and 1 hot leg pipe. The two steam generator enclosures extend approximately 25 ft above the operating deck into the "upper compartment". These enclosures contain the two steam generators, the pressurizer, and the quench tank. The safety injection tanks are located outside the secondary shield and steam generator enclosure walls at the 45 ft 0 in. elevation in the annular compartment. The emergency recirculation sump is also located outside the secondary shield wall, in the floor of the annular compartment.

The configuration of the reactor cavity and lower compartment is illustrated in Figures 4.1-1 and 4.1-2 and is shown schematically in Figure 4.1-3. The reactor cavity has a floor area of about 728 ft². Note that there are no lower head penetrations in the SONGS 2/3 reactor vessel since the incore instrumentation does not

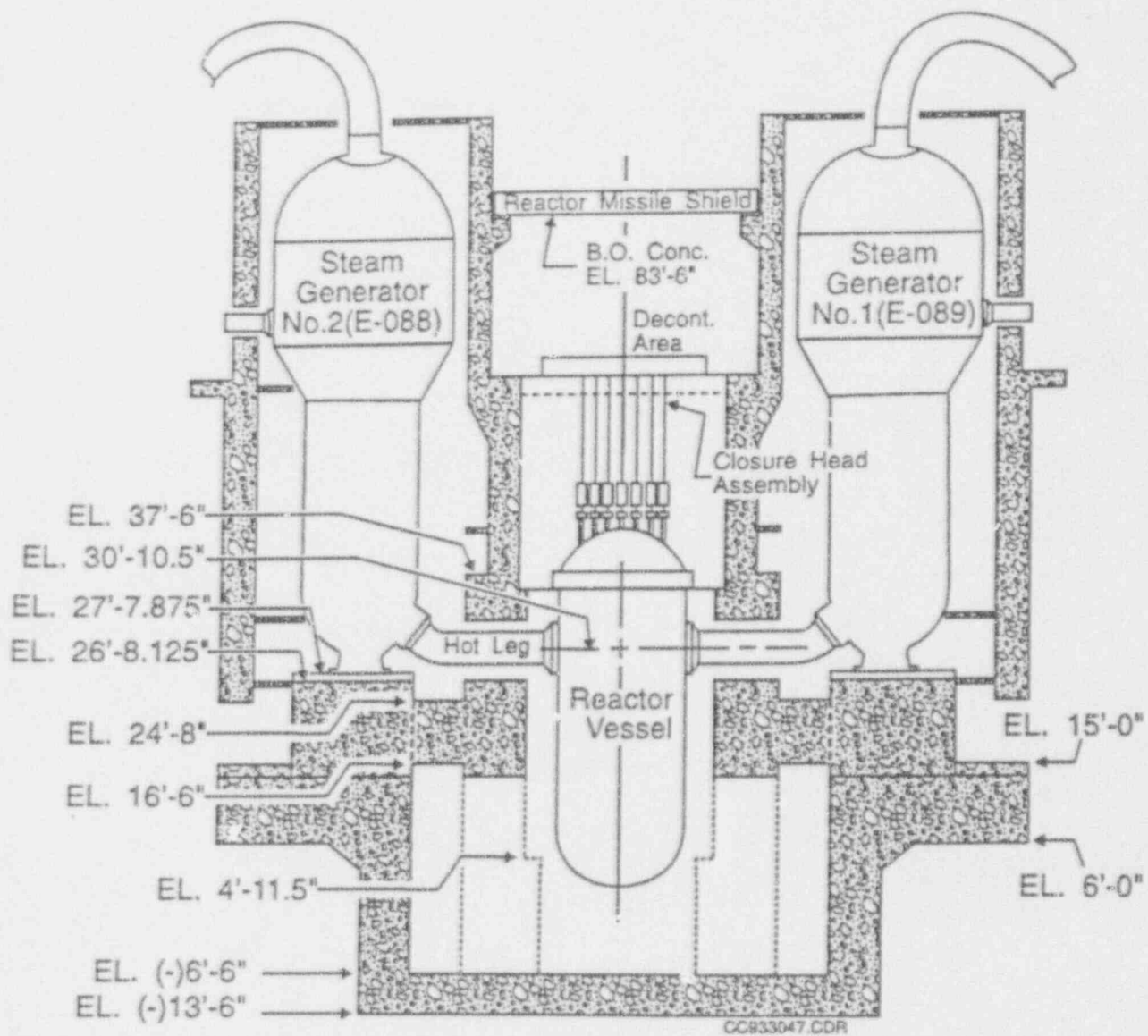
Table 4.1-1

SUMMARY OF SONGS CONTAINMENT DATA

Type	Combustion Engineering Large Dry
Architect/Engineer	Bechtel
Design Pressure	60 psig
Design Temperature	300°F
Internal Free Volume (Minimum)	$2.305 \times 10^6 \text{ ft}^3$
(Maximum)	$2.366 \times 10^6 \text{ ft}^3$
Interior Diameter	150 ft
Interior Height	172 ft
Height to Spring Line	97 ft 0 in.
Cylinder Wall Thickness	4 ft 4 in.
Dome Thickness	4 ft 0.5 in.
Liner Plate Thickness	1/4 in.
Base Slab Thickness	9 ft 0 in.
Cavity Floor Thickness	7 ft
Cavity Floor Area	728 ft ²
Cavity Floor to Vessel Bottom	6.91 ft

Figure 4.1-3

CONFIGURATION OF THE REACTOR CAVITY AND LOWER COMPARTMENT



enter the vessel from below. Figure 4.1-1 also illustrates the reactor cavity cooling ducts. The cavity ducts are designed to draw relatively cool air from the steam generator enclosures and discharge it at the reactor cavity floor (-6 ft 6 in elevation). Air circulation fans, located atop the cavity cooling duct inlets in the lower compartment, are not expected to function during a severe accident and are not credited in the IPE. Figure 4.1-4 shows a plan view of the four cavity cooling ducts. The configuration of the reactor cavity and cavity cooling ducts is an important feature of the SONGS 2/3 containment because it provides an effective structural barrier to debris entrainment from the cavity.

The SONGS containment does not facilitate flooding of the reactor cavity. Although water can easily drain from the upper compartment to the annular and lower compartment floors, the water on the lower compartment floor would have to reach a depth of 12.9 ft before it could spill into the reactor cavity through the cavity personnel hatch or the cavity ventilation ducts. This is unlikely to occur at SONGS 2/3, even during a severe accident in which the entire usable RWST volume (360,000 gal) is injected into the containment. On RPV failure, water injected into the RPV could enter the reactor cavity through the opening in the failed reactor vessel. If sufficient water is injected, the cavity will fill with water and the excess water will spill into the lower containment compartment. When the depth of water in the lower compartment exceeds approximately 6 inches, water will start to accumulate on the annular compartment floor and fill the containment emergency recirculation sump. Recirculation of water from the containment emergency sump through the HPSI and containment spray (CS) systems is possible when the NPSH requirements of the HPSI and CS recirculation systems are met.

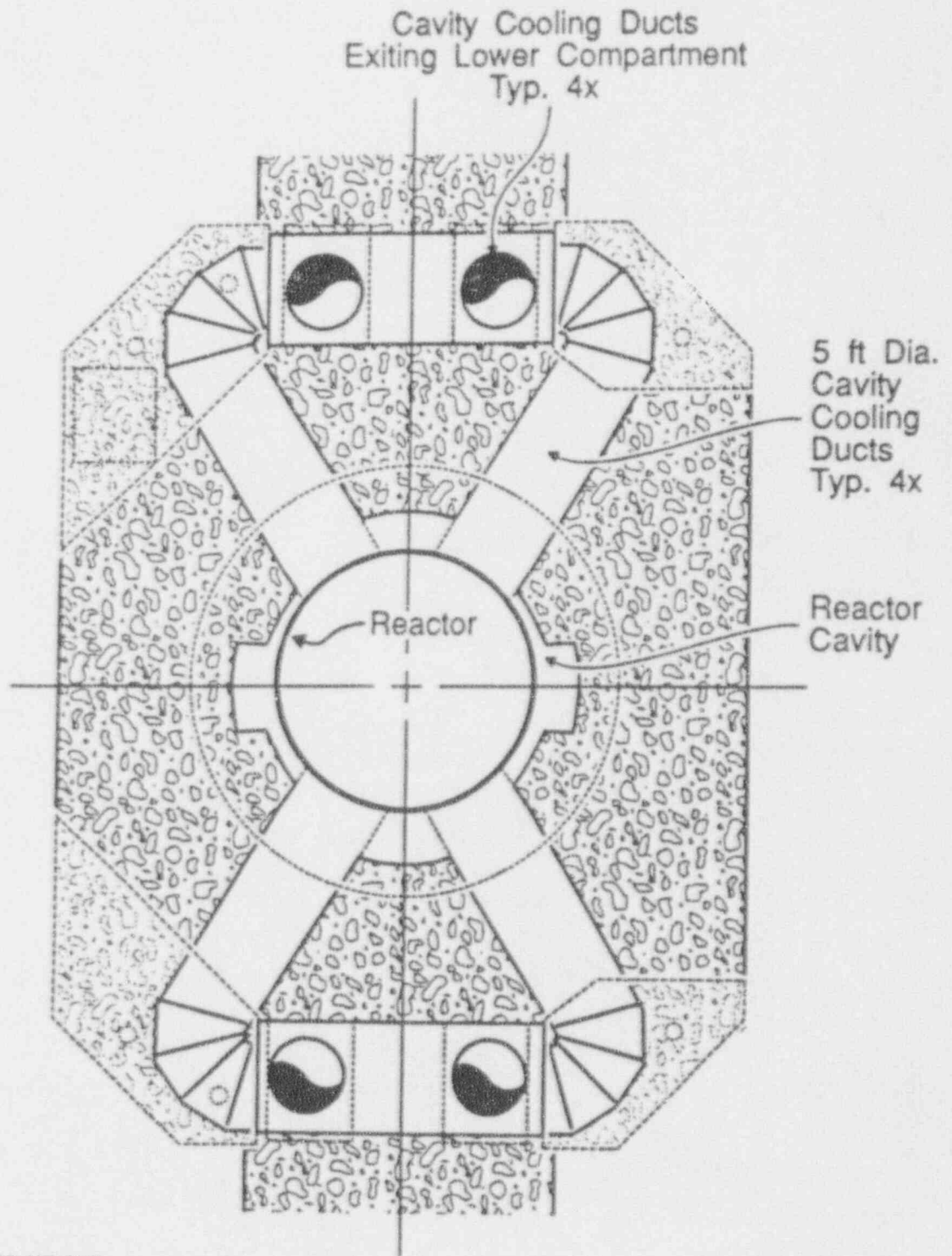
Personnel access to the containment is normally provided through an airlock with interlocked doors. This personnel access hatch is located in the upper compartment at elevation 62 ft 7 in (bottom of penetration). The equipment hatch and emergency personnel hatch are located in the annular compartment (i.e., lower containment) at elevations 28 ft 6 in and 32 ft 10.5 in respectively. These three access hatches are all fitted with non-metallic gaskets, employ double gasketed flanges, and contain provisions for leak testing of the flange gasket seal.

Single barrier piping penetrations are provided for all pipes passing through the SONGS 2/3 containments. Closure of these piping penetrations is provided by special flued welds which attach the process piping and penetration sleeve to the containment liner.

Two electrical penetration assembly (EPA) configurations are used for all SONGS 2/3 electrical conductors passing through the containment wall. The method of sealing the electrical

Figure 4.1-4

PLAN VIEW OF CAVITY AND CAVITY COOLING DUCTS



RA920075.CDR

penetrations depends on the type of cable and connector assemblies involved. A canister type assembly is used for medium voltage power circuits (6900 volts), whereas a modular-type assembly is used for the low voltage power circuits (600 volts and below). Insulated conductors passing through the header plate of a canister type penetration are potted to effect a pressure seal. Mechanical splices within the potting compound provide gas stops. High voltage insulating bushings and seals also contribute to the gas barrier. The modular type assemblies consists of a header plate in which a group of small, interchangeable modular penetrations fit. The header plate of this type of penetration mates with a flange welded to the penetration and bolted to a flange welded to the penetration sleeve. Double silicone O-rings provide a monitorable seal between the assembly's header plate and the penetration sleeve's flange.

The mechanical and electrical penetrations at the SONGS 2/3 containment employ: 1) metallic gaskets or seals which are not susceptible to thermal degradation due to containment gas temperatures and 2) non-metallic gaskets which can withstand containment temperatures up to and beyond 486°F.

4.1.2 Containment Systems

The SONGS 2/3 containment heat removal design includes two containment spray trains with heat exchangers and four containment emergency fan coolers (CEFCs). The containment spray system, in the recirculation mode, and the emergency fan cooler system are both designed for long term containment heat removal during a design basis accident (DBA) event. The HPSI recirculation system at SONGS 2/3, while capable of removing heat from the reactor vessel, is not able to remove heat from the containment due to the absence of heat exchangers. Brief descriptions of the containment spray system, the CEFCs and HPSI recirculation are provided in the following paragraphs. For further details on these systems refer to Section 3.2 of this report.

Containment Spray (CS) System

The CS system provides a means for injecting water into the containment. The CS system initially takes suction from the RWST and injects into the containment through spray headers located under the containment dome. The spray system provides both a potential pressure suppression mechanism and a means to remove fission products from the containment atmosphere.

At the RWST low level alarm, the switchover of the HPSI pumps and the CS pumps to recirculation mode is initiated. When the CS system is in the recirculation mode, the spray pumps take suction from the containment sump and discharge to the spray header. Heat exchangers located between the CS pumps and the spray headers are capable of removing decay heat from the sump water before the

water returns to the containment through the spray header. The CS system is shown schematically in Figure 4.1-5.

Containment Emergency Fan Coolers

Four emergency fan cooling units are located on the operating deck at the 63 ft 6 in. elevation in the upper containment. These units are located above the annular compartment and are approximately 90 degrees apart. During an accident, these cooling units take air suction from the region immediately above the operating deck and discharge to the bottom of the containment building through four concrete ducts. Each of the CEFCs discharge ducts has two different sizes of outlets, large and small. The four smaller (i.e., secondary) outlets are located along the inside wall of the annular compartment approximately 6 ft above the containment floor and are above the normal containment flooding height. The four larger (i.e., primary) CEFC outlets are located along the outside wall of the lower compartment. These four large discharge openings differ in size but generally extend between approximately 0.5 ft and 7.0 ft above the containment floor. Cool air discharged through the CEFC outlets in the lower compartment is forced to circulate upward and around the reactor coolant pumps and steam generators and then flows upward through openings in the steam generator and pressurizer enclosures to the upper containment.

The smaller CEFC discharge outlets in the annular compartment are located above the maximum calculated post LOCA water elevation. The bottom of the large CEFC discharge outlets in the lower compartment are close to the containment floor. These large air discharge outlets are provided with a backdraft damper and are protected with flood walls that extend 7 inches above the maximum calculated LOCA flood level of 24 feet 5 inches. In addition to the flood walls, there are umbrellas at large discharge outlets that prevent flooding from containment spray. The CEFCs are shown schematically in Figure 4.1-6.

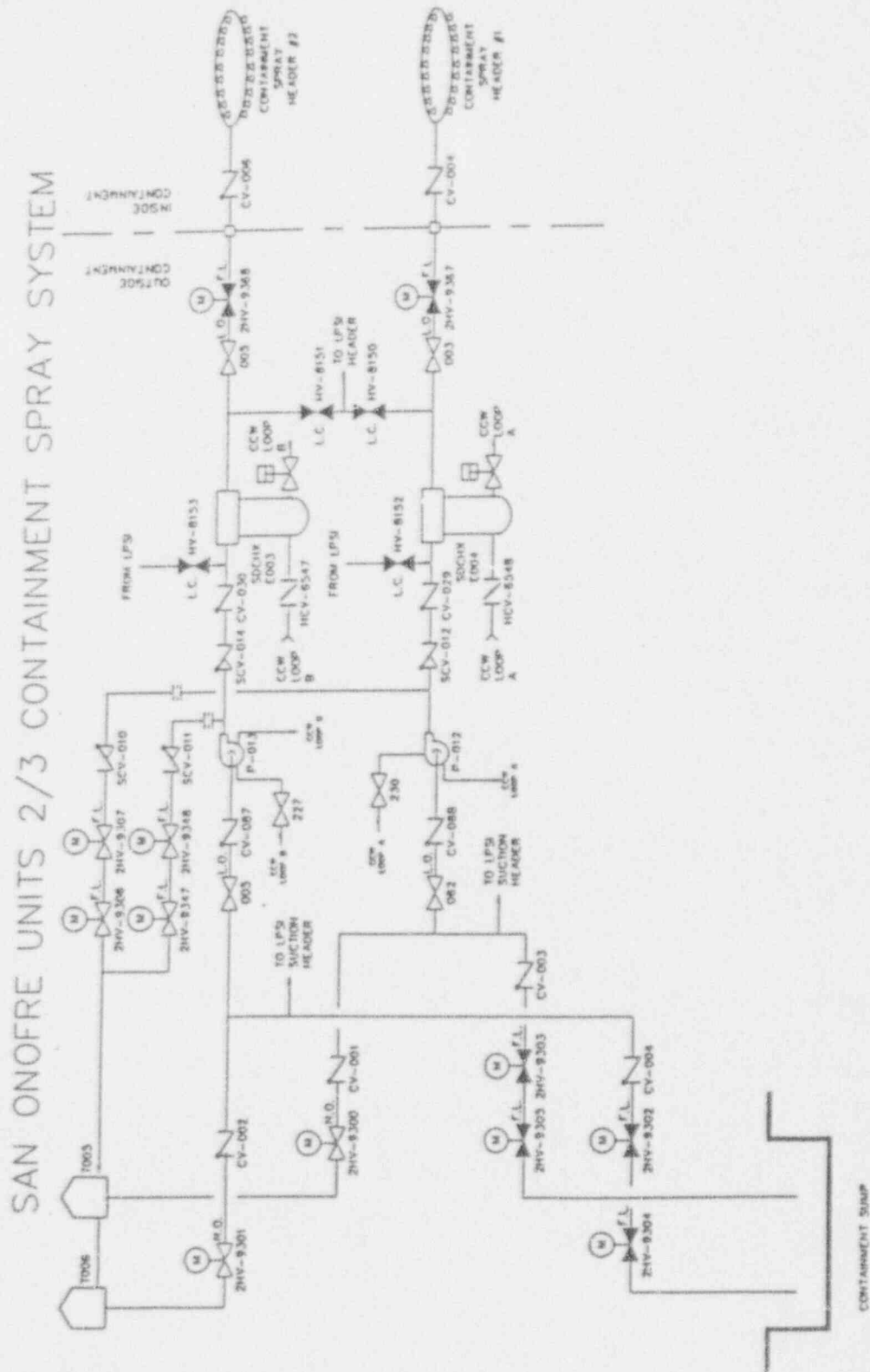
HPSI Recirculation System

During the emergency core cooling recirculation mode, the HPSI pumps take suction from the containment sump and discharge into the primary system cold leg piping. As indicated previously, there are no heat exchangers in the high pressure recirculation loops. As a result, while this system can remove decay heat from the reactor vessel and deposit it in the containment, it cannot remove decay heat from the containment. Only containment spray recirculation and the CEFCs can remove decay heat from the containment during a severe accident.

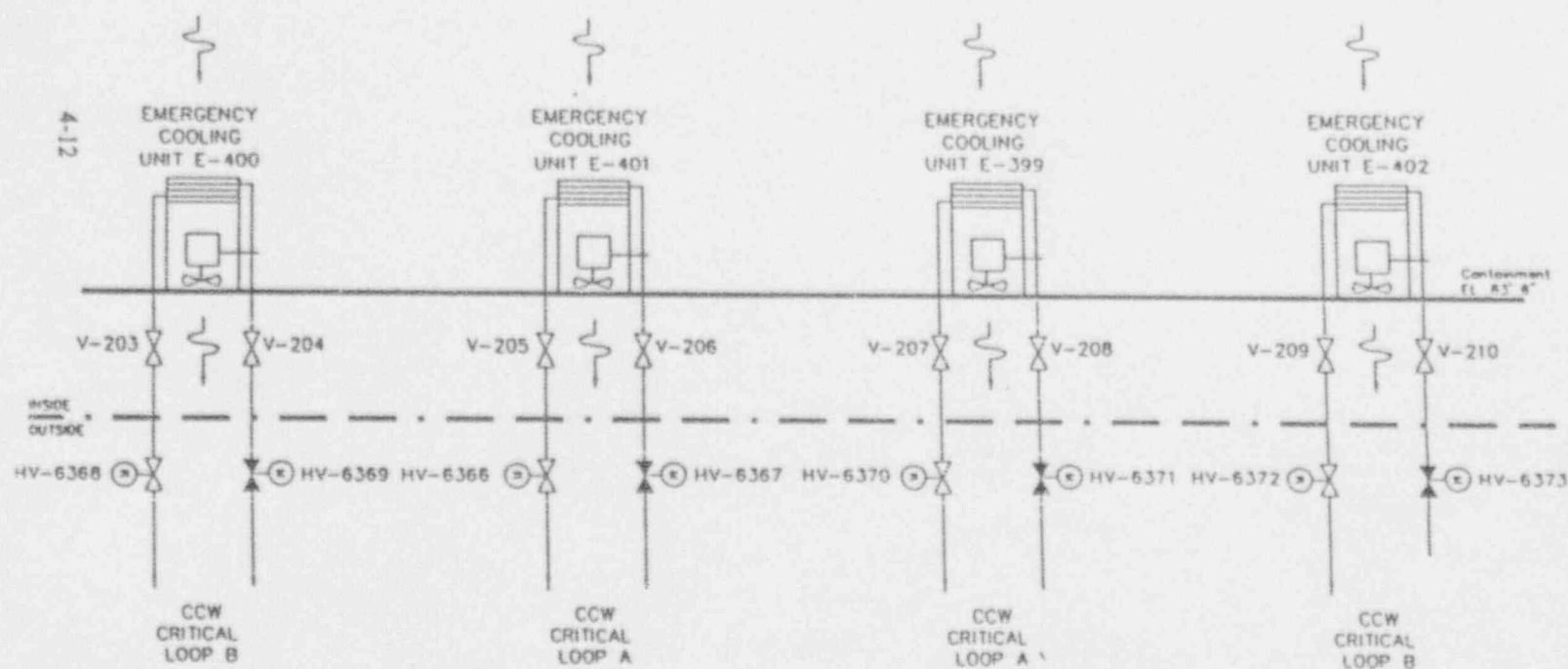
The two suction lines from the containment sump and the four sump isolation valves are shared by both the HPSI recirculation and CS recirculation systems before the piping of these systems diverge.

Figure 4.1-5

CONTAINMENT SPRAY SYSTEM SCHEMATICS



SAN ONOFRE UNITS 2/3 CONTAINMENT EMERGENCY COOLING SYSTEM



CONTAINMENT EMERGENCY FAN COOLER SYSTEM SCHEMATICS

Figure 4.1-6

Common cause failure of the sump isolation valves to open is the major reason for failure of both the HPSI recirculation and CS recirculation systems. The HPSI System is shown in Figure 3.2-5.

In addition to the containment structure and containment systems discussed in Section 4.1.1 and 4.1.2, additional plant drawings can be found in Appendix A. These drawings include:

- o Location of containment spray nozzles
- o Location of containment emergency fan coolers, including schematic air flow path and air duct layout
- o Location of containment sumps
- o Location of major containment penetrations e.g., equipment hatch, personnel airlock, etc.
- o Relation of containment building to safety equipment building
- o Location of major ECCS components
- o Personnel access to reactor cavity

4.1.3 Containment Data

A modified version of MAAP PWR 3.0B Revision 19.01 was used in the SONGS 2/3 IPE to provide an integrated approach to modeling of plant and containment thermal-hydraulic response and fission product behavior during core damage accidents. MAAP requires plant-specific input data which are compiled into a MAAP parameter file. The SONGS 2/3 parameter file provides a complete, realistic description of SONGS 2/3 for a MAAP simulation, and its data remain identical for all accident sequences. This SONGS 2/3 parameter file and its supporting documentation are included in the SONGS 2/3 Containment Data Collection Notebook.

4.2 Plant Models and Methods for Physical Processes

The SONGS 2/3 containment and source term analysis is part of the traditional Level II analysis. It includes plant models and physical processes which reflect the overall plant behavior following core damage. This is accomplished by coupling a probabilistic assessment of containment response to postulated initiating events with a physical model to examine plant response. Sequences with initiating events which are dominant contributors to plant risk and other sequences judged to be of interest are evaluated through this process. This process also incorporates the impact of phenomenological uncertainties.

The Level II probabilistic models are embodied in the Extended Event Trees (EETs) which consider the systems, operator actions, and containment functional events that are required to respond to a core damage event and to prevent or mitigate the release of radioactive fission products from the containment. The plant physical model is defined in the MAAP parameter file, as discussed in Section 4.1.3. This parameter file provides MAAP with information required by the code to perform calculations of plant

specific fission product transport and thermal hydraulic response to postulated accident sequences. It is also used to study the sensitivity of the source term to phenomenological uncertainties. The source term analysis used default values for MAAP model parameters (Reference 4.1-1). The sensitivity analysis (Section 4.7.4) identifies any variations from this approach. The MAAP analyses are supplemented with phenomenological evaluation summaries to provide a complete physical representation of SONGS 2/3.

Results obtained with the probabilistic and physical plant models are closely linked. For instance, the EET structure depends on MAAP analyses to 1) define EET nodal success criteria and 2) determine the accident sequence outcome. Furthermore, sequences demonstrated by the quantification task to be either dominant contributors to the overall core damage frequency or of structural interest become the basis for MAAP calculations in support of the source term analysis. Finally, MAAP analyses and phenomenological evaluation summaries are used to investigate the effect of phenomenological uncertainties on the source term assessment. The use of MAAP as suggested above provides the necessary deterministic complement to the probabilistic assessment. A discussion of the extended event tree models is provided in Section 4.3, along with the EETs themselves. The treatment of key phenomenological issues is described briefly below and detailed further in Section 4.4 of this submittal.

The SONGS 2/3 IPE project utilizes a modified version of MAAP PWR 3.0B Revision 19.01 to perform the containment and source term analysis. This version of the 19.0 code included planned modifications for the cavity and fan coolers. These changes enhanced the realism of the SONGS IPE source term calculations.

Source term analyses are performed following accident sequence quantification and designation of plant damage states. Plant damage states that are representative of containment performance have their source terms quantified by SONGS 2/3 MAAP analyses. The purpose of the source term analysis is to define and quantify the radionuclide release characteristics for a given accident sequence, including specification of containment failure timing and fission product release magnitudes. MAAP calculations provide release magnitudes for selected fission product groups, release timing, and associated energy rates.

Since assumptions regarding key severe accident phenomena may dictate the analysis outcome, due consideration of phenomenological uncertainties is essential to the containment and source term analysis. The SONGS 2/3 IPE methodology addresses the phenomenological issues through plant-specific phenomenological evaluations and MAAP sensitivity studies. This two prong approach provides a bounding assessment of source term release timing and magnitude.

SONGS 2/3 phenomenological evaluation summaries are the principle means of addressing the impact of phenomenological uncertainties on plant response. These evaluation summaries address a wide range of phenomenological issues and provide an in-depth review of plant specific features which influence the uncertainty or act to mitigate the consequences of such phenomena. The phenomenological evaluation summaries investigate both the likelihood of occurrence and the probable consequences of key severe accident phenomena.

The phenomenological evaluation summaries are supported by plant specific calculations, available experimental information from open literature, as well as information which has been developed using the FAI experimental facilities. Results of the FAI experimental efforts are incorporated into the appropriate phenomenological evaluation summaries.

The purpose of sensitivity studies is to determine which remaining phenomenological uncertainties have a significant impact on the likelihood or timing of containment failure and the magnitude of the source term release. In performing SONGS 2/3 MAAP calculations, a limited number of model parameters are investigated with respect to the influence of modeling uncertainties on the radionuclide source terms. In particular, uncertainties in the various physical processes are considered as documented in the IDCOR/NRC issue resolution process. The various phenomena and the uncertainties were described in letters from T. Speis of the NRC to A. Buhl of IT Corporation (References 4.2-1, 4.2-2, 4.2-3). GL 88-20 and NUREG-1335 provide summaries of those parameters that have been judged to have a significant effect on containment failure and source terms. Section 4.7.4 of this document provides a detailed review of the Level II SONGS 2/3 IPE sensitivity analysis methods and results.

In summary, the integrated approach to the assessment of total plant response adopted in the SONGS 2/3 IPE program links together probabilistic models in the EETs with physical plant models contained within MAAP. These models are supplemented through the use of SONGS 2/3 phenomenological evaluation summaries to provide in-depth technical arguments which reduce phenomenological uncertainties and examine realistic plant response to severe accident phenomena. Figure 4.2-1 provides an overview of the SONGS 2/3 Level II IPE process.

4.3 Bins and Plant Damage States

4.3.1 Level II Event Trees

The objective of developing the Level II event trees is to provide a systematic framework for displaying the sequence of events and spectrum of containment response to a severe accident. The end states and the frequencies of the Level II sequences form the basis for binning of like sequences to perform the source term

SONGS Level II Methodology

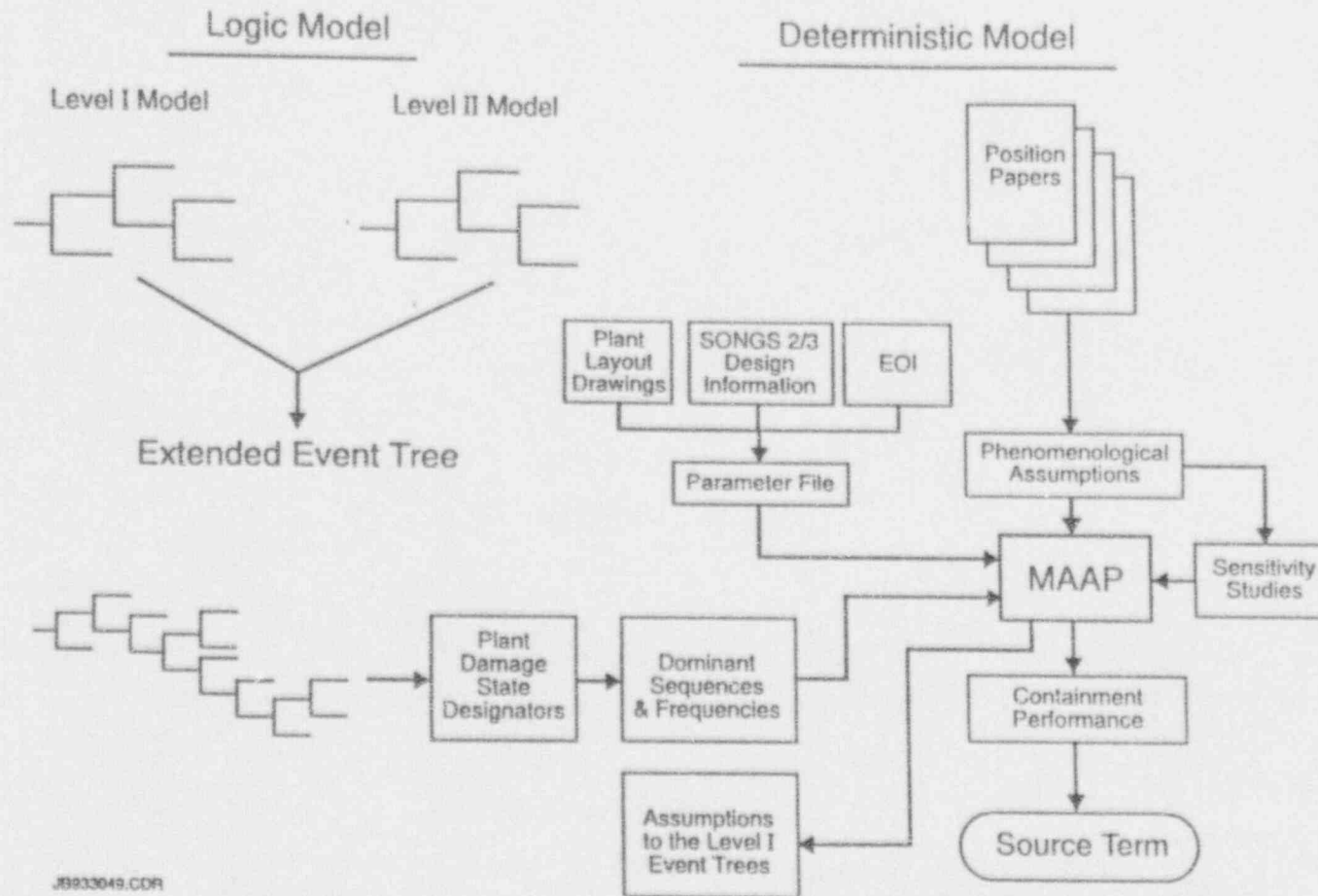


Figure 4.2-1

SONGS LEVEL 2 METHODOLOGY

analysis. The containment damage status provides a measure of the potential fission product releases for the dominant core damage sequences.

Top events are the key elements in the construction of an event tree and are selected to assess the critical characteristics of a potential accident scenario. The Level II top events evaluate the plant system responses after core damage. The functional features analyzed by the Level II top events include: containment isolation, core injection, containment heat removal, steam generator heat removal, and AC power recovery.

Level II event trees are generated by adding Level II top events to the end of the Level I event trees. As the original Level I event tree top events and structures are retained throughout the Level II analysis, these Level II trees are referred as "extended event trees" in the SONGS IPE. This terminology provides a direct linkage between the Level I and Level II analyses.

For a description of the Level I portion of the extended event trees refer to Section 3.1.2.

4.3.1.1 Overview of Level II Event Tree Structure

The nuclear industry guidelines for performing the back-end (Level II) IPE (Reference 4.3-1) are based on the bridge tree approach to linking the functional sequences identified by the Level I PRA to the availability of the containment safeguard systems. As was indicated in Reference 4.3-1, the entry state to the bridge tree is provided by the core-damage sequences generated from the front-end PRA.

Quantification of the SONGS 2/3 IPE was performed using a risk assessment software package named REBECA (Reference 4.3-2). REBECA was jointly developed by SCE and ERIN Engineering. After an evaluation of the REBECA software capabilities for Level II applications, it was decided to streamline the sequence quantification process by adding Level II top events directly at the end of the Level I event trees. This approach allows the Level II analysts to keep track of the Level I cutsets associated with the core damage sequences, and credits the Level I component success states in quantification of the Level II end states. In essence, the extended event trees combine the functions of both Level I event trees and the bridge trees mentioned in Reference 4.3-1.

