



Donald C. Shelton
Vice President - Nuclear
Davis-Besse

300 Madison Avenue
Toledo, OH 43652-0001
(419) 249-2300

Docket Number 50-346

License Number NPF-3

Serial Number 2119

February 26, 1993

United States Nuclear Regulatory Commission
Document Control Desk
Washington, D. C. 20555

Subject: Individual Plant Examination (IPE) for Severe Accident
Vulnerabilities for the Davis-Besse Nuclear Power Station,
Unit 1 (Response to NRC Generic Letter 88-20)

Gentlemen:

Nuclear Regulatory Commission Generic Letter (GL) 88-20, Individual Plant Examination for Severe Accident Vulnerabilities, dated November 23, 1988, and GL 88-20, Supplement 1, dated August 29, 1989, requested each utility to perform an Individual Plant Examination (IPE) to identify any severe accident vulnerabilities. In response to this request, by letter dated October 27, 1989 (Serial Number 1723), Toledo Edison (TE) committed to perform a Level 1 Probabilistic Risk Assessment (PRA) and a containment performance analysis for the Davis-Besse Nuclear Power Station (DBNPS). Toledo Edison has completed the IPE for the DBNPS. The purpose of this letter is to transmit the summary report for the DBNPS IPE.

The DBNPS IPE fulfills the NRC objectives for the IPE outlined in GL 88-20. The IPE was accomplished through the performance of a Level 2 PRA, using primarily TE personnel. This has resulted in TE obtaining the maximum benefit from the IPE, and development of in-house expertise for future use of the DBNPS IPE models. The models were developed and documented in a manner to accommodate possible future updating to reflect plant changes, emerging information on severe accident behavior, or to address safety and regulatory issues as they arise. In addition to extensive internal review by TE personnel, the DBNPS IPE process was reviewed by an independent consultant experienced in probabilistic risk assessment.

The results of the IPE provide a perspective on the types and frequencies of potential severe accident sequences that could be important for the DBNPS. Overall, the IPE identified no severe

9303030295 930226
PDR ADOCK 05000346
P PDR

Operating Companies:
Cleveland Electric Illuminating
Toledo Edison

ACH 1/1

accident vulnerabilities for the DBNPS. The IPE indicates that core damage frequency and containment performance for the DBNPS is comparable to that of other plants. Although no severe accident vulnerabilities or instances of unusually poor containment performance were identified, several potential enhancements based on the insights gained from the IPE are being considered for future implementation. These insights and potential enhancements are described in the summary report.

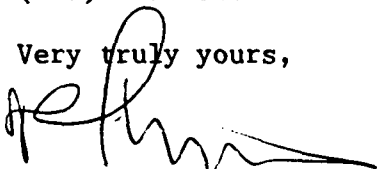
In addition to addressing Unresolved Safety Issue (USI) A-45, Shutdown Decay Heat Removal Requirements, as requested by GL 88-20, the IPE directly addresses other USI and Generic Safety Issues (GI) for the DBNPS. The USIs and GSIs addressed by the IPE include:

- USI A-17 Systems Interactions
- GI-23 Reactor Coolant Pump Seal Failures
- GI-105 Interfacing Systems Loss of Coolant Accidents in Pressurized Water Reactors
- GI-65 Probability of Core Melt due to Component Cooling Water System Failures
- GI-77 Flooding of Safety Equipment Compartments by Backflow Through Floor Drains
- GI-128 Electrical Power Reliability and Related Issues
- GI-143 Availability of Chilled Water Systems and Room Cooling
- GI-153 Loss of Essential Service Water in Light Water Reactors

Based on the results of the DBNPS IPE, TE considers these USIs and GSIs resolved.

If you have any questions regarding the information provided by this letter, please call Mr. R. W. Schrauder, Manager - Nuclear Licensing at (419) 249-2366.

Very truly yours,



PWS/dlc


Enclosures

cc: A. B. Davis, Regional Administrator, NRC Region III
J. B. Hopkins, NRC/NRR DB-1 Senior Project Manager
S. Stasek, NRC Region III, DB-1 Senior Resident Inspector
Utility Radiological Safety Board

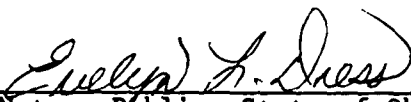
TRANSMITTAL OF SUMMARY REPORT
OF THE
INDIVIDUAL PLANT EXAMINATION
FOR SEVERE ACCIDENT VULNERABILITIES
FOR
DAVIS-BESSE NUCLEAR POWER STATION
UNIT NUMBER 1

IN RESPONSE TO GENERIC LETTER NUMBER 88-20

Toledo Edison's summary report of the Individual Plant Examination for the Davis-Besse Nuclear Power Station in response to Generic Letter Number 88-20 Individual Plant Examination for Severe Accident Vulnerabilities, is hereby submitted under letter Serial Number 2119.

By: 
D. C. Shelton,
Vice President Nuclear

Sworn and subscribed before me this 26th day of February, 1993.


Notary Public, State of Ohio
EVELYN L. DRESS
NOTARY PUBLIC, STATE OF OHIO
My Commission Expires July 26, 1994



DAVIS-BESSE NUCLEAR POWER STATION

INDIVIDUAL PLANT EXAMINATION



DAVIS-BESSE NUCLEAR POWER STATION

**INDIVIDUAL PLANT EXAMINATION
FOR THE
DAVIS-BESSE NUCLEAR POWER STATION**

submitted in response to

U.S. Nuclear Regulatory Commission Generic Letter 88-20

by

The Toledo Edison Company

February 1993

9303030304 930226
PDR ADDCK 05000346
P PDR

Summary Contents

<u>Section</u>	<u>Page</u>
Acronyms and Abbreviations	vii

Part 1: EXECUTIVE SUMMARY

1 BACKGROUND AND OBJECTIVES	1
2 PLANT FAMILIARIZATION.....	3
3 OVERALL METHODOLOGY	5
4 SUMMARY OF MAJOR FINDINGS	9
4.1 Findings from the Front-End Analysis.....	9
4.2 Findings from the Back-End Analysis	13
REFERENCES FOR PART 1	18

Part 2: EXAMINATION DESCRIPTION

1 INTRODUCTION.....	1
2 CONFORMANCE WITH THE GENERIC LETTER.....	3
3 GENERAL METHODOLOGY	9
3.1 Front-End Analysis.....	9
3.2 Back-End Analysis	14
3.3 Application of Results and Insights.....	18
4 INFORMATION ASSEMBLY.....	21
REFERENCES FOR PART 2	23

Summary Contents (continued)

<u>Section</u>		<u>Page</u>
	Part 3: FRONT-END ANALYSIS	
1	ACCIDENT SEQUENCE DELINEATION	1
1.1	Identification of Initiating Events	1
1.2	Definition of Core-Damage Sequences	30
1.3	Sequence Grouping in Back-End Analysis	114
2	SYSTEMS ANALYSIS	121
2.1	Overview of Systems Analysis	121
2.2	System Descriptions	132
3	SEQUENCE QUANTIFICATION	219
3.1	Data Analysis	219
3.2	Assessment of Human Interactions	241
3.3	Recovery Analysis	280
3.4	Quantification of Sequence Frequencies	285
4	RESULTS AND SCREENING PROCESS	291
4.1	Summary of Sequence Frequencies	291
4.2	Summary of Plant Vulnerabilities	307
4.3	Decay Heat Removal Evaluation	308
4.4	USI and GSI Resolution	310
	REFERENCES FOR PART 3	323

Summary Contents (continued)

<u>Section</u>	<u>Page</u>
Part 4: BACK-END ANALYSIS	
1	PLANT DATA AND PLANT DESCRIPTION 1
1.1	Site Location..... 1
1.2	Site Characteristics..... 1
1.3	Plant Description..... 1
1.4	Plant Systems..... 2
2	PLANT MODELS AND METHODS FOR PHYSICAL PROCESSES 55
2.1	Severe-Accident Response Using MAAP 55
2.2	Investigation of Specific Issues..... 66
3	BINS AND PLANT-DAMAGE STATES 77
3.1	Attributes of Plant-Damage States..... 77
3.2	Definition of Core-Damage Bins..... 81
3.3	Bridge Trees 84
3.4	Summary of Plant-Damage States 97
4	CONTAINMENT FAILURE CHARACTERIZATION..... 109
4.1	Capacity of the Containment Vessel 109
4.2	Other Potential Failure Mechanisms 111
4.3	Overall Containment Failure Characterization..... 117
5	CONTAINMENT EVENT TREE 119
5.1	Development of the Containment Event Tree 119
5.2	Top Events in the CET..... 126
6	ACCIDENT PROGRESSION AND QUANTIFICATION FOR THE CONTAINMENT EVENT TREE 199
6.1	Containment Response for Representative Accidents..... 199
6.2	Quantification of the CET 224
6.3	Frequencies for CET Outcomes..... 227
7	RADIONUCLIDE RELEASE CHARACTERIZATION 243
7.1	Estimation of Release Fractions..... 243
7.2	Definition of Release Categories..... 245
7.3	Estimated Release Frequencies 253
	REFERENCES FOR PART 4 261

Summary Contents (continued)

<u>Section</u>	<u>Page</u>
Part 5: IPE PERFORMANCE AND IMPLEMENTATION	
1 IPE PROGRAM ORGANIZATION.....	1
2 REVIEW ACTIVITIES	3
REFERENCES FOR PART 5.....	5
Part 6: PLANT IMPROVEMENTS AND UNIQUE SAFETY FEATURES	
1 UNIQUE SAFETY FEATURES.....	1
2 CONSIDERATION OF VULNERABILITIES.....	5
3 OTHER POTENTIAL PLANT IMPROVEMENTS.....	9
3.1 Insights Gained from the Front-End Analysis.....	9
3.2 Insights Gained from the Back-End Analysis	10
REFERENCES FOR PART 6.....	12
Part 7: SUMMARY AND CONCLUSIONS	
1 SUMMARY OF RESULTS FROM THE IPE	1
1.1 Results from the Front-End Analysis	1
1.2 Results from the Back-End Analysis.....	5
2 CONCLUSIONS.....	11

Acronyms and Abbreviations

ac	alternating current
AFP	auxiliary feedwater pump
AFW	auxiliary feedwater
ARTS	anticipatory reactor trip system
AVV	atmospheric vent valve
B&W	Babcock & Wilcox
BWST	borated water storage tank
CAC	containment air cooler
CBI	Chicago Bridge and Iron Company
CBO	controlled bleed-off orifice
CCW	component cooling water
CDF	cumulative distribution function
CET	containment event tree
COV	coefficient of variation
CPIP	Containment Performance Improvement Program
CRD	control rod drive
CS	containment spray
CST	condensate storage tank
dc	direct current
DSS	diverse scram system
DHR	decay heat removal
ECCS	emergency core cooling system
EDG	emergency diesel generator
EF	error factor
EFW	emergency feedwater
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ESF	engineered safety feature
ESW	essential service water
FMEA	failure modes and effects analysis
HPI	high pressure injection
HPR	high pressure recirculation
HVAC	heating, ventilating and air conditioning
IA	instrument air

Acronyms and Abbreviations (continued)

ICS	integrated control system
IDCOR	Industry Degraded Core (Program)
IGLD	International Great Lakes Datum
IM	integrated master
IPE	Individual Plant Examination
IREP	Interim Reliability Evaluation Program
ISLOCA	interfacing systems loss-of-coolant accident
kv(ac)	kilovolts (alternating current)
LCO	limiting condition for operation
LER	licensee event report
LPI	low pressure injection
LPR	low pressure recirculation
LOCA	loss-of-coolant accident
MCC	motor control center
MDFP	motor-driven feed pump
MFW	main feedwater
MSIV	main steam isolation valve
MSSV	main steam safety valve
MTC	moderator temperature coefficient
MWe	megawatts-electric
MWt	megawatts-thermal
MWO	maintenance work order
NCD	no core damage
NNI	non-nuclear instrumentation
NPE	Nuclear Power Experience
NPSH	net positive suction head
NRC	Nuclear Regulatory Commission
OTSG	once-through steam generator
PCS	power conversion system
PDS	plant-damage state
PORV	pilot-operated relief valve
PRA	probabilistic risk assessment
PSV	pressurizer safety/relief valve
PWR	pressurized water reactor

Acronyms and Abbreviations (continued)

RCP	reactor coolant pump
RCS	reactor coolant system
RPS	reactor protection system
SAC	station air compressor
SAIC	Science Applications International Corporation
SAROS	Safety and Reliability Optimization Services
SBODG	station blackout diesel generator
SERG	Steam Explosion Review Group
SFAS	safety features actuation system
SFRCS	steam and feedwater rupture control system
SGTR	steam generator tube rupture
SRO	senior reactor operator
SSC	system, structure, and component
STA	shift technical advisor
TAP	Transient Assessment Program
TBV	turbine bypass valve
THERP	Technique for Human Error Rate Prediction
TPCW	turbine plant cooling water
TSC	Technical Support Center
ULD	unit load demand
USAR	Updated Safety Analysis Report
vac	volts-alternating current
vdc	volts-direct current

Part 1
EXECUTIVE SUMMARY

Contents

<u>Section</u>	<u>Page</u>
1 BACKGROUND AND OBJECTIVES	1
2 PLANT FAMILIARIZATION.....	3
3 OVERALL METHODOLOGY	5
4 SUMMARY OF MAJOR FINDINGS	9
4.1 Findings from the Front-End Analysis.....	9
4.2 Findings from the Back-End Analysis	13
REFERENCES FOR PART 1	18

List of Illustrations

<u>Figure</u>	<u>Page</u>
4-1 Breakdown of Core-Damage Frequency by Category of Initiating Event	10
4-2 Conditional Probabilities of Containment Outcomes Given Core Damage.....	15

Section 1 BACKGROUND AND OBJECTIVES

This report describes the results of the individual plant examination (IPE) for the Davis-Besse Nuclear Power Station, performed in response to the request presented in Generic Letter 88-20 (Ref. 1). The Davis-Besse IPE was accomplished through the performance of a probabilistic risk assessment (PRA). The Toledo Edison Company chose PRA as the means to satisfy the IPE because of its utility in identifying potential severe accident vulnerabilities, while it could also provide meaningful insights into plant design and operations useful to decision-making beyond the scope and period of the IPE process. As defined by the PRA Procedures Guide (Ref. 2), this PRA constitutes a level 2 study (i.e., it includes both consideration of the sequences of events that could lead to core damage and the possible responses of containment to those sequences). This section and the remainder of Part 1 provide an overview of the PRA, including an overall summary of the methods used and a discussion of the major findings.

Toledo Edison originally performed limited PRA-related analyses in the early 1980's to investigate various aspects of plant safety. Following the loss-of-feedwater event of June 9, 1985, more extensive probabilistic assessments of the reliability of the auxiliary feedwater system were undertaken to help ensure that long-term responses to that event would be effective.