To perform the SONGS Level II IPE, fourteen Extended Event Trees were developed for the initiators identified in Section 3.1.2. These extended event trees are illustrated in Figures 4.3-1a to 4.3-14. Due to limitations of the REBECA software, several extended event trees are divided into subtrees for extended event tree quantification. The extended event tree designators that

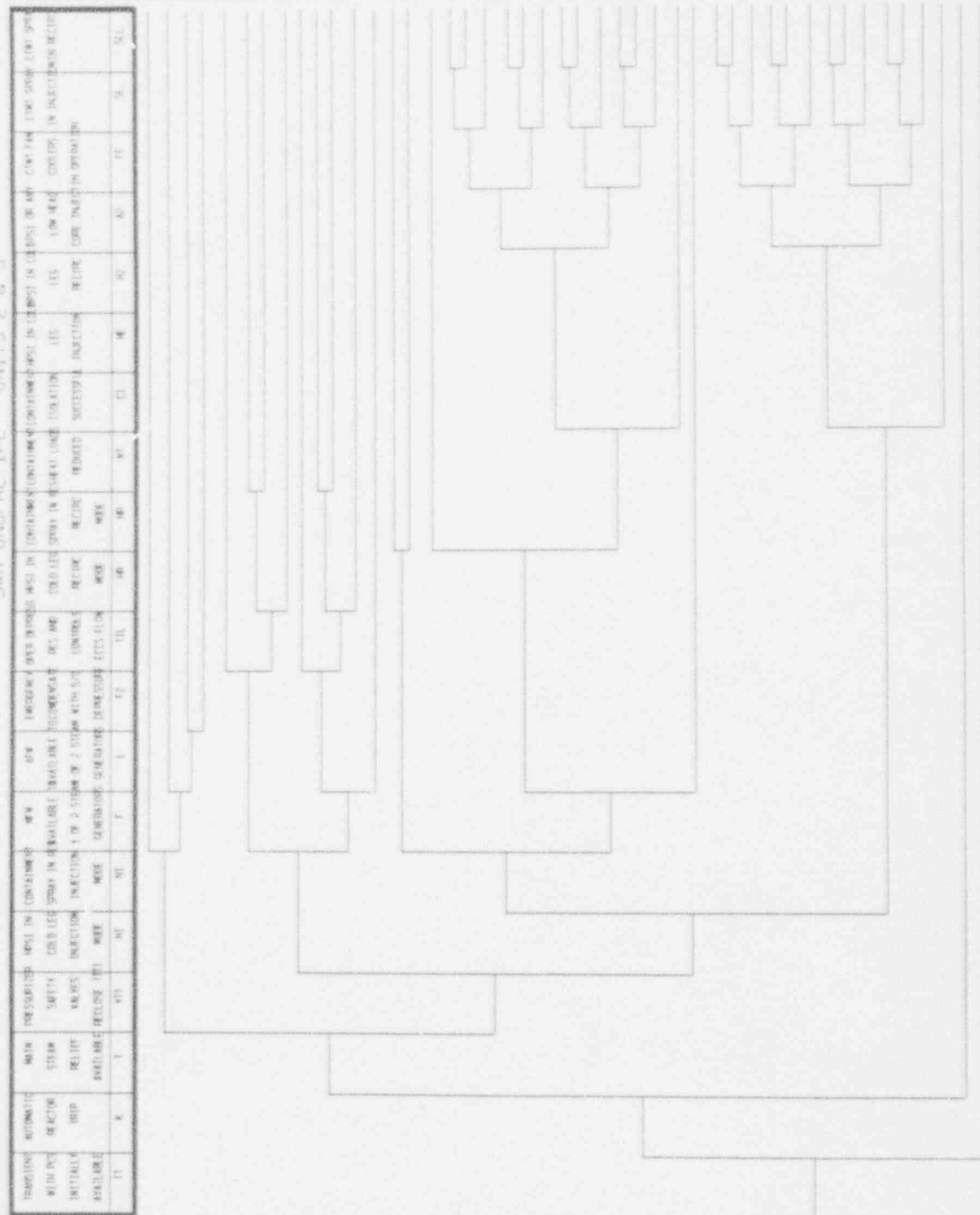
were used by REBECA in the analysis are shown in parentheses after each initiator.

1. Transient with power conversion system, PCS, initially available (T1E & T2E)
2. Loss of power conversion system (P1E & P2E)
3. Anticipated transient without scram (AWE)
4. Loss of offsite power (LPE)
5. Station blackout (SBE)
6. Main steam line break (MSE)
7. Large LOCA (LLE)
8. Medium LOCA (MLE)
9. Small LOCA (SLE)
10. Small-small LOCA (SSE)
11. Steam generator tube rupture (G1E & G2E)
12. Interfacing system LOCA (VLE)
13. Loss of component cooling water (CWE)
14. Loss of 125V DC Bus (LDE)

Figure 4.3-1a
EXTENDED EVENT TREE: TRANSIENT WITH POWER CONVERSION SYSTEM (PCS)
INITIALLY AVAILABLE (TT) PART I.

[illegible]

EXTENDED EVENT TREE; TRANSIENT WITH POWER CONVERSION SYSTEM (PCS)
INITIALLY AVAILABLE (TT) - PART II.



NUMBER	SEQUENCE DESIGNATION	ACCUMULATED FREQUENCY	SEQUENCE
1	11	1	
2	11-1	2	
3	11-1-1	3	
4	11-1-1-1	4	
5	11-1-1-1-1	5	
6	11-1-1-1-1-1	6	
7	11-1-1-1-1-1-1	7	
8	11-1-1-1-1-1-1-1	8	
9	11-1-1-1-1-1-1-1-1	9	
10	11-1-1-1-1-1-1-1-1-1	10	
11	11-1-1-1-1-1-1-1-1-1-1	11	
12	11-1-1-1-1-1-1-1-1-1-1-1	12	
13	11-1-1-1-1-1-1-1-1-1-1-1-1	13	
14	11-1-1-1-1-1-1-1-1-1-1-1-1-1	14	
15	11-1-1-1-1-1-1-1-1-1-1-1-1-1-1	15	
16	11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	16	
17	11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	17	
18	11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	18	
19	11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	19	
20	11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	20	
21	11-1	21	
22	11-1	22	
23	11-1	23	
24	11-1	24	
25	11-1	25	
26	11-1	26	
27	11-1	27	
28	11-1	28	
29	11-1	29	
30	11-1	30	
31	11-1	31	
32	11-1	32	
33	11-1	33	
34	11-1	34	
35	11-1	35	
36	11-1	36	
37	11-1	37	
38	11-1	38	
39	11-1	39	
40	11-1	40	
41	11-1	41	
42	11-1	42	
43	11-1	43	
44	11-1	44	
45	11-1	45	
Total Frequency		11-1	
		11-1	

Figure 4.3-3 EXTENDED EVENT TREE: ANTICIPATED TRANSIENT WITHOUT SCRAM (TWS).

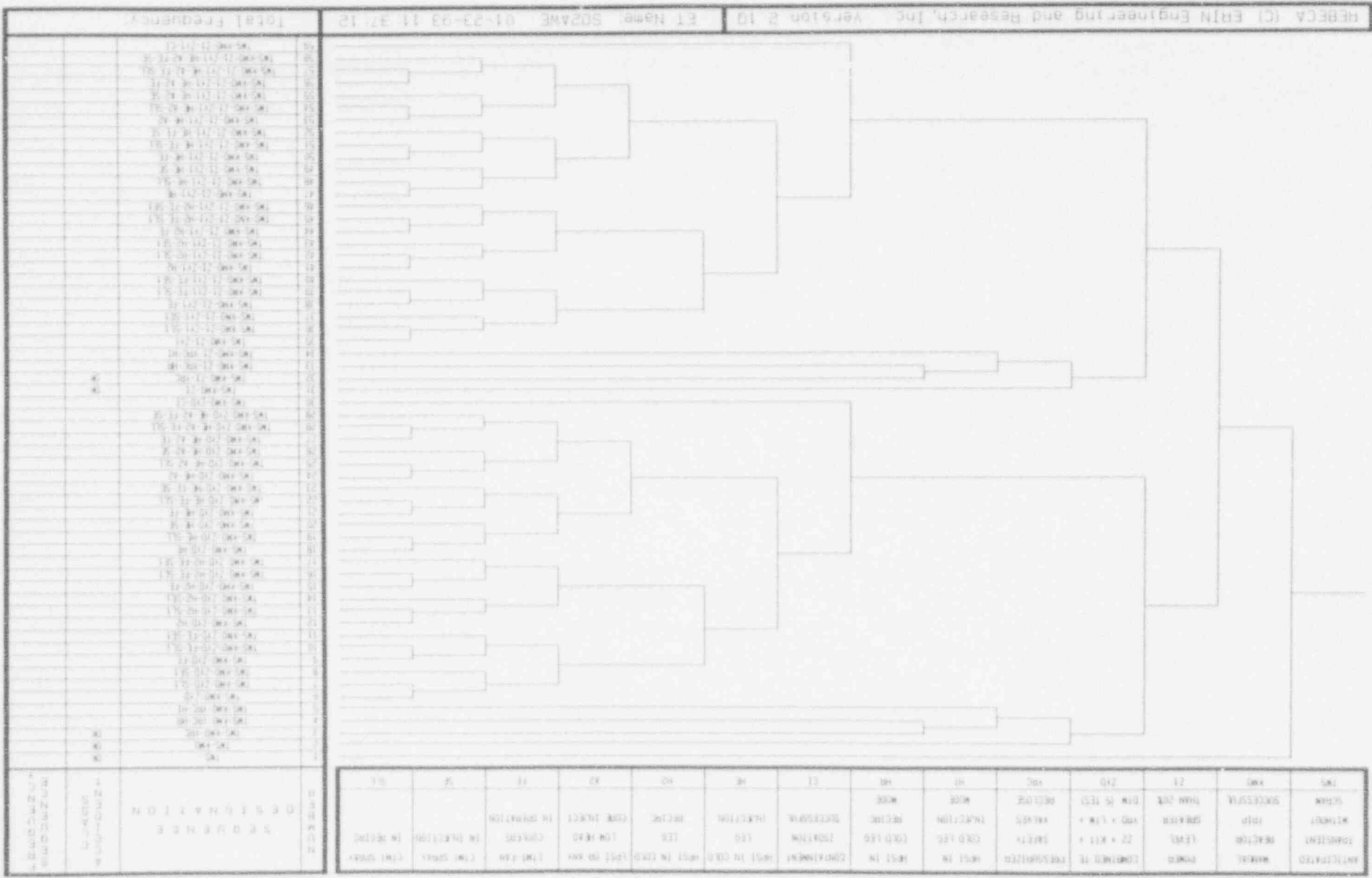


Figure 4.3-6

EXTENDED EVENT TREE: MAIN STEAM LINE BREAK (SLB).

SAN ONDRE IPE - UNITS 2 & 3

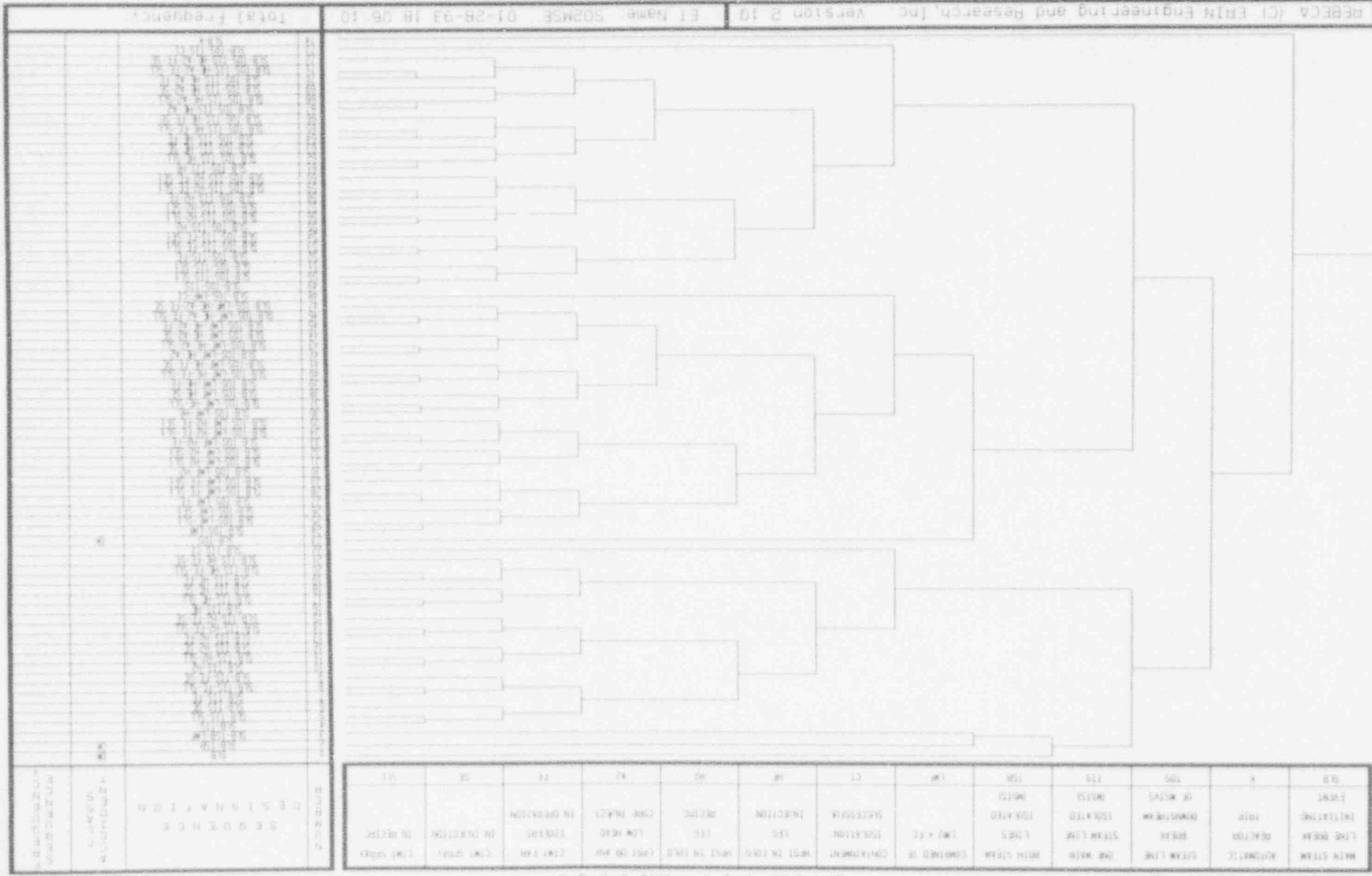
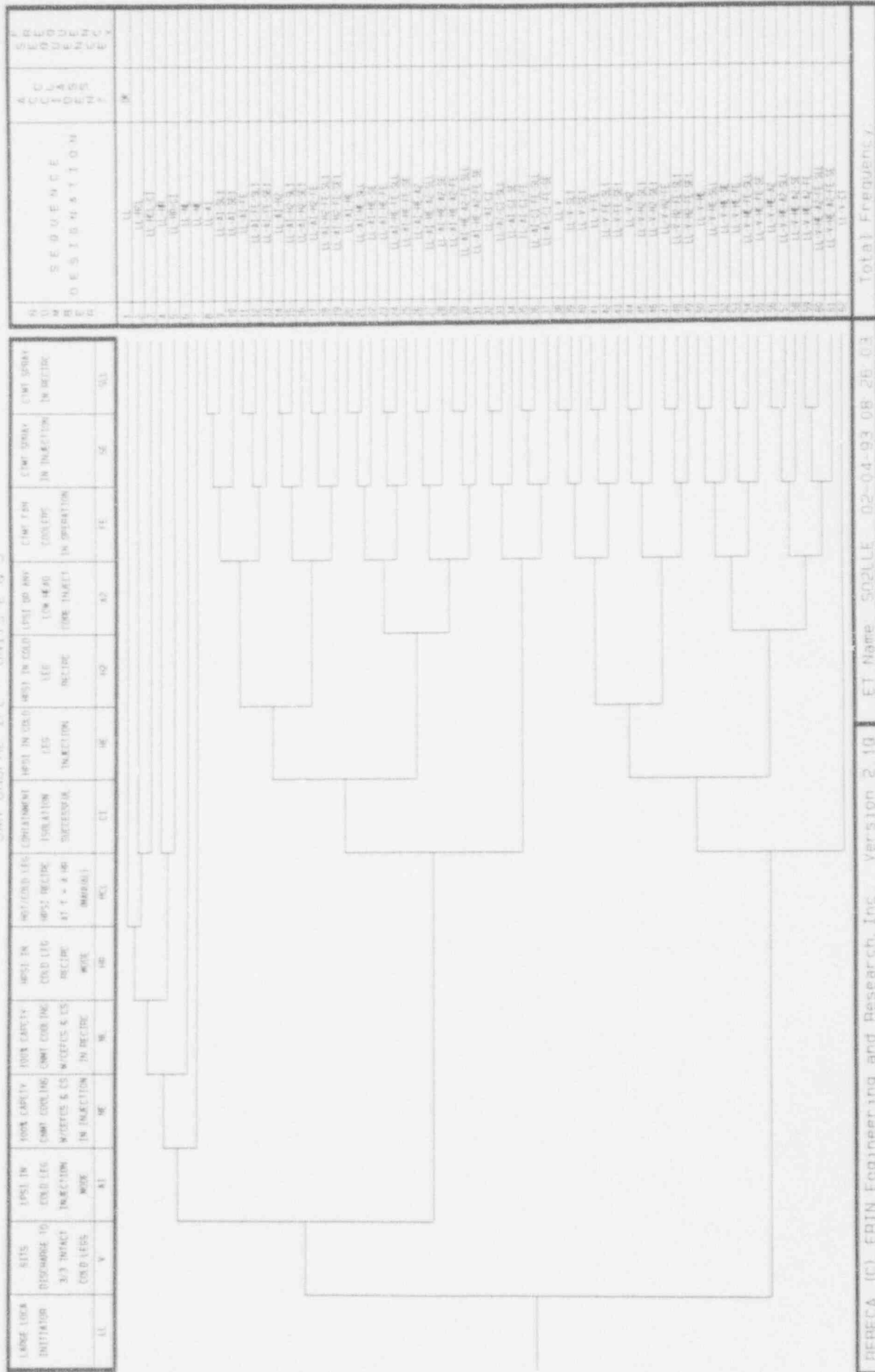


Figure 4.3-7

EXTENDED EVENT TREE: LARGE LOCA (LL)

SAN ONOFFR IPE - UNITS 2 & 3



SMALL LOCAL (SL).

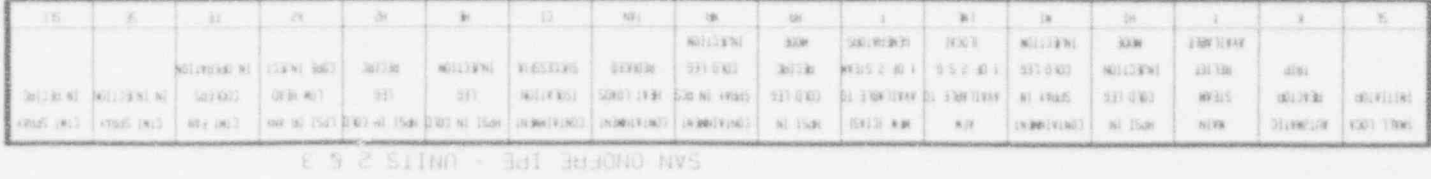


Figure 4.3-11b EXTENDED EVENT TREE: STEAM GENERATOR TUBE RUPTURE - PART II.

SAN ONOFFRE IPE - UNITS 2 & 3

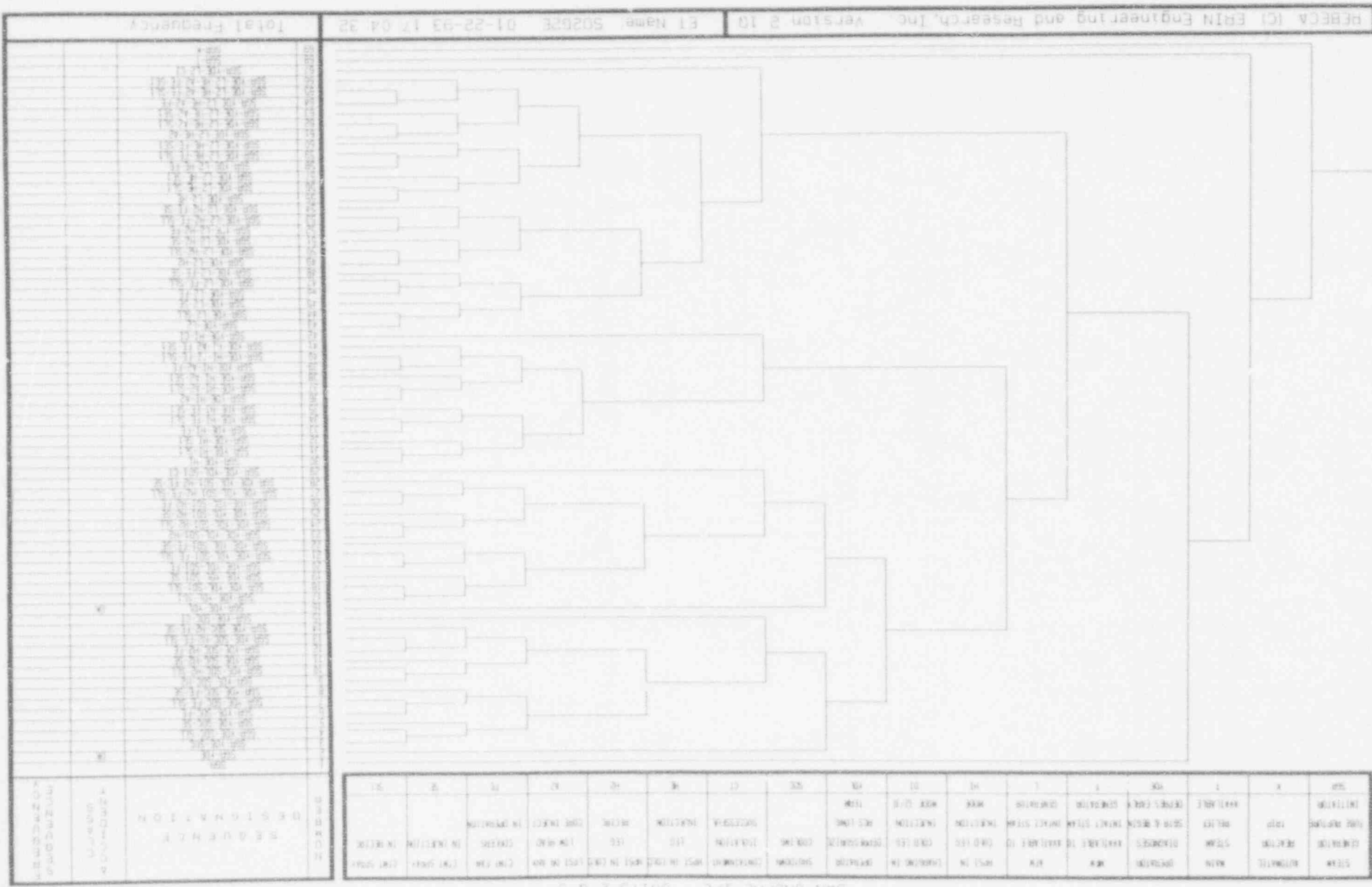


Figure 4.3-12

EXTENDED EVENT TREE: INTERFACING SYSTEMS LOCA (V-SEQUENCE).

SAN ONOFRE IPE - UNITS 2 & 3

INTERFACING SYSTEM LOCA INITIATOR	RECOVERY FROM INTERFACIN SYSTEM LOCA	CONTAINMENT ISOLATION SUCCESSFUL	MAIN STEAM RELIEF AVAILABLE	AFW AVAILABLE TO 1 OF 2 S.S.G. LOCAL	AFW AVAILABLE TO 1 OF 2 STEAM GENERATORS	HPST IN COLD LEG INJECTION	HPST IN COLD LEG RECIRC	LPST OR ANY LOW HEAD CORE INJECT	CTMT FAN COOLERS IN OPERATION	CTMT SPRAY IN INJECTION	CTMT SPRAY IN RECIRC	N U M B E R	SEQUENCE DESIGNATION	A C C I D E N T	F R E Q U E N C Y	
VL	VLR	C?	T	LNK	F	HL	HO	A2	FE	SE	SLL					
												1	VL	OK		
												2	VL-VLR			
												3	VL-VLR-C?			
												4	VL-VLR-T			
												5	VL-VLR-LNK			
												6	VL-VLR-F			
												7	VL-VLR-HL			
REBECA (C) ERIN Engineering and Research, Inc. Version 2.10												ET Name: SC2VLE 01-29-93 10:15:12			Total Frequency:	

EXTENDED EVENT TREE: LOSS OF 125V DC BUS (LDC).

[illegible]

4.3.1.2 Level II Event Tree Nodal Description

Extended Event Tree Assumptions

1. Level I core damage sequences below a frequency of $1E-09$ are not processed by the extended event trees since they cannot significantly affect the frequency of significant offsite release.
2. The culling limit for generation of minimum cutsets for the extended event tree end states is $5E-12/\text{yr}$.
3. No credit is taken for refilling of the RWST after completion of the injection phase.
4. The hydrogen recombiners are not included in the extended event trees. Their capacity is only 100 cfm each, and they would normally be shut off when the containment hydrogen concentration reaches 4%.
5. The culling limits for extended event tree nodes were set to values no larger than three orders of magnitude below the top event probability for each node. This culling limit criteria was selected to: (1) ensure that dominant cut sets would not be culled out and (2) enable extended event tree quantification in a timely manner (less than two weeks). Attempts were made to utilize the Level I event tree node culling limits (i.e., typically $1E-9$) for the extended event tree quantification, however, this resulted in unacceptably long event tree quantification times on the fastest available computer hardware. The use of larger cull limits for the Level II extended event tree nodes resulted in fewer cut sets being found in the Level II analysis than calculated in the Level I analysis. This process did not result in the culling of any dominant cutsets (i.e., greater than $1E-9$) Level I cutsets.
6. A few additional changes to the system fault trees made during the final review process resulted in the removal of additional conservatism from the Level I results. Due to the long time required for re-quantification, these changes were not be processed through the Level II extended event trees. An example of such a change was the addition of Charging pumps as a possible backup to HPSI Injection following a small-small LOCA. The exclusion of these changes from the Level II analysis results in conservatism.

Description of Level II Top Events

To assess the containment safeguard system status and to evaluate the RCS pressure in a severe accident, eleven back-end top events are developed for the extended event trees. Descriptions of these Level II top events are provided below:

1. Containment Isolation (CI)

The containment isolation conditional failure probability is processed by a fault tree analysis. Details of the analysis are presented in the Containment Isolation System Notebook.

Three split fractions are generated for this top event for quantification in the separate initiating events. For the situation where all supporting systems are available, the containment isolation conditional failure probability (GXBAS) is $6.5E-5$ per demand. For a loss of offsite power initiator, the corresponding conditional failure probability (GXLOP) is $8.6E-4$ per demand. In a station blackout, all AC powered MOVs will fail-as-is and give the highest containment isolation failure probability at $1.2E-2$ per demand.

On all extended event trees, the containment isolation top event (CI) is the first Level II top event added to the end of the Level I event trees. A branch is provided for all core damage sequences identified by the front-end work, except those sequences with core damage frequencies below the Level II cutoff level of $1E-9$ per year. Consideration of the remaining Level II top events does not occur for sequences with failure of containment isolation at a frequency below the $1.0E-9$ per year cutoff level.

2. HPSI in Cold Leg Injection (HE)

This top event typically examines HPSI pump injection after the molten fuel relocates to the lower head and causes creep rupture failure of the reactor vessel. Loss of the reactor vessel integrity depressurizes the reactor coolant system below the HPSI pump shutoff head and allows the high head pump to inject to the RCS. Cooling water provided to the core debris remains in the reactor cavity compartment and arrests molten core concrete interaction.

The fault tree generated for top event HI of the Level I event tree is used for top event HE for sequence quantification. The success criterion is that at least one high pressure injection path to the reactor core needs to be established and maintained. By adding top event HE, a branch is provided for the core damage sequences where HI was not checked in the Level I event tree.

3. HPSI in Cold Leg Recirculation (H2)

If HPSI succeeds in the injection mode, then the operability of HPSI recirculation needs to be assessed. Top event H2 analyzes the HPSI recirculation reliability after the RPV fails. This type of sequence includes core damage at an RCS pressure above the HPSI shutoff head, failure of the RPV, and consequent depressurization of the RCS below the HPSI shutoff head. The delayed HPSI injection phase is initiated after RPV failure and provides RWST water to the relocated core debris.

At the end of the cold leg injection phase, about 108,000 gallons of injected water are trapped in the reactor cavity and ventilation ducts up to an elevation of 24 feet 10-3/8 inches. The remaining injected RWST water overflows the cavity shield wall into the lower compartment via the concrete ventilation ducts. The minimum water depth on the lower compartment floor is approximately 1.5 feet, which is sufficient for HPSI and containment spray recirculation operation (Reference 4.3-3).

The fault tree generated for Level I top event HR is used for the Level II sequence quantification. The success criterion requires that at least one recirculation path be established and maintained. The top event H2 provides a branch for sequences where HPSI succeeds in the injection mode (HI or HE). Failure of event HI or HE results in the loss of H2. Pass-through of this top event is provided for sequences that check HR (HPSI in cold leg recirculation) in the Level II event tree.

RPV failure during a postulated core damage event at SONGS 2/3 is expected to occur at low RCS pressure and allow the majority of core debris to be retained in the cavity compartment (see Section 4.4 for discussion of high-pressure vessel melt-through and direct containment heating). However, in the less likely event that the reactor vessel fails under high RCS pressure, a significant portion of molten fuel can be driven into the containment lower compartment between the primary and secondary shield walls. In the SONGS 2/3 containment building, the emergency sump is located in the annular compartment outside the secondary shield. Based on this configuration, it is concluded that the operability of the emergency sump will not be adversely affected by RPV failure. As a result, it is acceptable to use the fault tree and component failure data developed for Level I top event HR in the analysis of the Level II top event H2.

4. LPSI or Any Low Head Core Injection (A2)

This top event evaluates the operability of LPSI and containment spray pumps for injection into the reactor core after the molten core debris fails the reactor vessel lower head and depressurizes the reactor coolant system below the low head pump shutoff head.

Cooling water would thereby reach corium in the cavity compartment and arrest the molten core concrete interaction. A separate fault tree, CN, is created to account for both the LPSI system and one containment spray pump aligned for reactor core injection.

A branch is provided for the core damage sequences with HPSI failure during injection (HI or HE), loss of LPSI in injection (AI), or loss of a containment spray pump in injection mode (NI). The success criterion is that at least one of the three low head pumps (two LPSI pumps and one containment spray pump) are started and maintain an injection path to the reactor core.

Failure is assumed for this top event for sequences with HPSI recirculation failure (HR or H2). This is based on the assumption that failure of recirculation implies there is no borated water in the RWST to be transferred into the reactor core, and refilling of the RWST is not credited as a potential recovery action in the SONGS IPE.

5. Containment Fan Coolers in Operation (FE)

This top event accounts for containment heat removal by the four containment emergency fan coolers. The success criterion requires at least one fan cooler to be started and operated throughout the accident scenario. The Level I fault tree developed for containment heat removal is used to model this node in the EET. This node is bypassed for those Level I core damage sequences where the question of containment heat removal was asked.

6. Containment Spray Injection (SE)

This top event examines the operation of containment spray pumps for containment heat removal. The success criterion requires that at least one spray pump is started to provide RWST water to the containment spray nozzles. The Level I fault tree developed for containment heat removal is used for this node. To keep track of the containment heat removal status, a branch is provided at this top event for both success and loss of containment cooling sequences.

7. Containment Spray Recirculation (SLL)

This top event assesses the operation of the containment spray pumps in recirculation mode for containment heat removal. The success criterion is for at least one spray pump to provide heat removal capability in the recirculation phase. The Level I fault tree developed for containment recirculation heat removal is used. Failure of top event SE (containment spray injection) guarantees the loss of SLL (containment spray recirculation). The top event SLL provides a branch for sequences where containment spray succeeds in the injection mode (SE). Failure of SE guarantees the

loss of SLL. Pass through of this top event is provided for sequences that have checked top event NL of the Level I event tree.

8-10. Other Top Events

Loss of Secondary Heat Sink Top Events

The progression of a severe accident scenario is heavily influenced by the reactor coolant system pressure after core damage. To determine the RCS pressure status for the interfacing system LOCA and loss of component cooling water initiators, three top events associated with the secondary heat removal are added to the extended event trees. These top events are identical to their counterparts on the Level I event trees. They are:

- Main Steam Relief Available (T)
- Auxiliary Feedwater Available to 1 of 2 Steam Generators (LNL)
- Main Feedwater Available to 1 of 2 Steam Generators (F)

AC Power Recovered Within 1 - 8 Hours (U9)

In the Level I station blackout event tree, failure to recover AC power within 60 minutes and loss of the turbine driven auxiliary feedwater pump leads to core damage. To assess the containment status after core damage, the availability of AC power must again be addressed. A top event (U9) is added to the extended event tree to evaluate this AC power recovery.

To simplify the analysis task, this top event credits the AC power recovery probability between the end of the first hour and the 8th hour after the initiating event, and postulates that debris cooling and containment heat removal are re-established after AC power becomes available.

4.3.2 Plant Damage State Characterization

Plant damage states (PDS) represent functional groupings of Level I core damage sequences. The grouping by plant damage state is predicated on plant characteristics such that Level I systemic sequences assigned to a plant damage state are expected to produce a similar containment response to a severe accident. For SONGS 2/3 the sequences quantified through the extended event trees (Section 4.3.1) are binned into the plant damage states. The criteria for binning the Level I systemic sequences into the plant damage states are based on the following five characteristics of each sequence:

Initiator

Core melt prevention is predicated upon the ability to keep the fuel assemblies covered with water so that decay heat removal can be maintained. This ability depends, of course, upon the rate at which water enters the vessel versus the rate at which water exits the vessel. The initiator defines the means by which a break in the primary system occurs and thus the rate at which water exits. A large LOCA, for example, causes rapid depletion of core inventory, unlike a general transient. The initiators utilized for Level I analysis are classified according to attributes which dictate the rate at which inventory is depleted. The following nomenclature is utilized for the first PDS character:

- | | |
|-------------------------|--|
| T - TRANSIENT: | An initiator which does not involve an initial break within the primary system. |
| L - LARGE BREAK: | An initiator which causes a break of sufficient size to depressurize the primary system, allowing low head injection to operate. |
| S - SMALL BREAK: | An initiator which causes a break sufficiently small to maintain high primary system pressure, precluding the use of low head injection. |
| G - CONTAINMENT BYPASS: | All steam generator tube ruptures (SGTR) and interfacing systems LOCAs (V-sequences). |

Time of Core Melt

Timing of core melt relative to accident initiation is important from the perspective of implementing Accident Management Strategies. Three time periods are considered: Early (0-2 hrs), Intermediate (2-6 hrs), and Late (>6 hrs). In the early time period plant activities are dominated by automatic initiations and diagnostic evaluations. Emergency Operating Instructions (EOIs) govern the direction which the plant staff takes during this time period. It is unlikely that diagnostic activities could be completed, strategies identified, and manpower and equipment assembled for implementation of actions which are outside the bounds of the existing EOIs. Within the Intermediate time frame, limited accident management strategies are achievable, but no support can be credited for manning offsite facilities. In the late phase of the accident, offsite facilities would be properly manned, and credit for successful accident management strategies can be taken. By forming plant damage states based on the timing of core melt, appropriate levels of recovery actions can be

identified. The nomenclature for this PDS character is as follows:

- | | |
|-------------------|---|
| E - Early: | Core damage occurs within 2 hours of the accident initiator. |
| I - Intermediate: | Core damage occurs within the range of 2-6 hours following the initiator. |
| L - Late: | Core damage occurs more than 6 hours after accident initiation. |

Status of ECCS

Core melt occurs when it is no longer possible to maintain water above the top of active fuel, implying that the rate of water exiting the vessel exceeds the rate at which it is being injected. The initiator defines the mechanism by which water leaves the vessel. The ECCS Status designator defines the rate at which water enters the vessel. For SONGS 2/3, ECCS status is based on the availability of secondary side cooling combined with injection and recirculation. Included in the description is the availability of water for injection or recirculation following vessel failure. The characters utilized for ECCS status are defined in Table 4.3-1.

Containment Heat Removal

Containment heat removal is achieved through either the recirculation mode of containment spray or the use of containment emergency fan coolers. Availability of either or both system is identified with a (Y) for yes, containment heat removal is available, or (N) for no, containment heat removal is not available.