Recognition of the growing role of PRA in safety analysis and regulatory interactions led to the initiation, in late 1986, of a level 1 PRA for Davis-Besse. The primary objective of that PRA was to begin to develop in-house capabilities to develop, maintain, and use PRA to address safety and regulatory issues. Completed in draft form in the fall of 1988, the original PRA considered a broad range of internal initiating events, with more limited assessment of internal flooding and fires (Ref. 3). Because the plant was undergoing significant changes at the time the draft was completed, the iteration and extensive review of the results that usually characterize the latter stages of a PRA were not performed.

Many changes to plant systems and procedures, largely as a result of the concerted response to the 1985 loss-of-feedwater event, continued to be made through the late 1980's. In addition, Generic Letter 88-20 (Ref. 1) was issued at about the time that the draft PRA was completed. Therefore, a new effort was initiated to develop a PRA that would both account for changes made since the baseline date for the draft study and satisfy specific items requested in the generic letter. Thus, although the PRA performed for the IPE drew from the draft level 1 effort, it represents essentially a complete re-examination of the plant. In addition to satisfying the NRC's request for an IPE, the technical objectives of the PRA included the following:

- To apply state-of-the-art PRA techniques to develop a more current understanding of the types of severe accidents that could be important for Davis-Besse,

- To identify any areas in which there might be the need or opportunity to reduce the frequency of core damage or of serious radiological releases in a cost-effective manner, and
- To provide the plant-specific inputs for an accident-management program.

Several additional objectives that affected the manner in which the PRA was structured and implemented to meet these overall objectives were identified. These additional objectives included the following:

- To develop a model for Davis-Besse that could be readily updated in the future, as changes are made to the plant or as additional insights into severe accident behavior become available, so that the model and results could be applied to address safety and regulatory issues as they arise;
- To continue to develop the expertise within the Toledo Edison Company necessary to perform the analyses for the IPE and to maintain and use them in these future applications; and
- To document the analyses in a manner that would both make the future applications tractable and provide the necessary bases for external reviewers to determine that the work had been accomplished in a thorough and competent manner.

To ensure that the models and results could be applied most effectively beyond the period of the IPE, most of the technical work was performed by Toledo Edison engineers. Through review processes and other interactions with various groups at Davis-Besse, the PRA models and data bases were developed in a matter that was as realistic and plant-specific as was practicable. Those interactions further enhance the usefulness of the IPE to address issues related to safety and reliability as they arise at Davis-Besse.

Section 2 PLANT FAMILIARIZATION

Davis-Besse is located on the southwestern shoreline of Lake Erie in Ottawa County, Ohio, approximately six miles northeast of the town of Oak Harbor. The site consists of 954 acres, of which approximately 600 acres is marshland leased to the U.S. Government as a national wildlife reserve. The topography is flat with marsh areas bordering the lake and the upland area rising to only 10 to 15 feet above the lake low water datum level. Areas surrounding the station structures have been built up 6 to 14 feet to an elevation of 584 feet above sea level to provide for flood protection. The station structures are located approximately in the center of the site and are built on a bedrock foundation.

Davis-Besse is a 906 MWe pressurized water reactor (PWR). The nuclear steam supply system was furnished by The Babcock & Wilcox Company. The Bechtel Corporation and its affiliate, The Bechtel Company, provided the architect-engineering services for the station design and construction management services for the construction. The construction permit was granted in March 1971, and the operating license was issued by the NRC in April 1977. Following initial fuel loading and testing, commercial operation began in July 1978.

The reactor containment consists of two structures: a steel containment vessel and a reinforced concrete shield building. The containment vessel is a large, dry, free-standing cylindrical steel pressure vessel with a hemispherical dome and ellipsoidal bottom. It is completely enclosed by the concrete shield building, and there is an annular space between the two. With the exception of the concrete under the containment vessel, there are no structural ties between the containment vessel and the shield building above the foundation, allowing virtually unlimited freedom for differential movement between the two. An emergency ventilation system maintains a negative pressure on this annulus during accident conditions and exhausts through a high efficiency filter network to prevent unfiltered leakage of contaminated air to the environment. The design maximum internal pressure for the steel vessel is 40 psig at a coincident temperature of 264 F.

The containment houses the reactor coolant system, which consists of the reactor vessel, two vertical once-through steam generators (OTSGs), four shaft-sealed reactor coolant circulating pumps, an electrically heated pressurizer, and interconnecting piping. The system is arranged into two transport loops, each containing two circulating pumps and one steam generator. The vertical OTSGs are raised above the core vessel nozzles to promote natural circulation and to provide an inventory of water to help cover the fuel during a loss-of-coolant accident (LOCA). The reactor coolant system is designed to contain and circulate reactor coolant at pressures and flows necessary to transfer the heat generated in the core to the secondary fluid in the steam generators. In addition to serving as a heat transport medium, the coolant also serves as a neutron moderator and reflector and as a solvent for the soluble boron used for chemical shim reactivity control. The secondary fluid is completely separate from the reactor coolant and is used to transfer energy from the steam generators to the main turbine generator and auxiliary loads.

Heat transfer from the primary coolant, via the steam generators, to the feedwater systems is the preferred means of decay heat removal following a reactor trip. This can be accomplished by either the main feedwater system or the auxiliary feedwater system. In the event the main feedwater system is unavailable, the turbine-driven auxiliary feedwater pumps are automatically initiated by the steam and feedwater rupture control system. As an additional backup, control room operators have the capability to start a motor-driven feed pump to supply feedwater in the event both the main and turbine-driven auxiliary feedwater pumps are not available. In addition, makeup/high pressure injection (HPI) cooling is available as yet another means of cooling the core if the steam generators are unavailable. The decay heat removal pumps provide normal cooldown of the primary at lower pressures and temperatures by transferring heat from the primary to the component cooling water system. The decay heat removal system can also provide low pressure injection from the borated water storage tank during a large LOCA. Heat transferred to the component cooling water system is then transferred to the service water system, and then to the ultimate heat sink (Lake Erie). Two-train independence for each of these systems prevents a single failure from disrupting functional operation.

Engineered safety features are provided to protect the fuel cladding, ensure containment vessel integrity, and reduce the driving force for containment leakage. Emergency injection of coolant to the reactor coolant system satisfies the first function, and cooling of the containment vessel atmosphere satisfies the latter two functions. The emergency core cooling system includes the core flood tanks, high pressure coolant injection and low pressure coolant injection. Containment spray and containment air coolers are responsible for removing heat and reducing pressure within containment during an accident. Each of these systems consists of two independent trains that are controlled automatically by the safety features actuation system (SFAS). SFAS continuously evaluates key parameters, and would sequentially initiate and coordinate appropriate equipment if a LOCA were to occur.

Plant equipment is normally supplied ac power from an auxiliary transformer connected to the plant's main generator. Two start-up transformers, supplied from different 345kv switchyard sections, serve as the reserve power source for the station auxiliaries in the event power from the main generator is not available. If the normal and reserve power supplies were both unavailable, two redundant emergency diesel generators are provided as onsite standby power sources. Each emergency diesel generator is connected to an essential 4kv bus and is capable of supplying all essential loads for one train. A third standby source, the station blackout diesel generator, would be available to supply power in the event the normal, reserve, and emergency power supplies failed. The station blackout generator can be manually started from the control room or at a local control station, and it has its own auxiliaries to provide independence from the normal plant systems.

Section 3 OVERALL METHODOLOGY

The PRA conducted to satisfy the IPE was comprised of two major areas of analysis: (1) the identification of sequences of events that could lead to core damage and the estimation of their frequencies of occurrence (the front-end analysis); and (2) the evaluation of the potential response of containment to these sequences, with emphasis on the possible modes of containment failure and the corresponding source terms (the back-end analysis). In addition to these analysis areas, a significant portion of the effort entailed consideration of the insights gained both from the analysis process itself and from the results that were obtained. The results and insights were important inputs to the process of considering possible changes to reduce risk to the plant further, and in some cases aided in the disposition of generic issues as they apply to Davis-Besse.

The overall methodology for the front-end analysis can be characterized as the "linked fault-tree" approach. Using this approach, a set of event trees and fault trees was developed that represent an integrated model of plant response and possible core-damage accidents.

The first step in defining the core-damage sequences was the definition of initiating events. This was accomplished through a variety of means to ensure that the list that was developed was as complete as possible. Initiating events were identified through a search of experience at other PWRs, a review of previous PRAs for other plants, consideration of design-basis accidents, examination of the operating experience, and careful review of the individual systems at Davis-Besse.

An event tree was developed for each category of initiating event. This was done by first defining the safety functions that must be achieved to prevent core damage. These safety functions were then related to plant systems that must function to accomplish them. The minimum criteria for success of each of these systems were determined from available information, supplemented with specific calculations when necessary. Event trees were then constructed to delineate the core-damage sequences. The top events for these event trees were usually represented in terms of the safety functions. The failure to accomplish each of these safety functions was developed through fault-tree logic at a high level to denote the corresponding system-level failures, and to represent the functional interrelationships among the systems.

The failure modes for plant systems were further developed through the construction of fault trees. The fault trees were developed to the level necessary to account for important failure modes, to assure proper treatment of both intra- and inter-system dependencies, and to be consistent with the availability of reliability data. The fault trees for the front-line systems (i.e., those reflected in the logic for the event trees) were constructed based on the minimum success criteria defined by the sequence logic.

The fault trees included explicit development for inter-tied front-line systems and for dependencies on support systems (e.g., electric power, service water, etc.). This ensured that

such dependencies were tracked through the modeling and quantification process in a direct manner. Development of the fault trees was also integrated with the assessment of human reliability, both to ensure that important interactions were included in the fault trees, and to supply the information needed to make a meaningful estimate of the probabilities for the interactions. Because of the redundancy in most of the systems and safety functions considered, an extensive effort was made to identify groups of components that could be subject to common-cause failure.

The reliability data base encompasses the frequencies of the initiating events, independent and common-cause failure rates for components, and estimates of unavailabilities due to test and maintenance activities. In each of these areas, both industry-wide and plant-specific information was used to develop the most appropriate estimates.

The human reliability assessment was conducted in a manner that emphasized making it an integral part of the process of developing and quantifying the models that define accident sequences and system failures. The identification and assessment of human actions also relied heavily upon interactions with current and former reactor operators at Davis-Besse to ensure that the roles and priorities of the members of the operating crew were properly represented. Quantification of the probabilities for the human interactions was accomplished using current methods. Where possible, the assessment of human interactions was supplemented with observations of exercises on the plant simulator.

The core-damage sequences were defined by the success or failure of top events in the event trees. These top events were, in turn, related to system-level failures and human interactions through fault-tree logic. To estimate the sequence frequencies, a master fault tree comprised of the relevant top events from the event tree was formed for each sequence. This permitted Boolean reduction of an integrated set of sequence and system models so that the core-damage sequences were defined in terms of combinations of specific initiating events, component faults, and human interactions (minimal cut sets).

After the sequence-level minimal cut sets were obtained, they were reviewed carefully to assure that the integration of separate models produced appropriate representations of the sequences. The information conveyed by the cut sets also permitted characterization of the post-initiator human interactions and of any relevant recovery actions in an appropriate context.

The integrative nature of the modeling and quantification process permitted explicit treatment of dependencies within and among systems. It also allowed consideration of potential human interactions and recovery actions in a sequence-specific context. As a result, insights into important aspects of the plant design and operating practices were gained both during the modeling process and as a consequence of review of the quantitative results.

The primary objective of the back-end analysis was to identify any plant features that implied a potential weakness with respect to the possibility of serious releases from containment following a core-damage accident. This was done through the systematic investigation of a broad range of potential types of accidents. The back-end analysis included

both extensive deterministic evaluations of expected containment response and a probabilistic evaluation of the range of responses that could be relevant for each type of accident. The deterministic evaluations were primarily made using the Modular Accident Analysis Program (MAAP). For the probabilistic assessment, a containment event tree was constructed and quantified.

An important element of the IPE was the careful coordination of the front-end and back-end analyses. This was done to ensure that the core-damage sequences were developed to the level of detail necessary for meaningful assessment of containment response, with a minimum of iteration between the two major analysis areas.

To characterize the containment response to a core-damage accident, the MAAP computer code, version 3.0B, was selected as the primary analytical tool (Ref. 4). In addition to the analyses made using MAAP, specific issues were investigated through reviews of technical literature and other calculations. Models of the RCS, the emergency core cooling system, and the containment were developed based on information derived from drawings of major components, plant drawings, walkdowns, system descriptions, etc., so that the models were entirely plant-specific. The MAAP calculations simulated the response of the RCS during the core degradation process, provided the pressure and temperature profiles in containment during the accidents, and tracked the locations and conditions of fission products.

For most types of accidents, however, the response of the containment cannot be predicted with certainty. A containment event tree was therefore constructed to provide a framework for investigating a range of possible outcomes given core damage. The top events in the containment event tree represent general types of containment failure modes and conditions that would affect the magnitude of release from containment. In a manner analogous to the event trees for the front-end analysis, each of the top events was developed further through fault-tree logic into the various combinations of phenomena, system operations, and human interactions. Thus, an integral model of potential containment responses was assembled. The containment event tree was quantified using a variety of sources of information, including the results from the MAAP calculations, sensitivity studies, review of other technical literature, and engineering judgment.

A characterization of the releases associated with each type of accident was also developed. This information provided further indication of the level of severity of the accidents, and would be necessary in the event that offsite consequences were to be calculated. The release magnitudes and other measures of interest were derived primarily from the results from MAAP, with some adjustments made to address types of accidents or phenomena that were not explicitly considered in the MAAP calculations.

The primary purpose of the PRA was to gain further insights into the features that are important with respect to the potential for severe accidents at Davis-Besse. These insights were gained during both the modeling process and the review of the results for the front-end and back-end analyses. As noted in the preceding sections, the quantitative results were

supplemented by sensitivity studies that aided in understanding the important risk contributors and helped to identify plant changes that might be most effective.

Based on this examination, it was concluded that there are no apparent vulnerabilities to severe accidents for Davis-Besse, and that no changes to reduce the frequency of core damage or of serious releases are critical to continued safe operation. Other changes that might be desirable from the standpoint of further reducing risk were identified and are being evaluated to ensure that the potential effects on plant operations and safety are fully understood. The results and insights were also used to address other issues, including the issue of the adequacy of provisions for decay heat removal.

Section 4 SUMMARY OF MAJOR FINDINGS

This section provides a summary of the results and insights gained during the performance of the IPE. The most important finding with respect to this submittal was that there do not appear to be any vulnerabilities to severe accidents for Davis-Besse. Although there is no widely accepted definition of a condition that would constitute a vulnerability, the following functional definition has been used for Davis-Besse:

- Any feature of the plant design or operating practice that leads to an unacceptably high frequency of one or more core-damage sequences or that implies an unusually large conditional probability for a serious release from containment given core damage; or
- Any single feature that contributes a large fraction of the frequency of core damage or of serious release, even if the overall frequencies are judged to be generally acceptable.

Neither of these conditions was found to be the present for Davis-Besse. As described in the following sections, neither the core-damage frequency nor the frequency of serious releases is high relative to risk estimates generally obtained for other plants. Although a small number of sequences dominates the frequency of core damage, these sequences are comprised of many different contributors, none of which is disproportionately large.

The plant features that were found to be among those that contributed most to the results, as well as those that tended to limit the frequencies of certain accidents, are summarized below. Further details regarding these findings can be found in Section 4 of Part 3 (relative to the assessment of core-damage sequences) and in Sections 6 and 7 of Part 4 (with respect to the containment response to severe accidents).

4.1 FINDINGS FROM THE FRONT-END ANALYSIS

The process of developing an integrated model of the sequences of events that could lead to core damage produced further insights into important features of the design and the operating practices at Davis-Besse. It should be noted, however, that Davis-Besse had undergone a rigorous and systematic examination before the PRA effort began, largely in response to the event of June 9, 1985 involving a total loss of feedwater. To some extent, therefore, the insights that might have been generated during the IPE had already been identified, and substantial changes have been made to the plant, to procedures, and to maintenance practices.

The total core-damage frequency was estimated to be 6.6×10^{-5} per year. As shown in Figure 4-1, most of this frequency was assessed to be due to sequences initiated by transients, with the remainder divided among loss-of-coolant accidents (LOCAs), steam generator tube ruptures (SGTRs), and internal floods.

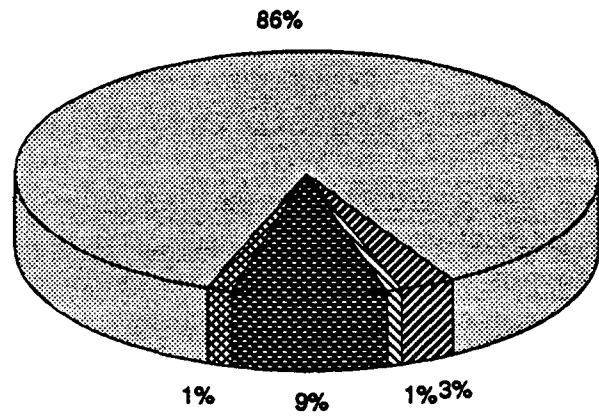
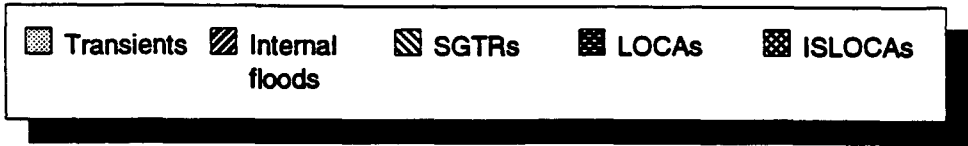


Figure 4-1. Breakdown of Core-Damage Frequency by Category of Initiating Event

The frequency of core damage resulting from transients was determined to be due largely to two types of functional sequences. The first sequence involves loss of heat removal via the steam generators and failure of direct core cooling by injection from the makeup system, with decay heat removed through the pressurizer relief valves (referred to as makeup/HPI cooling). This functional sequence would entail a loss of main feedwater, either as an initiating event or as a consequence of another initiating event. All three of the pumps in the auxiliary feedwater system (two turbine-driven and one motor-driven) would have to be unavailable to supply backup flow to the steam generators. Finally, makeup/HPI cooling, which can be accomplished by various redundant pathways, would have to fail.

Many different types of minimal cut sets contribute to this functional sequence, and no single or small number of plant features stands out. Many of the cut sets, however, share one of two characteristics that provide a link between the failure of feedwater for heat removal by the steam generators and the failure of makeup/HPI cooling. The first characteristic involves the need for certain operator actions. Among the important causes of failure of auxiliary feedwater are the failure of the operators to start the motor-driven feed pump if the turbine-driven pumps were not available, and the failure to control the turbine-driven pumps manually if automatic control were to fail. Makeup/HPI cooling would also require manual initiation. Although each of these actions was assessed to be reliable individually because of the availability of proper training and procedural guidance, a relatively high level of dependence was assessed between the failures related to the auxiliary feedwater system and the failure to initiate makeup/HPI cooling. This was particularly the case for the failure to start the motor-driven feed pump, since both that action and the need for makeup/HPI cooling would be direct responses to the loss of feedwater from other sources. Therefore, the cut sets involving combinations of these interactions were among the important contributors to the sequence frequency.

The second characteristic shared by some of the cut sets was a dependence on support systems. In this case, ac and dc power were especially important. In the event of loss of one of the two trains of safety-related dc power, the flow control valve for one train of turbine-driven auxiliary feedwater would fail open. Without operator action, the steam generator being supplied by that train could be overfired and, because of cross-connections in the steam supplies for the turbine-driven pumps, both pumps could be affected by water carryover into the steam lines. Depending on the specific power supply that was affected, the loss of dc power could cause unavailability of the pilot-operated relief valve, which could otherwise provide one of the paths for removing decay heat during makeup/HPI cooling. Makeup/HPI cooling could also be affected if the dc supply that was lost would cause unavailability of the control power needed to start one of the makeup pumps. The action to control the affected train of turbine-driven auxiliary feedwater manually was assessed to be reasonably reliable, since it is thoroughly documented in the emergency procedure (Ref. 5), is practiced, and has been used during upsets involving the control system in the past. Nevertheless, the dependence on dc power provided another link between the two possible modes of core cooling following loss of main feedwater. A failure of dc power could result from an initiating bus fault, from other system faults, or due to battery depletion following loss of offsite power

and failure of one of the diesel generators. The latter would also reduce the availability of the makeup system as well, since both makeup pumps are motor-driven.

Sensitivity studies were performed to aid in understanding these contributions. For example, the reliability of the human action to start the motor-driven feed pump and of the combinations involving that action and the initiation of makeup/HPI cooling were varied to determine if a change such as automating the starting of the motor-driven pump would be of significant benefit. None of the sensitivity studies that was performed indicated that substantial reductions in core-damage frequency would be obtained by making the implied changes.

The second type of transient-initiated sequence that was a significant contributor to the core-damage frequency was a loss of seal cooling for the reactor coolant pumps (RCPs), leading to a small LOCA due to failure of the seals, followed by failure to maintain adequate RCS inventory (i.e., failure of safety injection). For a seal LOCA to occur, the RCPs would have to continue operating while seal cooling was lost or degraded. Seal cooling is normally supplied by both injection from the makeup system and component cooling water (CCW). Loss of both these sources of cooling, or failure to maintain adequate seal return flow, could lead to degradation of the three stages of the seals.

The potential for failures of support systems played a dominant role for this type of sequence. Component cooling water is required for cooling of the pumps in both the makeup and HPI systems. Thus, if the CCW system were to fail, both sources of seal cooling (i.e., CCW and seal injection from makeup) would be lost, and there would be no means for safety injection at high pressure. Loss of cooling by the CCW system could also result from loss of the service water system, which serves as the heat sink for the CCW system. Both of these systems have significant redundancy, but they could be subject to common-cause failures. Various failures of the operators to restore cooling flow and to trip the RCPs when required are also important elements of the cut sets for this sequence.

Other types of small LOCAs have been found to be important at some PWRs. The frequency of core damage due to small LOCAs is relatively small for Davis-Besse for a variety of reasons, but partly because both the HPI and makeup systems can provide adequate control of RCS inventory, offering a degree of redundancy and diversity. In the long term, it would generally be possible to cool down to conditions at which core cooling could be provided by the decay heat removal (DHR) system, or high pressure recirculation could be established. For medium and large LOCAs, the dominant contributors were primarily common-cause failures or failures of the operating staff to establish recirculation. No individual failure modes were found to be particularly important.

Core-damage sequences initiated by SGTRs were also assessed to be relatively low in frequency. The primary reason for this was the very long time available for response in most cases. In general, the emergency procedure would lead to early cooldown to the point at which the steam generator containing the broken tube could be isolated, effectively terminating the leakage from the RCS. Even if this could not be accomplished for some

reason, the borated water storage tank (BWST), which is the supply source for the injection systems, normally contains nearly 500,000 gallons of water. For most scenarios, the lowering of RCS pressure would cause the leak rate to be reduced to the point at which this volume would last for a period of days. This would afford ample time for response and recovery of affected equipment.

The assessment of interfacing-systems LOCAs drew heavily upon an investigation performed for a generic Babcock & Wilcox plant for the NRC (Ref. 6). The frequencies of these LOCAs were assessed to be dominated by scenarios that would involve successful injection until the BWST contents were depleted. Therefore, in most cases there would be significant time for operator action to isolate the breaks. The generic assessment performed for the NRC was dominated by a scenario in which it was postulated that an operator error of commission could lead to premature entry into shutdown cooling while the RCS was still at high pressure. This scenario was reevaluated for applicability to Davis-Besse. There remains significant uncertainty with respect to whether or not it is credible for such an error to be made while RCS pressure is high enough to threaten the integrity of the DHR system. Nevertheless, it was retained and is the largest contributor to the frequency of core damage due to interfacing-systems LOCAs.

Internal flooding was also investigated in detail. Three areas were identified that were susceptible to flooding and that could have been important with respect to core damage: the room containing the service water pumps, the room containing the pumps and heat exchangers for the CCW system, and the rooms housing the HPI and DHR pumps. In the event of loss of any of these areas, however, there would still be options for maintaining core cooling. Therefore, internal flooding was not found to be as important for Davis-Besse as it has been for some other plants.

Section 4 of Part 3 provides a much more detailed discussion of the important core-damage sequences, the plant features that contribute most to them, and the areas that were investigated with respect to potential plant changes. In summary, while some changes continue to be considered, none was judged to be necessary to address a vulnerability or was found to be clearly desirable from a quantitative or qualitative perspective.

4.2 FINDINGS FROM THE BACK-END ANALYSIS

As noted in Section 3, the back-end analysis consisted of both extensive deterministic evaluations of containment response using the MAAP code and investigation of other possible accident progressions using a containment event tree. The calculations made using MAAP indicated that loadings due to severe accidents would remain within the capabilities of the containment for all accidents except those in which containment heat removal was unavailable; in that case, the containment could eventually overpressurize due to the evolution of steam and/or non-condensable gases.

Based on the quantification of the end states for the containment event tree, the conditional probabilities for various containment failure modes given core damage have been

calculated. They are summarized in Figure 4-2. This figure indicates general consistency with the MAAP results; no containment failure is predicted for about 84% of the sequences that comprise the core-damage frequency. For those cases in which containment failure would not be expected to occur, the core debris would be in a cooled state and containment heat removal would be functioning to limit the pressure rise inside containment.

As it is used here, early failure is a broad category that includes failures of containment isolation, bypass sequences, and failures due to internal loadings prior to or around the time of failure of the reactor vessel due to the molten core debris. Most of this contribution (2.6% of the total 3%) is from bypass sequences. Nearly 80% of the contribution from bypass sequences is from interfacing-systems LOCAs and initiating SGTRs; the remainder stems from tube ruptures that result from failure of the tubes during core degradation. The remaining small fraction of early failures is spread among several categories of low-probability challenges, including early hydrogen burns, in-vessel and ex-vessel steam explosions, and the loading at vessel breach due to steam generation and direct containment heating. Isolation failures were assessed to contribute a negligible amount to the potential for releases from containment.

Side wall failure refers to the potential for attack of core debris on the containment wall itself. This could occur in the event of transport of a significant portion of the core debris from the reactor cavity up to the basement level of containment at the time of vessel failure. The area to which this dispersion would take place would be adjacent to the containment wall. The steel wall is protected by a concrete curb that is 1.5 ft thick and 2.5 ft high, so that direct failure by the debris would not occur. If the core debris were cooled, as it would be expected to be for accidents in which the contents of the BWST were injected, no significant ablation of the concrete curb would be expected. If the debris were not cooled, however, the concrete could be ablated, leading to containment failure several hours after vessel failure.

Late failure would occur most frequently for cases in which no means of removing heat from containment was available. The generation of steam and/or non-condensable gases could eventually lead to overpressurization of the containment. A small contribution to late failure also results from the possibility of late burning of hydrogen and other combustible gases.

All sequences in which the core debris was not cooled but no other failure mode occurred were assigned to the category of basemat meltthrough. For some of these accidents, it is very likely that ablation of the concrete would cease before the basemat was penetrated, as decay heat diminished, cooling water was made available, etc. No attempt was made to discriminate these outcomes further.

The most important findings from the back-end analysis relate to the reasons that the containment was likely to retain its integrity for most types of accidents. Chief among these reasons is the very large free volume available in the containment. At 2.8×10^6 ft³, there is substantial margin to accommodate severe accident loadings without approaching pressures that would be likely to result in containment failure.

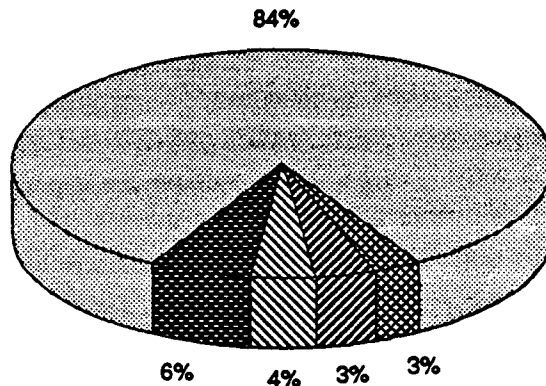
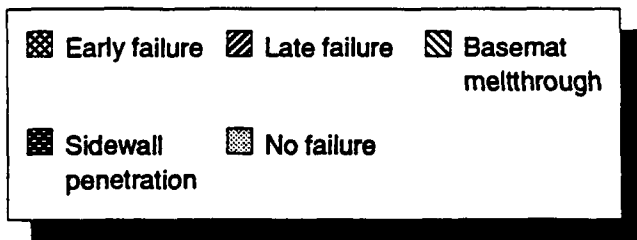


Figure 4-2. Conditional Probabilities of Containment Outcomes Given Core Damage

The geometry of the reactor cavity was also important. The cavity area is relatively large, so that even if the core debris were to be retained in the cavity, it is likely that it would form a coolable geometry. In addition, all areas of the containment drain eventually to the containment normal sump, which is located in the cavity region. Therefore, any water that is present in containment would be available for cooling debris in the cavity. If the contents of the BWST had been injected, a depth of water of approximately 25 ft would be present in the cavity. Even if only the original volume of the RCS and the core flood tanks were present, the debris would be covered by water at least 4 ft deep. This water would generally cause the debris to re-freeze, and with containment heat removal available, should allow a relatively stable condition to develop.

The cavity communicates with the containment basement primarily via the incore instrument tunnel. For accidents that would progress at relatively high RCS pressure (500 to 600 psig or greater), it is possible that debris would be dispersed to the basement. At that level, there would be an area over which the debris could spread even larger than the cavity. If the contents of the BWST were injected, there would be several feet of overlying water in that area as well. Therefore, a stable condition could be achieved similar to that in the cavity.

Because of the large volume of the containment, it would be very difficult for sufficient hydrogen to be generated or to accumulate to support a burn that could challenge the containment capacity. Similarly, pressurization due to direct containment heating or steam generation at vessel breach would not be likely to cause the capacity to be exceeded. Direct containment heating could be further limited because there would not be direct pathways for finely fragmented fuel to be transferred efficiently from the basement to the upper regions of containment.