Containment Status

The final plant damage state character addresses the status of the containment. The identifiers used are:

- | | |
|--------------------|---|
| S - SUCCESS: | No containment failure within 48 hours |
| I - ISOLATION: | Containment is not isolated (i.e., it is impaired) at the time of accident initiation |
| B - BYPASS: | Containment is bypassed (e.g., SGTR or V-sequence) |
| E - EARLY FAILURE: | Containment overpressure failure occurs early, less than 8 hours after RPV failure |
| L - LATE FAILURE: | Containment overpressure failure occurs late, more than 8 hours after RPV failure |

Table 4.3-1
PLANT DAMAGE STATE IDENTIFIERS FOR ECCS STATUS

<u>PDS</u> <u>Character</u>	<u>Description</u>
A	Secondary Side Cooling <u>not</u> available or <u>not</u> considered, HPSI available on safety signal, HPSI <u>not</u> available before core damage. Post Vessel Failure: HPSI/HPSI recirculation available for long term cooling of the core debris in the reactor cavity.
B	Secondary Side Cooling <u>not</u> available or <u>not</u> considered, No HPSI prior to vessel failure. Post Vessel Failure: LPSI available to supply water into reactor cavity through the failed reactor vessel, no HPSI/HPSI recirculation after vessel failure.
C	Secondary Side Cooling <u>not</u> available or <u>not</u> considered, No HPSI prior to vessel failure. Post Vessel Failure: No HPSI, LPSI or HPSI recirculation available to inject water into the reactor cavity through the failed reactor vessel.
D	Secondary Side Cooling available and HPSI available on safety signal, HPSI <u>not</u> available before core damage. Post Vessel Failure: HPSI/HPSI recirculation available for long term cooling of the core debris in the reactor cavity.
E	Secondary Side Cooling available, HPSI, HPSI recirculation <u>not</u> available. Post Vessel Failure: LPSI available to supply water to the reactor cavity through the failed reactor vessel.
F	Secondary Side Cooling Available, HPSI/HPSI recirculation <u>not</u> available. Post Vessel Failure: No HPSI, LPSI or HPSI recirculation available to inject water into the reactor cavity through the failed reactor vessel.
G	Secondary Side Cooling <u>not</u> considered, LPSI injection available, No HPSI recirculation available before vessel failure. Post Vessel Failure: HPSI recirculation not available for long term cooling of the core debris in the reactor cavity.
H	Secondary Side Cooling <u>not</u> considered, No LPSI injection before vessel failure, No HPSI recirculation available before vessel failure. Post Vessel Failure: HPSI recirculation available for long term cooling of the core debris in the reactor cavity.
I	Secondary Side Cooling <u>not</u> considered, No LPSI injection before vessel failure, No HPSI recirculation available before vessel failure. Post Vessel Failure: LPSI available for cooling of the core debris in the reactor cavity.

Table 4.3-1

PLANT DAMAGE STATE IDENTIFIERS FOR ECCS STATUS
(continued)

<u>PDS</u> <u>Character</u>	<u>Description</u>
J	Secondary Side Cooling <u>not</u> considered, No LPSI injection before vessel failure and No HPSI recirculation available before vessel failure. Post Vessel Failure: No long term cooling of the core debris in the reactor cavity.
K	Secondary Side Cooling <u>not</u> available or <u>not</u> considered, HPSI available on safety signal. Post Vessel Failure: HPSI recirculation not available for long term cooling of the core debris in the reactor cavity.
L	Secondary Side Cooling available and HPSI available on safety signal, HPSI recirculation <u>not</u> available before core damage. Post Vessel Failure: HPSI recirculation <u>not</u> available for long term cooling of the core debris in the reactor cavity.

NOTE: PDS Characters J, K & L are reserved for large LOCA and ATWS sequences.

The eight hour figure used to differentiate between early and late containment failure is based on the transportation of fission products following their release from the vessel. Following core damage, the fission product concentration in the containment gas space increases until the release rate from the vessel equals the rate of deposition. At this point, the aerosol concentration remains fairly constant until the fission product source stops, whereupon the airborne fission product concentration decays due to sedimentation. Airborne fission products are available for release from containment should there be a break in the containment structure. The timing of such containment failure is an important factor for source term analysis. Delay in the containment failure timing provides more time for natural removal of fission products from the containment gas space. For the cases of impairment and containment failure prior to vessel failure, an early release path is provided for the fission products as they escape from the vessel. Early containment failure is defined to occur up to the time when the airborne fission products begin to decay. This time period extends approximately 8 hours after vessel failure, with some variation depending upon the initiator. Late containment failure is defined to occur more than 8 hours after vessel failure.

4.3.3 Binning and Screening of Level II Sequences

Plant damage states are assigned to the quantified Level I core damage sequences once they have been passed through the extended event trees (EETs) described in Section 4.3.1. To ensure a correct transcription of information, these core damage sequences were organized according to their frequency values and key system attributes relating to systems availability for decay heat removal, containment heat removal, and debris coolability. This information is tabulated in Tables 4.3-2 through 4.3-5 for 121 systemic sequences which were identified through the EETs and which contribute greater than 10^{-9} /yr to the total core damage frequency. The 121 sequences are grouped into four tables according to their functional initiator (i.e., the first PDS character). Tables 4.3-2 through 4.3-5 illustrate, respectively, systemic sequences which are characterized as transients (T), large LOCAs (L), small LOCAs (S), and containment bypass (G). These systemic sequences are correlated to the EETs by the sequence numbers (shown in the first column of each table) which identify the applicable EET and EET end point. All 121 sequences were assigned plant damage state designators in accordance with Section 4.3.2. Table 4.3-6 lists the 42 plant damage states which result from extended event tree quantification, along with their frequencies, and their percent contribution to the total CDF. Selected plant damage states are analyzed for source term using MAAP. The selection of the important functional sequences is based on the criteria presented in Appendix 2 to GL 88-20. Table 4.3-7 itemizes the GL 88-20 requirements and indicates which

sequences from Table 4.3-6 are selected based on those criteria. The fifteen plant damage states which are selected for MAAP analysis are listed in Table 4.3-8. The selected cases encompass each functional initiator, impairment cases, and overpressure failures, and a spectrum of ECCS conditions. The 26 remaining plant damage states, representing 29 percent of the CDF, are bounded by the 15 analyzed cases. Additional details on the screening and binning of Level II sequences are provided in the discussion of CET methodology in Section 4.5.

4.4 CONTAINMENT FAILURE CHARACTERIZATION

Plant-specific phenomenological evaluations have been performed in support of the SONGS 2/3 IPE to determine the likelihood of all postulated containment failure modes and mechanisms identified in NUREG-1335. These detailed evaluations were performed systematically to address the controlling physical processes or events specific to the SONGS configuration. Modeling and bounding calculations, based upon extensively compiled experimental data and phenomenological uncertainties, (complemented with MAAP calculations in some cases) comprise the general approach utilized in these evaluations. As discussed in Section 4.4.2 the containment failure modes considered unlikely are hydrogen combustion, direct combustion heating, steam explosions, thermal attack of containment penetrations, and vessel thrust forces. Failure modes more likely to occur are containment overpressure, containment isolation failure, containment bypass, and MCCI induced failure of the reactor cavity floor. The evaluations of these postulated failure modes are described below.

4.4.1 Containment Ultimate Strength

A plant specific structural analysis of the SONGS 2/3 containment has been performed by a contractor, EQE International, to determine the ultimate internal pressure capacity and the most likely failure locations (Reference 4.4-1). The analysis included gross failures, smaller structural failures, and local failures of containment penetrations. In each case, failure was defined as incipient leakage or breach of the pressure boundary. Potential failure modes of specific containment features, due to temperature and pressure loading well beyond the design basis, were treated probabilistically. The pressure capacity of each potential failure mode was treated as a log-normally distributed random variable described by a median failure pressure and a logarithmic standard deviation.

The potential structural failures of the containment shell and basemat included: membrane tension failures of the cylinder and dome portions of the containment shell, flexural failure at the base of the containment wall and flexure failure and shear

Table 4.3-2

Page 1 of 2

"Transient" EET Sequences with Frequencies Greater Than 10^{-9} /yr

ACCIDENT SEQUENCE	PDS	FREQUENCY	PZR SAFETY CLOSED	AFW/ MPW AVAIL	HPI AVAIL	FANS	CONT SPRAYS	CONT SPRAYS RECIRC	AVF HPI LPI	AVF HPR	CAVITY WET
LOP-25	TEAYS	2.2E-6	NC	NO	YES	YES	YES	YES	YES	YES	YES
PCS1-4	TEAYS	2.0E-6	YES	NO	YES	YES	YES	YES	YES	YES	YES
SBO-15	TEAYS	1.8E-6	NC	NO	YES	YES	YES	YES	YES	YES	YES
TT1-4	TEAYS	1.4E-6	YES	NO	NC	YES	YES	YES	YES	YES	YES
LDC-4	TEAYS	2.1E-7	YES	NO	YES	YES	YES	YES	YES	YES	YES
SBO-4	TEAYS	2.1E-7	NC	YES	NO	NO	NO	NO	NO	NO	YES
SLB-24	TEAYS	1.7E-7	NC	NO	YES	YES	YES	YES	YES	YES	YES
TTI-6	TEAYS	4.3E-8	YES	NO	NC	YES	NO	(NO)	YES	YES	YES
PCS1-6	TEAYS	3.2E-8	YES	NO	NC	YES	NO	(NO)	YES	YES	YES
SLB-49	TEAYS	2.0E-8	NC	NO	YES	YES	YES	YES	YES	YES	YES
LDC-6	TEAYS	1.1E-8	YES	NO	NC	YES	NO	(NO)	YES	YES	YES
SLB-4	TEAYS	8.5E-9	NC	NO	YES	YES	YES	YES	NC	YES	YES
SLB-26	TEAYS	4.1E-9	NC	NO	YES	YES	NO	(NO)	NC	YES	YES
LDC-7	TEAYS	1.5E-9	YES	NO	NC	NO	YES	YES	YES	YES	YES
TT1-18	TEBYS	4.3E-8	YES	NO	NC	YES	NO	(NO)	YES	NO	T
PCS1-18	TEBYS	3.2E-8	YES	NO	NC	YES	NO	(NO)	YES	NO	T
TT1-35	TEBYS	1.5E-8	NO	NO	YES	NO	NO	NO	YES	NO	YES
LDC-16	TEBYS	6.2E-9	YES	NO	NC	YES	YES	YES	YES	NO	T
SLB-38	TEBYS	4.1E-9	NC	NO	NO	YES	NO	(NO)	YES	(NO)	T
LDC-12	TEBYS	1.9E-9	YES	NO	NC	YES	NO	(NO)	YES	NO	T
LDC-24	TECYS	3.1E-9	YES	NO	NO	YES	NO	(NO)	NO	(NO)	NO
SBO-7	TECNS	1.5E-8	NO	NO	NO	NO	NO	NO	NO	NO	NO

AVF: After Vessel Failure

NC: Not considered in EET

(NO): Consequential "NO"

(YES): Consequential "YES"

T: Temporarily

Table 4.3-2

Page 2 of 2

"Transient" EET Sequences With Frequencies Greater Than 10^{-9} /yr

ACCIDENT SEQUENCE	PDS	FREQUENCY	PZR SAFETY CLOSED	AFW/ MFW AVAIL	HPI AVAIL	FANS	CONT SPRAYS	CONT SPRAYS RECIRC	AVF HPI LPI	AVF HPR	CAVITY WET
SBO-10	TECNS	1.1E-9	NC	YES	NO	NO	NO	(NO)	NO	NO	NO
CCW-3	TEFYS	1.3E-7	NC	YES	NO	NO	NO	NO	NO	NO	NO
LOP-48	TECNL	2.1E-6	NC	NO	NC	NO	NO	(NO)	NO	(NO)	NO
SBO-16	TECNL	8.8E-9	NC	NO	NO	NO	NO	NO	NO	NO	NO
CCW-10	TEFNL	6.1E-9	NC	YES	(NO)	(NO)	(NO)	(NO)	(NO)	(NO)	NO
CCW-15	TEFNL	2.6E-9	NC	YES	(NO)	(NO)	(NO)	(NO)	(NO)	(NO)	NO
LOP-30	TEANL	4.0E-8	NC	NO	NC	NO	NO	(NO)	YES	YES	YES
PCS2-25*	TEBNL	3.2E-8	NO	NC	NO	NO	NO	(NO)	YES	(NO)	T
SBO-17 ISO FAIL	TEAYI	1.7E-8	NC	NO	YES	YES	YES	YES	YES	YES	YES
SBO-5 ISO FAIL	TECNI	1.9E-9	NC	YES	NO	NO	NO	NO	NO	NO	NO

AVF: After Vessel Failure

(NO): Consequential "NO"

T: Temporarily

NC: Not considered in EET

(YES): Consequential "YES"

*Pressurizer Safety Valves Stuck Open

Table 4.3-3

"Large LOCA" EET Sequences With Frequencies Greater Than 10^{-9} /yr

ACCIDENT SEQUENCE	PDS	FREQUENCY	PZR SAFETY CLOSED	APW/ MFW AVAIL	HPI AVAIL	FANS	CONT SPRAYS	CONT SPRAYS RECIRC	AVF HPI LPI	AVF HPR	CAVITY WET
ATWS-6	LEAYS	2.5E-6	NC	NC	NC	YES	YES	YES	YES	YES	YES
ATWS-35	LEAYS	2.6E-7	NC	NC	NC	YES	YES	YES	YES	YES	YES
LDC-50 (ATWS)	LEAYS	1.6E-8	NC	NC	NC	YES	YES	YES	YES	YES	YES
ATWS-7	LEAYS	3.1E-9	NC	NC	NC	YES	YES	NO	YES	YES	YES
ATWS-8	LEAYS	2.9E-9	NC	NC	NC	YES	NO	(NO)	YES	YES	YES
ATWS-13	LEBYS	2.2E-9	NC	NC	NC	YES	YES	NO	YES	NO	T
ATWS-20	LEBYS	1.2E-9	NC	NC	NC	YES	NO	(NO)	YES	(NO)	T
LLO-4	LEGYS	1.8E-6	NC	NC	NC	YES	YES	YES	YES	NO	T
LLO-8	LEHYS	7.1E-7	NC	NC	NO-LPI	YES	YES	YES	YES	YES	YES
LLO-38	LEHYS	4.7E-7	NC	NC	NO-SIT	YES	YES	YES	YES	YES	YES
LLO-10	LEHYS	4.6E-7	NC	NC	NO-LPI	YES	NO	(NO)	YES	YES	YES
LLO-2	LEHYS	3.7E-7	NC	NC	YES	YES	YES	YES	YES	YES	YES
LLO-22	LEIYS	5.4E-7	NC	NC	NO-LPI	YES	NC	(NO)	CSI	(NO)	T
LLO-20	LEIYS	1.0E-9	NC	NC	NO-LPI	YES	YES	YES	CSI	(NO)	T
LLO-28	LEJYS	4.3E-9	NC	NC	NO-LPI	YES	NO	(NO)	NO	(NO)	NO
LLO-13	LEHNL	6.2E-8	NC	NC	NO-LPI	NO	NO	(NO)	YES	YES	YES
LLO-34 ISOL FAIL	LEIYI	1.4E-9	NC	NC	NO-LPI	YES	NO	(NO)	YES	(NO)	T

AVF: After Vessel Failure
 NC: Not considered in EET
 (YES): Consequential "YES"

CSI: Containment Spray Pump for Core Injection
 (NO): Consequential "NO"
 T: Temporarily

Table 4.3-4

Page 1 of 3

"Small LOCA" EET Sequences With Frequencies Greater Than $10^{-9}/\text{yr}$

ACCIDENT SEQUENCE	PDS	FREQUENCY	PZR SAFETY CLOSED	AFW/ MFW AVAIL	HPI AVAIL	FANS	CONT SPRAYS	CONT SPRAYS RECIRC	AVF HPI LPI	AVF HPR	CAVITY WET
SSL-19	SEAYS	8.7E-7	NC	NO	NC	YES	YES	YES	YES	YES	YES
SLO-19	SEAYS	6.5E-8	NC	NO	YES	YES	YES	YES	(YES)	YES	YES
PCS1-45*	SEAYS	2.0E-8	NO	NO	YES	YES	YES	YES	(YES)	YES	YES
SSL-21	SEAYS	1.5E-9	NC	NO	NC	YES	NO	(NO)	YES	YES	YES
MLO-15	SEBYS	1.4E-6	NC	NC	NO	YES	YES	YES	YES	(NO)	T
SLO-49	SEBYS	8.2E-7	NC	NC	NO	YES	YES	YES	YES	(NO)	T
PCS2-20*	SEBYS	1.3E-7	NO	NC	NO	YES	YES	YES	YES	(NO)	T
SLO-51	SEBYS	6.8E-8	NC	NC	NO	YES	NO	(NO)	YES	(NO)	T
TT2-31*	SEBYS	4.5E-8	NO	NC	NO	YES	YES	YES	YES	NO	T
PCS2-22*	SEBYS	2.4E-8	NO	NC	NO	YES	NO	(NO)	YES	(NO)	T
MLO-17	SEBYS	1.6E-8	NC	NC	NO	YES	NO	(NO)	YES	(NO)	T
TT2-33*	SEBYS	8.0E-9	NO	NC	NO	YES	NO	(NO)	YES	NO	T
SLO-50	SEBYS	3.7E-9	NC	NC	NO	YES	YES	NO	YES	(NO)	T
MLO-16	SEBYS	3.1E-9	NC	NC	NO	YES	YES	NO	YES	(NO)	T
MLO-23	SECYS	8.5E-9	NC	NC	NO	YES	NO	(NO)	NO	(NO)	NO
SSL-3	SEEYS	9.4E-7	NC	YES	NO	YES	YES	YES	YES	(NO)	T
LOP-12	SEEYS	1.9E-8	NO	YES	NO	YES	YES	YES	YES	(NO)	T
LOP-14*	SEEYS	1.1E-8	NO	YES	NO	YES	NO	(NO)	YES	(NO)	T
SSL-5	SEEYS	1.0E-8	NC	YES	NO	YES	NO	(NO)	YES	(NO)	T
LOP-15*	SEEYS	3.7E-9	NO	YES	NO	NO	YES	YES	YES	NO	T

AVF: After Vessel Failure
 NC: Not considered in EET
 (YES): Consequential "YES"

* Pressurizer Safety Valve Stuck Open
 (NO): Consequential "NO"
 T: Temporarily

Table 4.3-4

Page 2 of 3

"Small LOCA" EET Sequences With Frequencies Greater Than $10^{-9}/\text{yr}$

ACCIDENT SEQUENCE	PDS	FREQUENCY	PZR SAFETY CLOSED	AFW/ MFW AVAIL	HPI AVAIL	FANS	CONT SPRAYS	CONT SPRAYS RECIRC	AVF HPI LPI	AVF HPR	CAVITY WET
SLO-33	SEEYS	2.5E-9	NC	YES	NO	YES	YES	YES	YES	(NO)	T
SSL-4	SEEYS	1.9E-9	NC	YES	NO	YES	YES	NO	YES	(NO)	T
PCS2-6*	SEEYS	1.0E-9	NO	YES	NO	YES	NO	(NO)	YES	(NO)	T
SSL-11	SEFYS	5.6E-9	NC	YES	NO	YES	NO	(NO)	NO	(NO)	NO
LOP-5*	SEFYS	4.6E-9	NO	YES	NO	YES	YES	YES	NC	NC	NO
SLO-57	SEJYS	4.5E-9	NC	NC	NO	YES	NO	(NO)	NO	(NO)	NO
MLO-4	SEKYS	2.1E-6	NC	NC	YES	YES	YES	YES	NC	(NO)	NO
MLO-2	SEKYS	6.4E-7	NC	NC	YES	YES	YES	YES	NC	(NO)	NO
TT1-39*	SEKYS	2.1E-7	NO	NO	YES	YES	YES	NO	NO	(NO)	NO
TT1-38*	SEKYS	3.6E-8	NO	NO	YES	YES	YES	YES	NO	(NO)	NO
TT1-45*	SEKYS	6.8E-9	NO	NO	YES	YES	YES	YES	YES	NO	T
PCS1-31*	SLDYS	4.1E-8	NO	YES	YES	---	---	---	(YES)	(YES)	YES
SLO-4	SLDYS	1.6E-8	NC	YES	YES	YES	NO	(NO)	(NC)	(YES)	YES
SLO-2	SLDYS	4.7E-9	NC	YES	YES	YES	YES	YES	NC	(YES)	YES
PCS1-32*	SLDYS	2.0E-9	NO	YES	YES	---	---	---	(YES)	(YES)	YES
SLO-10	SLLYS	1.8E-6	NC	YES	YES	YES	YES	NO	(NO)	(NO)	NO
PCS1-35*	SLLYS	5.6E-7	NO	YES	YES	YES	YES	NO	NC	(NO)	NO
SLO-9	SLLYS	3.1E-7	NC	YES	YES	YES	YES	YES	(NO)	(NO)	NO
PCS1-34*	SLLYS	9.9E-8	NO	YES	YES	YES	YES	YES	NC	(NO)	NO

AVF: After Vessel Failure
 NC: Not considered in EET
 (YES): Consequential "YES"

* Pressurizer Safety Valve Stuck Open
 (NO): Consequential "NO"
 T: Temporarily

Page 3 of 3

Page 3 of 3

"Small LOCA" EET Sequences With Frequencies Greater Than $10^9/\text{yr}$

[illegible]

* Pressurizer Safety Valve Stuck Open
(NO): Consequential "NO"
T: Temporarily

Table 4.3-5

Page 1 of 2

Containment Bypass EET Sequences With Frequencies Greater Than $10^{-9}/\text{yr}$

ACCIDENT SEQUENCE	PDS	FREQUENCY	PZR SAFETY CLOSED	AFW/ MFW AVAIL	HPI AVAIL	FANS	CONT SPRAYS	CONT SPRAYS RECIRC	AVF HPI LPI	AVF HPR	CAVITY WET
SGTR2-45	GEAYB	1.4E-7	NC	NO	NC	YES	NO	(NO)	YES	YES	YES
SGTR1-33	GEAYB	5.5E-8	NC	NO	NC	YES	NO	(NO)	YES	YES	YES
SGTR2-43	GEAYB	3.2E-8	NC	NO	NC	YES	YES	YES	YES	YES	YES
SGTR1-45	GLBYB	5.6E-8	NC	NO	NC	YES	NO	(NO)	YES	NO	T
SGTR2-57	GLBYB	4.0E-8	NC	NO	NC	YES	NO	(NO)	YES	(NO)	T
SGTR1-18	GLBYB	3.6E-8	NC	NO	NO	YES	YES	YES	YES	(NO)	T
SGTR1-31	GLCYB	1.7E-7	NC	NO	NO	YES	YES	YES	YES	YES	YES
SGTR2-63	GLCYB	9.2E-8	NC	NO	NC	YES	NO	(NO)	NO	(NO)	NO
SGTR1-26	GLCYB	1.2E-9	NC	NO	NO	YES	NO	(NO)	NO	(NO)	NO
SGTR2-17	GLDYB	4.1E-7	NC	YES*	YES	YES	YES	YES	NC	YES	YES
SGTR2-3	GLDYB	3.0E-8	NC	YES*	YES	YES	YES	YES	NC	YES	YES
SGTR2-19	GLDYB	3.9E-9	NC	YES*	YES	YES	NO	(NO)	NC	YES	YES
SGTR1-3	GLEYP	1.4E-7	NC	YES	NO	YES	YES	YES	YES	(NO)	T
SGTR1-5	GLEYP	8.6E-8	NC	YES	NO	YES	NO	(NO)	YES	(NO)	T
SGTR1-20	GLEYP	6.4E-8	NC	YES	NO	YES	NO	(NO)	YES	(NO)	T
SGTR2-30	GLEYP	8.6E-9	NC	YES*	NO	YES	YES	YES	YES	(NO)	T
SGTR2-32	GLEYP	7.5E-9	NC	YES*	NO	YES	NO	(NO)	YES	(NO)	T

AVF: After Vessel Failure

(NO): Consequential "NO"

T: Temporarily

NC: Not considered in EET

(YES): Consequential "YES"

Page 2 of 2

Page 2 of 2

Page 2 of 2

Containment Bypass EET Sequences With Frequencies Greater Than $10^9/\text{yr}$

[illegible]

AVF: After Vessel Failure
(NO): Consequential "NO"
T: Temporarily

Table 4.3-6

PLANT DAMAGE STATES

	PLANT DAMAGE STATE	FREQUENCY	PERCENT OF TOTAL CDF
1	TEAYS	8.0E-06	26
2	SEKYS	3.0E-06	10
3	LEAYS	2.8E-06	9
4	SLLYS	2.7E-06	9
5	SEBYS	2.6E-06	8
6	TECNL	2.1E-06	7
7	LEHYS	2.0E-06	7
8	LEGYS	1.8E-06	6
9	SEEYS	9.9E-07	3
10	SEAYS	9.5E-07	3
11	GILYB	6.5E-07	2
12	LEIYS	5.5E-07	2
13	GLDYB	4.4E-07	1
14	GLCYB	2.7E-07	-
15	SEBNL	2.6E-07	-
16	GLEYB	3.1E-07	-
17	GRAYB	2.2E-07	-
18	GLBYB	1.3E-07	-
19	TEFYB	1.3E-07	-
20	SEANL	1.2E-07	-
21	SLDNL	1.2E-07	-
22	SEENL	1.1E-07	-
23	TEBYS	1.0E-07	-
24	SLDYS	6.4E-08	-
25	LEHNL	6.2E-08	-
26	TEANL	4.0E-08	-
27	TEBNL	3.2E-08	-
28	GLENB	1.8E-08	-
29	TEAYI	1.7E-08	-
30	GLFYB	1.4E-08	-
31	SECYS	1.2E-08	-
32	SEFYB	1.0E-08	-
33	TEFNL	8.7E-09	-
34	GLCNE	8.7E-09	-
35	GLANB	8.3E-09	-
36	GLENB	4.7E-09	-
37	SEJYS	4.5E-09	-
38	LEJYS	4.3E-09	-
39	LEBYS	3.4E-09	-
40	TECYS	3.1E-09	-
41	TECNI	1.9E-09	-
42	LEIYI	1.4E-09	-
	TOTAL	3.1E-05	

Table 4.3-7

SEQUENCE SELECTION TO MEET REQUIREMENTS OF GL 88-20, APPENDIX 2

GENERIC LETTER REQUIREMENT	SELECTED PDS FROM TABLE 4.3-6
Any functional sequence that contributes $1E-6$ or more per reactor year to core damage	Items 1-8 ¹
Any functional sequence that contributes 5% or more to the total core damage frequency	Items 1-8
Any functional sequence that has a damage frequency greater or equal to $1E-6$ per reactor year and that leads to containment failure which can result in a radioactive release magnitude greater than or equal to the BWR-3 or PWR-4 release categories of WASH-1400	Potential sequences addressed in this table through the first two items
Functional sequences that contribute to a containment bypass frequency in excess of $1E-7$ per reactor year	Items 11, 13, 14, 16, 17, and 18
Any functional sequence judged to be important contributors to core damage frequency or from containment performance.	Items 15, 25, 29 and 42

1. For this analysis, item 5 is binned with item 2.

Table 4.3-8

PLANT DAMAGE STATES ANALYZED FOR SOURCE TERM

Analyzed Plant Damage State	Damage State Frequency
TEAYS	9.0×10^{-6}
SEKYS	6.8×10^{-6}
LEGYS	4.3×10^{-6}
LEAYS	2.8×10^{-6}
SLLYS	2.7×10^{-6}
TECNL	2.1×10^{-6}
GILYB	6.5×10^{-7}
SEBNL	6.9×10^{-7}
GLCNB	2.8×10^{-7}
GLEYB	7.9×10^{-7}
GEAYB	2.2×10^{-7}
GLANB	1.5×10^{-7}
LEHNL	6.2×10^{-8}
TEAYI	1.9×10^{-8}
LEIYI	1.4×10^{-9}

failures of the basemat. Of the major structural failure modes in the containment wall, the lowest pressure capacity is associated with a membrane failure of the cylinder due to hoop stress. In the basemat, the lowest pressure capacity is associated with a flexural failure near the junction with the containment wall. However, this failure mode has a median pressure capacity greater than that of the hoop membrane failure of the cylinder wall. In all cases for structural failure modes, it was assumed that the failure condition leads to a large leak area (about 1.0 ft²) and rapid depressurization of the containment.

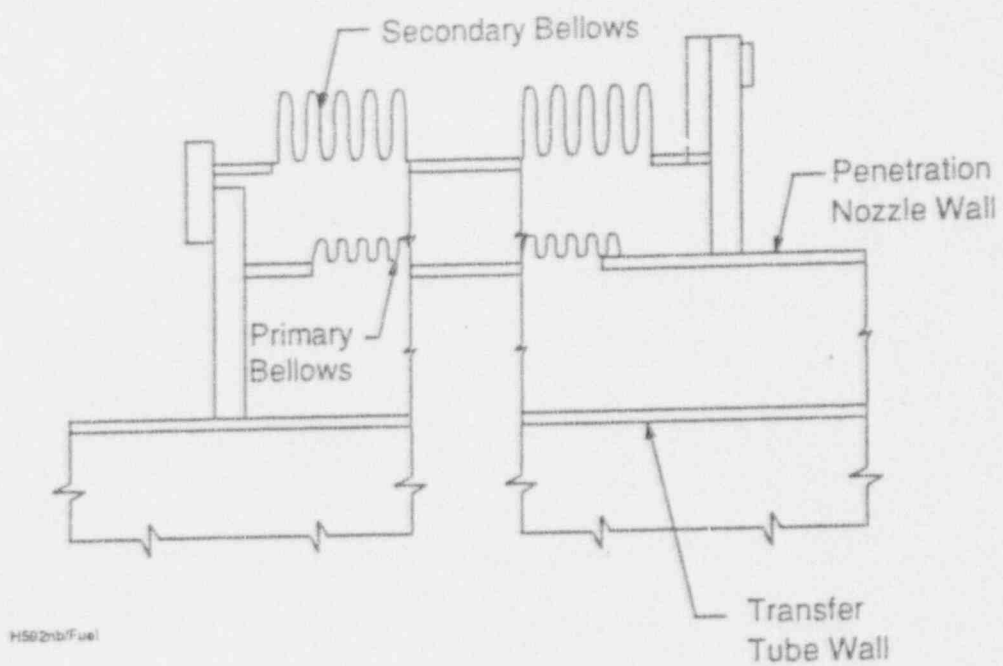
The potential for localized failure at a containment penetration was evaluated for the equipment hatch, the personnel airlock, and the fuel transfer tube, and a sampling of other pipe and electrical penetrations. The controlling failure mode of the fuel transfer tube was found to be buckling of the secondary bellows inside the containment building. The controlling failure mechanism associated with both the equipment hatch and personnel airlock is due to local liner strain concentrations around the penetration sleeves which lead to liner tearing. A breach of the pressure boundary at the other piping penetrations evaluated is not expected prior to other failure modes of the containment building.

By ranking the failure modes by their median pressure capacity, the most critical failure modes are associated with buckling of the secondary bellows of the fuel transfer tube at 157 psig, localized liner tearing at the equipment hatch at 160 psig, and localized liner tearing at the personnel hatch at 169 psig. Schematic drawings of the fuel transfer tube bellows and the liner transition region of the equipment hatch are shown in Figures 4.4-1 and 4.4-2. The next most critical failure mode corresponds to the hoop membrane failure in the cylindrical portion of the reactor building wall at 175 psig. The first three of these potential failure modes (157 psig, 160 psig, and 169 psig) may not create a failure area sufficient to depressurize containment. The containment failure area is assumed to be the sum of all containment failures (i.e., failure areas) bounded by the containment pressure.

To summarize the findings of the SONGS plant specific containment structural analysis, Table 4.4-1 outlines the median pressure capacities, the associated uncertainty of failure pressures, and the 95% nonexceedance pressures of the dominant containment failure modes. To establish the basis for assessing the extent of fission product release, Table 4.4-2 provides the failure areas of the top three containment failure locations.

Figure 4.4-1

FUEL TRANSFER TUBE BELLOWS INSIDE THE CONTAINMENT BUILDING



VERTICAL SECTION OF EQUIPMENT HATCH

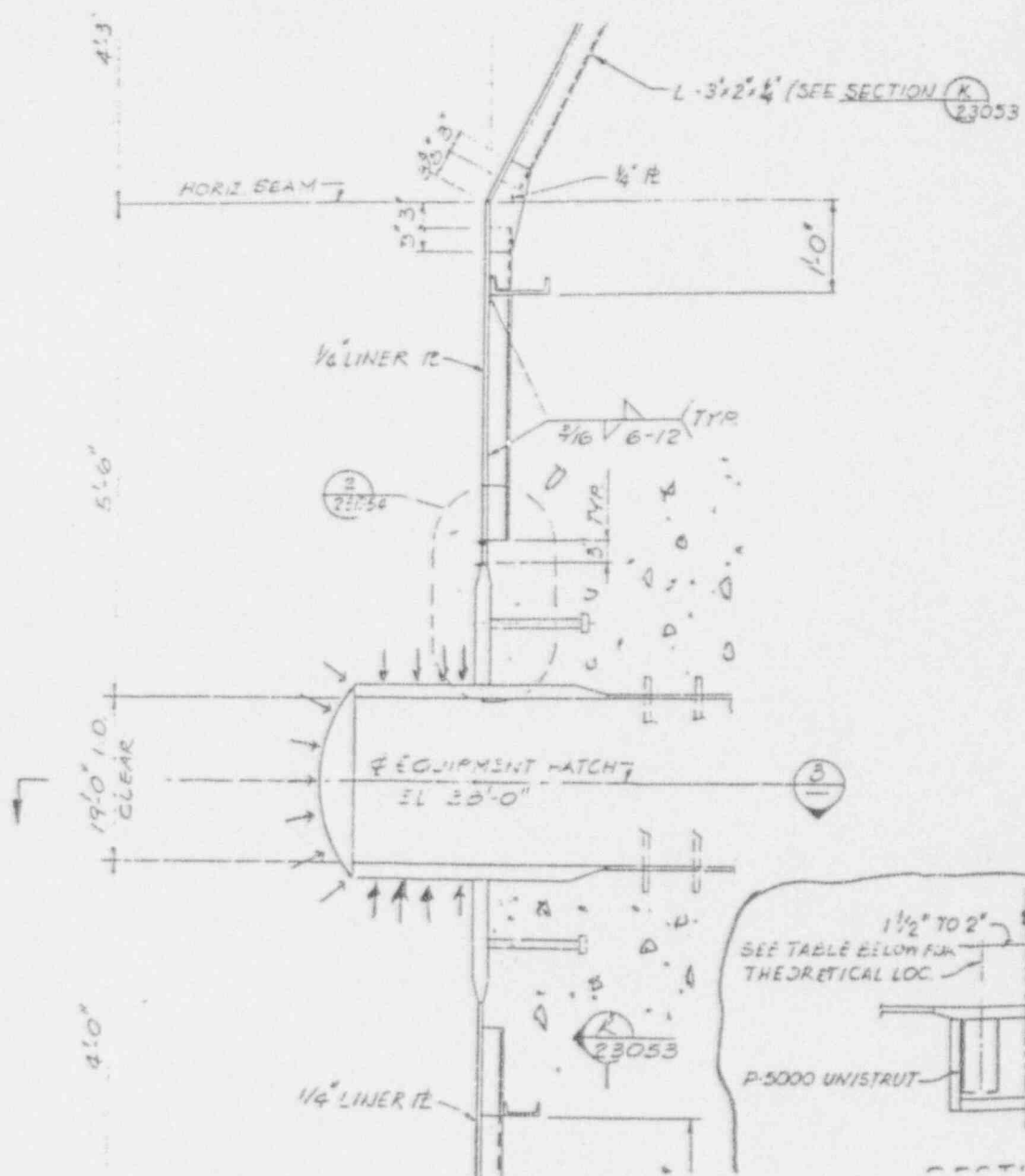


Table 4.4-1

PRESSURE CAPACITIES FOR THE CONTROLLING FAILURE MODES

Interior Temperature = 420°F

Failure Mode	Median Pressure Capacity (psig)	Overall Uncertainty (β_1)	95% Nonexceedance Pressure (psig)
Fuel Transfer Tube Secondary Bellows	157	0.28	99
Liner Tear at the Equipment Hatch	160	0.18	119
Liner Tear at the Personnel Airlock	169	0.15	132
Cylinder Hoop Membrane	175	0.14	139
Dome Membrane	185	0.15	144
Basemat Flexure	198	0.22	138
Wall Basemat Junction	232	0.21	164
Cylinder Meridional Membrane	232	0.15	181

Table 4.4-2

MEDIAN LEAK AREAS AND VARIABILITIES

Failure	Median Leak Area (in ²)	Uncertainty (β)
Buckling of Fuel Transfer Tube Secondary Bellows	0.45	0.70
Liner Tearing at Equipment Hatch	1.8	0.50
Liner Tearing at Personnel Airlock	1.6	0.53

4.4.2 Unlikely Failure Modes

Hydrogen Combustion

A phenomenological evaluation was performed to assess the susceptibility of the SONGS 2/3 containment to early failure due to hydrogen deflagration and detonation. The evaluation was based on conservative assumptions for a worst-case loss of secondary heat sink sequence.