Failure of containment isolation was found to be a negligible contributor to the potential for releases from the containment. This is due in part to administrative controls, especially those that prevent using the containment purge lines during power operation. Other penetrations are well monitored.

The possibility that core damage could be arrested prior to vessel breach was also considered. Two mechanisms were addressed in the containment event tree: restoration of cooling flow, such as by reducing RCS pressure sufficiently to allow low pressure injection; and cooling of debris, after it had slumped into the bottom head of the reactor vessel, via heat transfer to water surrounding the vessel.

Approximately 8% of the core-damage sequences led to conditions in which cooling was assessed to be restored while the core was still largely intact. Even in these cases, containment failure was still possible (e.g., due to burning of hydrogen generated during the initial degradation, or due to long-term overpressurization in the absence of containment heat removal). Direct containment heating and other loadings associated with vessel breach, as well as core-concrete interactions, would, however, be precluded.

The second possibility cited above refers to the potential for cooling by submergence of the reactor vessel. If the contents of the BWST were injected prior to vessel breach, the

vessel would be flooded up to about the level of the nozzles for the hot legs. Because uncertainties remain regarding the manner in which this mode of cooling might work (for example, the debris might still attack the vessel at the bottom-head penetrations), no credit was given to this possibility in the base-case assessment. A sensitivity study was performed in which it was assumed to be very likely that this mode of cooling would succeed if the BWST contents were injected. In this sensitivity study, the fraction of sequences in which vessel failure was prevented increased from 8% to 29%. The overall breakdown of containment failure modes remained largely unchanged, however, since containment failure would not have been predicted for the majority of affected sequences even in the base case. The major impact would be to prevent relatively low-probability failure modes, such as pressurization at vessel breach or ablation of concrete in the cavity or basement in the presence of overlying water.

Although they did not contribute to large frequencies of releases, some plant features have been identified that merit further consideration during the development of plans for accident management. These include measures relating to current instructions to start the reactor coolant pumps during a severe accident, provisions for managing the inventory in the BWST during LOCAs, and the monitoring of post-accident conditions.

The results of the back-end analysis are discussed more fully in Sections 6 and 7 of Part 4 of this submittal. Although a broad range of potential challenges to containment integrity were identified and investigated, the containment was generally found to be capable of accommodating those challenges. No vulnerabilities or serious weaknesses were identified relative to containment response.

REFERENCES FOR PART 1

1. Crutchfield, D. M. "Individual Plant Examination for Severe Accident Vulnerabilities." U.S. Nuclear Regulatory Commission Generic Letter 88-20, November 23, 1988.
2. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants.* American Nuclear Society, Institute of Electrical and Electronics Engineers, and U.S. Nuclear Regulatory Commission Report NUREG/CR-2300, January 1983.
3. Hengge, C. A., et al. *Davis-Besse Nuclear Power Station Level 1 Probabilistic Risk Assessment.* The Toledo Edison Company, November 1988.
4. *MAAP-3.0B—Modular Accident Analysis Program for LWR Power Plants.* Electric Power Research Institute Report NP-7071-CCML, November 1990.
5. "RPS, SFAS, SFRCS Trip, or SG Tube Rupture." Davis-Besse Nuclear Power Station Emergency Procedure DB-OP-02000, June 18, 1990.
6. Galyean, W. J., and D. I. Gertman. *Assessment of ISLOCA Risk—Methodology and Application to a Babcock and Wilcox Nuclear Power Plant.* U.S. Nuclear Regulatory Commission Report NUREG/CR-5604, April 1992.

Part 2
EXAMINATION DESCRIPTION

Contents

<u>Section</u>	<u>Page</u>
List of Tables	iv
List of Illustrations	iv
1 INTRODUCTION.....	1
2 CONFORMANCE WITH THE GENERIC LETTER.....	3
3 GENERAL METHODOLOGY	9
3.1 Front-End Analysis.....	9
3.1.1 Event Sequence Analysis.....	10
3.1.2 Analysis of Plant Systems.....	10
3.1.3 Development of the Reliability Data Base.....	12
3.1.4 Assessment of Human Interactions.....	13
3.1.5 Quantification of Sequence Frequencies	14
3.2 Back-End Analysis	14
3.2.1 Coordination of the Front-End and Back-End Analyses.....	16
3.2.2 Modeling of Containment Response and Accident Analysis	16
3.2.3 Containment Event Analysis.....	17
3.2.4 Assessment of Fission Product Releases.....	18
3.3 Application of Results and Insights.....	18
4 INFORMATION ASSEMBLY.....	21
REFERENCES FOR PART 2	23

List of Tables

<u>Table</u>		<u>Page</u>
2-1	Cross-Reference of IPE Submittal Contents	5

List of Illustrations

<u>Figure</u>		<u>Page</u>
3-1	Overview of Front-End Tasks	11
3-2	Summary of Back-End Tasks	15

Section 1 INTRODUCTION

This report describes the results of the individual plant examination (IPE) for the Davis-Besse Nuclear Power Station, performed in response to the request presented in Generic Letter 88-20 (Ref. 1). The Davis-Besse IPE was accomplished through the performance of a probabilistic risk assessment (PRA). The Toledo Edison Company chose PRA as the means to satisfy the IPE because of its utility in identifying potential severe accident vulnerabilities, while it could also provide meaningful insights into plant design and operations useful to decision-making beyond the scope and period of the IPE process. As defined by the PRA Procedures Guide (Ref. 2), this PRA constitutes a level 2 study (i.e., it includes both consideration of the sequences of events that could lead to core damage and the possible responses of containment to those sequences). This section and the remainder of Part 2 provide an overview of the PRA, including a general summary of the methods used.

Toledo Edison originally performed limited PRA-related analyses in the early 1980's to investigate various aspects of plant safety. Following the loss-of-feedwater event of June 9, 1985, more extensive probabilistic assessments of the reliability of the auxiliary feedwater system were undertaken to help ensure that long-term responses to that event would be effective.

Recognition of the growing role of PRA in safety analysis and regulatory interactions led to the initiation, in late 1986, of a level 1 PRA for Davis-Besse. The primary objective of that PRA was to begin to develop in-house capabilities to develop, maintain, and use PRA to address safety and regulatory issues. Completed in draft form in the fall of 1988, the original PRA considered a broad range of internal initiating events, with more limited assessment of internal flooding and fires (Ref. 3). A contractor, Science Applications International Corporation (SAIC), provided assistance in performing the PRA, training of Toledo Edison personnel, and the software needed to support the technical effort. In addition, Safety and Reliability Optimization Services, Inc. (SAROS) provided an independent overview of the efforts associated with the draft PRA. Because the plant was undergoing significant changes at the time the draft was completed, the iteration and extensive review of the results that usually characterize the latter stages of a PRA were not performed.

Many changes to plant systems and procedures, largely as a result of the concerted response to the 1985 loss-of-feedwater event, continued to be made through the late 1980's. In addition, Generic Letter 88-20 (Ref. 1) was issued at about the time that the draft PRA was completed. Therefore, a new effort was initiated to develop a PRA that would both account for changes made since the baseline date for the draft study and satisfy specific items requested in the generic letter. Thus, although the PRA performed for the IPE drew from the draft level 1 effort, it represents essentially a complete re-examination of the plant. In addition to satisfying the NRC's request for an IPE, the technical objectives of the PRA included the following:

- To apply state-of-the-art PRA techniques to develop a more current understanding of the types of severe accidents that could be important for Davis-Besse,
- To identify any areas in which there might be the need or opportunity to reduce the frequency of core damage or of serious radiological releases in a cost-effective manner, and
- To provide the plant-specific inputs for an accident-management program.

Several additional objectives that affected the manner in which the PRA was structured and implemented to meet these overall objectives were identified. These additional objectives included the following:

- To develop a model for Davis-Besse that could be readily updated in the future, as changes are made to the plant or as additional insights into severe accident behavior become available, so that the model and results could be applied to address safety and regulatory issues as they arise;
- To continue to develop the expertise within the Toledo Edison Company necessary to perform the analyses for the IPE and to maintain and use them in these future applications; and
- To document the analyses in a manner that would both make the future applications traceable and provide the necessary bases for external reviewers to determine that the work had been accomplished in a thorough and competent manner.

Because of personnel changes, a new project team was assembled at Davis-Besse to update the draft PRA and to complete the IPE. In addition, Safety and Reliability Optimization Services (SAROS), Inc., was retained to provide technical guidance and additional training, and to assist in specific technical areas. SAROS had also provided an ongoing independent review throughout the effort that led to the draft PRA. Toledo Edison personnel performed extensive updating of the system fault trees and the reliability data bases, quantified the frequencies of the core-damage sequences, developed and applied the tools for performing the containment analyses, and assembled insights that formed the basis for initial decisions regarding any changes that might be made to the plant. Overall, Toledo Edison personnel provided about 80% of the technical effort represented by the IPE. The composition of the project team and the extensive interactions of the team with other Davis-Besse staff are described in Part 5.

Section 2 CONFORMANCE WITH THE GENERIC LETTER

By letter dated October 27, 1989 (Ref. 4), Toledo Edison outlined its proposal for performing the IPE in accordance with NRC Generic Letter 88-20 (Ref. 1). This letter explained that a level 1 PRA and a containment performance analysis that followed the procedures described in NUREG/CR-2300 (Ref. 2) would be performed. In meeting this objective, a level 2 PRA was performed in accordance with the PRA Procedures Guide.

The letter further explained that the assessment would consider current severe accident phenomenological issues and would be based on current plant design. Although some earlier PRA work had been done for Davis-Besse, substantial modifications were made following the June 9, 1985, loss-of-feedwater event. During the eighteen months after that event, while the plant was shut down, a complete re-evaluation of plant operating and maintenance practices was performed. This re-evaluation resulted in many plant changes, including the addition of a third auxiliary feedwater pump (a motor-driven pump); enhanced makeup/high pressure injection cooling capability; significant procedural changes, including the development of several new procedures; improved operator training; and improvements in maintenance practices. Consequently, substantial changes were required in the success criteria and system modeling areas of the original PRA study. A cut-off date of June 1990 was chosen for the IPE to represent the current plant design and to support the plant-specific data collection effort. Because of the relatively few plant modifications made after June 1990, those implemented during the subsequent outage (the seventh refueling outage) were also incorporated into the models. Therefore, the PRA models reflect the as-built configuration of the plant as of the end of the seventh refueling outage. The eighth refueling outage will commence on March 1, 1993.

The front-end analysis (the level 1 portion of the PRA) entails the identification of the core-damage sequences and characterization of their frequencies. The methods used in this analysis are described in Section 3.1. In accordance with the generic letter, an evaluation of the decay heat removal function was also performed. The results of that evaluation are discussed in detail in Section 4 of Part 3 of this submittal.

The back-end analysis (i.e., the level 2 portion of the PRA) followed the general guidance provided in Appendix 1 to Generic Letter 88-20 (Ref. 1). The results provide insights into the dominant sequences leading to containment failure, the associated potential for fission-product releases, and the role of plant systems in limiting such potential failures and releases.

In performing the IPE, emphasis was placed on system modeling in accordance with the plant procedures, and current plant operating and maintenance procedures. Davis-Besse engineers were involved in all aspects of the examination such that the knowledge gained from the IPE can be factored into plant procedures and training programs.

While the submittal was prepared in accordance with NUREG-1335, minor changes were made in the way some sections were grouped for discussion purposes. Table 2-1 provides a cross-reference of the contents of the submittal to the specific guidance of NUREG-1335, Table 2.1, Standard Table of Contents for Utility Submittal (Ref. 5), and provides justification for any changes. It was intended that the information contained in this submittal provide the level of detail needed to enable reviewers to understand and determine the validity of all input data and calculation models used; to assess the sensitivity of the results to all key aspects of the analysis; and to audit any calculation. It should be noted, however, that substantially more information is available in the Davis-Besse project files. Thus, Davis-Besse has satisfied the requirements of the generic letter through a level 2 PRA evaluation performed primarily by in-house personnel and based on current plant design. All specific items requested in the generic letter and in NUREG-1335 have been addressed and are described in the remainder of this submittal.

Table 2-1
Cross-Reference of IPE Submittal Contents

NUREG-1335 Table of Contents	Davis-Besse IPE Contents
1. EXECUTIVE SUMMARY	Part 1: EXECUTIVE SUMMARY
1.1 Background and Objectives	1. Background and Objectives
1.2 Plant Familiarization	2. Plant Familiarization
1.3 Overall Methodology	3. Overall Methodology
1.4 Summary of Major Findings	4. Summary of Major Findings
2. EXAMINATION DESCRIPTION	Part 2: EXAMINATION DESCRIPTION
2.1 Introduction	1. Introduction
2.2 Conformance with GL and Supporting Material	2. Conformance with GL and Supporting Material
2.3 General Methodology	3. General Methodology
2.4 Information Assembly	4. Information Assembly
3. FRONT-END ANALYSIS	Part 3: FRONT-END ANALYSIS
3.1 Accident Sequence Delineation	1. Accident Sequence Delineation
3.1.1 Initiating Events	1.1 Identification of Initiating Events
3.1.2 Front-Line Event Trees	1.2 Event Trees for Core-Damage Sequences
3.1.3 Special Event Trees	None required; all event trees included in Section 1.2.
3.1.4 Support System Event Trees	None required; linked fault-tree approach employs explicit modeling of support systems.
3.1.5 Sequence Grouping and Back-End Interfaces	1.3 Sequence Grouping and Back-End Interface
3.2 Systems Analysis	2. Systems Analysis
3.2.1 System Descriptions	2.2 System Descriptions
3.2.2 Systems Analysis	2.1 Overview of Systems Analysis
3.2.3 System Dependence	The system dependencies are detailed in Section 2.2, and are summarized in Section 2.1.
3.3 Sequence Quantification	3. Sequence Quantification
	3.1 Data Analysis
3.3.1 List of Generic Data	3.1.1 Initiating Event Frequencies (both generic and plant-specific)
3.3.2 Plant-Specific Data Analysis	3.1.2 Generic Data Analysis (generic component failure rates only)
	3.1.3 Plant-Specific Data Analysis (plant-specific component failure rates and testing and maintenance unavailabilities)