A best-estimate assessment of the in-vessel hydrogen production at SONGS 2/3 is possible using the MAAP PWR Code 19.01. By accounting for: (1) the number and surface area of the fuel pins in the SONGS 2/3 core, (2) the flow area through the core and bypass, (3) limiting injection once the core has uncovered to 132 gpm (equivalent to 3 charging pump flows), and (4) postulating vessel failure 30 minutes after the core has relocated to the lower reactor head, MAAP calculates in-vessel hydrogen production of 1065 lbs, equivalent to 33 percent core cladding (core zircaloy) oxidization. The adiabatic isochoric complete combustion (AICC) of this hydrogen mass does not result in a pressure that exceeds the ultimate containment internal pressure capacity taken to be 189 psia. The amount of hydrogen that accumulates in the SONGS 2/3 containment can be increased by suppressing all burning and accounting for the ex-vessel hydrogen production which results from oxidization of zircaloy and iron in the relocated core debris found in the containment after vessel failure. This represents a worst-case estimate.

The potential containment pressurization resulting from hydrogen combustion is bounded by calculating the adiabatic isochoric complete combustion (AICC) of this assumed hydrogen inventory. The adiabatic calculation ignores the presence of any passive or active heat sinks in the SONGS 2/3 containment. Thus, all the combustion energy is used to heat the containment atmosphere and produce the largest possible pressure increase. The calculation assumes that all the hydrogen produced accumulates in containment and burns all at one time. It also ignores the possibility of hydrogen burning as it is released, in which case the containment pressurization would be much less severe. The selected worst-case scenario results in the global burning of 2433 lb of hydrogen and an estimated post-burn AICC containment pressure of 156 psia, which is well within the ultimate capacity 189 psia for the SONGS 2/3 containment. The 189 psia will result in a break large enough to depressurize the containment. The actual pressure rise calculated by MAAP for this burn is 115 psia. The MAAP calculation accounts for the operation of a single train of containment spray used to de-inert the containment and remove containment heat. The calculated pressure rise exceeds the 95% non-exceedance pressure (113 psia) for the fuel transfer tube secondary bellows. A break at this pressure would result in a 0.0031 ft² breach of the SONGS 2/3 containment which is not sufficient to depressurize containment. Note also that there is no potential for containment challenge due to hydrogen pocketing,

based on a walkdown of SONGS Unit 3 containment and review of SONGS 2/3 plant layout drawings.

The assessment of hydrogen detonation potential concludes that hydrogen detonation by direct energy deposition is not possible in the SONGS 2/3 containment since there are no potential ignition sources with sufficient energy to trigger such an event.

The potential for deflagration-to-detonation transition (DDT) was evaluated using engineering judgement and a procedure from Sherman and Borman (Reference 4.4-2). This procedure assumes that the potential for DDT can be assessed based on the mixture intrinsic flammability (detonation cell width) and type of geometry. Based on the open design of the SONGS 2/3 containment and its conduciveness to natural circulation, the containment gas is assumed to be uniformly mixed. The worst case hydrogen mass of 2433 lb cited above corresponds to 11.5% hydrogen in the 40% steam environment. This hydrogen concentration is inadequate to sustain a hydrogen detonation in the large open containment at SONGS. The DDT assessment concludes that failure of the SONGS 2/3 containment due to hydrogen detonation is very unlikely to occur.

Because only a small ignition source is required to initiate a deflagration, it is far more likely that combustible gases would be consumed within the containment by deflagration rather than detonation. However, even for a loss of secondary heat sink sequence (the worst-case SONGS 2/3 sequence with respect to hydrogen combustion), it is unlikely that enough hydrogen would accumulate to produce a deflagration that could challenge the containment ultimate pressure capacity. Typical SONGS 2/3 source-term MAAP runs, for example, show that molten core debris in the reactor cavity (when dry) acts as an ignition source and continuously burns hydrogen as it is generated during core-concrete attack. None of the sequences addressed in the SONGS 2/3 source-term analysis could realistically threaten containment due to hydrogen combustion.

Direct Containment Heating

Direct containment heating (DCH) is the process of directly heating the containment atmosphere by molten core debris should it be hydrodynamically forced out of the reactor cavity due to the primary system blowdown. A phenomenological evaluation was performed to examine the likelihood of SONGS 2/3 containment failure due to DCH. This evaluation was based on two different modes of vessel failure. This is necessary because the reactor vessels at SONGS 2/3 have no lower head penetrations.

In the absence of lower head penetrations, a very strong case can be made for depressurization of the primary system prior to the discharge of the core debris from the reactor vessel. If the primary system does not depressurize prior to core relocation into the lower plenum, natural circulation within the primary system will have heated the hot leg piping to a level where creep rupture failure would be predicted (Reference 4.4-3). Such a rupture

would result in failure over a large area of the hot leg and rapid depressurization of the primary system. If the primary system were not to depressurize prior to relocation of the core to the lower reactor plenum, but still remain at a high pressure, then natural circulation in the internally heated core debris would result in creep rupture failure of the reactor vessel somewhere along the belt line near the top of the core debris pool in the lower reactor vessel head (References 4.4-4, 4.4-5). Such a failure also results in a loss of the primary system gases before a large fraction of the core debris can be ejected from the vessel. Creep rupture failure of the primary system prior to the discharge of core debris from the reactor vessel implies that core debris is ejected from the vessel at a very low velocity. As a result, essentially all the core debris ejected from the failed reactor vessel remains in the cavity and DCH is not a concern.

The absence of lower head penetrations at SONGS 2/3 makes it difficult to assume vessel failure near the bottom of the core debris pool in the lower head. Such a failure at high RCS pressure would result in the core debris being ejected from the vessel at high velocity. Containment failure due to DCH as a result of a high pressure melt ejection from the SONGS 2/3 reactor vessel was evaluated. Based upon recent DCH experiments and the use of mechanistic models for debris dispersal, which take into account entrainment and de-entrainment of core debris at SONGS 2/3, the pressurization effect due to DCH at SONGS 2/3 is shown to be negligible.

DCH experiments for a large dry PWR (References 4.4-6, 4.4-7, 4.4-8, 4.4-9, 4.4-10) have shown that containment structures (geometry) have a first order (dominant) mitigating influence on the potential for DCH. For example, in the Argonne CWTI experiments (Reference 4.4-6), tests performed with a dry cavity compartment and the seal table structure present showed that only 1 to 5 percent of the debris that left the cavity contributed its energy directly to the air of the containment building. Comparison of the SONGS 2/3 and Zion cavity/instrument tunnel designs clearly indicates that the SONGS 2/3 geometry would trap and de-entrain more debris than in the Zion configuration. Therefore, the results of DCH experiments performed for Zion are a conservative estimate of what they might be for an analogous SONGS 2/3 DCH experiment.

The DCH modeling methodology focuses on:

- The debris mass that could potentially be particulated in the reactor cavity and cavity ventilation ducts
- That fraction of the entrained (particulated) debris which could escape the change in flow direction caused by the cavity ventilation ducts

The analysis is inherently conservative since it neglects all internal structure in the cavity and cavity cooling ducts (see Figure 4.1-1). That fraction of the debris not particulated would

have such a large characteristic dimension that the primary system piping, the steam generators, and the RCPs would collect it and prevent it from entering the containment atmosphere. The assessment of the entrained particle size utilizes a conservative approach based on the maximum gas velocity in the reactor cavity and a single droplet Weber number criterion (Reference 4.4-11).

The potential containment pressurization is bounded by assuming that the small fraction of the ejected debris mass which could potentially contribute to DCH (about 5 percent in a Zion-like cavity, and even less at SONGS 2/3) is 100 percent efficient at transferring its heat to the containment atmosphere. The initial debris temperature is assumed to be 4040°F at the time of RPV failure. DCH combined with a hydrogen burn is not considered feasible in the best estimate analysis. The resulting containment pressure rise due to DCH alone would be about 5 psig. This conservative estimate of the peak containment pressure due to DCH is well within the containment ultimate internal pressure capacity.

Steam Explosions

Steam explosion phenomena were evaluated for both in-vessel and ex-vessel events as potential mechanisms for early containment failure under severe accident conditions. A steam explosion refers to a boiling process in which steam production occurs at a rate larger than the rate at which the surrounding media can acoustically relieve the pressure increase. This leads to the formation of a shock wave.

The issue for in-vessel steam explosions is whether an explosion of sufficient magnitude to fail the reactor vessel, with consequential failure of the containment, could occur. This was addressed by evaluating the fundamental physical processes required to create an explosion of such magnitude. The analysis closely follows the IDCOR assessment of this phenomenon (Reference 4.4-12) and indicates that explosions of this magnitude are not likely to be established within the confines of the SONGS 2/3 reactor vessel. This is in agreement with the findings of the NRC-sponsored Steam Explosion Review Group (SERG, Reference 4.4-13) which concluded that an in-vessel steam explosion leading to containment failure was very unlikely.

Ex-vessel steam explosions are addressed by considering the potential for both the rapid steam generation that could occur as a result of the explosive interaction and the shock waves that could be formed and propagated to the containment boundary.

The absence of lower head penetrations at SONGS 2/3 has the effect of causing the RCS to fail due to creep rupture during a severe accident. This type of failure depressurizes the primary system before the majority of the core debris escapes. As a result, the amount of core debris ejected from the vessel at high velocity is only a small fraction of the total debris that relocates to the lower reactor vessel head.

The existing experimental work and analyses examined provide a thorough basis for evaluating steam overpressure challenges to containment integrity and strongly indicate that sufficient steam overpressure to challenge the containment integrity would not be achieved under realistic high pressure melt system conditions. The calculated increase in containment pressure caused by postulated steam generation during an ex-vessel steam explosion, 4 psig, is well within the capability of the containment. The calculated induced shock wave pressure at the containment wall is 13 psig. Since the containment has an ultimate capacity of 189 psia, blast effects from potential steam explosions are not a concern. Shock wave propagation to the containment boundary yields overpressure values well within the containment capability.

It is concluded that the slumping of molten debris into the RPV lower plenum could not result in sufficient energy release to threaten the vessel integrity and hence would not lead directly to containment failure. Likewise, evaluations of both the steam generation rate and shock waves induced by ex-vessel explosive interactions show that these would not be of sufficient magnitude to threaten the containment integrity.

Thermal Attack of Containment Penetrations

The susceptibility of SONGS 2/3 containment penetrations to failure due to thermal loading has been evaluated for severe accident conditions. Failure of the "leak-tightness" of containment penetrations could provide a pathway through the containment structure for the release of fission products. The locations of the penetrations were reviewed to assess the potential for direct contact of penetrations by core debris. Data on the non-metallic seal materials used in the SONGS 2/3 penetrations (Reference 4.4-8) were compiled and used in conjunction with existing, environmental qualification work to determine the penetrations response to expected worst-case severe accident conditions at SONGS.

The evaluation of debris dispersal in conjunction with the location of the mechanical and electrical penetrations reveals that it is unlikely for these penetrations to be in direct contact with molten debris dispersed during postulated high pressure melt ejection. The majority of entrained debris would be removed prior to reaching the lower compartment, and there are no direct paths by which core debris could contact any containment penetrations.

Personnel access to the containment operating deck is provided through an airlock with interconnected doors. This access hatch is located at elevation 62 ft 7 in (bottom of penetration). The equipment hatch and emergency personnel hatch are located in the annular compartment at elevations 28 ft 6 in and 32 ft 10.5 in respectively. These three access hatches all employ double gasketed flanges and contain provisions for leak testing of the flange gasket seal.

Single barrier piping penetrations are provided for all pipes passing through the SONGS 2/3 containment. Closure of these piping penetrations is provided by special flued welds which attach the process piping and penetration sleeve to the containment liner.

Two types of electrical penetration assembly (EPA) configurations are used for all SONGS 2/3 electrical conductors passing through the containment wall. The method of sealing the electrical penetrations depends on the type of cable and connector assemblies involved. A canister type assembly is used for medium voltage power circuits (6900 volts), whereas a modular-type assembly is used for the low voltage power circuits (600 volts and below). Insulated conductors passing through the header plate of a canister type penetration are potted to effect a pressure seal. Mechanical splices within the potting compound provide gas stops. High voltage insulating bushings and seals also contribute to the gas barrier. The modular type assemblies consist of a header plate in which a group of small, interchangeable modular penetrations fit. The header plate of this penetration mates with a flange welded to the penetration and bolted to a flange welded to the penetration sleeve. Double silicone O-rings provide a monitorable seal between the assembly's header plate and the penetrations sleeve's flange.

The mechanical and electrical penetrations that have metallic gaskets or seals are not susceptible to thermal degradation due to containment gas temperatures. Those penetrations which employ non-metallic gaskets can withstand containment temperatures up to and beyond 486°F. However, such elevated temperatures are not predicted for the SONGS 2/3 containment for sustained periods of time. Therefore, failure of containment due to thermal loading of penetration is not considered as a failure mode.

Vessel Thrust Force

In this phenomenological evaluation, a strategy was developed to account for postulated containment failure due to excessive thrust force caused by molten core debris being ejected from a failed reactor vessel. The concern is that the thrust force could cause the reactor vessel to shift position and tear out containment penetrations.

The maximum jet thrust force which could be expected during the expulsion of molten core debris through a failed SONGS 2/3 reactor vessel could not lift the vessel and its internals, even without considering the ability of the vessel support structure to withstand the thrust load. If the coolant loop piping and shield wall are considered, a much larger force would be required to dislodge the reactor vessel. Even if the vessel could shift, the SONGS 2/3 containment is configured in such a manner that reaction forces cannot be transmitted to the containment wall. Therefore, this postulated failure mode is prevented by the plant design.

4.4.3 Failure Modes Considered

Containment Overpressure

Containment overpressure caused by steaming and/or generation of noncondensable gases can be a potential late containment failure mode for SONGS 2/3. Depending on the specific accident sequence characteristics, overpressure failures may be observed across a wide range of event times. The potential for containment overpressure failure exists in severe accident scenarios where sufficient containment heat removal is not available. Thus, it is dominated by failure of secondary side cooling and an inability to inject the RWST, failure to align for recirculation, and failure of all containment heat removal.

As discussed in Section 4.4.1, the failure location would most likely be at the fuel transfer tube secondary bellow. Failure of the fuel transfer tube secondary bellow, however, is limited to an area of 0.0031 ft². This containment failure area is unlikely to relieve the rising containment pressure. As containment pressure continues to rise, failure is expected at other locations. Following the bellows failure, tearing of the equipment hatch is expected to occur at 175 psia with an area of .0125 ft². The failure areas of both the bellows and equipment hatch are summed to produce a total containment failure area. This process of summing failure areas continues as the pressure rises and other locations are affected until the ultimate capacity of 189 psia is reached. At this pressure the cylindrical loop tendons are assumed to break resulting in a failure area (currently modeled as 1 ft²) large enough to depressurize containment. Table 4.4-1 lists the assumed containment failure modes, their median pressure capacity, and uncertainty of failure pressure. Table 4.4-2 lists the maximum failure area of the first three containment failures. No attempt is made to implement a leak before break criteria on this incremental containment failure process. The result is that the short term fission product release from the containment may be slightly over-estimated.

Containment Isolation Failure

The Containment Isolation System (CIS) at SONGS 2/3 is designed to preserve the ability of the containment boundary to prevent or limit the escape of fission products that may result from postulated accidents. In the event of a possible radiation release from the SONGS 2/3 containment through process lines, the containment isolation system automatically isolates all lines penetrating the containment which do not serve an accident mitigating function. The design basis for the CIS is detailed in Section 6.2.4 of the SONGS 2/3 UFSAR and, therefore, is not duplicated in this analysis.

The CIS consists of two redundant trains, Train A and Train B. The instrumentation and controls of the valves in Train A are physically and electrically separated and independent of the instrumentation and controls of the valves in Train B.

Independence is adequate to retain the redundancy required to maintain the equipment functional capacity necessary to close the containment isolation valves following those accidents which require containment isolation.

The CIS is automatically actuated by the CIAS from the ESFAS by a two-out-of-four containment high pressure signal (≥ 3.4 psig), manual operation, or a loss of electrical power to two of the four measurement channels or actuating logics. To provide diversity in the parameters sensed for initiation, a SIAS will also actuate the CIS components with the exception of the Main Steam Isolation Valves, Main Feedwater Isolation Valves, and the Component Cooling Water containment isolation valves. In addition, the containment purge supply and exhaust isolation valves are closed by a Containment Purge Isolation Signal.

For the CIS at SONGS 2/3 to function successfully during required events, the following must occur:

- A single train of the Containment Isolation System must actuate;

- A single valve in each penetration must close

The frequency for failing to isolate the SONGS 2/3 containment on demand is calculated for this IPE using fault tree analysis in the SONGS IPE. The following assumptions are made in developing the CIS Fault Tree:

- Manual valves which are not opened during power operation and are assumed to remain closed during and after a severe accident;

- For normally closed valves which are not opened or realigned during power generation, the probability of failure to remain closed is negligible; therefore, these valves are not modeled;

- Only those penetrations directly connected to the containment atmosphere or which interface with reactor coolant are modeled;

- Only those penetration valves which are automatically closed by the Containment Isolation Signal are modeled. Hence, no operator action is taken to achieve isolation function.

All containment penetrations, regardless of size, which meet the criteria above were incorporated into the fault tree model.

The possibility of containment failure via accident mitigation system lines was also considered. If safety injection was terminated and RCS pressure remained high, reactor coolant could potentially leak past the injection valves, through the safety injection pumps, back to the RWST, and then out to the

environment. However, this sequence and those similar to it were dismissed as potential containment failures due to the design of the injection lines (two check valves inside containment and one check valve located on the suction and discharge sides of each pump).

Two factors eliminated the containment spray lines as potential leak paths. First, each spray line contains four check valves which isolate the containment (1 check valve inside containment, 2 check valves on the discharge side and 1 check valve on the suction side of the pump). Secondly, source term plate-out would reduce the radioactive release. Therefore, the containment spray lines were not modeled as significant radioactive release paths.

As a result of the CIS analysis fifteen cutsets were identified. The frequency for failing to isolate the SONGS 2/3 containment on demand was calculated to be $6.5E-5$. The dominant containment isolation failure mode was failure of the common circuitry for the CIAS Trains A & B with a frequency of $8.5E-6$. The frequency for failing to isolate individual containment penetrations ranged from $6.0E-6$ to $1.3E-7$.

Containment Bypass

Containment bypass is another possible failure mode for SONGS 2/3. Containment bypass refers to failure of the pressure boundary between the high pressure RCS and a lower pressure line penetrating containment. This results in a direct pathway from the reactor coolant system to the Auxiliary Building or the environment, bypassing the containment. Containment bypass is considered as an accident initiator that can lead to core damage because the loss of cooling fluid to a location outside containment disables the ECCS recirculation for long-term core cooling. The most likely mechanisms for this failure mode, identified for SONGS 2/3 as being significant in terms of potential consequences, are an ISLOCA or V-sequence, and a steam generator tube rupture. Note, however, that such bypass sequences (i.e., SGTR and ISLOCA) contribute about 7 percent to the total SONGS 2/3 core damage frequency.

Molten Core-Concrete Interaction

Molten core-concrete interaction (MCCI) was evaluated using a simple bounding analysis model to determine if the aggressive attack on concrete by molten core debris could lead to late containment failure. The analysis assumes that the concrete ablation rate is proportional to the total heat generation rate due to decay heat and chemical reactions. The model uses empirical parameters determined from available MCCI experimental data.

At SONGS 2/3, all core debris ejected from the reactor vessel is expected to be contained in the reactor cavity. MCCI in the

cavity is hypothesized to cause containment failure either by penetrating the cavity floor, liner, and basemat, or by weakening the RPV support sufficiently that the vessel and attached piping move and tear out associated containment penetrations. The combined thickness of the SONGS 2/3 cavity floor and basemat is 7 ft, while the cavity walls beneath the reactor vessel are at least 5 ft thick. Experimental evidence (Reference 4.4-14) suggests that the ratio of sideward to downward erosion rates is non-zero but much less than one. Even if this were not true, examination of the SONGS 2/3 cavity design and RPV supports indicates that failure at containment penetrations, caused by the erosion of the cavity walls and embedded structural steel columns that support the RPV, will not occur. Basemat penetration is, therefore, the only MCCI failure criterion for SONGS 2/3.

Although some fraction of the core could remain cooled in-vessel while the bulk of the core is expelled, it is convenient to make the conservative assumption that the entire core is expelled with its full initial inventory of fission products and zirconium. In many accident sequences, a substantial fraction of the zirconium can be oxidized in-vessel, as opposed to being oxidized during corium-concrete attack. This potentially decreases the duration of the zirconium oxidation phase and slows corium-concrete attack overall, since the chemical energy of the corium is decreased. This possibility is not considered here. Moreover, a substantial fraction of the core's initial fission product inventory would not reside in the corium attacking the basemat. Fission products are distributed throughout the primary system and containment compartments in a manner that depends upon the severe accident progression. Volatile fission products initially present in the corium can be vaporized or entrained to form aerosols which are transported throughout the containment. The net effect of these (neglected) mechanisms is to reduce the mass of fission products and decay heat in the corium as it attacks the cavity floor.

The estimation of containment failure time due to MCCI in the cavity accounts for changes in the governing phenomena as time progresses. The first phase of the erosion process is considered to be the interval during which unoxidized zirconium in the core debris reacts with steam and carbon dioxide liberated by the concrete erosion. During the second phase, the chemical reaction energy is considered negligible and the concrete decomposition enthalpy is reduced to reflect the lack of chemical reaction. The calculation method determines whether containment failure would occur before the zirconium in the core debris bed is depleted. If containment failure occurs first, the time at which containment failure would occur is obtained by straightforward calculation. If zirconium depletion occurs first, the calculation procedure becomes more complicated. First, the time interval to reach zirconium depletion is determined. Then, an iterative process is required to determine the predicted depth of concrete erosion corresponding to zirconium depletion. Finally, the additional concrete mass that must be eroded to cause containment failure and its corresponding time interval is determined.

The SONGS 2/3 analysis of basemat melt-through assumes that the ratio of sideward to downward ablation rate is constant and equal to between 0.2 and 0.5. The cavity dry-out time for a station blackout is about 6 hours after trip, based on typical SONGS 2/3 MAAP results, and the nominal full power for SONGS 2/3 is 3411 MW (11.6×10^9 Btu/hr). Assuming these values results in containment failure due to basemat melt-through between 16 and 24 hours after vessel failures.

Molten Core Concrete Interaction can be excluded from consideration as early containment failure mechanism at SONGS 2/3. It can, however, be considered a potential late containment failure mechanism which does not have the immediate source term consequences of those containment failures which result in airborne releases. The fact that an MCCI failure of the cavity floor results in a ground release path to the outside environment implies some scrubbing effects. Therefore, the immediate source term release due to MCCI induced failure of the cavity floor would be small. This fact is due to both the late containment failure time and the release location (below ground). Severe accident recovery actions are only considered for SBO sequences. A recovery action which would result in continuous flooding of the reactor cavity would arrest MCCI.

4.4.4 Summary of Containment Failure Characterization

Several postulated containment challenges have been demonstrated, through the phenomenological evaluations, to be inconsequential for the SONGS 2/3 containment. These potential failure modes are considered to be highly unlikely to occur at SONGS 2/3 since the predicted pressures resulting from a realistic assessment of these failure mechanisms are far less than the containment ultimate strength. Table 4.4-3 summarizes the results of these containment failure mode evaluations.

4.5 Containment Event Tree (CET)

The SONGS 2/3 IPE used extended event trees (EETs) that incorporated containment event tree aspects, as documented in Section 4.3.1. A separate CET was developed in parallel to the assignment of plant damage states (PDS) to the EET endstates. This parallel development provided a check of the EET analysis documented in Section 4.3.1, and provided a convenient tool to assist in the PDS binning and screening process (Section 4.3.3).

Table 4.4-3

**PHENOMENOLOGICAL EVALUATION SUMMARIES
ON POSTULATED CONTAINMENT FAILURE MODES**

Failure Mode	Phenomena	Issue/Failure Mechanism	Major Uncertainty	Impact
Hydrogen combustion	In-vessel H ₂ generation Ex-vessel H ₂ generation Steam inerting Auto ignition	Breach containment by overpressurization due to H ₂ burn or detonation	Amounts of H ₂ and CO Flammability of containment atmosphere	No early containment failure Steam inerting can prevent long-term containment failure due to hydrogen burns
Direct containment heating (DCH)	RPV failure Debris dispersion Influence of containment structures Hydrogen combustion/steam inerting Thermal exchange with entire air space	Early breach of containment by rapid overpressurization High-pressure melt ejection from the RPV is not expected to occur	Degree of dispersal in containment Hydrogen combustion	Containment pressures for DCH far less than ultimate structure capability
Steam explosions	Missile generation Rapid steam generation Shock waves	Missile impact Early containment overpressurization and breach	Occurrence of multiple conditions required to produce large scale steam explosion	No threat to RPV or containment Promotes debris dispersal and cooling
Molten core-concrete interactions (MCCI)	Concrete ablation and decomposition Gas evolution (H ₂ , CO, CO ₂) Debris spreading H ₂ recombination	Basemat penetration after several days of attack Failure of containment penetration lines connected to RPV if RPV supports fail due to sideward ablation of concrete	Presence of water to quench debris Debris coolability	If the reactor cavity remains dry, MCCI induced failure of the cavity floor can occur within 16 to 24 hours of vessel failure.

Table 4.4-3

**PHENOMENOLOGICAL EVALUATION SUMMARIES
ON POSTULATED CONTAINMENT FAILURE MODES
(continued)**

Failure Mode	Phenomena	Issue/Failure Mechanism	Major Uncertainty	Impact
Vessel blowdown	RPV rupture RPV thrust forces RPV restraints	Failure of containment penetration lines connected to RPV	RPV failure and failure size	None or limited RPV displacement Challenge bounded by design basis
Thermal loading on penetrations	Degradation of non-metallic components	Containment breach; leakage path	Magnitude and duration of elevated containment gas temperature Behavior of non-metallic materials at high temperature	No loss of containment integrity expected Potential for long-term loss of electrical functionality
Overpressurization	Noncondensable gas generation Steam generation H ₂ burn	Containment breach	Timing, size, and location of containment breach	FP release to environment (air or soil) or other buildings
Containment isolation failure	Containment piping Operator response Signal dependency	FP release path through unisolated piping	FP plate-out/plugging	Low probability of direct FP path to environment or Auxiliary Building
Containment bypass	Interfacing Systems SGTR	FP release path that does not pass through containment air space	FP deposition in building outside containment Number of ruptured SG tubes Size location of break outside containment Water scrubbing at break location FP deposition outside containment	Low probability of direct FP path to environment or Auxiliary Building

The CET used in the SONGS 2/3 IPE (Figure 4.5-1) assisted in the assignment of PDS designators to the systemic sequences from the EETs. However, there is not a one-to-one correspondence between the plant damage states and the CET end states, since more than one PDS can correspond to a single CET end state. Thus, the CET provides a natural tool for binning certain PDS together. This is effectively what was done in Section 4.3.3. The advantage of using the CET is that a PDS with important source term characteristics but a relatively low frequency (e.g., a PDS which represents a unique systemic sequence) can be easily distinguished from PDS with higher probabilities.

Three CET endstates (6, 8, and 10) were identified as representing systemic sequences with significant source term consequences but low frequencies. These endstates provided the logical basis for selecting additional plant damage states of interest for source term analysis, as shown in Table 4.3-7.

4.5.1 Overview of CET Structure

In using the CET to assess the containment conditions following the onset of core melt, the following characteristics are considered:

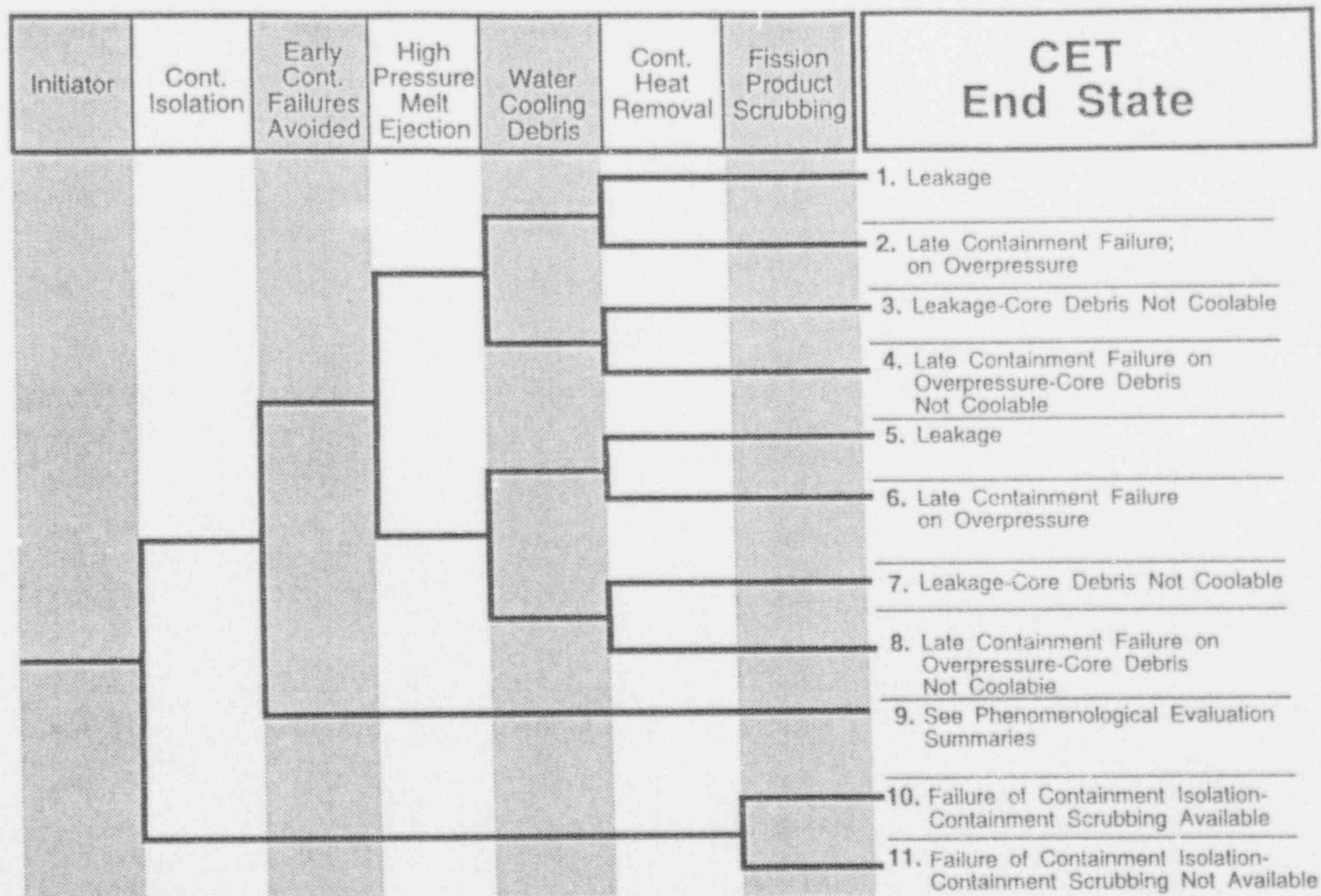
- (1) the accident initiator,
- (2) the status of containment isolation,
- (3) the relative pressure at which the core debris is ejected from the reactor vessel,
- (4) the ability to cool the core debris ex-vessel,
- (5) the availability of containment heat removal and
- (6) the ability to scrub fission products from the containment atmosphere.

All of the severe accident sequences binned to a particular CET end state can be characterized by the same source term release. To determine the nature of the source term releases it is necessary to analyze a severe accident scenario from each CET end state. The selection of the accident scenarios to be analyzed as representative of a particular CET end state is based on selecting either the sequence with the highest frequency or the sequence which would be expected to result in the largest source term release.

The general guidelines used for development of the SONGS 2/3 CET are summarized below:

1. The CET top events reflect but do not alter the quantification of the SONGS 2/3 Level I and extended event trees.

Containment Event Tree



RA92D005.CDR

2. The CET top events and structure provide the detail necessary to characterize the fission product source term releases.
3. The CET considers factors which dominate the containment response. Thus, the top events consider broad categories of containment behavior.
4. The CET considers early containment failure timing (i.e., containment failure at or shortly after vessel failure). The impact of postulated early containment failure mechanisms on the SONGS 2/3 containment has been described in phenomenological summaries (Section 4.4.2). The results indicate a negligible impact on containment performance.

Based upon these guidelines, the SONGS 2/3 CET has been arranged to first determine the status of the containment (i.e., bypassed, intact, or failed), and then to consider the accident progression and containment safeguards availability. The final node in the CET focuses on the containment spray systems ability to reduce the airborne residence time of fission products released to the containment atmosphere. It is important to realize that the nodes of the CET describe the integrated accident progression and cannot be considered independent of each other.

The first two nodes determine the containment status during a severe accident. The first node addresses the class of accident initiator. It therefore immediately identifies which sequences result in containment bypass (i.e., SGTR and V-sequences) and prompt depressurization of the primary system (i.e., large LOCAs). The second node in the CET addresses the status of containment isolation.

To be consistent with the guidelines provided in Appendix A of NUREG-1335, the third node of the CET differentiates between the possibility of early, dynamically induced containment overpressurization of the containment versus gradual overpressurization. This node is provided as a point of reference, since a review of the phenomenological evaluation summaries shows that there are no dynamic challenges to the containment associated with vessel failure. The fourth CET node addresses the way in which the reactor vessel fails. This node is also provided as a point of reference. The absence of lower reactor head penetrations at SONGS 2/3 allows a strong case to be made for creep rupture failure of the primary system piping or reactor vessel before a significant portion of the core debris in the lower reactor vessel can be ejected. Likely creep rupture failure of the primary system or reactor vessel implies that the

primary system is expected to be at low pressure when corium is ejected from the reactor vessel.

Node five of the CET addresses the question of whether or not water is available to cool the ex-vessel core debris. Since the postulated low pressure melt ejection from the SONGS 2/3 reactor confines core debris to the reactor cavity, the only means of cooling this debris is by injecting water through the failed reactor vessel. The sixth node of the CET concerns whether or not there is adequate containment heat removal to prevent overpressurization of the containment. This node addresses the operability of the containment spray system in recirculation mode and/or the operability of the four containment emergency cooling units CEFCs. The seventh and final CET node addresses the SONGS 2/3 containment systems ability to scrub fission products from the containment atmosphere.

4.5.2 CET Top Events and Success Criteria

In section 4.5.1 the top nodes of the SONGS 2/3 CET are briefly described. In this section, the top nodes of the CET are described in detail, and the success criteria for the top nodes of the CET are defined. The consequences of some assumptions made in the SONGS 2/3 IPE Level II analysis and their effect on the SONGS 2/3 CET are also discussed.

Initiator

The SONGS 2/3 Level I IPE identifies fourteen different types of severe accident initiators. By the onset of core melt, most of the distinguishing characteristics of the accident initiator have disappeared. The Level I accident initiators can therefore be binned into a few general accident initiators as described in Section 4.3.2. The four general accident initiators defined for the SONGS 2/3 Level II Plant Damage States are:

- 1) Large LOCAs (i.e., ≥ 6 " ID break), which include ATWS accidents,
- 2) Small LOCAs (i.e., < 6 " ID break in the primary system), which include transients with stuck open pressurizer safety valves;
- 3) Containment Bypass accidents, which include steam generator tube ruptures and V-sequences, and
- 4) Transients

Transients are generally characterized by the absence of an uncontrolled loss of water from the primary system. Thus, steamline and feedwater line breaks are designated as transients.

The CET accident initiator's main purpose is to provide an initial binning of the Level I accident sequences which meet the core damage screening criteria. The binning by these four initiator types impacts the timing of core damage due to the rate at which primary system water is lost. The most important consequence of this CET accident initiator is that it immediately identifies sequences which result in containment bypass (i.e., SGTR and V-Sequences) and prompt depressurization of the primary system (i.e., Large LOCAs).

Containment Isolation

Containment isolation, as defined in the CET, refers to the closure of the containment penetrations, on demand, to limit the release of radioactive fission products from the containment following the onset of core damage.

The success or failure of containment isolation primarily affects the timing of fission product release from the containment. A failure of containment isolation results in the release of fission products from the containment beginning shortly after the onset of core damage. Failure to isolate the containment results in an early and sustained release of fission product to the outside environment. This source term release may be quite large depending on the size of the unisolated penetration and the containment pressure time history. The operation of containment sprays would scrub the containment atmosphere, thus limiting the fission product release through any unisolated opening.