**Table 2-1 (continued)
Cross-Reference of IPE Submittal Contents**

NUREG-1335 Table of Contents	Davis-Besse IPE Contents
3. FRONT-END ANALYSIS (continued)	Part 3: FRONT-END ANALYSIS (continued)
3.3.3 Human Failure Data	3.2 Quantification of Human Interactions
	3.2.1 Integration of Human Interactions into Plant Models
	3.2.2 Quantification of Human Interactions
	3.2.3 Review Activities related to Assessment of Human Interactions
3.3.4 Common-Cause Data	3.1.4 Common-Cause Failure Data
3.3.5 Quantification of Unavailability of Systems and Functions	Covered in Sections 3.2, Systems Analysis and 3.4, Quantification of Sequence Frequencies.
3.3.6 Generation of Support System States and Quantification of Their Probabilities	Not relevant; in the linked fault tree approach, support systems are modeled explicitly.
3.3.7 Quantification of Sequence Frequencies	3.4 Quantification of Sequence Frequencies
3.3.8 Internal Flooding Analysis	3.3 Recovery Analysis
	3.1.5 Data Assessment for Frequencies of Internal Floods
3.4 Results and Screening	4. Results and Screening Process
3.4.1 Application of Generic Letter Screening Criteria	4.1 Summary of Sequence Frequencies
3.4.2 Vulnerability Screening	4.2 Summary of Plant Vulnerabilities
3.4.3 Decay Heat Removal Evaluation	4.3 Decay Heat Removal Evaluation
3.4.4 USI and GSI Screening	4.4 USI and GSI Screening
4. BACK-END ANALYSIS	Part 4: BACK-END ANALYSIS
4.1 Plant Data and Plant Description	1. Plant Data and Plant Description
4.2 Plant Models and methods for Physical Processes	2. Plant Models and Methods for Physical Processes
	2.1 Assessment of Severe Accident Response Using MAAP
	2.2 Investigation of Specific Issues
4.3 Bins and Plant Damage States	3. Bins and Plant-Damage States
	3.1 Attributes of Plant-Damage States
	3.2 Definition of Core-Damage Bins
4.3 Bins and Plant Damage States (continued)	3.3 Containment Systems Event Tree
	3.4 Summary of Plant Damage States
4.4 Containment Failure Characterization	4. Containment Failure Characterization
4.5 Containment Event Trees	5. Containment Event Tree
	5.1 Development of the CET
	5.2 Top Events in the CET

**Table 2-1 (continued)
Cross-Reference of IPE Submittal Contents**

NUREG-1335 Table of Contents	Davis-Besse IPE Contents
4. BACK-END ANALYSIS (continued)	Part 4: BACK-END ANALYSIS (continued)
4.6 Accident Progression and CET Quantification	6. Accident Progression and Quantification for the Containment Event Tree
	6.1 Containment Response for Representative Accidents
	6.2 Quantification of the CET
	6.3 Frequencies for CET Outcomes
4.7 Radionuclide Release Characterization	7. Radionuclide Release Characterization
	7.1 Definition of Release Categories
	7.2 Estimated Release Frequencies
5. UTILITY PARTICIPATION AND INTERNAL REVIEW TEAM	Part 5: IPE PERFORMANCE AND IMPLEMENTATION
5.1 IPE Program Organization	1. IPE Program Organization
5.2 Composition of Independent Review Team	2. Review Activities
5.3 Areas of Review and Major Comments	
5.4 Resolution of Comments	
6. PLANT IMPROVEMENTS AND UNIQUE SAFETY FEATURES	Part 6: PLANT IMPROVEMENTS AND UNIQUE SAFETY FEATURES
	1. Unique Safety Features
	2. Consideration of Vulnerabilities
	3. Other Plant Improvements
7. SUMMARY AND CONCLUSIONS	Part 7: SUMMARY AND CONCLUSIONS



Section 3 GENERAL METHODOLOGY

The PRA conducted to satisfy the IPE was comprised of two major areas of analysis: (1) the identification of sequences of events that could lead to core damage and the estimation of their frequencies of occurrence (the front-end analysis); and (2) the evaluation of the potential response of containment to these sequences, with emphasis on the possible modes of containment failure and the corresponding source terms (the back-end analysis). In addition to these analysis areas, a significant portion of the effort entailed consideration of the insights gained both from the analysis process itself and from the results that were obtained. The results and insights were important inputs to the process of considering possible changes to reduce plant risk further, and in some cases aided in the disposition of generic issues as they apply to Davis-Besse. The methods used in the front-end and back-end analyses and the process of evaluating the results and insights are summarized in the sections that follow. These areas are discussed much more extensively in Parts 3, 4 and 6 of this submittal.

3.1 FRONT-END ANALYSIS

As noted previously, a level 1 PRA was originally completed in draft form in 1988. Many changes were made to important plant systems and to the operating procedures after the baseline date that defined the reference plant configuration for the development of the models for the draft PRA. Therefore, an extensive updating of the draft models was performed during the preparation of the PRA for the IPE submittal.

The principal tasks for the front-end analysis are summarized in Figure 3-1. The overall methodology can be characterized as one in which core-damage sequences were represented by event trees whose top events defined success or failure of safety functions, with further development of the top events accomplished through the construction of system-level fault trees. The fault trees for each top event were linked according to the logic defined by the event trees. This linking allowed the frequencies of core-damage sequences to be estimated by obtaining sequence-level minimal cut sets (i.e., the combinations of initiating events, equipment failures, and human interactions that would lead to the sequences of interest). The quantification was accomplished using a combination of the best available sources of reliability data derived from operating experience at Davis-Besse and the nuclear industry as a whole. The assessment of human reliability was performed through the careful identification of potential interactions and the application of methods for quantifying their probabilities that are among the most recent that are currently being used.

The integrative nature of the modeling and quantification process permitted explicit treatment of dependencies within and among systems. It also allowed consideration of potential human interactions and recovery actions in a sequence-specific context. As a result, insights into important aspects of the plant design and operating practices were gained both during the modeling process and as a consequence of review of the quantitative results.

The approach taken for each of the general tasks identified in Figure 3-1 is summarized in the sections that follow. References to more detailed discussion of particular aspects of the tasks in Part 3 of this submittal are also provided where appropriate.

3.1.1 Event Sequence Analysis

The event sequence analysis encompassed the definition of initiating events that should be considered and the development of event trees to delineate the possible core-damage sequences that could result from those initiators.

The definition of initiating events was accomplished through a variety of means to ensure that the list that was developed was as complete as possible. Initiating events were identified through a search of operating experience at other PWRs, a review of previous PRAs for other plants, examination of the trip experience at Davis-Besse, and careful review of the individual systems at Davis-Besse. Initiating events were included in the study if they could cause a reactor trip and a unique challenge to plant systems needed to maintain core cooling. A total of nine initiating events involving loss-of-coolant accidents (LOCAs), 19 transients in which there was no initial breach of the reactor coolant system (RCS), and six internal floods were included in the analysis.

An event tree was developed for each category of initiating event. This was done by first defining the safety functions that must be achieved to prevent core damage. These safety functions were then related to plant systems that must function to accomplish them. The minimum criteria for success of each of these systems were determined from available information, supplemented with specific calculations when necessary. Event trees were then constructed to delineate the core-damage sequences. The top events for these event trees were usually represented in terms of the safety functions. The failure to accomplish each of these safety functions was developed through fault-tree logic at a high level to denote the corresponding system-level failures, and to represent the functional interrelationships among the systems. These system failures were further developed through detailed fault trees. Taken together, the event trees, supporting logic, and system-level fault trees comprise an integrated model of the core-damage sequences.

End states were selected for the event-tree development based on the minimum stable conditions that, if achieved, would ensure that core cooling could be sustained in the long term. In some cases, top events were included in the event trees to permit the end states to be further discriminated according to the implications with respect to subsequent containment response. This is discussed further in Section 3.2.1. The selection of initiating events and development of the event trees is discussed in detail in Section 1 of Part 3 of this report.

3.1.2 Analysis of Plant Systems

The failure modes for plant systems were further developed through the construction of fault trees. The fault trees were developed to the level necessary to account for important

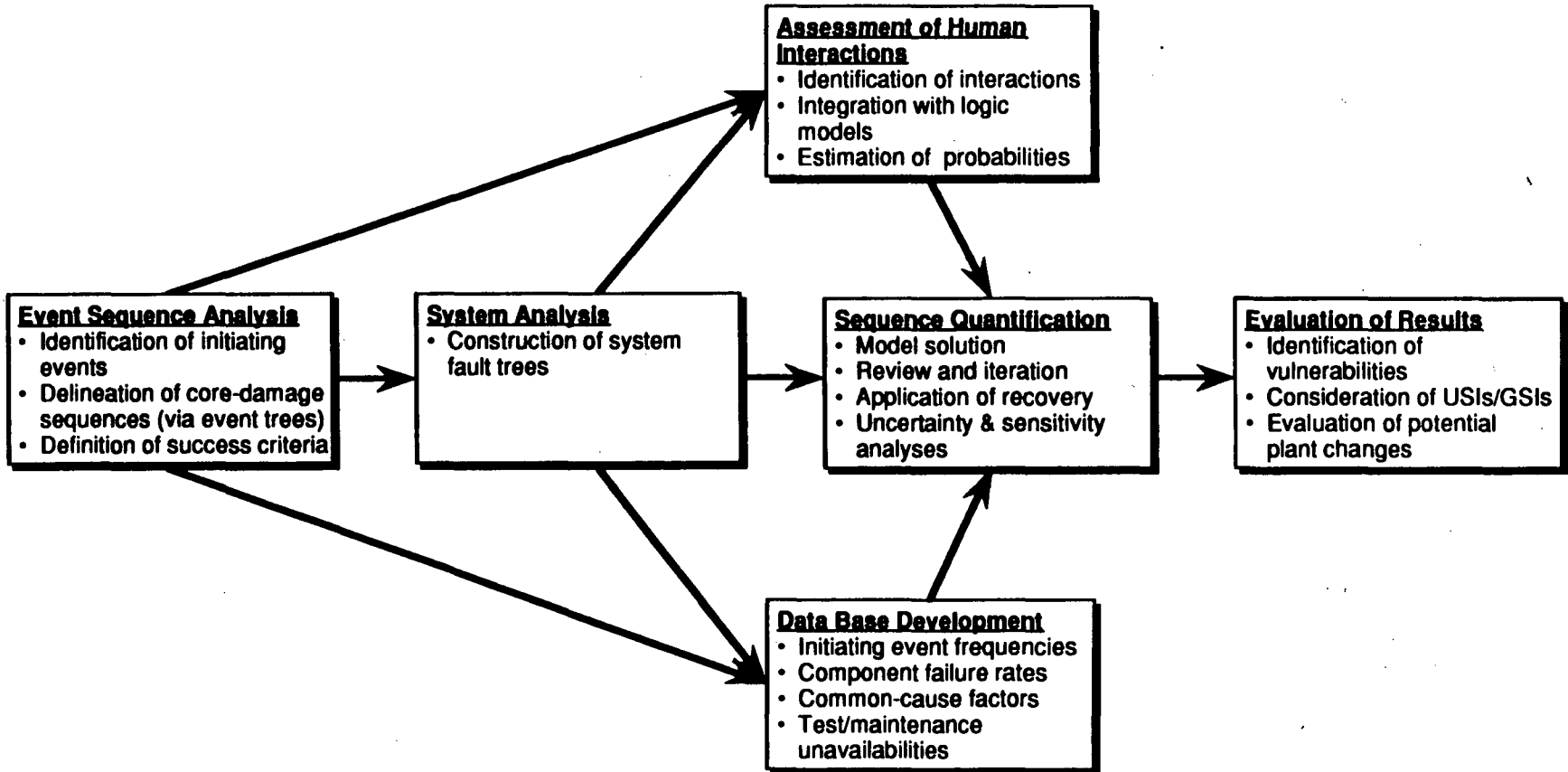


Figure 3-1. Overview of Front-End Tasks

failure modes, to assure proper treatment of both intra- and inter-system dependencies, and to be consistent with the availability of reliability data. The fault trees for the front-line systems (i.e., those reflected in the logic for the event trees) were constructed based on the minimum success criteria defined by the sequence logic.

The fault trees included explicit development for inter-tied front-line systems (i.e., the systems that are called upon to prevent core damage) and for dependencies on support systems (e.g., electric power, service water, etc.). This ensured that such dependencies were tracked through the modeling and quantification process in a direct manner. Development of the fault trees was also integrated with the assessment of human reliability, both to ensure that important interactions were included in the fault trees, and to supply the information to make a meaningful estimate of the probabilities for the interactions. Because of the redundancy in most of the systems and safety functions considered, an extensive effort was made to identify groups of components that could be subject to common-cause failure.

The fault trees were constructed with the aid of the CAFTA workstation. In addition to facilitating the construction of the fault trees, the workstation permitted efficient coordination of the basic events in the fault trees with the reliability data bases, substantially aided revision of the fault trees when necessary, and provided for the quantification of sequence frequencies.

A system notebook was assembled for each system analyzed. The notebooks contain the fault trees themselves, as well as the detailed design information, specification of procedures used, notes and assumptions, etc. that are the basis for the system analysis. The system analyses are summarized in Section 2 of Part 3. The notebooks contain the information required for a detailed review of the fault trees.

3.1.3 Development of the Reliability Data Base

The reliability data base encompasses the frequencies of the initiating events, independent and common-cause failure rates for components, and estimates of unavailabilities due to test and maintenance activities. In each of these areas, both industry-wide and plant-specific information was used to develop the most appropriate estimates.

The manner in which initiating event frequencies were estimated depended on the nature of the initiators themselves. For rarer events (most LOCAs, steam line breaks, etc.), generic experience for PWRs was used. For some events for which plant-specific experience was relevant but was inadequate to support direct estimation of their frequencies, generic and plant-specific data were combined through a Bayesian updating process. For still other initiating events (e.g., loss of main feedwater), the plant-specific experience was judged to be adequate and most appropriate for use in estimating frequencies.

Failure rates were developed for all components and failure modes based on generic data. For many of the more important plant components, the operating experience at Davis-Besse was assembled as well. In these cases, the generic and plant-specific data were

combined, again through Bayesian updating. Test and maintenance unavailabilities were calculated based on a review of operating experience.

Common-cause failure rates were developed using the methods developed jointly by the NRC and the Electric Power Research Institute (EPRI, Ref. 6). In addition to producing quantitative estimates that can be used in the estimation of sequence frequencies, these methods can aid in understanding further the causes of failure that might affect multiple components in a system or across systems. The effects of internal flooding were included explicitly in the plant models as potential sources of common-cause failure.

The methods used to develop the various reliability data bases and the data bases themselves are described in more detail in Part 3, Section 3.1.

3.1.4 Assessment of Human Interactions

The human reliability assessment was conducted in a manner consistent with the framework established by the Systematic Human Action Reliability Procedure (SHARP1, Ref. 7). This procedure emphasizes making the human reliability assessment an integral part of the process of developing and quantifying the models that define accident sequences and system failures. Two types of interactions were considered extensively in the study: (1) those that would take place prior to an initiating event and could leave a portion of a system unavailable; and (2) those that would involve response of the operating crew following an initiating event. The identification and assessment of human actions also relied heavily upon interactions with current and former operators at Davis-Besse.

Pre-initiator human interactions were identified and included in the system fault trees with other failure modes for the systems. High screening values were applied to these interactions in the models initially. During the quantification process, the probabilities for those interactions that were identified as potentially important were estimated more carefully using a somewhat simplified form of the Technique for Human Error Rate Prediction (THERP, Ref. 8).

Post-initiator human interactions were also identified during the process of constructing the event trees and fault trees. Some of these events, such as those that represented failure to initiate the function of a manually-actuated system, were included explicitly in the fault-tree logic. These events were all assigned probabilities of failure of 1.0 during the initial quantification. This ensured that no combinations of human interactions were erroneously treated as independent. The individual interactions and the combinations of interactions were then quantified on a sequence-specific basis after the minimal cut sets had been obtained. In some cases, additional interactions were added to the cut sets to account for potential recovery via use of alternative system configurations, etc. In all cases, there was at least some level of procedural guidance for the interactions that were considered. For nearly all of the cases, the interactions were detailed explicitly in the emergency or other operating procedures. The quantification was performed using methods developed by EPRI (Refs. 9 and 10). To the extent possible, the assumptions regarding the nature of the

interactions, operator priorities, timing, etc. were confirmed through observation of simulator exercises.

The methods used for the human reliability analysis and the results obtained are detailed in Sections 3.2 and 3.3 of Part 3. The details of the calculations for individual human interactions are available in the project files at Davis-Besse.

3.1.5 Quantification of Sequence Frequencies

The core-damage sequences were defined by the success or failure of top events in the event trees. These top events were, in turn, related to system-level failures and human interactions through fault-tree logic. To estimate the sequence frequencies, a master fault tree comprised of the relevant top events from the event tree was formed for each sequence. This permitted Boolean reduction of an integrated set of sequence and system models so that the core-damage sequences were defined in terms of combinations of specific initiating events, component faults, and human interactions (minimal cut sets).

After the sequence-level minimal cut sets were obtained, they were reviewed carefully to assure that the integration of separate models produced appropriate representations of the sequences. The information conveyed by the cut sets also permitted characterization of the post-initiator human interactions and of any relevant recovery actions in an appropriate context.

During the quantification process, the probability distributions for the basic events in the models were propagated to produce a representation of the uncertainty in the core-damage frequency. A series of sensitivity studies was also performed to provide further insights into the plant features that dominated the core-damage frequency and to investigate the potential benefits of changes that might be made to the plant or operating procedures.

The process of performing the quantification for the front-end analysis is described in Section 3.4 of Part 3. The results of this quantification are described in Section 4 of that part of the submittal.

3.2 BACK-END ANALYSIS

The primary objective of the back-end analysis was to identify any plant features that implied a potential weakness with respect to the possibility of serious releases from containment following a core-damage accident. The tasks that comprised the back-end analysis are summarized in Figure 3-2.

The back-end analysis included both extensive deterministic evaluations of expected containment response and a probabilistic evaluation of the range of responses that could be relevant for each type of accident. The deterministic evaluations were primarily made using the MAAP computer code. For the probabilistic assessment, a containment event tree was constructed and quantified. The tasks for the back-end analysis are summarized briefly

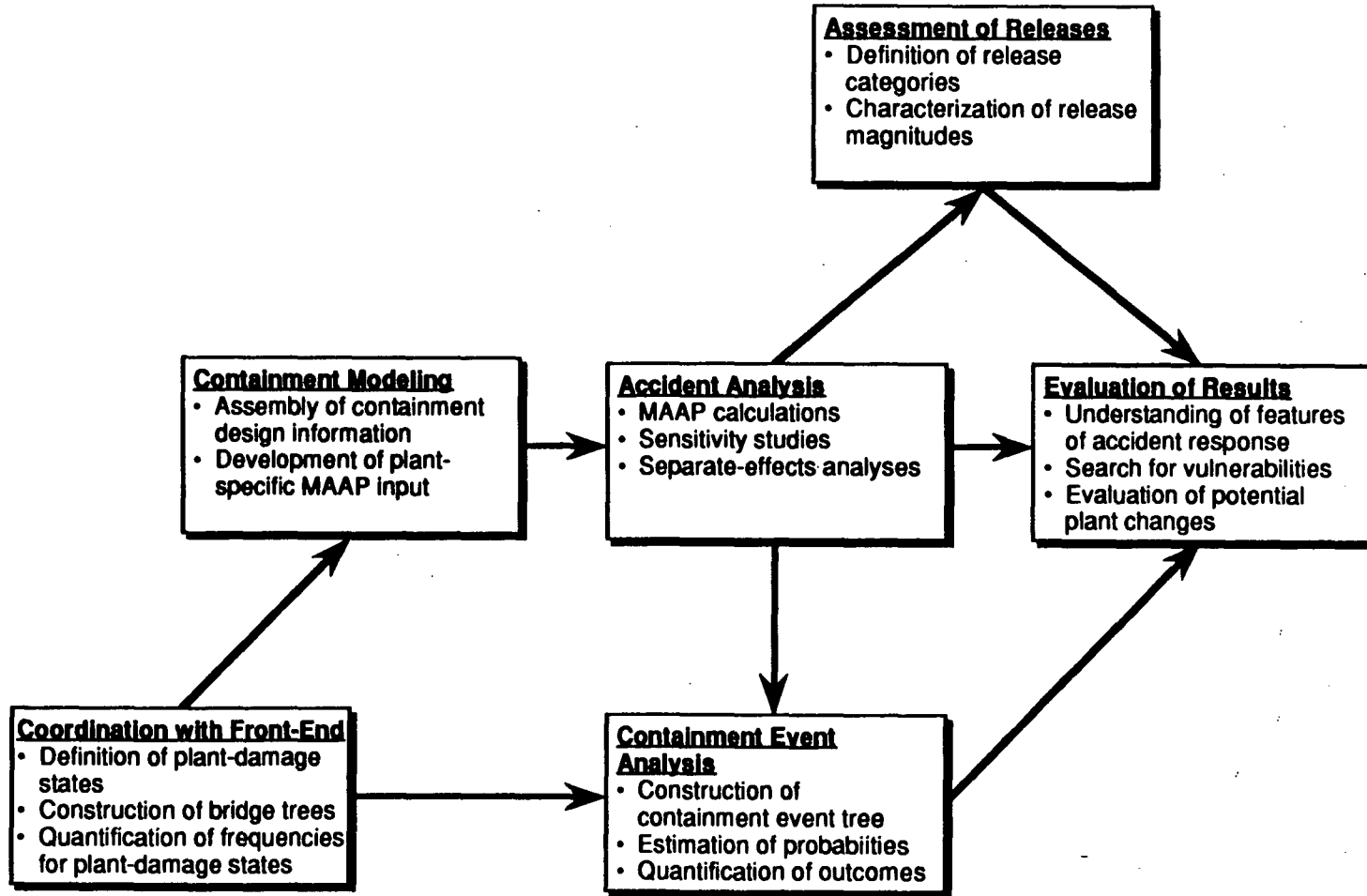


Figure 3-2. Summary of Back-End Tasks

below. More detailed descriptions of the tasks and the results that were obtained are provided in Part 4 of this submittal.

3.2.1 Coordination of the Front-End and Back-End Analyses

An important element of the IPE was the coordination of the front-end and back-end analyses. This was done to ensure that the core-damage sequences were developed to the level of detail necessary for meaningful assessment of containment response, with a minimum of iteration between the two major analysis areas. This coordination was accomplished through the definition of plant-damage states. The plant-damage states reflect binning of accident sequences at two major levels. First, the accident sequences up to the onset of core damage were grouped into core-damage bins according to similarities in their impact on subsequent containment response. These bins helped to ensure that the core-damage sequences were developed in sufficient detail to permit them to be tracked properly in the containment event tree. The second level encompassed the status of the containment systems (the containment air coolers, containment spray, etc.). The status of these systems defined in large measure the capability of the containment to prevent a serious release as a result of the core-damage accidents. The core-damage bins together with the states for the containment systems comprise the plant-damage states.

The core-damage sequences from the front-end event trees were grouped into core-damage bins. These bins were the inputs to a set of event trees that linked the core-damage sequences to the containment event tree. The top events in these linking, or bridge, trees reflected the containment safety features. Thus, the end states from the bridge trees corresponded to plant-damage states. The sequence cut sets that defined the core-damage sequences were combined with those for the states in the bridge trees to quantify the frequencies of the plant-damage states. Section 3 of Part 4 discusses the development of the bridge trees and defines the plant-damage states.

3.2.2 Modeling of Containment Response and Accident Analysis

To characterize the containment response to a core-damage accident, the Modular Accident Analysis Program (MAAP), version 3.0B (Revision 18), was selected as the primary analytical tool (Ref. 11). In addition to the analyses made using MAAP, specific issues were investigated through reviews of technical literature and other calculations. Models of the RCS, the emergency core cooling system, and the containment were developed based on information derived from drawings of major components, plant drawings, system descriptions, etc., so that the models were entirely plant-specific.

MAAP is intended to serve as a tool to perform realistic analyses of severe core-damage accidents. Evaluations using MAAP were made for a representative set of the plant-damage states. The results of these MAAP calculations were assumed to reflect the nominal or expected response of containment to the accidents. These results include a very large

number of parameters defining the conditions in the RCS and containment, the location of core debris, and the transport of fission products as a function of time.

Because many of the phenomena accounted for in the MAAP code are subject to potentially significant uncertainties, a series of sensitivity studies was conducted. These sensitivity studies were primarily derived from a set of standard studies recommended for PWRs (Ref. 12). In addition, calculations were made using separate tools to investigate such issues as the possible pressures that could be generated by hydrogen burns, the potential for creep rupture of RCS components subjected to very high temperatures and pressures, and cooling of core debris in various configurations.

In addition to these analyses, an assessment was made of the capacity of the containment vessel to retain its integrity when exposed to internal pressurization. The analysis investigated various mechanisms for containment failure to identify those that might limit its capacity. The expected yield strength was calculated and, based on variability in the materials used in the containment vessel and uncertainty in the method used to calculate the yield strength, a probability distribution for containment failure as a function of internal pressure was developed. A second distribution was developed to apply for scenarios in which pressurization would occur over a long period of time, such that the heating of the containment might reduce the strength of the containment shell.

These assessments are all described in some detail in Part 4 of this submittal. The development of the plant-specific model for the MAAP code and the separate investigations of specific issues are described in Section 2. The containment response to particular accidents, as characterized by MAAP, is summarized in Section 6.1. Section 4 provides a discussion of the assessment of containment capacity. In each of these areas, the detailed calculations and results are organized in project files at Davis-Besse.

3.2.3 Containment Event Analysis

For most types of accidents, the specific response of the containment cannot be predicted with certainty. A containment event tree was therefore constructed to provide a framework for investigating possible outcomes given core damage. The top events in the containment event tree represent general types of containment failure modes and conditions that would affect the magnitude of release from containment. In a manner analogous to the event trees for the front-end analysis, each of the top events was decomposed further through fault-tree logic into the various combinations of phenomena, system operations, and human interactions that could bring them about. Thus, an integral model of potential containment responses was developed.

The probabilities of the occurrence or of the severity level for various phenomena were quantified by a number of means. Although only point estimates were developed for these events, they reflected an appropriate assessment of uncertainties. In many cases the results of MAAP calculations formed the primary inputs. The MAAP results were supplemented heavily by input from other technical efforts, and especially from the analyses

performed in support of NUREG-1150 (Ref. 13); by sensitivity studies; and by engineering judgment.

The probabilities of the end states for the containment event tree were quantified for each of the plant-damage states. This quantification produced an estimate of the conditional probability of each type of containment failure mode and permitted estimation of the frequencies for each type of release from containment. To aid in understanding the elements that contributed to these results, some of the key event probabilities were varied in a series of sensitivity studies.

The containment event tree and its supporting logic are described in Section 5 of Part 4 of this submittal. Sections 6.2 and 6.3 discuss the quantification of the event tree and summarize the results that were obtained.

3.2.4 Assessment of Fission-Product Releases

Associated with each combination of plant-damage state and containment event tree outcome is a particular type of release of fission products from containment. A characterization of these releases provides further indication of the level of severity of the accidents, and would be necessary in the event that offsite consequences were to be calculated. For convenience in the analysis and in the presentation of results, the releases have been grouped into nine release categories. Thus, each outcome from the containment event tree is assigned to one of the release categories.

In addition to providing a representation of the containment response, the MAAP code tracked the status of fission products in the RCS, the containment, and as they were released from the containment. The MAAP results for different cases were grouped according to the release fractions for important species of fission products, and were used to suggest representative release fractions for each release category. In some cases, adjustments were made to the release fractions available from the MAAP results to reflect containment outcomes that were not explicitly calculated using MAAP. This was done, for example, to adjust the release fractions from a case in which containment sprays were not available to apply for a release category in which scrubbing by the sprays would have been available.

The development of the release categories and the results in terms of frequencies of release are summarized in Section 7 of Part 4.

3.3 APPLICATION OF RESULTS AND INSIGHTS

The primary purpose of the PRA was to gain further insights into the features that are important with respect to the potential for severe accidents at Davis-Besse. These insights were gained during both the modeling process and the review of the results for the front-end and back-end analyses. As noted in the preceding sections, the quantitative results were supplemented by sensitivity studies that aided in understanding the important risk contributors and helped to identify plant changes that might be most effective.

Based on this examination, it was concluded that there are no apparent vulnerabilities to severe accidents for Davis-Besse, and that no changes to reduce the frequency of core damage or of serious releases are critical to continued safe operation. Other changes that might be desirable from the standpoint of further reducing risk were identified and are being evaluated to ensure that the full ramifications are understood. The results and insights were also used to address other issues, including the issue of the adequacy of provisions for decay heat removal, as discussed in Section 4 of Part 3.

Section 4 INFORMATION ASSEMBLY

The use of many different sources of information is an inherent part of the overall PRA process. As such, each report section identifies the key sources of information used for each part of the analysis. It should also be noted that additional sources of information used in the PRA are contained in the Davis-Besse IPE project files in the form of system notebooks, database notebooks, human reliability analysis notebooks, etc.

The IPE work drew upon other PRA studies, especially those done for plants similar in design and operation to Davis-Besse (e.g., Oconee and Crystal River) for additional sources of information. In addition to these studies, other available PRAs, including the NUREG-1150 studies, were also used as references for the IPE work.

As a starting point for the level 1 portion of the IPE, a previous draft level 1 PRA performed at Davis-Besse was utilized. This earlier work was based on the plant configuration and operating and maintenance practices prior to the June 9, 1985 loss of feedwater event. The plant was subsequently shut down for eighteen months, during which hardware and procedure changes were implemented and substantial changes were made in areas such as operator training and operating and maintenance practices. In addition to plant changes, the earlier PRA work reflected data and technology of the mid 1980's. A substantial amount of new data has been collected since that time. Similarly, improvements have been made in PRA technology, including in methods for human reliability analysis and sequence quantification. Although this earlier PRA work was available, the models used for the IPE were essentially redeveloped from the current plant information and based on current PRA technology.

Copies of updated plant drawings, the Updated Safety Analysis Report, current Technical Specifications, current operator training drills, and system operating and maintenance procedures were assembled as the basis for the system models. A listing of plant modifications implemented following the June 9, 1985 outage also aided in model development. Operator logs for cycles 5 and 6 were used for determining system maintenance unavailabilities. Copies of plant trip reports and maintenance work orders were collected and used in the data-base development. The system notebooks include the plant drawings used in their development. Also included were all references used in developing the model, including appropriate procedures and drawings, Technical Specifications, etc. A copy of the emergency procedure and applicable abnormal procedures are kept by the PRA staff for use in the PRA. In addition, system walkdowns were performed to provide the analyst with yet another look at the system components and their surroundings for considerations such as support system requirements and spatial interactions for internal flooding effects and were an integral part of the system modeling. In addition to equipment walkdowns, operator training drills observed on the plant simulator provided key insights into preferences and timing considerations associated with operator actions. All of this updated information is integrated into all aspects of the IPE. Once integration was completed, independent reviews were conducted.