Early Containment Failures Avoided

Late containment failure occurs long after vessel failure and thus allows time for natural fission product removal mechanisms to reduce the mass of airborne fission products in the containment. The mode of containment failure (early or late) has a large impact on the source term release. Success of this mode for a given sequence, which is defined as a late containment failure or a sequence limited to containment leakage (i.e., no containment failure), are determined based on the results of phenomenological evaluation summaries and MAAP analyses.

NUREG-1335 has identified a number of phenomena which might result in early containment failure. Since the likelihood of early containment failure due to these phenomenological uncertainties is highly dependent on plant specific geometry, the present methodology treats these items individually in phenomenological evaluation summaries. These summaries provide detailed SONGS 2/3 specific analysis of the various phenomena and discuss the likelihood and consequences of the phenomena. The results are summarized in Section 4.4.

Success of this node implies that none of the pertinent phenomenological uncertainties result in early containment failure. For SONGS 2/3, it has been determined that the occurrence of the phenomena listed in Table 4.4-1 will not threaten the containment integrity or result in early containment failure. Therefore, this node always has a probability for success of 1.

Although no early containment failures are expected, the phenomenological uncertainties could impact the long term ex-vessel sequence progression. Also, no early containment failure mechanisms have been identified during the investigation of phenomenological uncertainties. This top event has been included primarily for completeness and to indicate that phenomenological uncertainties have been considered through the phenomenological evaluation papers.

High Pressure Melt Ejection

The purpose of this node is to allow binning of severe accident scenarios on the basis of high pressure or low pressure core melt ejection. Since a strong case can be made for creep rupture induced failure of the SONGS 2/3 reactor vessel or RCS piping prior to discharge of core debris from the reactor, the SONGS 2/3 reactor will discharge its core debris at low pressure into the reactor cavity. In the absence of high pressure melt ejection, the core debris remains in the reactor cavity and many of the severe accident phenomena associated with early containment failure become irrelevant. The phenomenological consequences of assuming high pressure melt ejection from the SONGS 2/3 reactor are treated in the phenomenological evaluation summaries (Section 4.4). For completeness, the effects of high pressure melt ejection and the discharge of corium into the lower containment compartment are bounded by a sensitivity analysis. The results of this sensitivity analysis can be found in Section 4.7.

Water Cooling Debris

A consequence of assuming creep rupture induced failure of the SONGS 2/3 reactor vessel prior to the discharge of corium from the reactor vessel is that most of the core debris ejected from the failed vessel will be deposited on the reactor cavity floor. Since water on the lower containment floor at SONGS 2/3 cannot normally enter the reactor cavity, debris coolability and fission product aerosol generation become important issues at SONGS 2/3.

Cavity debris cooling involves injection of water through the failed reactor vessel into the cavity. This method relies on automatic ECCS injection and recirculation at SONGS 2/3 and an interpretation of existing Emergency Operation Instructions. Overfilling the reactor cavity causes water to spill into the

lower containment compartment. When sufficient water accumulates on the lower compartment floor, it may be recirculated back into the reactor vessel (subject to the availability of the HPSI Recirculation System). Without the availability of the HPSI recirculation system, the water injected into the reactor cavity will eventually be boiled off due to the decay heat in the corium. The absence of heat exchangers on the HPSI recirculation system however, eventually results in the heatup of the recirculated water. When the water temperature exceeds the saturation temperature of the containment it begins to flash to steam and pressurize the containment atmosphere. One possible means of extending debris coolability indefinitely is by using the containment cooling systems to condense the steam from the containment atmosphere and return the condensate to the lower compartment floor, where it can be recirculated back to the debris in the cavity through the failed reactor vessel.

This node considers the core debris to be coolable if sufficient water can be injected through the failed reactor vessel to fill the cavity. The effect of filling the cavity with water after vessel failure, when no containment cooling is available, is to delay molten core concrete interaction (MCCI) within the cavity and decrease the time required to fail the containment due to overpressurization. If the cavity can be filled with water after vessel failure and containment cooling is available, MCCI can be minimized and the containment geometry preserved intact.

Containment Heat Removal

The interaction of core debris with containment concrete, containment water pools, mechanical structures, and the containment atmosphere leads to the eventual heatup and pressurization of the containment. This pressurization is a function of the containment free volume, the rates of condensible and non-condensable gas generation, and the rate at which the containment temperature increases. The gas generation and temperature rise in the containment can be characterized by the level of decay heat and exothermic chemical energy generated in the core debris, plus any contribution due to the combustion of containment gases. In order to prevent the overpressure failure of the containment, it is necessary to establish some form of containment heat removal that meets or exceeds the total of all heat generating sources in the containment. Failure to establish some form of containment heat removal eventually results in sustained containment pressurization and eventual failure of the containment boundary.

Containment heat removal at SONGS 2/3 can be achieved with either:

- 1 of 2 containment spray pumps in recirculation mode in combination with 1 of 2 containment spray heat exchangers or
- 1 of 4 containment emergency cooling units (i.e., containment fan coolers).

Success of this node requires that sufficient containment heat removal be available to prevent late containment failure due to overpressurization. Either of the above combinations of equipment can accomplish this task. Without some way of getting water into the reactor cavity, however, there is no way to cool the core debris in the cavity and prevent substantial MCCI and possible melt-through of the basemat.

The potential for MCCI melt-through of the cavity floor at SONGS 2/3 is discussed in a phenomenological evaluation summary (Section 4.4.2).

Fission Product Scrubbing

The quantity and types of radionuclides released following vessel failure are sensitive to the mechanisms available for fission product scrubbing. Fission product scrubbing refers to the removal of radioactive fission products from the containment gas space. In the absence of some form of air filtration, fission products must be scrubbed from the air through the use of containment sprays, or allowed to settle under the influence of gravity from the containment air space. Water in the form of a fine spray is a very effective tool for removing airborne fission products, since this mechanism is much faster than gravitational settling of the fission product aerosols.

Success of this node implies that at least one train of containment spray is operating at full capacity in its recirculation mode following the onset of core damage. Note that success of the containment spray heat exchanger is not required for the success of this node.

Injecting water into the reactor cavity after vessel failure will submerge the core debris under more than six feet of water and afford some degree of fission product scrubbing. This mode of fission product scrubbing is, however, not accounted for in the CET. It is, however, accounted for in the MAAP source term calculations.

4.5.3 CET Structure and End-States

The CET top events, as described in the previous section, have been arranged in a manner which takes into account the sequence progression and provides insights into the containment response

to the postulated core damage accident. The combination of top event success and failure states leads to 256 theoretically possible CET end states. Only 11 are shown and in Figure 4.5-1. Of these 11 CET end states, only 6 represent severe accident scenarios with frequencies above the $1E-9$ /yr cutoff frequency. CET end states 5, 6, 7, 8, 10 and 11 provide a qualitative description of the ex-vessel sequence progression and source term release. These 6 end states and their possible outcomes are described below:

- 5 Leakage - The containment integrity is not challenged due to either overpressurization or MCCI. Minor releases of airborne fission products occur along normal leakage pathways.
- 6 Late Containment Failure on Overpressure - Containment failure due to overpressurization occurs, resulting in fission product release. No fission product scrubbing is available.
- 7 Leakage With Core Debris Not Coolable - Late containment failure is expected due to cavity floor failure due to prolonged molten core-concrete interaction (MCCI). This CET end-state assumes cavity floor failure prior to overpressurization failure. This mode of containment failure will not occur within 48 hrs.
- 8 Late Containment Failure on Overpressure - Core Debris Not Coolable - Containment failure due to overpressurization occurs, resulting in fission product release. No fission product scrubbing is available. Since the core debris is not coolable, the amount of containment fission product aerosol in the containment is increased.
- 10 Failure of Containment Isolation - Containment Scrubbing Available - Failure to isolate the containment results in the release of fission products to the outside environment shortly after the onset of core damage. Operation of containment spray reduces the amount of airborne fission products in the containment and reduces the containment pressure driving airborne fission products from the containment.
- 11 Failure of Containment Isolation - Containment Scrubbing Not Available - Failure to isolate the containment results in the release of fission products to the outside environment shortly after the onset of core damage. No rapid containment aerosol scrubbing is credited (i.e., containment sprays fail to operate).

4.6 Accident Progression and CET Quantification

Loss of coolant from the primary system, either through a break in the RCS or a loss of heat sink (which in turn promotes overpressurization of the RCS and subsequent loss of fluid through the safety valves), coupled with failure to inject the RWST, eventually results in uncovering of the reactor core. Core damage occurs once oxidation of the zircaloy fuel cladding begins. This exothermic chemical reaction between steam and zircaloy generates heat and produces hydrogen. The reaction is controlled by the availability of steam, which continues to be generated as the primary system inventory boils off. The reaction rate accelerates when the temperature of the zircaloy exceeds 2,871°F (1,850 K), and the chemical energy released at this time in the transient exceeds the local decay heat generation. Core melt begins when the fuel temperature reaches the eutectic melt temperature of 4,040°F (2,500 K).

As the core melts, molten material candles downward until it refreezes on cooler material below. Eventually it melts and moves further downward. This downward progression is mainly a function of the temperatures encountered by the melt. Once the melt leaves the core boundaries, it begins attacking the core support structures. Large holes in the lower core support plate allow relocation of the core to the lower plenum of the reactor vessel without melting the entire lower core support plate structure.

In the absence of external cooling of the RPV, relocation of the molten core into the lower head is assumed to lead directly to failure of the reactor vessel; no attempt is made to take credit for potential in-vessel recovery. If the RCS is at high pressure at the time of vessel failure, high pressure melt ejection (HPME) could possibly displace or entrain a small amount of core debris out of the cavity. However, the majority of this debris would be de-entrained by containment structures. If the RCS is at low pressure at the time of vessel failure, the expected case at SONGS 2/3, then low pressure melt ejection results in no core debris escaping the cavity.

MCCI takes place if water is not available to cool the core debris or if the debris dries out. Concrete decomposition generates noncondensable gases and also releases a significant amount of water from the concrete, resulting in additional chemical heat generation and hydrogen evolution due to oxidation of metallic constituents within the molten debris. The containment continues to pressurize due to heating of the containment atmosphere and noncondensable gas generation. If containment heat removal is not available, this pressurization induces containment failure.

The time required to fail the containment by overpressurization depends upon the steaming rate and on the rate of noncondensable gas generation. The failure mechanism associated with containment overpressure is due to exceeding the ultimate strength of certain key structural components or attachments. This limit is most likely to be approached gradually.

The severity of the source-term depends strongly on the containment failure timing. Failure during or immediately after core damage is clearly the most serious, as the overall airborne fission product mass produced during a severe accident is greatest during this time period. Whenever containment pressurization lags considerably behind vessel failure, substantial fission product retention through naturally occurring deposition mechanisms (for example, sedimentation, impaction, etc.) is facilitated.

Finally, failure to isolate the containment results in the direct release of fission products from the containment following core damage. The source-term for sequences involving a failure to isolate the containment is to a large degree determined by the area of the isolation failure, the pressure in the containment, and the time at which core damage begins.

Sequence quantification is documented in Section 4.3.1. CET quantification is implicit in the quantification of the EETs.

4.7 Radionuclide Release Characterization

The purpose of the SONGS 2/3 source term analysis was to quantitatively describe the magnitude and composition of radionuclide releases to the environment resulting from the core damage accidents defined in the front-end analysis. Before source term calculations were actually performed, the front-end results were reorganized into a suitable form. This involved grouping sequences with similar source term characteristics into accident sequence "bins" to reduce the total number of sequences to be analyzed. Source term quantification was then performed by analyzing a single, representative accident sequence from each bin.

4.7.1 Overview

To arrive at fission product releases, a number of phenomena and fission product pathways must be considered through all phases of severe accident sequence progression. For instance, fission products must pass through multiple barriers located along the release pathways, starting with the oxide fuel and followed by fuel pin cladding, the RCS, the containment structure, and depending upon the release category, the Auxiliary Building structures.

Transport of fission products from the initially intact fuel matrix to the environment can best be presented by considering the chronological progression of a core damage accident. During a core damage accident, the transport of fission products, including their transport state and the timing of their release from the intact or molten fuel, varies significantly between volatile and non-volatile fission products and noble gases. Due to the chemical characteristics of volatile fission products, a substantial fraction of these isotopes diffuse through the oxide fuel structure and are released into the fuel pin-cladding gap. Nonvolatile fission products have a much lower affinity for diffusion through the fuel oxide and are retained within the fuel material. Eventually the fuel cladding would rupture due to the pressure buildup from the volatile gases being released from the fuel material. Concurrent with the cladding failure would be a release into the primary system of the accumulated volatile fission product vapors and the resident noble gases.

In a steam environment, most of the volatile fission product vapors condense and form aerosols. These released fission products may be transported to the containment (or Auxiliary Building) atmosphere via flow paths through the pressurizer safety valves and pressurizer quench tank rupture disk, or, more directly, via pathways due to breaches in the RCS pressure boundary. In the case of the volatile fission products, significant retention within the primary system could occur as the aerosols deposit on the primary system structures. These "deposited" fission products may revaporize late in an accident sequence, however, and follow established pathways out of the RCS.

The onset of core damage accelerates the fission product diffusion process, allowing nearly all of the volatile fission products to be released from the fuel material to the primary system. Volatile fission product transport through the primary system and into the containment would then proceed as discussed above. Once again, the non-volatile fission products would be retained in the (molten) fuel material. Thus, during the early stages of a core damage accident, most volatile fission products would be released to the primary system and containment while the non-volatile fission products would flow with the molten core material. This implies that the non-volatile fission products are transported first to the reactor vessel lower head and then, following lower head failure, to the containment cavity or to both the cavity and the lower compartment regions.

Once in the containment, the molten core debris may begin to attack concrete structures. If this concrete attack occurs, then the ensuing chemical interactions between non-volatile species and the concrete constituents may vaporize some non-volatile

fission products and release them to the containment gas space in the form of aerosols.

Fission products, both volatile and non-volatile, which accumulate in the containment gas space, are sensitive to a number of fission product removal mechanisms. These mechanisms are important to the fission product retention capability of the containment barrier, especially following breach or impairment of the containment structure. For airborne fission products to be released to the environment they must be transported along with the gas flow through the containment breach. If active or natural removal mechanisms such as inertial impaction, gravitational settling, or water scrubbing take effect along the pathway from the containment to the outside environment, then a significant reduction in source term release may occur. Fission product pathways encountered in certain severe accident sequences may bypass the containment altogether (i.e., SGTR or V-sequences) or lead to early releases from an unisolated containment, and thus do not benefit from some or all of the aforementioned removal mechanisms. These types of sequences are expected to have larger source term releases.

To adequately address the complexities associated with fission product transport and release, and to account for the specific front-end sequence definitions, including operator actions, the SONGS 2/3 source term analysis relies on the integrated severe accident analysis code, MAAP. This code couples the plant thermal-hydraulic responses and fission product behavior to properly model feedback between the two. Furthermore, MAAP can analyze all phases of severe accident progression accounting for the impact of the primary system, containment, engineered safety features (ESFs), and operator actions.

In regard to fission product transport, MAAP begins tracking the fission products as they exist in the normally intact fuel matrix. This initial fission product inventory is organized by chemical properties into 12 groups within MAAP. The estimated initial inventory of each of the 12 fission product groups specific to SONGS 2/3, as derived from the MAAP parameter file, is shown in Table 4.7-1. This total inventory of fission products is generally characterized as noble gases (group 1), volatile fission products (groups 2, 6, 11) and non-volatile fission products (groups 3, 4, 5, 7, 8, 9, 10, 12). The SONGS 2/3 source term analysis reports the mass fraction released for each of these three categories.

4.7.2 Source Term Sequence Selection

The screening process of Section 4.3.3 identified 15 plant damage states from Table 4.3-6 as being representative of all the sequences quantified through the extended event tree. These

Table 4.7-1

INITIAL SONGS 2/3 INVENTORY OF FISSION PRODUCT GROUPS

Fission Product Group		Initial Inventory (lb)
1)	Noble Gases (Xe, Kr)	1025
2)	CsI & RbI (volatile)	87
3)	TeO ₂	0
4)	SrO	220
5)	MoO ₂	826
6)	CsOH (volatile)	731
7)	BaO	300
8)	La ₂ O ₃ (& Pr ₂ O ₃ + Nd ₂ O ₃ , Sm ₂ O ₃ + Y ₂ O ₃)	1614
9)	CeO ₂	670
10)	Sb	3
11)	Te ₂ (volatile)	78
12)	UO ₂ (&NpO ₂ + PuO ₂)	230060

fifteen plant damages states form the basis for the source term analysis. As mentioned in Section 4.3, the key functions with respect to potential radiological release from containment are containment status, availability of debris cooling and containment heat removal, and the RCS pressure at vessel failure. This information is all embodied in the plant damage state designators (see Section 4.3.2). In assuming that the SONGS 2/3 reactor vessel should always fail at low pressure, the importance of this designator is diminished. In general, the screened sequences, when passed through the CET, are binned according to the last two characters of the plant damage state designator. Containment bypass sequences are not completely specified by the PDS designator as a result of the systemic accident initiator (i.e., ISLOCA or SGTR). The existence of two distinct functional initiators binned together as containment bypass sequences requires closer inspection. In the case of SONGS 2/3 it is sufficient to identify and analyze separate plant damage states representing ISLOCAs and SGTRs. Sequences having the same PDS designator are expected to have similar containment responses from the standpoint of a potential radiological source term release.

A representative systemic sequence from each of the fifteen bins (termed the "analyzed sequence") was selected for the source term analysis. The analyzed sequence was chosen because it had the highest frequency of occurrence of any sequence within the bin or because it was expected to bound all other sequences in the bin. Selection of a sequence other than that with the highest frequency occurred when that sequence could result in earlier core damage and vessel failure. Results of the SONGS 2/3 source term selection process, shown in Table 4.7-2, identified 15 analyzed sequences which were used to represent the 121 systemic sequences or 41 plant damage states resulting from the EET quantification. The fifteen analyzed sequences are described in detailed in Section 4.7.3.

The source term for each analyzed sequence was computed by performing a MAAP analysis. The source term results for the analyzed sequence were then assigned to all sequences in that bin. This was accounted for by summing the frequencies of all sequences in a bin to determine the cumulative frequency associated with the source term release of the analyzed sequence. The SONGS 2/3 source term analysis reports source term results for 99% of the total core damage frequency. To illustrate this process refer to Table 4.7-2 and consider the following example. Source term bin 8 contains five plant damage states: TEBNL, TEANL, SEANL, SEBNL, and SEENL (see Section 4.3.2 for designator definitions). Although two of these damage states represent transients and three of these sequences represent small LOCAs, all five states have the same characteristics which include:

Table 4.7-2

IPE BACK-END SEQUENCE SELECTION SUMMARY
FOR SONGS 2/3

Source Term Bin	Analyzed Systemic Sequence	Analyzed Plant Damage State	CET End State	Bounded Plant Damage States	Source Term Bin Frequency (per year)	Percent of Total Core Damage
1	PCS-4	TEAYS	5	SEAYS	9.0E-6	29
2	MLO-4	SEKYS	7	SEBYS, SECYS, SLDYS, SEEYS, SEFYS, TEBYS, TEFYS, TECYS	6.8E-6	22
3	ATWS-6	LEAYS	5	LEBYS	2.8E-6	9
4	LLO-4	LEGYS	5	SEJYS, LEIYS, LEHYS, LEJYS	4.3E-6	14
5	SGTR-33	GEAYB	11	None	2.2E-7	<1
6	VSEQ-2	GILYB	11	None	6.5E-7	2
7	SGTR-20	GLEYP	11	GLDYB, GLFYB, GLENB	7.9E-7	3
8	MLO-20	SEBNL	8	TEBNL, TEANL, SEANL, SEENL, SLDNL	6.9E-7	2
9	SBO-17	TEAYI	10	TECNI	1.9E-8	<1
10	LLO-13	LEHNL	6	NONE	6.2E-8	<1
11	LLO-34	LEIYI	10	NONE	1.4E-9	<1
12	LOP-48	TECNL	8	TEFNL	2.1E-6	7
13	SGTR2-66	GLCNB	11	GLCYB	2.8E-7	1
14	SGTR2-48	GLANB	11	GLBYB, GLBNB	1.5E-7	<1
15	PCS-35	SLLYS	5	NONE	2.7E-6	9
TOTAL					3.1E-5	100%

1. A lack of high pressure injection prior to core damage
2. Vessel failure within 8 hours
3. Isolated containment
4. No containment heat removal
5. Vessel fails at low pressure
6. Post vessel injection allows the debris in the cavity to be covered with water

Since these plant damage states involve the slow overpressurization of the containment, the initiating event has a very limited effect on the source term release. SEENL allows for some decay heat removal from the core prior to core damage and should have the longest time to vessel failure of the five cases. The presence of HPSI recirculation in sequences TEANL and SEANL, following vessel failure, delays containment pressurization until all the water on the lower compartment floor reaches the saturation temperature of the containment. The two remaining cases, SEBNL and TEBNL, are almost identical. Since SEBNL occurs with a higher frequency, this is the analyzed plant damage state for source term bin 8.

To determine the source term for bin 8, a MAAP analysis was performed on a specific systemic sequence from plant damage state SEBNL. MLO-20 was analyzed since it has the highest frequency in the PDS SEBNL. The calculated source term results for systemic sequence MLO-20 are a best estimate for SEBNL, and a bounding estimate on the expected results from the plant damage states TEANL, TEBNL, SEANL, and SEENL. The frequency associated with this calculated source term release was therefore taken to be the cumulative frequency of all five plant damage states comprising source term bin 8.

4.7.3 Source Term Analysis

The significance of a release of radionuclides is best characterized by the amount of volatile fission products released. Release categories considered for SONGS 2/3 are defined in Table 4.7-3 in terms of the containment failure mode (not failed, overpressure, not isolated, or bypassed) and the airborne fractional release of fission products from the containment. Based on the source term results of the analyzed sequences, appropriate release categories were assigned to each of the analyzed sequences and thus to the bins which they represent.

Table 4.7-3

RELEASE CATEGORY DEFINITIONS

Release Category	Definition
B	Containment bypassed with noble gases plus less than 0.1% of the volatiles released.
C	Containment bypassed with noble gases plus up to 1% of the volatiles released.
D	Containment bypassed with noble gases and up to 10% of the volatiles released.
E	Containment failure prior to vessel failure with noble gases and less than 0.1% of the volatiles released (containment not isolated).
F	Containment failure prior to vessel failure with noble gases and up to 1% of the volatiles released (containment not isolated).
G	Containment failure prior to vessel failure with noble gases and up to 10% of the volatiles released (containment not isolated).
H	Early containment failure with the noble gases and less than 0.1% volatiles released (containment failure within six hours of vessel failure; containment not bypassed; isolation successful prior to core damage).
I	Early containment failure with noble gases and up to 1% of the volatiles released (containment failure within six hours of vessel failure; containment not bypassed; isolation successful prior to core damage).
J	Early containment failure with noble gases and up to 10% of the volatiles released (containment failure within six hours of vessel failure; containment not bypassed; isolation successful prior to core damage).
K	Late containment failure with noble gases and less than 0.1% volatiles released (containment failure greater than six hours after vessel failure; containment not bypassed; isolation successful prior to core damage).

Table 4.7-3 (Continued)

RELEASE CATEGORY DEFINITIONS

Release Category	Definition
L	Late containment failure with noble gases and up to 1% of the volatiles released (containment failure greater than six hours after vessel failure; containment not bypassed; isolation successful prior to core damage).
M	Late containment failure with noble gases and up to 10% of the volatiles released (containment failure greater than six hours after vessel failure; containment not bypassed; isolation successful prior to core damage).
N	Late containment failure with noble gases and up to 1% of the volatiles and up to 0.1% of the non-volatiles released (containment failure greater than six hours after vessel failure; containment not bypassed, isolation successful prior to core damage).
S	Success (leakage only, successful maintenance of containment integrity; containment not bypassed; isolation successful prior to core damage).
T	Containment bypassed with noble gases and more than 10% of the volatiles released.
U	Containment failure prior to vessel failure with the noble gases and more than 10% of the volatile fission products released (containment isolation impaired).
V	Early containment failure with noble gases and more than 10% of the volatiles released (containment failure within 6 hours of vessel failure; containment not bypassed; isolation successful prior to core damage).
W	Late containment failure with noble gases and more than 10% of the volatiles released (containment failure greater than 6 hours after vessel failure; containment not bypassed; isolation successful prior to core damage).

The MAAP results indicate that the SONGS 2/3 source term release falls into seven release categories: B, D, G, L, S, T, and W. The total release by fission product group calculated by MAAP for each of the 15 analyzed sequences is shown in Table 4.7-4. The cumulative frequency of each release category (see Table 4.7-5) represents all analyzed and bounded plant damage states in that category.

Table 4.7-6 presents selected accident progression parameters for each analyzed sequence. In addition to radiological release, this table contains information on accident timing, containment conditions, and hydrogen burn data. The fifteen analyzed sequences are described below. Each systemic sequence number refers to both the extended event tree and to a particular sequence path on that tree (PCS-4 refers to the fourth sequence on the first loss of power conversion tree; SGTR2-48 refers to the forty-eighth sequence on the second steam generator tube rupture tree). Also shown are the plant damage state identifiers. The systemic EET paths used to model each analyzed sequence are illustrated in Section 4.3.1.

TEAYS: Sequence PCS-4

The initiating event for PCS-4 is a loss of power conversion, followed by failures which include: (1) the operator fails to provide CST makeup per procedures, (2) MFW and condensate pumps are not recoverable within 60 minutes and/or (3) failure/unavailability of the APW system. No seal leakage is modeled and the pressurizer safety relief valves open and close upon demand.

Containment cooling is available in two forms: (1) the emergency containment fan coolers and (2) the containment spray and recirculation system. The emergency containment fan coolers at SONGS 2/3 are not capable of preventing the containment pressure from exceeding the pressure set point of the containment spray system. As a result, both of these systems are activated during this analyzed sequence.

At the onset of this scenario only the three charging pumps are capable of injecting water into the reactor vessel. Without secondary side cooling, the SONGS 2/3 reactors have no way of depressurizing and allowing the HPSI pumps to inject sufficient water to cool the reactor vessel. As a result, the SONGS 2/3 reactor remains near the pressurizer safety setpoint as inventory is lost from the vessel through the pressurizer safety relief valve. As the core uncovers and melts, the temperatures in the primary system piping increase. Shortly after the core relocates to the lower reactor head, the temperature in the hot leg piping causes the plastic limit for the steel to decrease below the internal stress on the hot leg piping, resulting in creep rupture

Table 4.7-4

Page 1 of 3

AIRBORNE FISSION PRODUCT RELEASE (%)
48 HOURS AFTER ACCIDENT INITIATION

Fission Product Group	Airborne Release (%) @ 48 Hours				
	PCS-4	MLO-4	ATWS-6	LLO-4	LOP-48
1) Nobles	0.1	0.1	0.1	0.3	14.4
2) CsI	1×10^{-4}	2×10^{-4}	1×10^{-4}	5×10^{-3}	0.1
3) TeO ₂	0	5×10^{-6}	1×10^{-4}	2×10^{-4}	0
4) SrO	0	2×10^{-5}	2×10^{-5}	8×10^{-5}	8×10^{-5}
5) MoO ₂	0	2×10^{-7}	1×10^{-7}	2×10^{-7}	3×10^{-7}
6) CsOH	7×10^{-5}	2×10^{-4}	1×10^{-4}	4×10^{-3}	0.1
7) BaO	0	9×10^{-6}	1×10^{-5}	4×10^{-5}	4×10^{-5}
8) La ₂ O ₃	0	7×10^{-6}	4×10^{-6}	7×10^{-6}	4×10^{-5}
9) CeO ₂	0	2×10^{-5}	2×10^{-5}	5×10^{-5}	8×10^{-5}
10) Sb	3×10^{-6}	2×10^{-4}	2×10^{-4}	6×10^{-3}	4×10^{-2}
11) Te ₂	0	2×10^{-4}	6×10^{-5}	2×10^{-3}	1×10^{-2}
12) UO ₂	0	0	0	2×10^{-7}	3×10^{-7}
Release Category	S	S	S	S	L

Table 4.7-4
Page 2 of 3

AIRBORNE FISSION PRODUCT RELEASE (%)
48 HOURS AFTER ACCIDENT INITIATION

Fission Product Group	Airborne Release (%) @ 48 Hours				
	PCS-35	MLO-20	LLO-13	SBO-17	LLO-34
1) Nobles	0.2	100.0	100.0	54.8	43.1
2) CsI	7×10^{-3}	12.0	4×10^{-1}	2.0	6×10^{-1}
3) TeO_2	3×10^{-3}	0	0	2×10^{-1}	0
4) SrO	7×10^{-5}	3×10^{-5}	2×10^{-4}	6×10^{-2}	2×10^{-2}
5) MoO_2	6×10^{-4}	5×10^{-4}	1×10^{-5}	8×10^{-5}	7×10^{-5}
6) CsOH	6×10^{-3}	12.1	7×10^{-1}	2.0	7×10^{-1}
7) BaO	3×10^{-5}	7×10^{-5}	8×10^{-5}	3×10^{-2}	8×10^{-3}
8) La_2O_3	1×10^{-6}	5×10^{-4}	2×10^{-5}	6×10^{-3}	5×10^{-2}
9) CeO_2	3×10^{-5}	5×10^{-4}	8×10^{-5}	5×10^{-2}	5×10^{-2}
10) Sb	4×10^{-3}	5.0	1×10^{-1}	1.4	2×10^{-1}
11) Te_2	0	4×10^{-3}	2×10^{-2}	1.9	4×10^{-1}
12) UO_2	7×10^{-8}	0	5×10^{-7}	2×10^{-4}	5×10^{-5}
Release Category	S	W	L	G	G

Table 4.7-4
Page 3 of 3

AIRBORNE FISSION PRODUCT RELEASE (%)
48 HOURS AFTER ACCIDENT INITIATION

Fission Product Group	Airborne Release (%) @ 48 Hours				
	VSEQ-2	SGTR-20	SGTR-33	SGTR2-48	SGTR2-66
1) Nobles	99.8	16.8	6.5	97.4	19.5
2) CsI	84.2	2.6	1×10^{-1}	5.5	2.5
3) TeO ₂	1×10^{-1}	0	0	0	0
4) SrO	2×10^{-1}	2×10^{-4}	3×10^{-5}	2×10^{-4}	2×10^{-4}
5) MoO ₃	8×10^{-1}	2×10^{-4}	4×10^{-5}	3×10^{-4}	1×10^{-4}
6) CsOH	84.2	2.1	1×10^{-1}	3.3	2.1
7) BaO	4×10^{-1}	9×10^{-4}	2×10^{-4}	2×10^{-3}	4×10^{-4}
8) La ₂ O ₃	5×10^{-3}	3×10^{-4}	5×10^{-7}	4×10^{-4}	1×10^{-5}
9) CeO ₂	4×10^{-2}	3×10^{-5}	5×10^{-7}	4×10^{-6}	1×10^{-4}
10) Sb	8.5	4×10^{-1}	5×10^{-2}	5×10^{-1}	3×10^{-1}
11) Te ₂	7.6	6×10^{-1}	6×10^{-7}	1×10^{-3}	7×10^{-1}
12) UO ₂	2×10^{-4}	6×10^{-8}	0	0	7×10^{-8}
Release Category	T	D	B	D	D

Table 4.7-5

SONGS UNITS 2 AND 3
AIRBORNE RELEASE CATEGORY AND PROBABILITY

Release Category	Definition	Release Frequency (per year)	P(RC CD) ¹
S	Success, no containment failure within 48 hrs, < 0.1% volatiles released	2.6×10^{-5}	0.838
T	Containment bypassed, > 10% volatiles released	6.5×10^{-7}	0.021
B	Containment bypassed, < 0.1% volatiles released	2.2×10^{-7}	0.007
D	Containment bypassed, up to 10% volatiles released	1.2×10^{-4}	0.039
G	Isolation failure, Containment failure prior to vessel failure, up to 10% volatiles released	2.0×10^{-4}	0.001
L	Late containment failure, up to 1% volatiles released	2.2×10^{-4}	0.072
W	Late containment failure, more than 10% volatiles released	6.9×10^{-7}	0.022

1. Conditional probability of release category given core damage.

Table 4.7-6

(Page 1 of 2)

**SOURCE-TERM ANALYSIS RESULTS
MAAP RUN SUMMARY TABLE**

SEQUENCE TYPE								
Sequence No.	PCS-4	MLO-4	LLO-4	ATWS-6	LOP-4B	PCS-35	MLO-20	LLO-13
Plant Damage State Designator	TEAYS	SEKYS	LEGYS	LEAYS	TECNL	SLLYS	SEBNL	LEHNL
Source Term Release Category	S	S	S	S	L	S	W	L
PDS Bin Frequency (yr ⁻¹)	9.0E-6	6.8E-6	4.3E-6	2.8E-6	2.1E-6	2.7E-6	6.9E-7	6.2E-8
CORE/CONTAINMENT RESPONSE								
Time of Core Uncovery (hr)	1.2	0.9	0.006	0.006	1.2	9.2	0.9	0.006
Onset of Core Melt (hr) (4039°F)	1.7	1.3	1.2	0.6	1.7	10.3	1.3	0.6
Time of Vessel Failure (hr)	2.5	2.4	2.4	1.6	2.6	11.5	3.6	1.7
Time of Containment Failure (hr)	---	---	---	---	39.8	---	26.5	22.3
Maximum Containment Pressure (psia)	29.8	38.4	99.0	43.4	178.4	30.2	188.9	188.9
Maximum Containment Temperature (°F)	347	309.4	426.5	360.2	426.5	326.5	381.1	377.6
Cavity Water Level @ End of Mission Time	33.2	0.0	0.0	0.0	0.0	0.0	8.4	11.1
Fraction of Clad Reacted in Vessel	0.32	0.22	0.19	0.21	0.29	0.32	0.29	0.24
H ₂ Mass Burned (lbm)	0.0	2398.	992.	2240.	0.0	2823.	0.0	0.0
Cavity Concrete Ablation Depth at End of Mission Time (ft)	0.0	7.0	7.1	7.0	6.9	4.2	0.0	0.0
FISSION PRODUCT DISTRIBUTION AT END OF 48 HRS								
Noble Release (%)	0.1	0.1	0.3	0.1	14.5	0.2	100.	100
Volatile FP Release (%)	1E-4	2E-4	3E-3	2E-3	1E-1	7E-3	12.0	7.E-1
Non-Volatile FP Release (%)	0.0	1.E-5	4E-5	1E-5	8E-5	4E-5	7E-3	8E-5
Volatile FP Retained in Primary System (%)	59%	44%	50%	28%	36%	43%	42%	52%

- GENERAL NOTES:
- S of the Source Term Release Category indicates safe stable state achieved ex-vessel (i.e., no over-pressurization failure of containment, however, MCCI induced containment, failure may occur).
 - Mission time for Level II is 48 hours.
 - Containment bypass (SGTR, VSEQ).
 - MCCI Failures - See Table 4.3-2 through 4.3-5 (Cavity Wet = No) for sequences and frequency.