One of the primary analytical tools utilized for the level 2 portion of the IPE was the MAAP-3.0B computer code. A totally plant-specific MAAP model was developed from plant drawings, vendor drawings (e.g. reactor vessel internals), on-line plant data, etc. Containment walkdowns were performed to help assure all important structures and components were properly considered in the model. Active participation in the MAAP Users Group provided up-to-date information on code enhancements and applications.

Development of the plant-specific containment event tree (CET) utilized a generic B&W plant CET as a starting point. Modifications to the tree were performed to accommodate plant differences between Davis-Besse and other B&W units, as well as to incorporate more refined phenomenological modeling in certain instances. Review of literature, previous industry level 2 analyses, NUREG-1150, and other technical reports formed much of the basis for the CET development and quantification.

These independent, in-house reviews provided added assurance of the accuracy of the IPE models. The review teams generally consisted of the applicable system engineers, appropriate design engineers, operations personnel and maintenance engineers. In addition, personnel with current or previous operating licenses (including senior reactor operators) were an integral part of the independent review. Comments received from the review teams were incorporated as appropriate. In all cases, a consensus was reached on every comment received from the review team.

In summary, the Davis-Besse IPE represents the as-built, as-operated plant through the use of up-to-date plant information, interactions with other staff members including, for example, systems engineers and licensed senior reactor operators, and the use of independent review teams.

REFERENCES FOR PART 2

1. Crutchfield, D. M. "Individual Plant Examination for Severe Accident Vulnerabilities." U.S. Nuclear Regulatory Commission Generic Letter 88-20, November 23, 1988.
2. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants.* American Nuclear Society, Institute of Electrical and Electronics Engineers, and U.S. Nuclear Regulatory Commission Report NUREG/CR-2300, January 1983.
3. Hengge, C. A., et al. *Davis-Besse Nuclear Power Station Level 1 Probabilistic Risk Assessment.* The Toledo Edison Company, November 1988.
4. Shelton, D. C. "Response to NRC Generic Letter 88-20, Individual Plant Examination for Severe Accident Vulnerabilities." Letter to U.S. Nuclear Regulatory Commission, Serial Number 1723, October 27, 1989.
5. *Individual Plant Examination: Submittal Guidance.* U.S. Nuclear Regulatory Commission Report NUREG-1335, August 1989.
6. Mosleh, A., et al. *Procedures for Treating Common Cause Failures in Safety and Reliability Studies.* U.S. Nuclear Regulatory Commission Report NUREG/CR-4780, Electric Power Research Institute Report NP-5613, January 1988.
7. Wakefield, D. J., et al. *SHARP1—A Revised Systematic Human Action Reliability Procedure.* Electric Power Research Institute Report NP-7183-SL (Interim Report), December 1990.
8. Swain, A. D. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure.* U.S. Nuclear Regulatory Commission Report NUREG/CR-4772, February 1987.
9. Parry, G. W., et al. *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment.* Electric Power Research Institute Report TR-100259 (Draft), November 1991.
10. Moieni, P., et al. *Modeling of Recovery Actions in PRAs.* Report APG #15 (NUS-5272) for Electric Power Research Institute (Draft), April 1991.
11. *MAAP-3.0B—Modular Accident Analysis Program for LWR Power Plants.* Electric Power Research Institute Report NP-7071-CCML, November 1990.
12. Kenton, M. A. and J. R. Gabor. *Recommended Sensitivity Studies for an Individual Plant Examination Using MAAP 3.0B.* Electric Power Research Institute Report (Draft), March 1991.
13. *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants.* U.S. Nuclear Regulatory Commission Report NUREG-1150, June 1989.

Part 3
FRONT-END ANALYSIS

Contents

<u>Section</u>	<u>Page</u>
List of Tables	v
List of Illustrations	vi
1 ACCIDENT SEQUENCE DELINEATION	1
1.1 Identification of Initiating Events.....	1
1.1.1 Loss-of-Coolant Accidents.....	2
1.1.2 Transient Initiators.....	12
1.1.3 Internal Floods.....	25
1.1.4 Summary of Initiating Events	30
1.2 Definition of Core-Damage Sequences	30
1.2.1 Event Trees for Loss-of-Coolant Accidents.....	35
1.2.2 Event Trees for Transient Initiators.....	83
1.2.3 Event Trees for Internal Floods.....	114
1.3 Sequence Grouping in Back-End Analysis	114
2 SYSTEMS ANALYSIS	121
2.1 Overview of Systems Analysis.....	121
2.1.1 System Modeling Guidance.....	122
2.1.2 System Dependencies.....	129
2.1.3 System Modeling for Internal Flood Analysis	132
2.2 System Descriptions	132
2.2.1 Decay Heat Removal	132
2.2.2 High Pressure Injection	138
2.2.3 Makeup and Purification	141
2.2.4 Core Flood	147
2.2.5 Reactor Coolant.....	148
2.2.6 Power Conversion	157
2.2.7 Auxiliary Feedwater.....	172
2.2.8 Containment Spray	177
2.2.9 Containment Air Cooling	178
2.2.10 Containment Isolation	186
2.2.11 Reactor Trip	188
2.2.12 Safety Features Actuation System	189
2.2.13 ECCS Room Ventilation.....	191
2.2.14 Integrated Control System	192
2.2.15 Electric Power	195
2.2.16 Service Water	201
2.2.17 Component Cooling Water	208
2.2.18 Instrument Air	213

Contents (continued)

<u>Section</u>	<u>Page</u>
3 SEQUENCE QUANTIFICATION.....	219
3.1 Data Analysis.....	219
3.1.1 Initiating Event Frequencies.....	219
3.1.2 Generic Data and Analysis	224
3.1.3 Plant-Specific Data and Analysis.....	224
3.1.4 Common-Cause Failure Data	236
3.1.5 Data Assessment of Frequencies for Internal Floods.....	241
3.2 Assessment of Human Interactions.....	241
3.2.1 Integration of Human Interactions Into Plant Models	242
3.2.2 Quantification of Human Interactions.....	246
3.2.3 Review Activities for Assessment of Human Interactions	278
3.2.4 Summary of Human Interaction Assessment	280
3.3 Recovery Analysis.....	280
3.3.1 Identification of Recovery Actions.....	281
3.3.2 Quantification of Non-Recovery Events	283
3.4 Quantification of Sequence Frequencies	285
4 RESULTS AND SCREENING PROCESS	291
4.1 Summary of Sequence Frequencies	291
4.1.1 Summary of Contributing Core-Damage Sequences	291
4.1.2 Summary of Core Damage Sequences with HRA Sensitivity	304
4.2 Summary of Plant Vulnerabilities	307
4.3 Decay Heat Removal Evaluation	308
4.4 USI and GSI Resolution.....	310
4.4.1 USI A-17, Systems Interactions in Nuclear Power Plants	311
4.4.2 GI-23, Reactor Coolant Pump Seal Failures.....	312
4.4.3 GI-105, Interfacing Systems LOCA in PWRs.....	317
4.4.4 GI-77, Flooding of Compartments by Backflow Through Floor Drains	318
4.4.5 GI-128, Electrical Power Reliability, and Related Issues	318
4.4.6 GI-143, Availability of Chilled Water Systems and Room Coolers.....	319
4.4.7 GI-153, Loss of Essential Service Water in LWRs	320
4.4.8 GI-65, Probability of Core-Melt Due to Component Cooling Water System Failures	320
REFERENCES FOR PART 3	323

List of Tables

<u>Table</u>	<u>Page</u>
1-1 Survey of Penetrations Relative to Potential for Interfacing-Systems LOCAs	6
1-2 Summary of IPE Treatment of Interfacing-Systems LOCAs from NUREG/CR-5604.....	9
1-3 Treatment of Loss-of-Coolant Accidents in Relevant PRAs.....	11
1-4 Comparison of Plant Transients from Other Relevant PRAs	14
1-5 Cross-Reference of Transient Initiators to NP-2230	26
1-6 Summary of Initiating Events for Davis-Besse.....	31
1-7 Safety Functions for Preventing Core Damage	33
1-8 Summary of Characteristics for Core-Damage Bins.....	36
1-9 Success Criteria for Large LOCA.....	38
1-10 Success Criteria for Medium LOCA.....	43
1-11 Success Criteria for Small LOCA	48
1-12 Success Criteria for a Steam Generator Tube Rupture.....	62
1-13 Success Criteria for Transients	84
1-14 Specific Success Criteria for Makeup/HPI Cooling.....	95
1-15 Assumed Effects of Relevant Factors for Failure to Trip After Loss of Feedwater	106
1-16 Success Criteria Following Failure to Trip.....	107
1-17 Summary of Core-Damage Bins and Sequence Assignments.....	115
2-1 Systems Analysis Summary	123
2-2 Overall System Dependency Matrix.....	130
3-1 Summary of Initiating Event Frequencies	221
3-2 Summary of Generic Data	225
3-3 Summary of Plant-Specific Data.....	231
3-4 Summary of Maintenance Unavailabilities.....	235
3-5 Summary of Common-Cause Data	237
3-6 Basic Cases for Pre-Initiator Human Interactions	249
3-7 Summary of Pre-Initiator (Type A) Human Interactions	255
3-8 Availability of Staff to Respond to Abnormal Events	259
3-9 Assumed Levels of Dependence for Recovery Factors Applied to Detection/Diagnosis/Decision-Making Portion of Human Interactions.....	261
3-10 Assumed Levels of Dependence for Recovery Factors Applied to Execution Portion of Human Interactions	263
3-11 Summary of Type CP Human Interactions.....	272

List of Tables (continued)

<u>Table</u>		<u>Page</u>
3-12	Summary of Type CR Human Interactions	277
3-13	Uncertainty Parameters for Human Interactions	279
3-14	Failures Comprising Example Non-Recovery Event	284
3-15	Summary of Non-Recovery Events	287
4-1	Summary of Core-Damage Frequencies	292
4-2	Summary of Frequencies for Core-Damage Bins	297

List of Illustrations

<u>Figure</u>	<u>Page</u>
1-1 Simplified Diagrams of the Potential Pathways for Interfacing-Systems LOCAs	7
1-2 Event Tree for Sequences Initiated by a Large LOCA	39
1-3 Supporting Logic for Top Events U_A and X_A of the Large LOCA Event Tree	41
1-4 Event Tree for Sequences Initiated by a Medium LOCA	44
1-5 Supporting Logic for Top Event U_M of the Medium LOCA Event Tree	46
1-6 Supporting Logic for Top Event X_M of the Medium LOCA Event Tree	46
1-7 Event Tree for Sequences Initiated by a Small LOCA	52
1-8 Supporting Logic for Top Event B_S of the Small LOCA Event Tree	53
1-9 Supporting Logic for Top Event U_S of the Small LOCA Event Tree	55
1-10 Supporting Logic for Top Event X_S of the Steam Generator Tube Rupture Event Tree	56
1-11 Event Tree for Sequences Initiated by a Steam Generator Tube Rupture	64
1-12 Supporting Logic for Top Event C_R of the Steam Generator Tube Rupture Event Tree	66
1-13 Supporting Logic for Top Event B_U of the Steam Generator Tube Rupture Event Tree	67
1-14 Supporting Logic for Top Event C_U of the Steam Generator Tube Rupture Event Tree	69
1-15 Supporting Logic for Top Event B_R of the Steam Generator Tube Rupture Event Tree	70
1-16 Supporting Logic for Top Event U_R of the Steam Generator Tube Rupture Event Tree	71
1-17 Supporting Logic for Top Event I of the Steam Generator Tube Rupture Event Tree	74
1-18 Supporting Logic for Top Event P_R of the Steam Generator Tube Rupture Event Tree	75
1-19 Supporting Logic for Top Event X_R of the Steam Generator Tube Rupture Event Tree	75
1-20 Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_H	81
1-21 Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_L	81
1-22 Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_D	82
1-23 Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_S	82
1-24 Event Tree for Sequences Initiated by a Transient	86
1-25 Supporting Logic for Top Event B_T of the Transient Event Tree	88
1-26 Supporting Logic for Top Event P of the Transient Event Tree	90

List of Illustrations (continued)

<u>Figure</u>	<u>Page</u>
1-27	Supporting Logic for Top Event Q of the Transient Event Tree 92
1-28	Supporting Logic for Top Event U_T of the Transient Event Tree 96
1-29	Supporting Logic for Top Event W of the Transient Event Tree 99
1-30	Supporting Logic for Top Event X_T of the Transient Event Tree 100
1-31	Event Tree for Sequences Involving Failure to Trip 108
1-32	Supporting Logic for Top Events B and L of the Event Tree for Failure to Trip 110
1-33	Supporting Logic for Top Event P_K of the Event Tree for Failure to Trip 111
1-34	Supporting Logic for Top Event K_2 of the Event Tree for Failure to Trip 113
2-1	Typical Table of Contents for a System Notebook 127
2-2	DHR System Functional Drawing 135
2-3	DHR System Dependencies 137
2-4	HPI System Functional Drawing 139
2-5	HPI System Dependencies 142
2-6	Makeup and Purification System Functional Drawing..... 143
2-7	Makeup and Purification System Dependencies..... 146
2-8	Core Flood Functional Drawing..... 149
2-9	Reactor Coolant System Functional Drawing 151
2-10	Reactor Coolant Pump Dependencies 154
2-11	PORV Dependencies 155
2-12	Pressurizer Spray Dependencies..... 156
2-13	Main Steam System Functional Drawing..... 159
2-14	Main Feedwater System Functional Drawing 161
2-15	Condensate System Functional Drawing 163
2-16	Main Feedwater System Dependencies..... 166
2-17	AVV Dependencies 167
2-18	MSIV Dependencies..... 168
2-19	TBV Dependencies..... 169
2-20	Condensate System Dependencies..... 170
2-21	Auxiliary Feedwater System Functional Drawing 173
2-22	Auxiliary Feedwater System Dependencies 176
2-23	Containment Spray System Functional Drawing..... 179
2-24	Containment Spray System Dependencies 181

List of Illustrations (continued)

Figure		Page
2-25	Containment Air Cooler Functional Drawing.....	183
2-26	Containment Air Cooler Dependencies.....	185
2-27	SFAS Functional Drawing.....	190
2-28	ECCS Dependencies	193
2-29	Ac Electrical One-Line Diagram.....	197
2-30	Dc & Instrumentation Ac Electrical One-Line Diagram	199
2-31	Diesel Generator Dependencies.....	202
2-32	Dc Power Dependencies	203
2-33	Service Water System Functional Drawing.....	205
2-34	Service Water System Dependencies	207
2-35	Component Cooling Water System Functional Drawing	209
2-36	Component Cooling Water System Dependencies	212
2-37	Instrument Air System Functional Drawing	215
2-38	Instrument Air System Dependencies	217
3-1	Example of the Detailed Treatment of a Type A Human Interaction	252
3-2	Example of the Treatment of a Type CP Human Interaction	264
3-3	Example Assessment of Combination of Type CP Human Interactions	270
3-4	Example Assessment for a Type CR Human Interaction	276
3-5	Distributions for Non-Recovery of Offsite Power.....	287

Section 1 ACCIDENT SEQUENCE DELINEATION

The delineation of accident sequences entails defining the general ways in which core damage might occur for Davis-Besse. This process encompasses the following activities:

- Identifying the events that could initiate an upset condition in the plant, such that the systems provided to maintain stable core cooling are challenged;
- Defining the safety functions that must be accomplished to preserve core cooling under upset conditions;
- Identifying the normal and backup systems available for accomplishing those safety functions for each type of initiating event;
- Identifying the aspects of the core-damage sequences that are important with respect to determining subsequent containment response, so that the proper interface can be made between the front-end and back-end analyses; and
- Constructing event trees to lay out the various core-damage sequences, reflecting the safety functions and the systems that accomplish those functions (and particularly the interrelationships among those systems).