Table 4.7-6
(Page 2 of 2)SOURCE-TERM ANALYSIS RESULTS
MAAP RUN SUMMARY TABLE

SEQUENCE TYPE							
Sequence No.	SBO-17	LLO-34	VSEQ-2	SGTR-20	SGTR-33	SGTR2-48	SGTR2-66
Plant Damage State Designator	TEAY1	LEIY1	GILYB	GLEYB	GEAYB	GLANB	GLCNB
Source Term Release Category	G	G	T	D	B	D	D
PDS Bin Frequency (yr ⁻¹)	1.9x10 ⁻⁸	1.4x10 ⁻⁸	6.5x10 ⁻⁷	7.9x10 ⁻⁷	2.2E-7	1.5E-7	2.8E-7
CORE/CONTAINMENT RESPONSE							
Time of Core Uncovery (hr)	1.2	.006	4.8	9.3	1.2	9.3	9.3
Onset of Core Melt (hr) (4039°F)	1.7	0.6	5.6	10.4	1.7	10.4	10.4
Time of Vessel Failure (hr)	2.7	1.7	8.0	11.6	2.7	11.6	11.4
Time of Containment Failure (hr)	(ISOL FAILS)	(ISOL FAILS)	BYPASS	---	---	41.2	---
Maximum Containment Pressure (psia)	46.0	58.0	23.6	77.1	35.0	188.9	147.3
Maximum Containment Temperature (°F)	462.2	360.5	402.3	439.8	236.1	369.8	456.5
Cavity Water Level @ End of Mission Time	32.9	0.5	0.0	0.1	32.9	9.3	0.1
Fraction of Clad Reacted in Vessel	0.32	0.23	0.28	0.33	0.31	0.32	0.30
H ₂ Mass Burned (lbm)	238.	0.0	1967.	0.0	97.	0.0	0.0
Cavity Concrete Ablation Depth at End of Mission Time (ft)	1.7	0.0	6.2	3.3	0.1	0.0	3.2
FISSION PRODUCT DISTRIBUTION AT END OF 48 HRS							
Noble Release (%)	94.7	99.9	100.0	16.8	6.5	97.4	19.5
Volatile FP Release (%)	5.2	2.3	84.2	2.6	1.E-1	5.5	2.5
Non-Volatile FP Release (%)	0.3	0.1	0.8	9E-4	2E-4	2E-3	4E-4
Volatile FP Retained in Primary System (%)	68%	43%	14%	88%	50%	51%	88%

- GENERAL NOTES:
- S of the Source Term Release Category indicates safe stable state achieved ex-vessel (i.e., no over-pressurization failure of containment, however, MCCI induced containment, failure may occur).
 - Mission time for Level II is 48 hours.
 - Containment bypass (SGTR, VSEQ).
 - MCCI Failures - See Table 4.3-2 through 4.3-5 (Cavity Wet = No) for sequences and frequency.

failure. The size of the creep rupture failure is assumed to be large enough to depressurize the primary system.

The temperature of the core debris in the lower reactor head is expected to be hotter near the top of the debris pool than near the bottom. Preferential heat transfer to the steel of the reactor vessel near the top of the debris pool eventually raises the temperature sufficiently to allow the vessel to fail due to creep under its own weight without internal-pressure induced stresses. Slight irregularities in the heat transfer process would cause a single location along the reactor belt line to fail preferentially. Failure of the lower head due to creep rupture allows the debris in the lower head to flow into the cavity. This failure is postulated to occur 30 minutes after the core relocates to the lower reactor vessel head. Creep rupture failure of the hot leg piping followed by core relocation and creep rupture failure of the lower head is expected for sequences where the primary system pressure remains high and secondary side cooling is not available.

To initiate a creep rupture failure in the primary system it is necessary to heat the primary system piping to high temperatures while retaining the primary system at high (pressurizer setpoint) pressure. The only time such temperatures would exist in the primary system is after the onset of significant core damage. To model this process using MAAP 3.0B, HPSI and LPSI are blocked from starting until the core temperature exceeds 4039°F (2500K). Thus, even though the hot leg creep rupture would lead to a depressurized primary system, allowing injection to occur, the injection is blocked to conservatively allow lower head heat-up and creep rupture failure.

The amount of water injected from the three charging pumps (132 GPM) at SONGS 2/3 is insufficient, by itself, to remove decay heat. Its presence, however, may enhance the amount of steam passing through the core and therefore the amount of hydrogen produced when steam reacts with the zircaloy cladding at elevated temperatures. For this reason, charging pump injection is assumed to continue regardless of the temperature of the SONGS 2/3 reactor core.

Injection following vessel failure occurs via HPSI, followed by HPSI recirculation once the RWST is depleted. In this sequence, long term containment heat removal is accomplished using both the emergency containment fan coolers and the containment spray recirculation system. Recirculation of water from the lower compartment, through the failed reactor vessel, and into the reactor cavity, cools the core debris and prevents any core concrete attack. As a result, 48 hours into this analyzed sequence the containment is intact and at a relatively low pressure.

SEKYS: Sequence MLO-4

This sequence is initiated by a medium LOCA. HPSI is successful, but due to equipment failures the switch to HPSI recirculation is unsuccessful. Secondary side cooling was not modelled in the MAAP analysis due to its absence from the EET. Containment cooling is achieved through containment spray recirculation. All available charging pumps, high pressure injection pumps and containment spray pumps are assumed to inject on demand. This assumption minimizes the time between the initiating event and core uncover or core damage. Since the RWST is drained and HPSI recirculation fails prior to the onset of core damage, there is no injection or recirculation through the failed reactor vessel.

As in the previous case, the reactor vessel eventually fails due to creep rupture and the debris flows from the lower vessel head into a dry cavity. Since the cavity remains dry in this accident sequence, the core debris in the cavity remains above the melt temperature of the containment concrete. As a result, the molten core debris can attack and melt the concrete of the cavity floor and side walls.

The high temperature of the core debris in the cavity also allows for a natural circulation flow to be established between the lower compartment and the cavity. This natural circulation flow and the high temperature of the corium causes a large amount of the hydrogen generated during the core melt and concrete ablation process to burn in the cavity.

LEAYS: Sequence ATWS-6

This sequence is initiated by a transient followed by a failure to scram at 100% reactor power. High MTC conditions are assumed to exist. For this sequence it has been assumed that the ATWS results in a large break LOCA at time zero in the hot leg piping connected to the pressurizer, and that no water is injected into the reactor vessel until after the core has melted.

The containment is isolated and containment cooling is available through the emergency containment fan coolers and containment spray recirculation. The emergency containment fan coolers at SONGS 2/3 are not capable of preventing containment pressure from exceeding the set point of the containment spray system; thus, both of these systems become activated during this sequence.

Injection following vessel failure occurs with the initiation of HPSI followed by HPSI recirculation once the RWST is depleted.

LEGYS: Sequence LLO-4

This sequence is initiated by a large cold leg LOCA with a break size of 3.5 ft². Failure to align for recirculation is the only other failure considered in this sequence. Containment cooling

is achieved through containment spray recirculation, although the emergency containment fan coolers may be available. All available charging pumps, high pressure injection pumps, low pressure injection pumps and containment spray pumps are assumed to inject on demand. This assumption minimizes the time between the initiating event and core uncover or core damage.

As in analyzed sequence MLO-4, the reactor vessel eventually fails due to creep rupture and the debris flows from the lower vessel head into a dry cavity. Since the cavity remains dry in this accident sequence, the core debris in the cavity remains above the melt temperature of the containment concrete. As a result, the molten core debris can attack and melt the concrete of the cavity floor and side walls.

The high temperature of the core debris in the cavity also allows for a natural circulation flow to be established between the lower compartment and the cavity. This natural circulation flow and the high temperature of the corium cause a large amount of the hydrogen generated during the core melt and concrete ablation process to burn in the cavity.

TECNL: Sequence LOP-48

The initiating event for LOP-48 is a loss of offsite power. This sequence was treated conservatively under Level I by not addressing the availability of cooling. As a result, this sequence is bounded by an unrecovered station blackout. Without AC power available, ECCS injection from the RWST to the primary system and containment cooling is not available. The restoration of AC power is not modeled in this IPE.

Without secondary side cooling the reactor remains at the pressurizer safety set point as primary system inventory is lost from the vessel. As the core uncovers and melts, the temperatures in the primary system piping increase. Shortly after the core relocates to the lower reactor head, the temperature in the hot leg piping causes the plastic limit for the steel to decrease below the internal stress on the hot leg piping, resulting in creep rupture failure. The size of the creep rupture failure is assumed to be large enough to depressurize the primary system.

The temperature of the core debris in the lower reactor head is expected to be hotter near the top of the debris pool than near the bottom. Preferential heat transfer to the steel of the reactor vessel near the top of the debris pool eventually raises the temperature sufficiently to allow the vessel to fail due to creep under its own weight without internal-pressure induced stresses. Slight irregularities in the heat transfer process would cause a single location along the reactor belt line to fail preferentially. Failure of the lower head due to creep rupture allows the debris in the lower head to flow into the cavity.

Currently this failure is postulated to occur 30 minutes after the core relocates to the lower reactor vessel head. Creep rupture failure of the hot leg piping followed by core relocation and creep rupture failure of the lower head is expected for sequences where the primary system pressure remains high and secondary side cooling is not available.

Without ECCS injection, pressurization of the containment is limited by the amount of water that can be liberated and flashed during the MCCI process. Steam inerting of the containment during this accident prevents hydrogen burning from contributing to containment pressurization. Without containment heat removal the containment eventually fails at 40 hours due to overpressurization. Due to late failure of the containment, a limited release of volatile fission products is observed.

SLLYS: Sequence PCS-35

The initiating event for PCS-35 is loss of power conversion, followed by failures which include: (1) failure of the pressurizer safety valve once open to close (This failure is postulated to result from the over-filling of the pressurizer and the release of two-phase water through the pressurizer safety valve.), (2) failure to switch to the HPSI recirculation mode when the water level in the RWST reaches the low level alarm setpoint, and (3) failure to switch to the CS recirculation mode when the water level in the RWST reaches the low alarm setpoint. Failure of the pressurizer's safety valve to close upon demand has the effect of transforming this severe accident scenario from a transient to a small LOCA.

Long term containment cooling is available through the emergency containment fan coolers. The emergency containment fan coolers cannot limit containment pressure from exceeding the set point for the containment spray system. The containment spray system will be activated in its injection mode, and failure to switch the CS to its recirculation mode prevents this system from providing long term containment cooling.

The RWST is depleted of water prior to vessel failure. However, failure to recirculate water from the containment sumps into the primary system using the HPSI recirculation mode, results in late core damage and eventual vessel failure. Prior to depleting the RWST, auxiliary feedwater is lost due to depletion of the CST. The subsequent failure to align for recirculation results in the primary system pressure increasing to the pressurizer safeties. Without recirculating water from the lower containment compartment, through the failed vessel, the corium discharge to the reactor cavity remains dry and MCCI is allowed to proceed unabated.

The operation in this sequence of a single emergency containment fan cooler is sufficient to prevent the overpressure of the

SONGS 2/3 containment. MCCI continues and may lead to melt-through of the cavity floor at SONGS 2/3. This would, however, result in a ground release. The late failure time associated with an MCCI induced containment failure would permit most of the volatile fission products to settle out in the SONGS 2/3 containment. The high resistance associated with a ground release path and the temperature of the earth should minimize the release of noble gases and volatile fission products until cavity cooling can be established.

SEBNL: Sequence MLO-20

The sequence is initiated by a medium LOCA with a break size of 0.0218 ft². Mechanical, operational or maintenance induced failures assumed for this accident scenario include: (1) loss of 3 HPSI pumps, (2) loss of 2 CS pumps, and (3) loss of all 4 emergency containment fan coolers. No credit is taken for the use of the charging pumps and secondary side cooling to delay the onset of core damage in this accident scenario. After the reactor vessel has failed, this accident scenario assumes that the LPSI pumps are used for a limited time (approximately 30 minutes) to inject water through the failed reactor vessel into the reactor cavity.

The use of the LPSI pumps to inject water through the failed reactor vessel and into the cavity in the absence of any containment cooling system may prevent MCCI but results in a containment overpressure failure. The time at which the overpressure failure occurs is dependent on the size of the medium LOCA and the amount of steaming to the containment prior to vessel failure. The assumed break size for this sequence results in containment failure at 26.5 hours.

LEHNL: Sequence LLO-13

The initiating event for LLO-13 is a 3.5 ft² cold leg break. Mechanical, operational, or maintenance induced failure associated with this accident scenario include: (1) loss of the 2 LPSI pumps, (2) failure of the 4 emergency containment fan coolers and (3) loss of the 2 containment spray pumps. No credit is taken for the use of the 3 HPSI pumps prior to vessel failure. Following vessel failure, the HPSI injection and recirculation modes are used to inject water through the failed reactor vessel and into the reactor cavity.

Accident scenario LLO-13 is very similar to MLO-20 except for the size of the initiating LOCA. The fact that LLO-13 is initiated by a large LOCA results in a shorter time to vessel failure and containment overpressure failure. HPSI injection and recirculation cools the debris in the cavity by absorbing energy from the debris and transferring it to the containment as steam. Without containment cooling, steam from the cavity will eventually overpressurize and fail the SONGS 2/3 containment.

The large LOCA assumed for this sequence results in containment failure at 22.3 hours. This is approximately 4.2 hours earlier than the containment failure time calculated for the preceding severe accident MLO-20. Volatile Fission product retention in the primary system explains why this sequence has a smaller source term release than MLO-20.

TEAYI: Sequence SBO-17

The initiating event for this sequence is a Station Blackout (SBO) with loss of the turbine-driven auxiliary feedwater pump and failure to isolate the containment. Power recovery is assumed to occur 8 hours after the initiating event.

This analyzed sequence is again a variation of sequence PCS-4. The ability to inject water into the SONGS 2/3 reactor vessel, without the benefit of secondary side cooling, is limited to the three charging pumps at 132 gpm. The nature of the event is such that even this injection source is rendered inoperative for the first 8 hours.

In this sequence containment isolation is assumed to fail, leaving a 0.05 ft² flow path between the upper containment and the outside environment. This assumption is conservative since the outboard ends of most containment penetrations are enclosed in a support structure such as the auxiliary building.

The radionuclide release to the environment from this analyzed sequence is greatly increased due to failure of containment isolation. Failure of containment isolation results in a direct flow path from the containment to the outside environment during the core melt and relocation phase of a severe accident. In this sequence the problem is compounded since the SBO prevents the use of the containment spray system to scrub the containment atmosphere of fission products as they are released from the primary system. Gravitational settling of fission products would require a minimum of 6 to 8 hours to significantly reduce the environmental release of fission products from the SONGS 2/3 containment.

As long as electrical power cannot be recovered, due to the SBO event, all containment cooling remains inoperative. When power is recovered 8 hours after the initiating event, both the emergency containment fan coolers and the containment spray systems are assumed to be initiated manually.

HPSI is initiated manually when power is recovered. This allows water to be injected through the failed reactor vessel into the cavity. Once the cavity fills with water, any overflow from the cavity spills onto the lower containment compartment floor. When the RWST water level decreases to 8.82 ft, HPSI is assumed to switch to its recirculation mode. The presence of a sustained amount of water in the cavity allows removal of decay heat from

the core debris. The amount of decay heat removed from the debris in this sequence, once water is injected into the reactor cavity, is sufficient to terminate concrete ablation.

LEIYI: Sequence LLO-34

The initiating event for LLO-34 is a 3.5 ft² cold leg break. Mechanical, operational and maintenance induced failures associated with this accident scenario include: (1) loss of the 2 LPSI pumps, (2) a failure to isolate the containment on demand, and (3) loss of containment spray during injection. The isolation failure area assumed for this sequence is equal to the area of a 3 inch diameter pipe (0.05 ft²). This area bounds approximately 95% of the isolation failure calculated for SONGS 2/3. The upper bound isolation failure area is analyzed as sensitivity sequence

LLO-34-IF1. The containment isolation failure is assumed to occur when the containment pressure first exceeds 15 psia. The isolation failure results in a direct release to the outside environment. No credit is taken for a more probable release to the auxiliary building where settling and plate-out would occur, thus minimizing any release to the outside environment. Credit is not taken for operating the 3 HPSI pumps prior to vessel failure. Following vessel failure, however, the HPSI injection and recirculation modes are used to inject through the failed reactor vessel into the reactor cavity. Long term containment cooling for this sequence is provided by a single emergency containment fan cooler.

The absence of containment sprays precludes the immediate reduction of airborne containment fission products as they are released from the primary system. Containment cooling using the fan coolers and gravitational settling of the fission product aerosols are much too slow to prevent most of the noble gases and some of the volatile fission products from escaping the unisolated containment. The fact that this severe accident is initiated by a large LOCA, however, does result in a slightly higher percentage of volatile fission products being retained in the primary system when compared with a transient induced severe accident with isolation failure such as SBO-17.

GILYB: Sequence VSEQ-2

The initiating event in this analyzed sequence is a 2.5 in² interfacing systems LOCA. The break occurs in a low pressure section of piping in one of the pump room cubicles of the Safety Equipment Building. Secondary side cooling is available, and credit is taken for HPSI until the RWST is empty.

There is no way of isolating the ISLOCA defined in this analyzed sequence. To conservatively assess the impact of containment bypass after reactor vessel failure, containment cooling is not credited in this analyzed sequence.

This accident scenario results in the onset of core uncover at 5.6 hrs., with the majority of the fluid loss from the primary system entering the Safety Equipment Building. Between the onset of core melt, at 5.6 hrs., and vessel failure, at 8.0 hrs., the majority of the noble gases and volatile fission products released from the melting fuel escape the primary system, bypassing the containment, and also enter the Safety Equipment Building. The airborne fission product release (from the containment) to the outside environment for this sequence presented in Table 4.7.4 is an upper bound estimate. No credit is taken for the plate-out of the volatile and non-volatile fission products as they pass through the Safety Equipment Building.

GLBYB: Sequence SGTR-20

The initiating event of this analyzed sequence is a double ended break of a single steam generator tube. Additional failures included failure (in the open position) of one of the steam generator pressure relief valves and no HPSI. Primary system injection is still possible using the three charging pumps, but no cooldown and depressurization of the primary system is credited. The stuck open steam generator relief valve is assumed to be the result of steam generator overfill.

The analyzed sequence is modeled with the steam generator ADV stuck open from the onset of the accident. The steam generator water level in the faulted steam generator is maintained at its normal water level until the CST is depleted.

The containment would remain bypassed until the stuck open steam generator ADV is closed. The majority of fission product release from the containment in this analyzed sequence occurs during the core melt and relocation phase of the accident, before the primary system fails due to creep rupture of the hot leg piping.

In this sequence the emergency fan coolers are not credited and the containment sprays are only allowed to operate in the injection mode. As a result neither of these systems is available for long term containment cooling. In this scenario the fission product release from the containment following vessel failure is slightly higher than it would be if some form of long term containment cooling is available. The total fission product release for this scenario, however, is dominated by the bypass release prior to vessel failure.

The possibility of HPSI, LPSI, and HPSI recirculation after the vessel fails is accounted for by allowing the LPSI pumps to start only after the core debris from the failed vessel has relocated to the reactor cavity. The HPSI pumps are assumed to have failed during the injection phase of this accident. Therefore, neither HPSI nor HPSI recirculation are available after vessel failure.

GLAYB: Sequence SGTR-33

The initiating event of this analyzed sequence is a double-ended break of a single steam generator tube. Additional failures include: (1) no secondary side cooling, and (2) no primary system injection other than the three charging pumps.

In this sequence the emergency fan coolers are not credited. Once the setpoint for actuating the containment spray system is reached, however, the containment spray recirculation system is available for long term containment cooling. In this scenario, the fission product release from the containment is typical of expected release from any sequence in which containment cooling is available.

Injection following vessel failure occurs with the initiation of HPSI followed by HPSI recirculation once the RWST is depleted.

GLANB: Sequence SGTR2-48

The initiating event for SGTR2-48 is a double ended break of a single steam generator tube. Mechanical, operational, and maintenance induced failures assumed for this sequence include: (1) failure of the operators to identify the SGTR and begin early primary system depressurization, (2) loss of auxiliary feedwater to the intact steam generators, (3) loss of 2 CS pumps, and (4) loss of all 4 emergency containment fan coolers. Loss of secondary side cooling and failure to depressurize the primary system, preclude HPSI injection due to primary system pressure until after vessel failure. The 3 charging pumps are, however, allowed to inject in order to maximize the amount of hydrogen produced in vessel.

In this accident scenario, the containment is bypassed for the duration of time where primary system pressure exceeds the steam generator relief pressure. Once the primary system pressure drops below the relief pressure the steam generator atmospheric dump valve closes isolating the primary system from the outside environment. The absence of containment cooling coupled with the HPSI injection and recirculation of water through the failed reactor vessel and into the reactor cavity results in an overpressure failure of the containment approximately 41 hours after the initiating event.

GLCNB: Sequence SGTR2-66

The initiating event for SGTR2-66 is a double ended break of a single steam generator tube. Mechanical, operational, and maintenance induced failures assumed for this sequence include: (1) failure of the operators to identify the SGTR and begin early primary system depressurization, (2) loss of auxiliary feedwater to the intact steam generators, (3) loss of 2 CS pumps, (4) loss of all emergency containment fan coolers, (5) loss of 3 HPSI

pumps and (6) loss of 2 LPSI pumps. The 3 charging pumps are, however, allowed to inject in order to maximize the amount of hydrogen produced prior to vessel failure.

Sequence SGTR2-66 and sequence SGTR2-48 are similar up to the time of vessel failure, and in the fact that both lack some form of containment heat removal. The ability to fill the reactor cavity with water differentiates sequence SGTR2-48 from SGTR2-66.

The loss of HPSI and LPSI pumps in sequence SGTR2-66 prevents filling the reactor cavity with water and cooling the corium deposited there after vessel failure. Since the mass of corium discharged to the reactor cavity following vessel failure is large, failure of the cavity floor due to MCCI can be expected to occur in the absence of further intervention in this sequence. An MCCI induced failure of the cavity floor, however, provides a ground release path to the outside environment. In the event that an MCCI induced failure of the cavity floor does not provide sufficient pressure relief to the containment to prevent further pressurization, more than 48 hours must elapse before sequence SGTR2-66 would fail the SONGS 2/3 containment by overpressurization.

4.7.4 Sensitivity Analysis

NUREG-1335, Appendix A, identified potential in-vessel and ex-vessel phenomena that might impact containment failure timing and the source term release should a core damage accident occur. Sensitivity analyses were performed as part of the SONGS 2/3 IPE to address these phenomena and their uncertainties. Sensitivity analyses were also performed as part of the SONGS 2/3 IPE to address the questions concerning equipment operation during a severe accident.

4.7.4.1 Methodology

Table 4.7-7 identifies the phenomena identified in NUREG-1335 for sensitivity study, along with the means by which these sensitivities were addressed in the SONGS 2/3 IPE. The issues of interest include:

Hydrogen burn completeness

In-vessel hydrogen production and core relocation

Hot-leg creep rupture failure in a high pressure sequence

High Pressure Melt Ejection (HPME)

RPV failure modes

Containment failure pressure and area

Table 4.7-7

(Page 1 of 3)

**SONGS 2/3 SENSITIVITY ANALYSES TO ADDRESS UNCERTAINTIES
IDENTIFIED IN NUREG-1335**

Phenomena	Analyses Performed	MAAP Sensitivity Case Identifiers (Where Applicable)
<ul style="list-style-type: none"> • Performance of containment heat removal systems during core meltdown accidents 	<ul style="list-style-type: none"> • The equipment qualification of the containment heat removal systems is not violated by containment conditions expected for a severe accident at SONGS 2/3. Plate-out of fission products on the coils of the CEFCs is not addressed (see Section 4.7.4.3 on discussions of equipment survivability in a severe accident environment). 	--
<ul style="list-style-type: none"> • In-vessel phenomena 		
<ul style="list-style-type: none"> - H₂ production and combustion in containment 	<ul style="list-style-type: none"> • Hydrogen combustion was discussed in a phenomenological evaluation summary (see Section 4.4.2). 	--
	<ul style="list-style-type: none"> • MAAP sequence with an increased value of "flame flux multiplier (speed)" to promote burn completeness is detailed in a phenomenological summary (see Section 4.4.2 and section 4.7.4.2). 	--
<ul style="list-style-type: none"> - Core relocation characteristics 	<ul style="list-style-type: none"> • MAAP sequence with core blockage parameter varied. Conservatively modeled with no core blockage assumption. 	--
<ul style="list-style-type: none"> - High Pressure Melt Ejection 	<ul style="list-style-type: none"> • MAAP sequence for a high pressure transient was modeled. Vessel was allowed to fail at high pressure at the bottom of the reactor vessel (i.e., beneath the core debris). 	HPME1 HPME2

Table 4.7-7
(Page 2 of 3)

SONGS 2/3 SENSITIVITY ANALYSES TO ADDRESS UNCERTAINTIES
IDENTIFIED IN NUREG-1335

Phenomena	Analyses Performed	MAAP Sensitivity Case Identifiers (Where Applicable)
<ul style="list-style-type: none"> In-vessel phenomena (continued) <ul style="list-style-type: none"> Fuel/coolant interactions Mode of RPV melt-through Induced failure of RCS pressure boundary at high RCS pressure/temperature Ex-vessel phenomena <ul style="list-style-type: none"> Direct containment heating (at high RCS pressure) Potential for early containment failure due to pressure load 	<ul style="list-style-type: none"> In-vessel steam explosions addressed in phenomenological evaluation summary (see Section 4.4.2), no further sensitivity analysis is required. Thrust forces at RPV failure addressed in phenomenological evaluation summary (see Section 4.4.2), no further sensitivity analysis is required. Base-case ATWS assumes an induced large LOCA. All Level 1 transients account for probability of a stuck open safety valve. MAAP sequence with hot leg creep rupture failure was performed for a high-pressure transient with no core blockage. Hot leg creep rupture is basis of SONGS 2/3 primary system failure for all high pressure transients. DCH was addressed in a phenomenological evaluation summary (see Section 4.4.2). Sensitivity analysis for HPME also applies. Potential early containment failure due to ex-vessel steam explosions or hydrogen combustion were addressed in phenomenological evaluation summaries (see Section 4.4.2), no further sensitivity analyses are required. 	<ul style="list-style-type: none"> -- -- -- -- All analyzed sequences HPME1 HPME2 --

Table 4.7-7
(Page 3 of 3)

SONGS 2/3 SENSITIVITY ANALYSES TO ADDRESS UNCERTAINTIES
IDENTIFIED IN NUREG-1335

Phenomena	Analyses Performed	MAAP Sensitivity Case Identifiers (Where Applicable)
<ul style="list-style-type: none"> Ex-vessel phenomena (cont) <ul style="list-style-type: none"> Early failure via debris attack of containment penetrations Long-term core-concrete interaction -- Water availability -- Debris coolability -- Containment Failure at 95% non-exceedance pressure -- Containment Failure Area -- Isolation Failure Area -- Reactor Cavity Natural Circulation -- Ex-Vessel Cooling V-sequence (ISLOCA) 	<ul style="list-style-type: none"> Containment penetration thermal attack was addressed in a phenomenological evaluation summary (see Section 4.4.2), no further sensitivity analysis is required. Molten core-concrete interaction (MCCI) was addressed in a phenomenological evaluation summary (see Section 4.4.2). Also, most base case MAAP analyses showed long-term MCCI; no further sensitivity analysis is required. In most base cases the core debris remained uncooled in the (dry) cavity; no further sensitivity analysis is required. Analyzed sequences consider range of conditions from debris coolable (wet cavity) to debris uncoolable (dry cavity). Containment Failed at 95% non-exceedance pressure Containment Failure Area increased Containment Isolation Failure Area increased Reduced Flow Area through cavity to determine effect on H₂ burning in cavity Effect of ex-vessel cooling investigated MAAP sequence with very large ISLOCA was performed to reduce uncertainty concerning break size. 	<ul style="list-style-type: none"> -- -- Bounded by analyzed sequences Bounded by analyzed sequences PCS4-CHF1 ML020-PCF1 LOP48-PCF1 ML020-PCF2 LOP48-PCF2 SB017-IF1 LL034-IF1 PCS35-ATNBP PCS4-EVC3 VSEQ2-LARGE

Volatile fission product release/retention in the primary system

Ex-vessel debris coolability

A two part approach is employed in addressing uncertainties associated with the back-end analysis. The first part (primary approach) addresses the phenomena identified in NUREG 1335 by performing detailed phenomenological evaluations as described in Section 4.4. These plant-specific evaluations are primarily concerned with the postulated early containment failure mechanisms, core-concrete interaction, and containment fragility. Uncertainties associated with modeling the phenomena are identified in NUREG-1335. Most of these uncertainties were addressed in the individual evaluations, but they did not impact the conclusions of the phenomenological summaries.

The second part (secondary approach) addresses phenomenological uncertainties which were not considered in the phenomenological evaluations, by performing MAAP sensitivity analyses. This was accomplished by varying certain MAAP parameters in selected base case sequences. The recommended ranges of MAAP parameter variation for the IPE sensitivity analyses have been documented by EPRI (Reference 4.7-1). Sensitivity sequences analyzed for the SONGS 2/3 IPE are shown in Table 4.7-7. Results of these sensitivity analyses are shown in Table 4.7-8. The sensitivity sequence identifiers indicate the source term sequences upon which the sensitivity runs are based and include a description indicative of the sensitivity issue. Sensitivity sequence identifiers are listed in Tables 4.7-7 and 4.7-8 to correlate the MAAP sensitivity runs to the accident phenomena they address.

The above two part approach addresses all identified phenomenological and modeling uncertainties relevant to the SONGS 2/3 back-end analysis. Insights or uncertainties identified during the SONGS 2/3 back-end analysis which did not fit into the standard back-end analysis were incorporated in the sensitivity analyses as needed.

4.7.4.2 MAAP Sensitivity Sequences

Sequences used in investigating phenomenological and modeling uncertainties are based upon the analyzed source term sequences discussed in Section 4.7.3. Hereafter, the analyzed source term sequences will be referred to as base cases and identified by their EET systemic sequence numbers. In the sensitivity sequence descriptions which follow, only the deviations from the base case sequences are emphasized.

Table 4.7-8
(Page 1 of 2)

SOURCE TERM SENSITIVITY ANALYSIS RESULTS
MAAP RUN SUMMARY TABLE

SEQUENCE TYPE								
Sequence No.	HPME1	HPME2	MLO20-PCF1	LOP48-PCF1	MLO20-PCF2	LOP48-PCF2	PCS4-CHF1	PCS35-ATNBP
Plant Damage State Designator	TEAYS	TECNL	SEBNL	TECNL	SEBNL	TECNL	TEAYS	SLLYS
Source Term Release Category	S	L	W	L	W	L	S	S
PDS Bin Frequency (y^{-1})	-	-	-	-	-	-	-	-
CORE/CONTAINMENT RESPONSE								
Time of Core Uncovery (hr)	1.2	1.8	0.9	1.2	0.9	1.2	1.2	9.2
Onset of Core Melt (hr)	1.7	2.5	1.3	1.7	1.3	1.7	1.7	10.3
Time of Vessel Failure (hr)	2.5	3.3	3.6	2.6	3.6	2.6	2.5	13.3
Time of Containment Failure (hr)	-	-	18.8	24.9	18.8	24.9	-	-
Maximum Containment Pressure (psia)	30.1	156.1	151.9	146.0	151.9	146.0	30.3	30.2
Maximum Containment Temperature ($^{\circ}$ F)	352.5	561.3	364.6	508.0	364.6	508.0	457.0	311.2
Cavity Water Level @ End of Mission Time	1.3	5.9	8.4	0.0	8.4	0.8	33.2	0.1
Fraction of Clad Reacted in Vessel	0.32	0.28	0.29	0.29	0.29	0.29	0.29	0.36
H ₂ Mass Burned (lbm)	139.	35.	0.0	0.0	0.0	0.0	530.	3388.
Cavity Concrete Ablation Depth at End of Mission Time (ft)	0.0	0.0	0.0	6.9	0.0	6.9	0.6	3.4
FISSION PRODUCT DISTRIBUTION AT END OF MISSION TIME								
Noble Release (%)	.2	20.2	100.0	37.4	100.0	37.4	0.1	0.1
Volatile FP Release (%)	1.E-4	2E-2	12.6	5.E-1	12.8	5.E-1	1.E-4	6.E-3
Non-Volatile FP Release (%)	0	1.E-3	2.E-1	1.E-1	2.E-1	1.E-4	0	3E-4
Volatile FP Retained in Primary System (%)	58.	97.	42.	36	39.3	36	55.	17.

GENERAL NOTES:

- S of the Source Term Release Category indicates safe stable state achieved ex-vessel (i.e., no over-pressurization failure of containment, however, MCCI induced containment, failure may occur).
- Mission time for Level II is 48 hours.
- Containment bypass (SGTR, VSEQ).
- MCCI Failures - See Table 4.3-2 through 4.3-5 (Cavity Wet = No) for sequences and frequency.

Table 4.7-8
(Page 2 of 2)

SOURCE TERM SENSITIVITY ANALYSIS RESULTS
MAAP RUN SUMMARY TABLE

SEQUENCE TYPE						
Sequence No.	SB017-IF1	LL034-IF1	PCS4-EVC3	VSEQ2-LARGE		
Plant Damage State Designator	TEAYI	LEIYI	TEAYS	GILYB		
Source Term Release Category	G	G	S	T		
PDS Bin Frequency (yr ⁻¹)	-	-	-	-		
CORE/CONTAINMENT RESPONSE						
Time of Core Uncovery (hr)	1.2	0.006	1.2	1.1		
Onset of Core Melt (hr)	1.7	0.6	1.7	1.6		
Time of Vessel Failure (hr)	2.5	1.7	-	2.8		
Time of Containment Failure (hr)	(ISOL FAILS)	(ISOL FAILS)	-	-		
Maximum Containment Pressure (psia)	47.7	43.3	30.0	19.1		
Maximum Containment Temperature (°F)	279.1	361.2	227.0	428.5		
Cavity Water Level @ End of Mission Time	33.2	0.5	10.2	0.0		
Fraction of Clad Reacted in Vessel	0.29	0.23	.31	0.22		
H ₂ Mass Burned (lbm)	2.	0.0	46.	2066.		
Cavity Concrete Ablation Depth at End of Mission Time (ft)	1.3	0.1	0.0	6.9		
FISSION PRODUCT DISTRIBUTION AT END OF MISSION TIME						
Noble Release (%)	96.7	100.	0.2	100.		
Volatile FP Release (%)	8.5	4.1	8.E-5	93.2		
Non-Volatile FP Release (%)	0.2	0.3	6E-5	0.9		
Volatile FP Retained in Primary System (%)	41.	40.	68.	5.		

- GENERAL NOTES:
- S of the Source Term Release Category indicates safe stable state achieved ex-vessel (i.e., no over-pressurization failure of containment, however, MCCI induced containment, failure may occur).
 - Mission time for Level II is 48 hours.
 - Containment bypass (SGTR, VSEQ).
 - MCCI Failures - See Table 4.3-2 through 4.3-5 (Cavity Wet = No) for sequences and frequency.

High Pressure Melt Ejection (HPME1 & HPME2)

As already discussed, a severe accident at either SONGS 2 or 3 should result in creep rupture of the hot leg piping before the reactor vessel fails. Low pressure creep failure of the reactor vessel would then result in the molten vessel internals dropping into the reactor cavity. These sensitivity cases examine what would happen if the SONGS 2/3 reactors failed at high pressure due to melt-through at the base of the lower head. The base case for HPME1 is PCS4 and the base case for HPME2 is LOP48.

High pressure melt ejection from a failed reactor vessel has been a concern since the TMI accident. Phenomena associated with a high pressure melt ejection include vessel thrust forces, direct containment heating, ex-vessel steam explosions and hydrogen deflagration and detonation. Evaluation summary reports dealing with these issues have been prepared for SONGS 2/3 (References 4.7-3, 4.7-4 and 4.7-5). These reports discuss the effects of failing the SONGS 2/3 reactor vessel at high pressure and at the bottom of the reactor vessel. They conclude that the four phenomena listed above cannot breach or significantly impair the SONGS 2/3 containment.

With respect to source term, there is very little difference between creep rupture failure of the RCS and a HPME. The geometry of the reactor cavity in SONGS 2/3 is very open. There is a cylindrical central chamber directly beneath the reactor vessel. Four 5 ft. diameter ventilation ducts lead from this central chamber up to the lower containment. The pathways from the SONGS 2/3 reactor cavity are large enough to prevent a large pressure differential from developing. Furthermore, core material (corium) exiting the bottom of the reactor vessel at high pressure may not escape the reactor cavity. To escape the SONGS reactor cavity, a HPME would have to reverse direction 180 degrees or pass through two sharp turns totaling more than 210 degrees.

Two HPME scenarios completely bound the subject of high pressure melt ejection at SONGS 2/3. HPME1 and HPME2 are variations of the dominant sequences PCS4 and LOP48 respectively. In both sequences the reactor vessel fails at high pressure. By assumption, most of the core debris can escape the SONGS 2/3 reactor cavity and enter the lower containment compartment. The major difference between these two high pressure melt sequences is that in HPME1 containment cooling is available and in HPME2 it is not.

The pressure and temperature time-histories of sequences PCS4 and HPME1 are very similar. Both sequences result in a maximum containment pressure of approximately 30 psia and a maximum containment temperature of 350°F. Discharge of hot corium into the lower containment compartment allows the burning of 139 lb. of hydrogen in HPME1. No hydrogen is burned in sequence PCS4 due

to cavity flooding immediately after vessel failure. There is almost no difference in the fission product release from containment calculated for sequence PCS4 and HPME1. The fact that most of the corium is submerged under water, following vessel failure, accounts for much of the similarity. The operational containment spray, with its ability to quickly scrub the containment atmosphere of fission products, also contributes to the similarity in these sequences.

Sequences LOP48 and HPME2, unlike the preceding two sequences, show significant differences. Sequence LOP48, which assumes creep rupture failure of the hot leg piping before vessel failure, reaches a higher pressure and ablates more cavity concrete at 48 hours than HPME2. Sequence HPME2, the high pressure discharge case, however, results in the higher containment temperature and a greater fission product release from the containment. In terms of source term release category, sequences LOP48 and HPME2 are identical. Another difference between sequence LOP48 and HPME2 is that sequences HPME2 results in the burning of about 35 lb. of hydrogen in containment.

The major differences between assuming vessel failure by high pressure melt ejection and vessel failure by creep rupture is that a HPME failure does not necessarily confine core debris to the reactor cavity. For those accident scenarios where the reactor cavity remains dry, confining the core debris to the cavity results in a large amount of concrete ablation at SONGS 2/3. As a result of MCCI in the SONGS 2/3 cavity, containment failure by melt-through of the cavity floor can be expected to occur between 16 and 24 hours after vessel failure.

Containment Failure Pressure (ML020-PCF1 and LOP48-PCF1)

These sequence assess the effect of reducing the containment failure pressure from best-estimate values to the 95% non-exceedance values. Assuming the 95% non-exceedance values for containment failure results in the following failure criteria:

1. If the containment pressure is less than 113 psia the containment failure area is assumed to be 0.0 ft².
2. If the containment pressure is greater than or equal to 113 psia but less than 133 psia the containment failure area is assumed to be 0.0031 ft².
3. If the containment pressure is greater than or equal to 133 psia but less than 146 psia the containment failure area is assumed to be 0.0156 ft².
4. If the containment pressure is greater than or equal to 146 psia but less than 152 psia the containment failure area is assumed to be 0.0267 ft².

5. If the containment pressure is greater than or equal to 152 psia the containment failure area is assumed to be 1.0 ft².

The MAAP parameter controlling the containment overpressure failure area is PCF. No changes are assumed in the containment failure areas associated with a particular containment failure. In this sensitivity study, the staged containment failure pressures assumed are the 95% non-exceedance pressures calculated for the SONGS 2/3 containments. The first containment failure pressure drops from its base case value of 171 psia to 113 psia; the second containment failure drops from its base case value of 174 psia to 133 psia; the third containment failure drops from its base case value of 183 psia to 146 psia and the fourth containment failure area drops from its base case value of 189 psia to 152 psia.

Reducing the containment failure pressure in sequence LOP48-PCF1 reduces the containment overpressure failure time by approximately 15 hours compared to sequence LOP48. The containment failure time of sequence ML020-PCF1 is more than 7.5 hours earlier than that calculated for sequence ML020. In spite of the difference in the containment failure pressures assumed, the source term releases calculated for sensitivity sequences LOP48-PCF1 and ML020-PCF1 are almost identical to those calculated for the base cases LOP48 and ML020. The containment failure times in sensitivity case LOP48-PCF1 and ML020-PCF1 are 24.9 hours and 18.8 hours, respectively, after the initiating event. These containment failure times are 2 to 3 times that required for gravitational settling of containment aerosols to significantly reduce the amount of airborne fission product in the SONGS 2/3 containment.

Containment Failure Area (LOP48-PCF2 and ML020-PCF2)

These sequences assess the effect of the containment failure area on the source term release. Since sequences involving earlier containment overpressure failures are more sensitive to this uncertainty, sequences LOP48-PCF1 and ML020-PCF1 are assumed for the base cases.

The containment failure area in MAAP is controlled by parameter ACFPR. This failure area, however, cannot be arbitrarily changed. The first three containment failure locations at SONGS 2/3 do not result in major structural failure of the SONGS 2/3 containment. The growth of these particular containment failures are limited by structural considerations (Reference 4.4-1). Therefore, the failure areas associated with: (1) buckling of the fuel transfer tube secondary bellows, (2) liner tearing at the equipment hatch and (3) liner tearing at the personnel airlock are assumed to remain at their median value (see Table 4.4-2).

Of the major structural failure modes in the containment wall at SONGS 2/3, the lowest pressure capacity is associated with a membrane failure of the cylinder due to hoop stress. The containment failure area in the base cases, LOP48-PCF1 and ML020-PCF1, is assumed to be approximately 1.0 ft². In the sensitivity cases, LOP48-PCF2 and ML020-PCF2, this containment failure area is increased to 10.0 ft² when the containment pressure is greater than or equal to 152 psia.

The results of these sensitivity studies are nearly identical to their respective base cases. The instantaneous jump in the containment failure area from 0.0267 ft² to 1.0 ft² or 10.0 ft² appears to have very little effect on the outcome of the modeled sequences.

Isolation Failure Size (SB017-IF1 and LL034-IF1)

These sequences assess the effect of an increase in the isolation failure size on containment performance and the source term release. The isolation failure modeled in sequences SB017-IF1 and LL034-IF1 is 7 times larger than the isolation failure modeled in sequences SB017 and LL034. When compared with sequences SB017 and LL034, sequences SB017-IF1 and LL034-IF1 result in:

- (1) an increase in the amount of noble gases released from containment at 48 hours,
- (2) a doubling of the volatile fission product release from the containment at 48 hours, and
- (3) varying percentages of increase and decrease in the non-volatile fission product release from the containment 48 hours.

These differences do not represent a very large increase in the radioactive release from the containment considering the difference in the isolation failure areas assumed. Furthermore, the calculated release from these sequences places them in the same release category as sequences SB017 and LL034.

As expected, changing the size of the isolation failure does not greatly affect the primary system performance for a large LOCA. Assuming a larger isolation failure area does limit the maximum containment pressurization observed in these sensitivity analyses.

The source term release for sequences SB017-IF1 and LL034-IF1 are, as expected, larger than those of their respective base cases. Even though the isolation failure is increased by approximately 7 times, a corresponding increase in the source term release is not observed. The source term release bins for these sensitivity analyses are the same as for their respective base cases.

Reduced Debris Coolability (PCS4-CHF1)

This sequence assesses the effect of reduced debris coolability on containment performance and the source term release. Sequences where the core debris is covered with water following vessel failure would be most sensitive to this uncertainty. Therefore, the most probable severe accident involving injection through the failed reactor vessel and the flooding of the reactor cavity, PCS4, is assumed for the base case.

The critical heat flux at the debris-water interface is controlled by MAAP parameter FCHF. In this sensitivity analysis FCHF is reduced from 0.1 to 0.02. This assumption results in only 20% of the normal, best-estimate, heat transfer from the corium to the cavity water.

Reduction in the debris coolability has no effect on accident progression timing. The peak containment pressure in the sensitivity case, PCS4-CHF1, is approximately 8 psi less than that calculated for sequence PCS4. Reduced steaming from the cavity water pool is responsible for this condition. An increase in maximum containment temperature is also observed in the sensitivity case. This is also a result of reduced steaming modeled in PCS4-CHF1. The sensitivity case results in slightly less cladding oxidized than in the base case. Otherwise, this case is nearly identical to the base case. A negligible difference in the source term release is calculated for PCS4-CHF1 when compared to the base case.

Reactor Cavity Natural Circulation (PCS35-ATNEP)

This sequence assesses the effect of reducing the flow area surrounding the hot and cold leg piping as it passes through the reactor shield wall. The area through the reactor shield wall is part of a natural circulation flow which allows hot gases escaping the reactor cavity to be replaced by colder gas from the lower containment compartment at SONGS 2/3.

A sustainable natural circulation flow from the lower containment through the reactor shield wall to the cavity, and back to the lower compartment via the four cavity ventilation ducts, is observed to exist whenever SONGS 2/3 is modeled with a dry cavity after vessel failure. As the differential temperature between the lower containment compartment and the cavity increases, this flow is observed to increase. The result of this natural circulation is to provide a slow but sustainable flow of oxygen to the SONGS 2/3 reactor cavity. Hydrogen generated by hot metal-water interaction in the SONGS 2/3 reactor cavity will burn in the cavity as long as oxygen is present and the temperature of the cavity exceeds the autoignition temperature for hydrogen. By increasing the amount of natural circulation through the SONGS 2/3 reactor cavity, the amount of hydrogen burned in the reactor cavity can be increased.

The flow area coupling the lower containment compartment, through the reactor shield wall, to the reactor cavity is specified by MAAP parameter ATNBP. In the SONGS 2/3 containment, the minimum flow area connecting the lower compartment and reactor cavity is the opening area between cavity wall and the reactor vessel. By considering the cavity area occupied by the cavity shield plug and the four reactor vessel support columns, a best-estimate value of ATNBP of 47.25 ft² is assumed for the base cases. In this sensitivity analysis, however, the value of ATNBP is reduced to 11.81 ft². This assumption reduces the flow area into the reactor cavity to 25% of the best-estimate value.

Reduction of the flow area coupling the lower containment compartment and the reactor cavity has no effect on accident progression timing. The later vessel failure time calculated in PCS35-ATNBP, when compared to the base case PCS35, is the result of the SONGS safety injection tanks discharging into the primary system before vessel failure. In the base case, the safety injection tanks are not depleted until after vessel failure. The increase in vessel clad oxidation calculated in PCS35-ATNBP is also a result of injecting the SONGS safety injection tanks after core uncover but before vessel failure. Compared with the base case, the only observable effect of decreasing the flow area ATNBP is an approximate 500 lb increase in the amount of hydrogen burned in the lower containment and cavity.

Ex-Vessel Cooling (PCS4-EVC3)

This sequence assesses the affect of ex-vessel cooling and the retention of the relocated core in the reactor vessel. To assess this sequence, a special version of MAAP 17.02 with a lower head coolability option is used (Reference 4.7.2). The SONGS 2/3 cavity is assumed to be floodable by the removal of the blank flanges from the two 3-inch reactor cavity suction lines.

The results of this sensitivity analysis are essentially identical to the base case analysis, PCS4, up to 2.5 hours. At this time, the base case analysis predicts failure of the reactor vessel. No such failure is predicted by this sensitivity analysis. The heat from the core debris in the lower head is transferred by conduction from the molten corium, through a corium crust, through the reactor vessel lower head and into the water surrounding the reactor vessel. Heat from the molten corium also radiates to the steel reactor vessel and the vessel internals not in contact with the core debris.

The lower head coolability model used in this analysis does not start removing heat from the primary system until the core has relocated to the reactor vessel's lower head. In any event, hot leg creep rupture occurs shortly after the core relocates to the lower vessel head. More nobles and volatile fission products are retained in the primary system by this analysis than are retained in the base case. Ex-vessel cooling of the primary system

between the time the core relocates and the time creep rupture fails the primary system explains most of this fission product retention.

The conduction-limited process of removing heat from the core debris results in a central pool of molten superheated debris. Where the core debris contacts the cooled inside surface of lower vessel head a crust of core debris forms. The thickness of this oxide crust determines and limits the rate at which heat is transferred from the debris pool, through the reactor vessel lower head, to water in the reactor cavity.

The inability to rapidly cool the core debris in the lower vessel head is responsible for the non-volatile fission products release from the reactor vessel to the containment which is calculated in this sensitivity analysis. The non-volatile fission product release to the containment calculated for this sensitivity is larger than that calculated for any other accident scenario. MAAP is over-estimating the temperature dependent release rate of the non-volatiles in the reactor vessel lower head. The non-volatile fission product release from containment for this sensitivity analysis, however, is approximately the same as the base case analysis.

Hydrogen Production and Combustion in Containment

The phenomenological summary on hydrogen deflagration and detonation for SONGS 2/3 bounds the sensitivity issues raised by EPRI concerning the modeling of hydrogen burning using the MAAP code. These concerns include but are not limited to: (1) the effect of suppressing the burning of a hot (1450°F) hydrogen and/or carbon-monoxide jet entering an oxygen bearing room, (2) the effect of suppressing the recombination (autoignition) of hot (1310°F) hydrogen and/or carbon-monoxide in the presence of oxygen, (3) the effect of enhanced turbulence (an increase flame flux speed) due to fans or sprays on incomplete hydrogen combustion. None of the EPRI concerns regarding the burning of hydrogen affect the SONGS 2/3 containment or the source term release from a severe accident. The major concern regarding the accumulation and burning of hydrogen at SONGS 2/3 containment is discussed in Section 4.4.2, "Unlikely Failure Modes, Hydrogen Combustion".

Large Containment Bypass (VSEQ2-LARGE)

This sequence assesses the effect of increasing the size of an interfacing system LOCA containment performance and the source term release. Class V-Sequences and certain types of SGTR are classified as containment bypass scenarios in this IPE. This sensitivity analysis is only concerned with the effects of a large V-sequence as defined by base sequence VSEQ2.

The MAAP parameter ABB is used to specify the area of a V-sequence break when used in conjunction with Event codes 209 and 238. Event code 209 tells MAAP to open the break in the primary system. Event code 238 tells MAAP to not discharge the break flow into the containment. In this sensitivity case the size of the break in the primary system is increased from 2.5" diameter to 10" diameter.

The time to core uncover and vessel failure is reduced by the increased size of the V-sequence break. The amount of cladding reacted in vessel is also reduced. A reduced residence time for water in the primary system, during the core melt phase of this severe accident, is responsible for this response. The increased cavity concrete ablation in this sensitivity case, when compared to sequence VSEQ2, is the result of the earlier vessel failure time. A negligible difference in the source term release is calculated for VSEQ2-LARGE when compared to the base case. Due to the large source term release associated with the base case, the 9% increase in the non-volatile release is small. The source term bin for the V-sequence appears to be independent of the break size at least for the dominant V-sequence at SONGS 2/3.

4.7.4.3 Equipment Survivability

The engineered safety features are expected to survive the pressure, temperature, radiation, debris and steam conditions expected during a severe accident. This evaluation covers critical equipment located inside the containment and the safety equipment building.

ESF Equipment Inside the Containment

After reviewing the environmental parameters of a severe accident and the critical components located inside the containment building, it is concluded that the issues associated with ESF equipment operability inside the containment are: aerosol accumulation on the containment spray nozzles and high temperature, plugging, and radiation, effects on the containment emergency fan coolers. Discussions on the survivability of these two sets of safety related equipment are provided below:

Containment Spray Nozzles. Debris aerosol should not plug the containment spray nozzles. The containment spray system design specifies that the nozzles have an approximately 3/8-inch spray orifice and will not be subject to clogging by particles less than 1/4-inch in maximum dimension. Particles greater than 1/4 inch are not expected to reach the containment spray nozzles due to their location in the ceiling of the containment.

Emergency Fan Coolers. As long as an emergency fan cooler or containment spray pump actuates and continues to operate in a post accident environment, then the containment temperature can be maintained below the acceptance level developed by the

environmental qualification tests. As a result, air temperature is not expected to affect the emergency fan cooler operability if the containment heat removal capability can be maintained.

It is conservatively assumed that operability of the containment fan coolers could be challenged if significant aerosol generation developed inside the containment. The aerosol generation could lead to fan cooler failure from the effects of high radiation on the non-metallic materials or plugging. This situation can only occur after reactor vessel failure, followed by corium-concrete interaction, and the lack of a fission product scrubbing in the containment. This scenario can be developed after the following conditions are met:

- failure of reactor vessel,
- the reactor cavity is dry,
- a containment spray pump unavailable, and
- at least one containment emergency fan cooler is operable.

Accident sequences listed in Tables 4.3-2 through 4.3-5 meeting the above conditions are identified and listed in Table 4.7-9. The containment integrity can be maintained if the emergency fan operability is maintained through the postulated severe accident scenario. If the emergency fan coolers are the only means of containment heat removal, aerosol plate-out on the fan cooler tubes could lead to the failure of EFCS. If this were to occur then a late containment failure might result.

Table 4.7-9 shows that the accumulated frequency of this category of sequences amounts to $7.9\text{E-}7/\text{yr}$ or about 2.6% of the core damage frequency. By incorporating this conservative assessment into the results shown in Table 4.7-5, the late containment failure category (release categories L and W) increases from 9.4% to 13%, while the "no containment failure" category (release category 9) decreases from 84% to 81%.

ESF equipment outside the containment

This issue focuses on HPSI and containment spray recirculation operation after RPV failure. If the CCW flow to the HPSI and containment spray pumps is not interrupted in a severe accident, then the critical components of these pumps can be adequately cooled and maintain operability in the recirculation mode. This conclusion is based on a review of the post accident recirculation sump water temperature, temperature of critical pump components and the pump motor cooling. In addition, a review of environmental qualification results of the pump power cables indicated that these cables will remain operable at the elevated room temperature. An ESF pump room equipment inventory survey shows that there is no other heat sensitive equipment inside the room.

TABLE 4.7-9

ACCIDENT SEQUENCES WITH THE POTENTIAL FOR
LONG TERM CONTAINMENT FAILURE

ACCIDENT SEQUENCE	FREQUENCY
TT1-18	4.3E-8
PCS1-18	3.2E-8
SLB-38	4.1E-9
LDC-12	1.9E-9
LDC-24	3.1E-9
ATWS-20	1.2E-9
LL0-22	5.4E-7
LL0-28	4.3E-9
LL0-34	1.4E-9
SL0-51	6.8E-8
PCS2-22	2.4E-8
ML0-17	1.6E-8
TT2-33	8.0E-9
ML0-23	8.5E-9
LOP-14	1.1E-8
SSL-5	1.0E-8
PCS2-6	1.0E-9
SSL-11	5.6E-9
SL0-57	4.5E-9
SL0-11	2.9E-9
TOTAL FREQUENCY	7.9E-7

NOTE: Accident sequences with dry or temporarily wet cavity, and no containment spray are included. Loss of emergency fan cooler due to aerosol plate-out could lead to long term containment failure.

4.8 Summary of Back-End Results

The design of the SONGS 2/3 containment reduces the frequency and magnitude of potential radiological releases. The large, dry containment provides for approximately 2.3 million cubic feet of free volume. A containment capacity evaluation revealed that the containment can withstand pressures more than twice the design pressure. The structural strength and volume features allow the containment to withstand a large mass and energy release without failing.

It is worth noting that the configuration of the reactor cavity and cavity cooling ducts provides an effective structural barrier to debris dispersal from the cavity following vessel failure. However, the containment design does not facilitate flooding of the reactor cavity. Thus, the majority of SONGS 2/3 core damage sequences would be expected to have significant core-concrete attack in the absence of vessel injection after vessel failure.

The SONGS 2/3 source term analysis has estimated sequence progression and source term releases for those event sequences which are significant contributors to the total SONGS 2/3 core damage frequency. The back-end analysis thereby considers and reports source term results for over 99% of the total core damage frequency as defined in the EETs (see culling limit Section 4.3.1.2). Not only have the source term results provided quantitative information regarding containment failure probabilities and source term releases, but it has yielded useful, quantitative insights into the performance of the SONGS 2/3 containment as well.

Results of the SONGS 2/3 Back-end analysis are summarized in Table 4.8-1. This table provides the release categories, range of the volatile fission product released, frequency of the release category, and the conditional probability of the release category given a core damage event has occurred.

The results indicate that, given core damage, there is an 84% probability that the containment will successfully maintain its integrity and prevent an uncontrolled fission product release.

The most likely mode of release from the containment is a late overpressure failure whose conditional probability is 9.4%. Containment bypass, with a conditional probability of 6.7%, is the next most likely mode of fission product release. Of these bypass sequences 70% are attributable to steam generator tube rupture with the remaining 30% attributable to interfacing system LOCAs. Finally, failure of the containment to isolate is expected to occur with a conditional probability of 0.1% per core damage event. The overall conditional containment failure probability of 16% is comparable with other PWRs.

The results of the back-end analysis indicate that there are no vulnerabilities or indication of unusually poor containment performance requiring immediate attention to improve the plant risk profile. Vulnerability screening was performed based on the screening criteria provided in Generic Letter 88-20, Appendix 2, "Criteria for Selecting Important Severe Accident Sequences." The criteria states as follows:

"Any functional sequence that has a core damage frequency greater than or equal to $1.0E-6$ per year and that leads to containment failure which results in a radioactive release magnitude greater than or equal to the BWR-3 or PWR-4 release category of WASH-1400."

A review of Table 4.8-1 indicates that no such functional sequence exceeds this criteria and thus no vulnerabilities are identified. The PWR-4 release category was estimated as 10% of the volatile fission product.

A number of features were identified through the course of the back-end analysis which contribute to the performance of the containment. These include the following:

- The most important feature of the SONGS 2/3 containment with respect to fission product retention is its ability to remain intact for several tens of hours following core damage. This robustness allows natural deposition mechanisms to remove airborne fission products from the containment atmosphere, and provides adequate time for additional accident mitigation activities to be implemented.
- SONGS 2/3 is not vulnerable to early containment failure.
- Hydrogen recombiner and purge systems are of minimal value under severe accident conditions. However, the robust SONGS 2/3 containment can withstand very large hydrogen burns.
- The inability to get water into the SONGS 2/3 reactor cavity prevents external cooling of the intact reactor vessel.
- The absence of any penetration in the SONGS 2/3 lower vessel head coupled with natural circulation in the primary system during a high pressure core melt is expected to induce creep rupture failure in the hot leg pipe prior to vessel failure. Failure through creep rupture of the hot leg is also expected prior to failure of the steam generator tubes due to the types of materials used at SONGS 2/3.

- Depressurization of the SONGS 2/3 primary system prior to vessel failure, as a result of creep rupture failure of a hot leg pipe, should preclude concerns about high pressure severe accident phenomena (i.e., ex-vessel steam explosion, direct containment heating and vessel thrust forces).
- If the primary system piping does not fail by creep rupture prior to vessel failure, the absence of penetrations in the lower vessel head at SONGS 2/3 coupled with the heat distribution of the internally heated core debris should result in vessel failure at or near the top of the debris pool in the lower head and not at the bottom of the vessel's lower head. Failing the SONGS 2/3 reactor vessel at or near the top of the debris pool in the lower head minimizes the amount of core debris that can exit the vessel before the primary system has depressurized. This failure mechanism should preclude concerns about high pressure severe accident phenomena.
- The basaltic concrete used in the construction of the SONGS 2/3 cavity requires less energy to melt than domolitic or domolitic - common sand concrete. This fact explains the concern about MCCI at SONGS 2/3. However, the decomposition of basaltic concrete does not produce flammable or non-condensable gaseous by-products, carbon monoxide and carbon dioxide, which results from the decomposition of domolitic or domolitic common sand concretes. Hydrogen generated during the core ablation process is the result of metal oxidation (i.e., zircaloy or iron). Retention of the core debris in a dry cavity at SONGS 2/3 may induce MCCI melt through of the cavity floor if the core debris cannot be cooled by water.
- Injecting water through a failed reactor vessel at SONGS 2/3, in an attempt to cool the core debris in the cavity, may or may not be advisable depending on the status of containment cooling. Injecting water into a cavity filled with hot core debris results in the formation of hot steam. If containment cooling is available this steam is condensed when it reaches the upper containment of SONGS 2/3. If no containment cooling is available steaming from the cavity can eventually overpressurize the SONGS 2/3 containment. The radiological release consequences of inducing an overpressurization failure of the SONGS 2/3 are expected to be greater than those associated with MCCI failure of the cavity floor at SONGS 2/3.

Table 4.8-1

SONGS UNITS 2 AND 3
AIRBORNE RELEASE CATEGORY AND PROBABILITY

Release Category	Definition	Release Frequency (per year)	P(RC CD) ¹
S	Success, no containment failure within 48 hrs, < 0.1% volatiles released	2.6×10^{-5}	0.838
T	Containment bypassed, > 10% volatiles released	6.5×10^{-7}	0.021
B	Containment bypassed, < 0.1% volatiles released	2.2×10^{-7}	0.007
D	Containment bypassed, up to 10% volatiles released	1.2×10^{-6}	0.039
G	Isolation failure, Containment failure prior to vessel failure, up to 10% volatiles released	2.0×10^{-6}	0.001
L	Late containment failure, up to 1% volatiles released	2.2×10^{-6}	0.072
W	Late containment failure, more than 10% volatiles released	6.9×10^{-7}	0.022

1. Conditional probability of release category given core damage.

- Steam inerting of the SONGS 2/3 containment during a severe accident can prevent hydrogen deflagration. Steam inerting of the containment is very likely to occur if containment cooling is unavailable.

With the high probability of containment success under severe accident conditions and no vulnerabilities, the back-end analysis has concluded that the SONGS 2/3 containment is not susceptible to unusually poor performance. The insights gained through the analysis of severe accident progression and the detailed study of related phenomena has provided SCE with a detailed understanding of the plant behavior under severe accident conditions. The knowledge developed will form a sound basis for future developments in accident management.

4.9 References

Section 4.1

- 4.1-1 "MAAP 3.0B Code Manual, "EPRI NP-777-1-CCML, 1990.

Section 4.2

- 4.2-1 T. Speis, USNRC, Letter to A. Buhl, IT Corporation, "Transmittal of Final NRC Technical Issue Positions for Issues 1, 2, 3, 5, 6, 11, 13A, and 17," September 22, 1986.
- 4.2-2 T. Speis, USNRC, Letter to A. Buhl, IT Corporation, "Transmittal of Final NRC Technical Issue Positions for Issues 4, 9, 10, 12, 13B, 15 and 16," November 26, 1986.
- 4.2-3 T. Speis, USNRC, Letter to A. Buhl, IT Corporation, "Position Papers for the NRC/DCOR Technical Issues," March 11, 1987.

Section 4.3

- 4.3-1 "Generic Framework for IPE Back-End (Level II) Analysis", NSAC/159, October 1991.
- 4.3-2 "REBECA Version 1.2Q Users Manual" ERIN Engineering and Research Inc., January 1992.
- 4.3-3 SONGS FSAR Section 6.2.1.1.2.4.

Section 4.4

- 4.4-1 EQE, 1991, "Probabilistic Evaluation of SONGS Units 2 and 3 Containment Performance for Beyond Design Basis Conditions", EQE PN 52114.01.

- 4.4-2 Sherman, M. P. and Borman, M., 1987, The Possibility of Local Detonation During Degraded Core Accidents in the Bellefonte Nuclear Plant, NUREG/CR-4803, SAND86-1180, Sandia National Laboratories.
- 4.4-3 Lutz, R. J., 1988, "Creep Rupture Failure of Primary Coolant Piping Prior to Reactor Vessel Failure for Severe Accidents," WCAP-11910.
- 4.4-4 Epstein, M. and Fauske, H. K., 1989, "The Three Mile Island Unit 2 Core Relocation - Heat Transfer Mechanism," Nuclear Technology, Vol. 87, pp 1021-1035.
- 4.4-5 O'Brien, J. E. and Hawkes, G. L., 1991, "Thermal Analysis of a Reactor Lower Head with Core Relocation and External Boiling Heat Transfer," AIChE Symposium Series, Heat Transfer - Minneapolis, Vol. 87, No. 283, pp 159-168.
- 4.4-6 Spencer, B. W., et al., 1988, "Results of EPRI/ANL DCH Investigations and Model Development," ANS/ENS Conference on Thermal Reactor Safety, Avignon, France.
- 4.4-7 Allen, M. D., Blanchat, T. K., Pilch, M. M. and Nichols, R. T., 1992a, "Quick-Look Report on the Fourth Integral Effects Tests (IET-4) in the Surtsey Test Facility," Sandia National Laboratories Report.
- 4.4-8 Allen, M. D., Blanchat, T. K., Pilch, M. M. and Nichols, R. T., 1992b, "Quick-Look Report on the Fourth Integral Effects Tests (IET-6) in the Surtsey Test Facility," Sandia National Laboratories Report.
- 4.4-9 Allen, M. D., Pilch, M. M., Griffith, R. O., Nichols, R. T., and Blanchat, T. K., 1992c, "Experiments to Investigate the Effects of 1:20 Scale Zion Structures on Direct Containment Heating (DCH) in the Surtsey Test Facility: The IET-1 and the IET-1R Tests," Sandia National Laboratories Report, SAN92-0255.UC-523.
- 4.4-10 Allen M. D., Blanchat, T. K., Pilch, M. M. and Nichols, R. T., 1992d, "Quick-Look Report on the Fourth Integral Effects Tests (IET-7) in the Surtsey Test Facility," Sandia National Laboratories Report.
- 4.4-11 Henry, R. E., 1989, "An Evaluation of Fission Product Release Rates During Debris Dispersal," Proc. of the ANS/ENS Intl. Topical Mtg. on Probability, Reliability and Safety Assessment, Vol. 1, pp, 375-383.
- 4.4-12 IDCOR, 1983, "Key Phenomenological Models for Assessing Explosive Steam Generation Rates," Technical Report 14.1A.

- 4.4-13 NRC, 1985, "A Review of the Current Understanding of the Potential for Containment Failure from In-Vessel Steam Explosion," NUREG-1116.
- 4.4-14 Alsmeyer, H., et al., 1987, "Beta Experimental Results on Melt/Concrete Interactions: Silicate Concrete Behavior," Proceedings of the Committee on the Safety of Nuclear Installation (CSNI) Specialists' Meeting on Core Debris-Concrete Interactions, EPRI NP-5054-SR.
- 4.4-15 Leak Rate Assessment for Epoxy Cable Seals in the SONGS Containment Walls, FAI internal memo from M. A. Grolmes to W. E. Berger, Jr., November 2, 1992.

Section 4.7

- 4.7-1 "Recommended Sensitivity Analyses for an Individual Plant Examination Using MAAP 3.0B," EPRI TR-100167, 1991.
- 4.7-2 FAI, 1991, "Lower Head Coolability Model For Use With The PWR MAAP 3.0B Code," FAI/91-173.
- 4.7-3 FAI, 1992, "Phenomenological Evaluation Summary on Steam Explosions in Support of the Individual Plant Evaluation," FAI/92-57.
- 4.7-4 FAI, 1992, "Phenomenological Evaluation Summary on High Pressure Melt Ejection and Direction Containment Heating," FAI/92-60.
- 4.7-5 FAI, 1992, "Phenomenological Evaluation Summary on the Probability and Consequences of Deflagration and Detonation of Hydrogen in Support of the Individual Plant Evaluation," FAI/92-86.

5.0 UTILITY PARTICIPATION AND INTERNAL REVIEW TEAM

5.1 IPE Program Organization

The IPE program at SCE was managed and conducted by the Nuclear Safety Group, which is part of the Safety Engineering Section of the Nuclear Oversight Division. The Nuclear Safety Group Supervisor was the IPE Project Manager, with overall responsibility for the program budget, schedule, and resource allocation, in addition to the responsibility for resolution of major technical issues. The PRA Group, a subgroup in the Nuclear Safety Group, provided the core project team members. The PRA Group Supervisor was the IPE Technical Manager, with overall responsibility for providing technical direction to the SCE Task Leaders and resolving day-to-day technical issues. SCE Task Leaders were assigned responsibility for completing various major program tasks including: Level I event tree and system analyses, Human Reliability Analysis, Level II analysis, and MAAP code analyses.

Consultants from ERIN Engineering, IPE Partnership, NUS Corporation, and EQE International assisted SCE in the preparation of the IPE through various scopes including: technical project management, initial fault tree development, flooding analysis, RETRAN analyses, containment strength analysis, and report preparation. ERIN Engineering was selected as the prime contractor responsible for conducting the Level I IPE analysis with the assistance of SCE PRA personnel. IPE Partnership was selected as the prime contractor responsible for conducting the Level II IPE analysis with the assistance of SCE PRA personnel. TENERA, a member of the IPE Partnership, was responsible for the Level II overall project and technical interface with SCE. FAI, another member of the IPE Partnership, was responsible for conducting the Level II IPE analysis with the assistance of SCE PRA personnel. NUS Corporation assisted SCE in performing numerous RETRAN analyses used for Level I success criteria development. EQE International was selected to perform the containment strength and failure mode analysis.

SCE PRA personnel took the lead in the preparation of several analyses including: the human reliability analysis, event tree development, Level I and II model quantification, Level I success criteria analysis, MAAP parameter file development, vulnerability analysis, and comment resolution. SCE has assumed full ownership of the IPE through technology transfer from the consultants and documented reviews of all analyses performed by other organizations.

The SCE PRA Group is made up of eight engineers, most having advanced engineering degrees and several having extensive prior PRA experience as consultants. Other PRA trained engineers from

the Nuclear Safety Group assisted in various tasks including system analysis reviews and comment incorporation. Other SCE organizations assisted in the IPE analysis as indicated below:

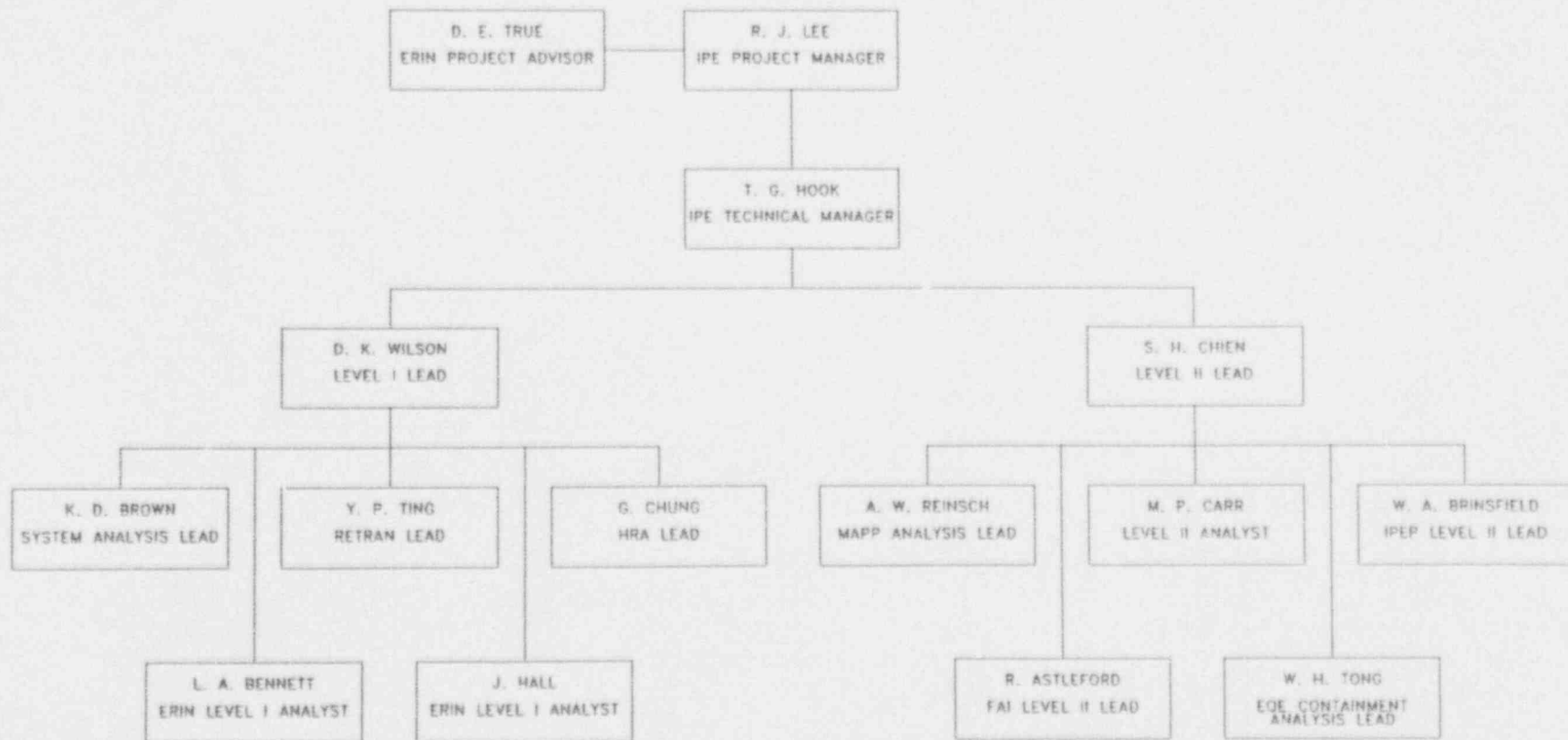
- **Nuclear Engineering Design Organization (NEDO)** - NEDO personnel provided engineering analyses (e.g. thermal hydraulic analysis, room heat-up calculations), documented reviews of the system analyses, fault trees, and the containment failure mode analysis, and overall review of the IPE submittal.
- **Nuclear Fuels Management** - Nuclear Fuels Management personnel performed source term ORIGEN analyses, reviewed all the RETRAN analysis used for determining system success criteria, and reviewed the submittal.
- **Station Engineering** - Station Technical personnel provided system operating experience data, assistance with system interviews and walkdowns, and overall review of the IPE submittal.
- **Licensing** - Licensing personnel provided scheduling assistance, guidance on the IPE requirements, interface with the NRC on IPE/PRA issues, and overall review of the IPE submittal.
- **Operations** - Operations personnel participated in control room simulator exercises with scenarios developed by the IPE team, reviewed all pre- and post-initiator human reliability calculations, and reviewed the IPE submittal.
- **Maintenance** - The maintenance organization provided input on equipment unavailability and maintenance test failure data.
- **Training** - Training personnel provided insights on the various aspects of operator actions including quality of the training, operational philosophy, and prioritization of the operator tasks. They also facilitated use of the control room simulator for the purpose of observing key operator actions in scenarios developed by the IPE team.

The general project organization is depicted on Figure 5-1.

5.2 Composition of Independent Review Team

In accordance with Generic Letter 88-20, SCE has conducted independent reviews of the SONGS 2/3 IPE to ensure the accuracy of the documentation and to validate both the IPE process and its results. These independent reviews were performed at various

FIGURE 5-1
SONGS 2/3 IPE PROJECT ORGANIZATION CHART



stages in the project by in-house personnel and external contractors, depending on the level of technical expertise required for the particular analysis. In general, most analyses were reviewed both in-house and externally. In addition all IPE Program procedures, analyses, and calculations were reviewed and documented in accordance with accepted departmental quality assurance procedures for "quality affecting" activities. While Generic Letter 88-20 did not require that the IPE be performed in accordance with the requirements of 10CFR50, Appendix B, SCE concluded that the application of "quality affecting" quality assurance requirements to the IPE Program was appropriate.

Each of the independent reviews including the composition of the review teams is discussed below:

- **An Independent Quality Assurance Audit** was conducted by the Assessment Engineering group early in the project to ensure adequate control of project activities and adherence to department procedures. All recommendations from the audit pertaining to the IPE submittal were implemented.
- **An Independent Review of the Human Reliability Analyses** was conducted by Dr. G. William Hannaman of Science Applications International Corporation (SAIC). The scope of Dr. Hannaman's review included the overall HRA program and methodology, all pre- and post-initiator operator action analyses and the simulator observations. The recommendations from the review were addressed and incorporated in the final results.
- **In-house SCE Review** was performed to ensure that the plant fault tree models and associated assumptions were consistent with the design and operation of the units. The system analysis reviews were performed by the associated system design engineers in the Nuclear Engineering and Design Organization (NEDO). The RETRAN based success criteria analyses affecting the fault tree model assumptions were independently reviewed by RETRAN experts in the Nuclear Fuel Group. The MAAP based success criteria analyses affecting the fault tree model assumptions were independently reviewed by another SCE PRA analyst. The comments resulting from the reviews were documented and incorporated to the satisfaction of the reviewer. Also, this submittal was reviewed by all applicable SCE Nuclear departments including NEDO, the Station Technical Organization, Nuclear Fuel, Operations, Maintenance, and Licensing.
- **Independent Consultant Reviews** were performed during the IPE project as various portions of the analysis were completed. The Level I consultant, ERIN Engineering, performed an

independent review of the Level II work. The Level II consultant, IPE Partnership, performed an independent review of the Level I work. Comments from the consultants were incorporated into the analyses as the project proceeded.

6.0 SAFETY FEATURES AND POTENTIAL PLANT IMPROVEMENTS

6.1 Safety Features

The SONGS 2/3 plant design has a number of features which were shown in the performance of the IPE to contribute to the achievement of a relatively low overall plant risk.

For transient events, there is very little interaction between the main and auxiliary feedwater systems from a support system standpoint. The main feedwater system is available for secondary heat removal after most transient events. Thus, main feedwater and auxiliary feedwater systems can be considered as essentially independent and redundant sources of coolant makeup for secondary heat removal.

Under LOCA conditions requiring recirculation from the containment sump, the Recirculation Actuation Signal (RAS) automatically realigns the suction of the HPSI pumps to the containment sump when the RWST reaches its low level setpoint. Furthermore, while procedures call for operator action to isolate the RWST after the realignment has been completed, no loss of function will result if this action is not taken due to system hydraulics. Therefore, successful transfer from injection to recirculation has very little dependency on human reliability.

Following loss of coolant accidents where sufficient time exists, the Containment Spray pumps can be used as a back-up means of low pressure RCS makeup in both the injection and recirculation modes of operation.

Containment heat removal and pressure control can be achieved through utilization of either the containment spray system or the containment emergency fan cooling units. In fact, containment pressure can be maintained well below actual containment capability with either of two spray pumps or with any of four emergency fan coolers, (i.e. any one of six components).

Reactor Coolant Pump (RCP) seals are normally cooled by the Component Cooling Water (CCW) system. The SONGS RCP seals can operate without CCW for approximately 30 minutes without failing while the RCPs are running. If the RCPs are tripped, the seals can maintain leakage within acceptable limits indefinitely without CCW cooling.

Following a station blackout, two of the four station batteries can be maintained operable for up to 8 hours for control of auxiliary feedwater if operator action is taken, per existing procedures, to shed unnecessary loads.

Following loss of offsite power where one of the two units is blacked-out but at least one emergency diesel generator starts and runs at the opposite unit, the capability exists to supply 4kv power from the operating diesel to the blacked-out unit.

The SONGS 2/3 containment provides for approximately 2.3 million cubic feet of free volume and has a pressure capacity of more than twice the design pressure. Its ability to remain intact for several tens of hours following core damage allows natural deposition mechanisms to remove airborne fission products from the containment atmosphere, and provides adequate time for additional accident mitigation activities to be implemented. The structural strength also allows the containment to withstand large hydrogen burns.

6.2 Potential Plant Improvements

During the performance of the IPE, it was determined that loss of normal room cooling to the ESF inverter/distribution rooms was not clearly annunciated. Preliminary scoping calculations indicated that loss of cooling to these rooms could be a significant contributor to the total core damage frequency (possibly tripling the final risk value) and that installation of high temperature annunciation would be cost effective. Subsequently, a plant modification was made which provides for control room annunciation of high ambient temperature in any of the inverter/distribution rooms. This annunciation enables the operators to respond by manually actuating the safety related room cooling system which does not start automatically without a Safety Injection Actuation Signal (SIAS).

Based on the final results of the Individual Plant Examination conducted for San Onofre Units 2 and 3 and the definition of vulnerability provided in Section 3.4.2, no further modifications to either hardware or procedures were indicated.

7.0 SUMMARY AND CONCLUSIONS

Front-End Results

The calculated total mean core damage frequency for SONGS 2/3 from the Level I analysis was calculated to be $3.0 \times 10^{-5}/\text{yr}$ or roughly 1 in 33,000 years. This is approximately a factor of three below the NRC's proposed safety goal of $1 \times 10^{-4}/\text{yr}$ or 1 in 10,000 years and compares favorably with the core damage frequency reported for other PWRs.

Back-End Results

Overall, the results of the Level II analysis show that should a core damage event occur at SONGS 2/3, there is an 84% probability of containment success. In other words, there is an 84% probability that the final barrier to fission product release will not be breached, impaired, or bypassed. This result is comparable with other PWRs.

Conclusion

In November 1988, the NRC issued the final Generic Letter 88-20, "Individual Plant Examination for Severe Accident Vulnerabilities," requesting each utility to perform a plant-specific, integrated analysis of plant and system response to a wide spectrum of internal, randomly initiated events such as reactor scrams, loss of off-site power, and loss of coolant accidents with an emphasis on quantification of plant core damage frequency and evaluation of containment performance. The objectives of this analysis as stated in the Generic Letter were for the utility:

- (1) to develop an appreciation of severe accident behavior,
- (2) to understand the most likely severe accident sequences that could occur at its plant,
- (3) to gain a more quantitative understanding of the overall probabilities of core damage and fission product releases, and
- (4) if necessary, to reduce the overall probabilities of core damage and fission product releases by modifying, where appropriate, hardware and procedures that would help prevent or mitigate severe accidents.

Compliance with the first three objectives was achieved in that the majority of the modeling, quantification, and prioritization of core damage and significant release sequences associated with the IPE were performed by SCE personnel.

Compliance with the fourth objective was achieved in that SCE aggressively sought to identify plant vulnerabilities to severe accidents. A single possible vulnerability associated with potentially inadequate room temperature annunciation was identified and promptly addressed via a plant modification. No further modifications to either hardware or procedures were indicated by the IPE analysis.

APPENDIX A

ADDITIONAL PLANT DRAWINGS

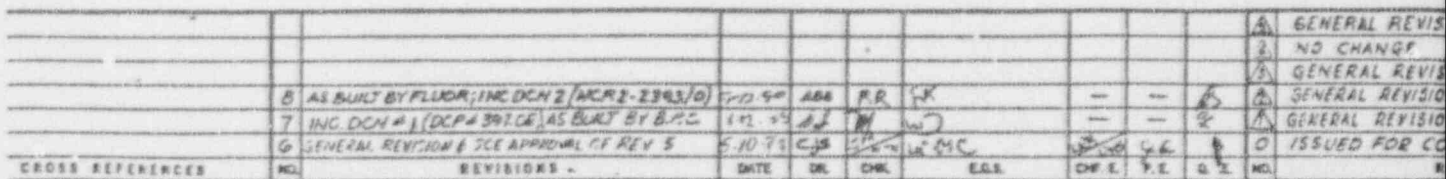


Figure A.1 Section of Containment, Auxiliary Feedwater Pump Building, and Auxiliary B

Also Available On
Aperture Card



9305040247-04

Also Available On
Aperture Card



UNIT 2 A. 2

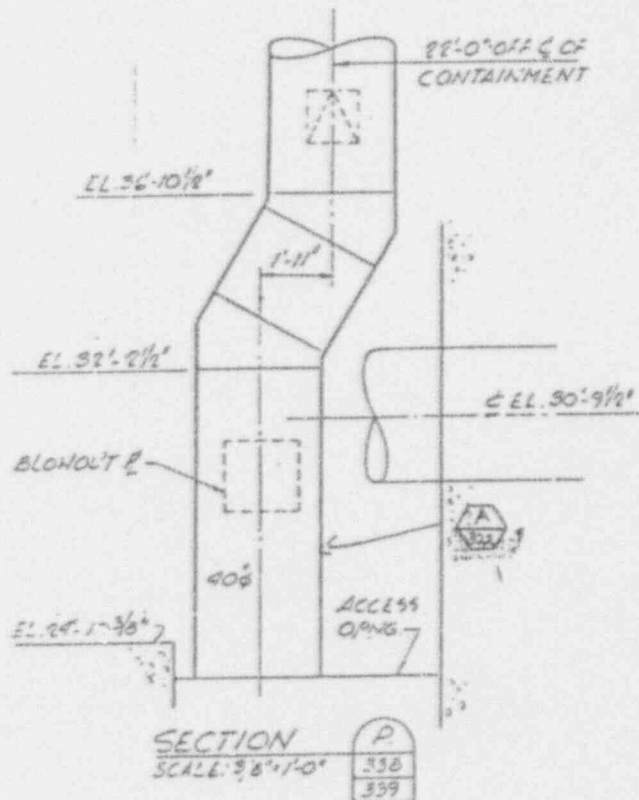
[illegible]

40005-8

rol Area).

A-3

9305040247-05

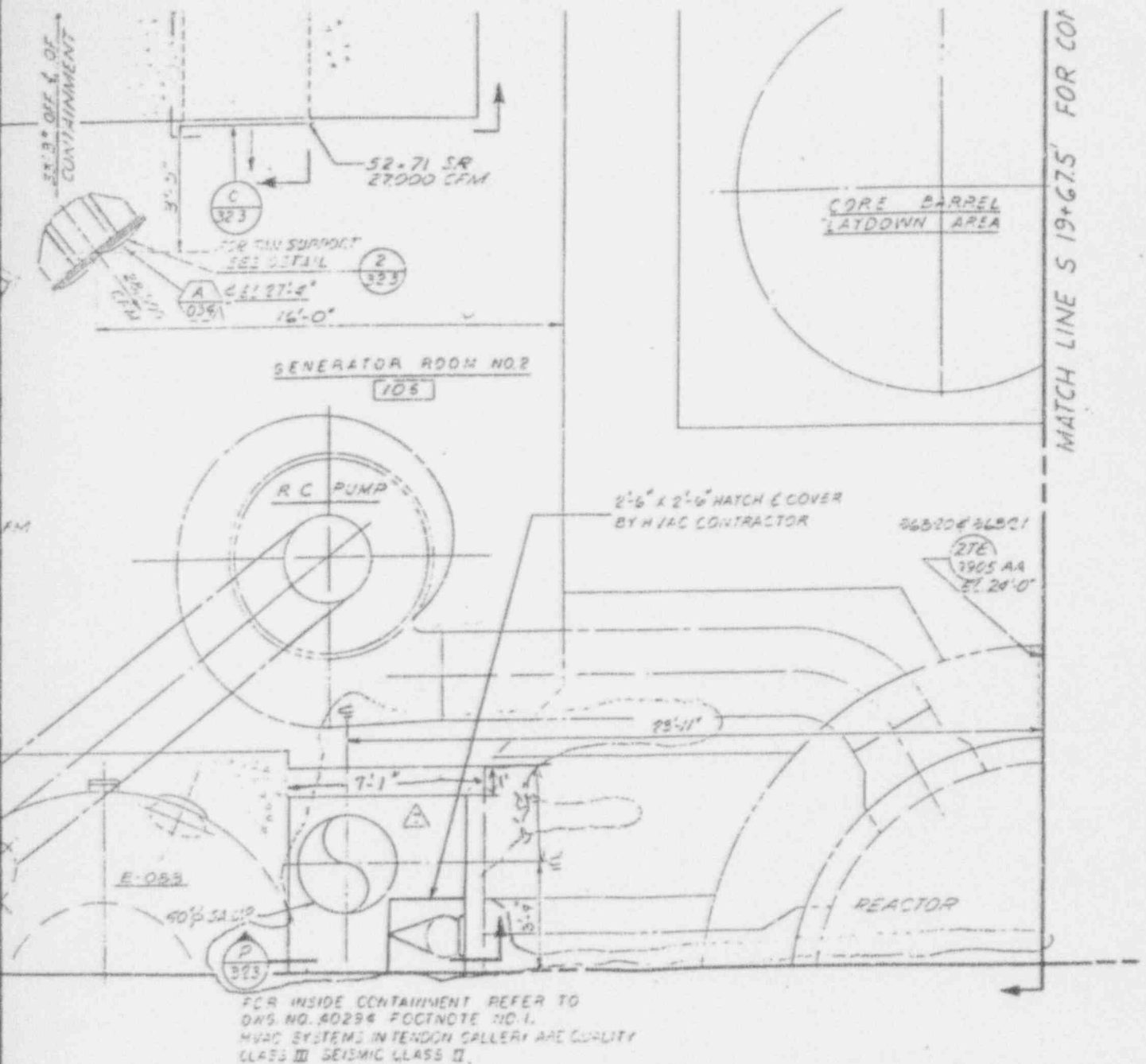


UNIT 2 QUALITY CLASS II									
5-11-78	GR	10-10-78	10-10-78	10-10-78	10-10-78	10-10-78	10-10-78	10-10-78	10-10-78
10-27-78	MC	10-27-78	10-27-78	10-27-78	10-27-78	10-27-78	10-27-78	10-27-78	10-27-78
1-7-77	AMR	1-7-77	1-7-77	1-7-77	1-7-77	1-7-77	1-7-77	1-7-77	1-7-77
1-23-76	JF	1-23-76	1-23-76	1-23-76	1-23-76	1-23-76	1-23-76	1-23-76	1-23-76
8-20-75	ME	8-20-75	8-20-75	8-20-75	8-20-75	8-20-75	8-20-75	8-20-75	8-20-75
DATE	DR	CHK	EGS	CHK	P.E.	QAE	I.D. NO.		
							SAN ONOFRE NUCLEAR GENERATING STATION		
							FILE		
							CONTAINMENT - HV & AC SECTION		
							SOUTHERN CALIFORNIA EDISON COMPANY		
							SCALE NOTED		
							LOS ANGELES, CALIF.		

40323 -8

Figure A.3

Reactor Cavity Ventilation Duct and



UNIT 2

QUALITY CLASS II

1/2\"/>

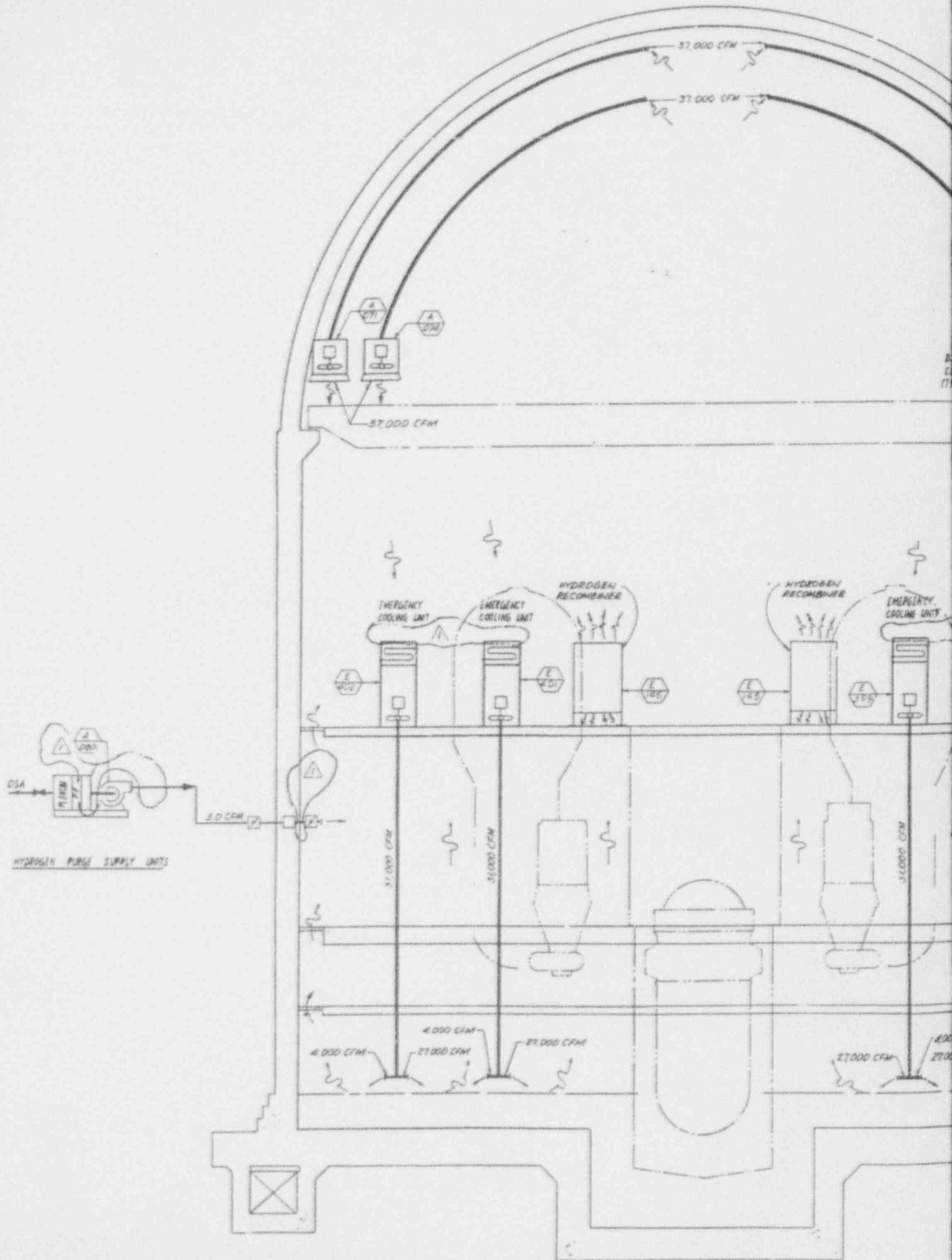
SI

APERTURE CARD

Also Available On
Aperture Card

A-4

9305040247-06



SI APERTURE CARD

Also Available On
Aperture Card

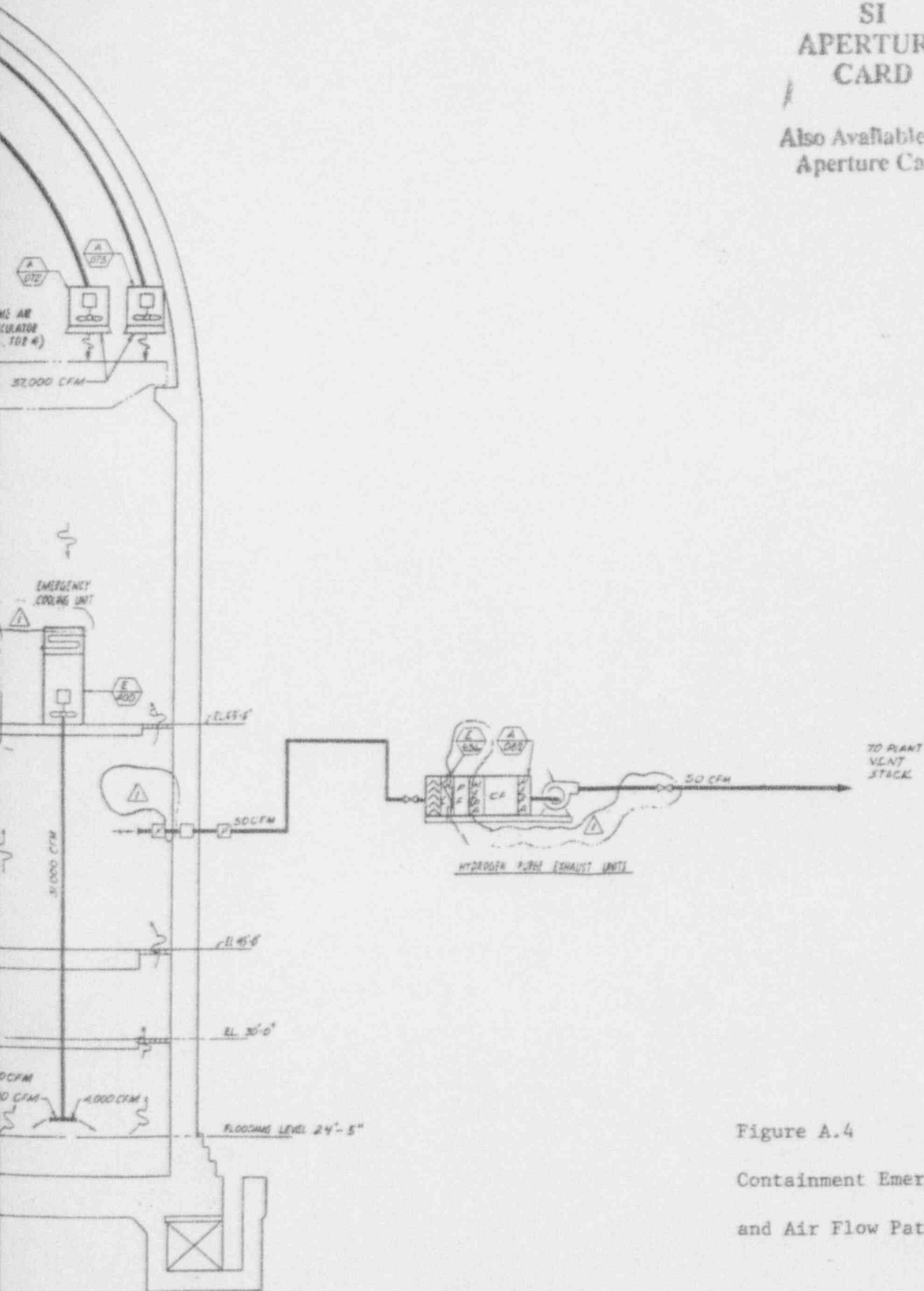


Figure A.4

Containment Emergency Fan Coolers
and Air Flow Path.

A-5
9305040247-07



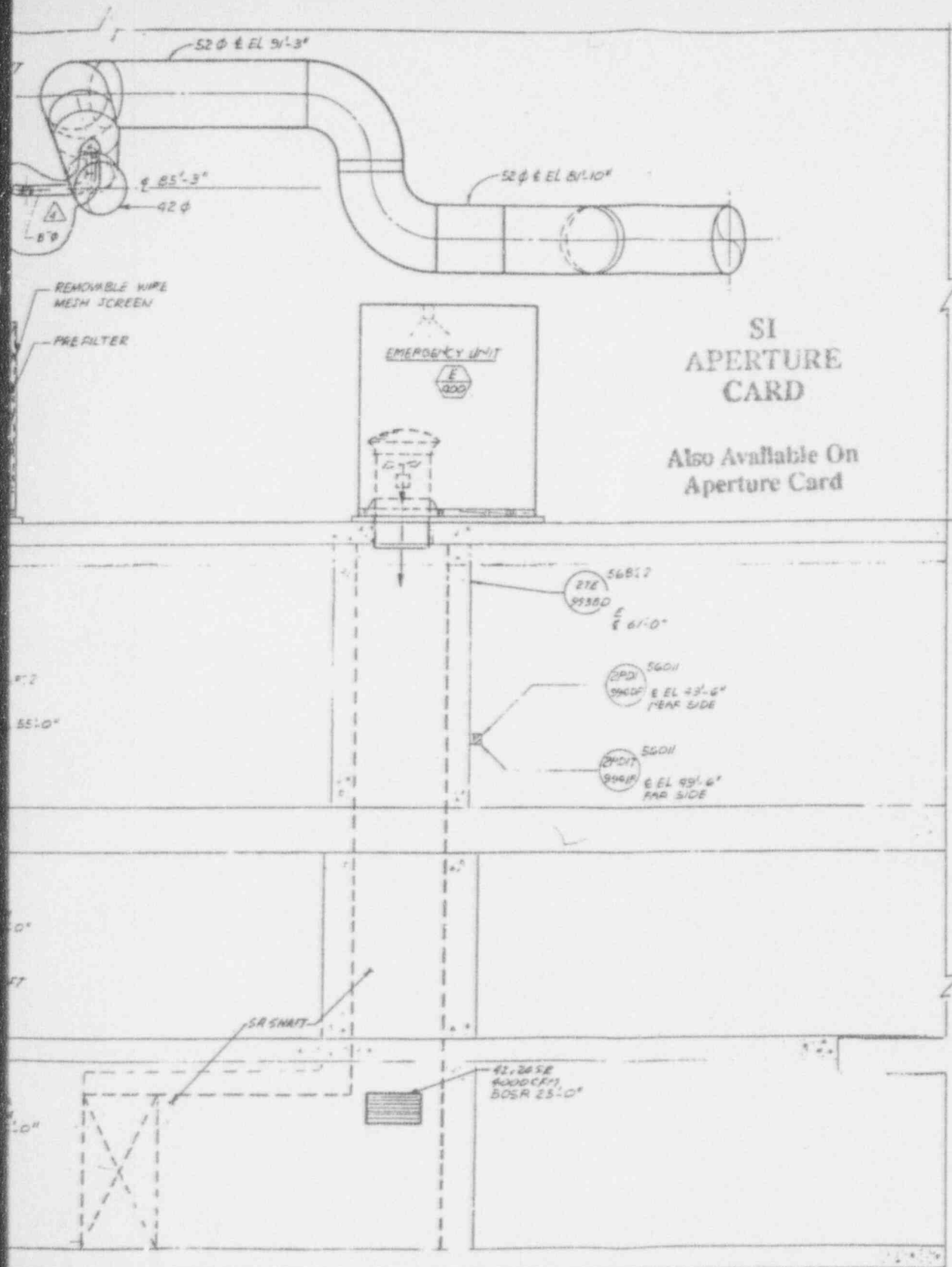
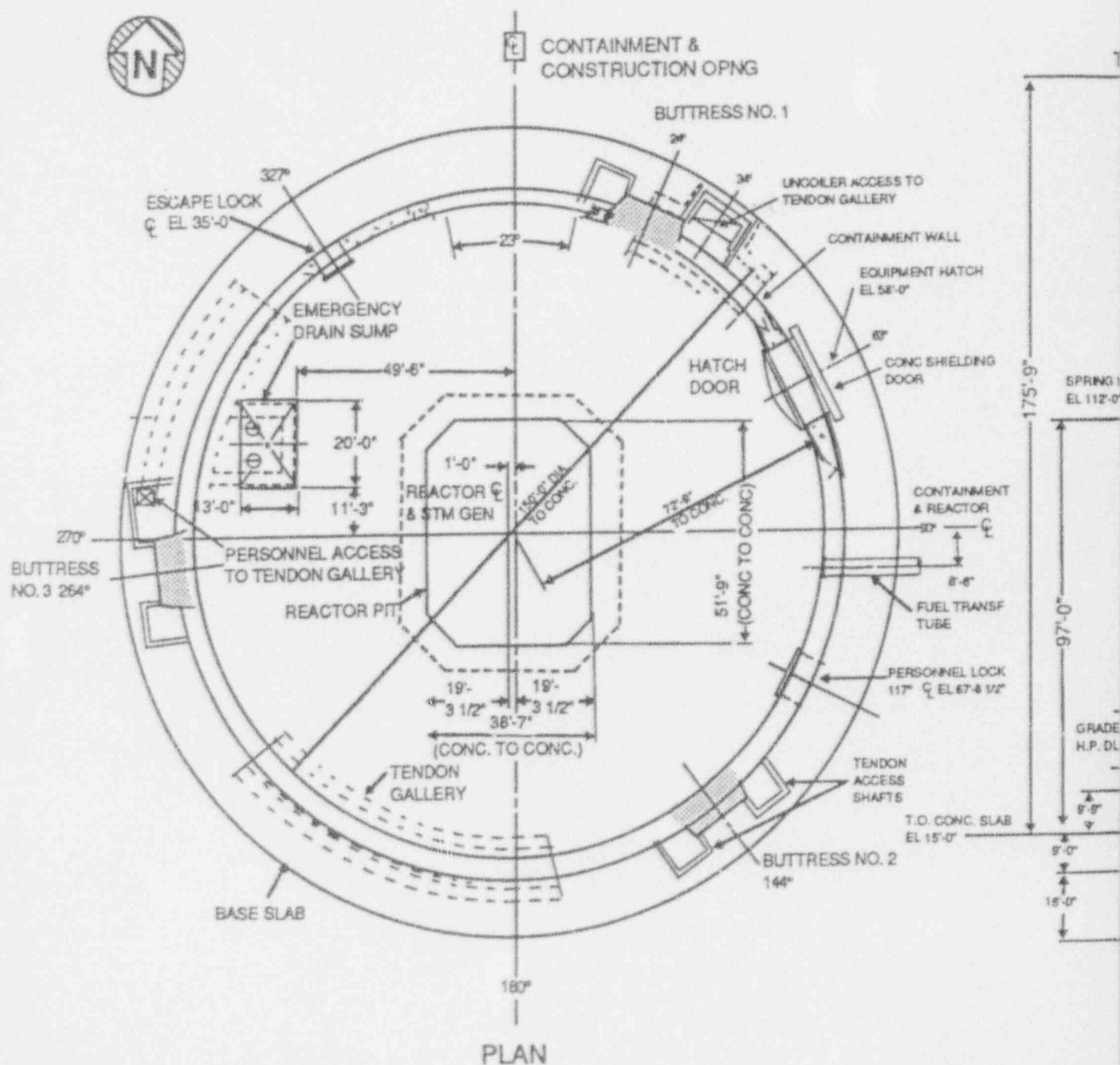


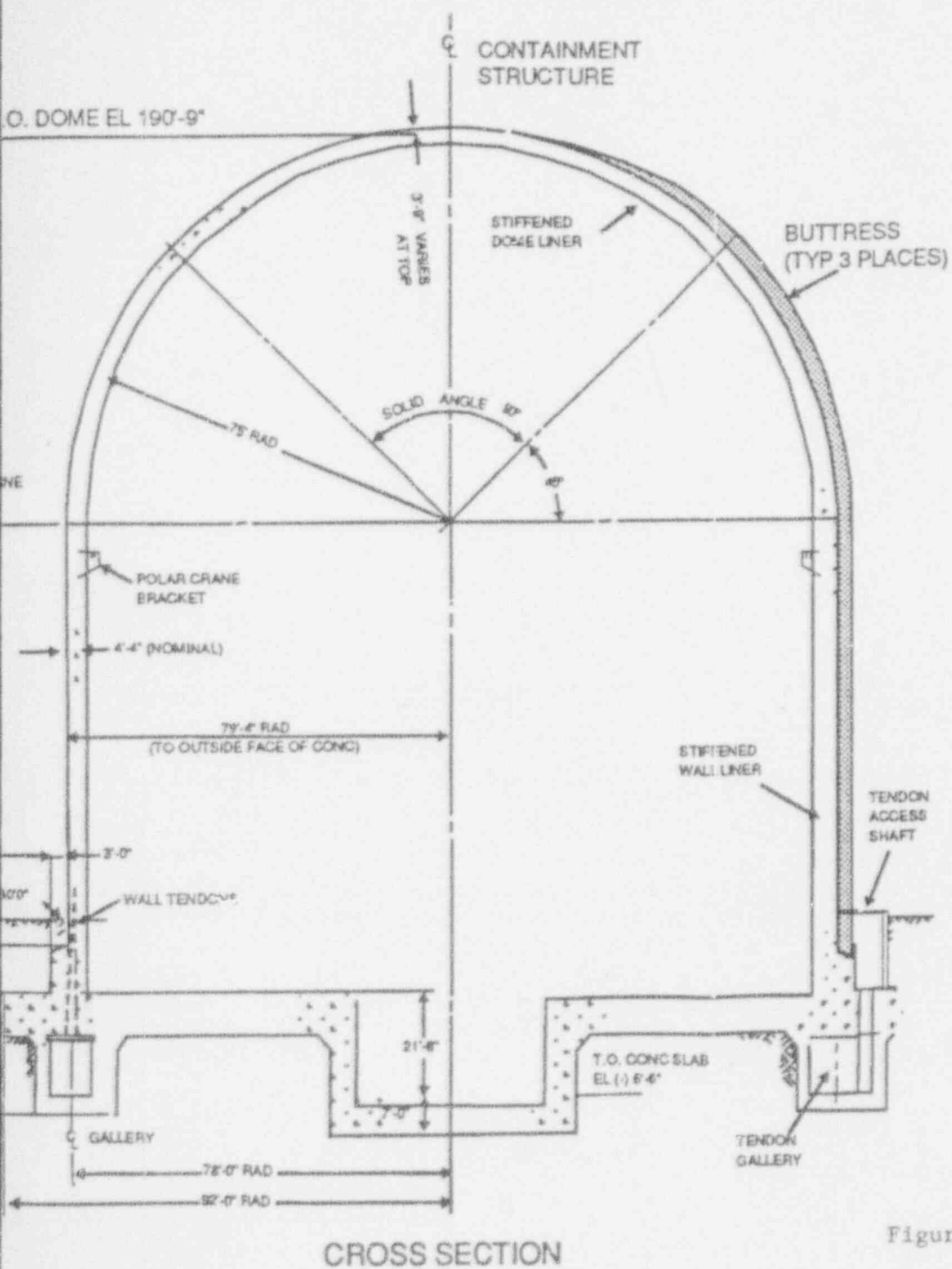
Figure A.5

Ventilation Air Duct of the
Emergency Fan Cooler.

9305040247-08



UNIT 2 - SHOWN
UNIT 3 - OPPOSITE HAND ABOUT 90° - 270° AXIS



SI
APERTURE
CARD

Also Available On
Aperture Card

Figure A.6

Containment Structure General
Arrangement.

9305040247-09