The section that follows describes the process and results that led to the definition of the set of initiating events considered in the examination of Davis-Besse. Subsequent sections describe the event trees that define the core-damage sequences.

1.1 IDENTIFICATION OF INITIATING EVENTS

The identification of potential initiating events must be comprehensive if the PRA is to attain the level of completeness desired for it to yield useful results and insights. The events selected for evaluation for Davis-Besse were initially identified through a three-stage process:

- Available sources, including previous PRAs of plants with features similar to those at Davis-Besse, were reviewed to suggest candidate initiating events. This review produced a broad range of loss-of-coolant accidents (LOCAs) and transients that could be relevant for Davis-Besse.
- A thorough review was made of each system at Davis-Besse to identify events that could be of a unique nature or that would not be well characterized by analyses or operating experience for other plants. This review yielded additional initiating events involving failures of particular electrical power buses and other support systems.
- The operating experience for Davis-Besse was examined to determine if it suggested any additional types of events that were not identified elsewhere.

Individual initiators that would have the same impact on the availability of the systems that would be called upon to maintain core cooling were then grouped into categories. The

manner in which these events were identified and grouped is described in the sections that follow for LOCAs, for transient events, and for internal floods.

1.1.1 Loss-of-Coolant Accidents

A continuous range of LOCAs up to the equivalent of a double-ended rupture of a large pipe in the reactor coolant system (RCS) or a gross failure of the reactor vessel can be postulated. The task of identifying a discrete set of events that adequately characterizes this range must reflect three considerations:

- (1) The capabilities of the plant systems to maintain inventory in the RCS and core heat removal for different equivalent sizes of breaks;
- (2) The potential for LOCAs associated with particular locations to have unique effects on the systems that must respond (for example, a LOCA in one of the injection lines could make that path unavailable for makeup to the RCS); and
- (3) Differences in the impact on containment response of LOCAs of different sizes and locations.

In defining specific LOCA initiating events, two primary types of inputs were taken into account. The first reflected the definitions from existing PRAs, and particularly those for other plants using reactors designed by Babcock & Wilcox. The second was comprised of the evaluations of the capabilities of the emergency core cooling system (ECCS) specific to Davis-Besse, including those provided in the Updated Safety Analysis Report (USAR, Ref. 1). At the time this work was completed, PRAs were available for three other Babcock & Wilcox plants: the Oconee PRA (Ref. 2); the Interim Reliability Evaluation Program (IREP) study of Arkansas Nuclear One, Unit 1 (ANO-1, Ref. 3); and the preliminary PRA for Crystal River-3 (Ref. 4). LOCAs for potential consideration were divided into four general categories: small, medium, large, and rupture of the reactor vessel. In addition to these general categories, the special cases of a steam generator tube rupture (SGTR) and an interfacing-systems LOCA (i.e., a LOCA that could directly impair the core cooling systems while simultaneously presenting a breach in containment) were included.

The definitions of specific initiating events corresponding to these general categories of LOCAs are provided below. The selection of LOCA initiators is then summarized.

Large LOCA

A large LOCA is, by definition, sufficient to depressurize the RCS to the point at which reflooding of the core would be required by the core flood tanks, with makeup sustained in the longer term by the decay heat removal (DHR) system operating in the low pressure injection (LPI) mode. Decay heat would be removed through the break to the containment. Cooling via the steam generators would be neither required nor effective in removing decay heat. It is assumed that the rate of loss from the RCS would be large enough that the high pressure injection (HPI) and makeup pumps would not be capable of providing sufficient flow to keep the core covered without running out.

The break size that defines the large LOCA therefore ranges from the smallest break that could be accommodated solely by LPI and the core flood tanks, up to a double-ended rupture of a reactor coolant hot or cold leg. The large LOCA, designated as event A in this study, is therefore any break whose equivalent flow area exceeds 0.5 ft^2 (Ref. 1).

Medium LOCA

A medium LOCA would involve a smaller break that would blow down the RCS to an intermediate pressure. Makeup would typically be required from a combination of high and low pressure injection and the core flood tanks. As was the case for the large LOCA, the rate of coolant flow from the break would be sufficient to provide a pathway for the removal of decay heat, irrespective of the status of cooling by the steam generators.

With respect to the equivalent flow area, therefore, the medium LOCA is defined to encompass the range starting with the smallest break capable of accommodating the equivalent of full decay heat, up to the beginning of the range for the large LOCA. For Davis-Besse, this corresponds to a range of equivalent break areas of 0.02 to 0.5 ft^2 (Ref. 1).

It should be noted that, at the lower end of this range (approximately 0.02 to 0.1 ft^2), the success criteria are actually substantially less restrictive than are those applied later for the full range of medium breaks. While this smaller range is still adequate to remove decay heat, only HPI is needed to provide adequate makeup to the RCS. From a qualitative perspective, therefore, it is conservative to include these smaller breaks in the medium LOCA category. As a practical matter, the frequency of a medium LOCA is estimated in part based on evidence that there have been no initiating breaks in this range. Hence, it is reasonable to define one event that covers the full range to simplify the analysis; no potentially important sequences are overlooked, and the frequencies of sequences involving medium LOCAs should not be overpredicted.

Small LOCA

A leak in excess of the normal capacity of the makeup system, but too small to remove full decay heat, would constitute a small LOCA. If heat removal were available via the steam generators, the RCS would depressurize to the point at which the HPI system would be actuated automatically. Without steam-generator cooling, the break alone would not be sufficient to remove decay heat. Inventory control by the HPI and/or makeup pumps would be required, depending on the mode of core heat removal. The corresponding break range is from 0.003 to 0.02 ft^2 (Ref. 1). It should be noted that LOCAs resulting from stuck-open relief valves on the pressurizer or failures of the reactor coolant pump seals due to loss of seal cooling are modeled explicitly in the transient event tree; this category of initiating events, referred to as event S, involves only spontaneous small LOCAs (excluding SGTRs).

Steam Generator Tube Rupture

A SGTR would correspond to a break within the definition of a small LOCA, but such a break could be especially important because leakage through it would bypass the

containment and might lead to a release directly to the atmosphere. It is therefore analyzed as a separate initiating event. Potential tube failures range in severity from leaks of a few gpm to ruptures of multiple tubes, with leakage on the order of 1000 gpm. For purposes of establishing success criteria and event timing, the SGTR is assumed to correspond to a complete, double-ended rupture of a single tube.

This choice was made on the basis that a less-than-complete failure of a tube will result in much smaller leakage rates, generally within the capacity of the normal makeup system. Such an event would not place a significantly greater stress on the systems for core cooling than other shutdown events. Multiple-tube scenarios were not explicitly addressed because it is judged that they are much less likely to occur than the rupture of a single tube, and because the success criteria for systems called upon to respond are not much different from the case of one broken tube. In fact, multiple-tube failures could actually aid in depressurizing the RCS, which would be beneficial in responding to the event. Because of the near symmetry in the plant systems, it is assumed that the break occurs in steam generator 1. The SGTR is referred to as event R in this analysis.

Instrument Tube Rupture

The potential for one of the in-core instrumentation tubes to break presents a special case of a small-break LOCA. If the resulting blowdown forces on the broken tube were to cause it to whip, there is the possibility that additional tubes could be broken. With a break location below the level of the core, the discharge would be subcooled liquid for a long period of time, so that the rate at which mass would be lost would be greater than for a comparable small LOCA elsewhere in the RCS. The instrument tube break, however, would not tend to depressurize the RCS quickly.

To determine whether or not to include an in-core instrumentation tube failure as a separate LOCA initiator, a screening assessment was made. It was determined that, because of the small size of the tubes, the largest equivalent break size that could be reasonably postulated would fall within the capability of the normal makeup system (Ref. 5). Therefore, no separate LOCA category was defined for these breaks.

Interfacing-Systems LOCA

Although interfacing-systems LOCAs have not previously been assessed to be dominant contributors to the frequency of core damage, they can be significant with respect to the potential for releases of radionuclides since, by definition, they involve a bypass of containment. An effort was made to identify and evaluate all potentially important causes of interfacing-systems LOCAs. This effort also drew upon a recently published study of interfacing-systems LOCAs at a reference Babcock & Wilcox plant similar to Davis-Besse (NUREG/CR-5604, Ref. 6).

A survey was made of all piping at Davis-Besse that could communicate with the RCS and that penetrates the containment boundary. Each such penetration was screened to

determine if the potential exists for an interfacing-systems LOCA. Penetrations were eliminated from further consideration if they satisfied any of the following criteria:

- The design pressure of the system was greater than one-half the nominal RCS pressure. In such a case, it is very unlikely that a significant failure of the pressure boundary would occur, even if the system were exposed to full RCS pressure.
- The system was provided with adequate capacity for pressure relief inside containment, such that the system would not be exposed to high pressure, even if the boundary between the system and the RCS were breached.
- The pathway from the RCS to a point outside containment was via a small pipe that included substantial flow resistance (e.g., pressure-reducing orifices) and/or multiple normally-closed isolation valves.

The survey of the penetrations for systems that could communicate with the RCS is summarized in Table 1-1. Based on the survey, three types of locations were identified as meriting further evaluation:

- The injection lines for the HPI system,
- The injection lines for the DHR system, and
- The suction lines from the RCS to the DHR pumps used during normal shutdown cooling.

The configurations of these three portions of the systems are shown in Figure 1-1. Separate initiating events were identified based on the sequences of failures leading to the initial break and the potential for isolation.

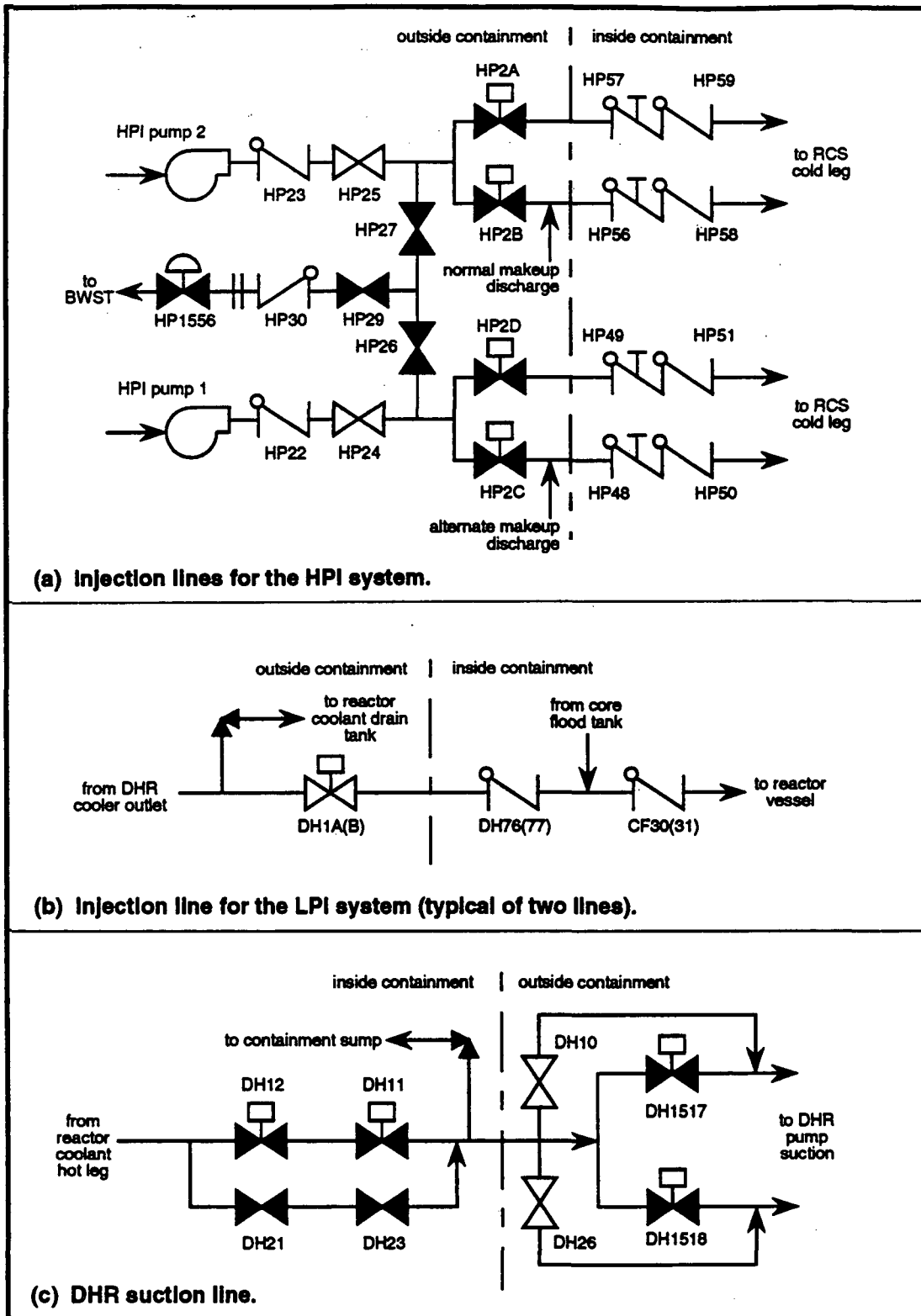
As Figure 1-1 indicates, the low-pressure portions of the HPI system are isolated from RCS pressure via two check valves inside containment, a motor-operated isolation valve that is normally closed outside containment and the check valve at the discharge of the HPI pump. The most likely break scenario would entail opening of the isolation valve at the time of its quarterly stroke test, with failure of the check valves inside containment and the pump discharge check valve such that they permitted reverse flow. Reclosure of the isolation valve would have the potential to isolate the resulting break. Therefore, one potential interfacing-systems LOCA to be evaluated is the rupture of HPI piping due to this scenario.

A somewhat analogous case exists for the injection lines for the LPI system. In this case, isolation is provided by two check valves inside containment; the low-pressure interface is upstream from the normally-open isolation valve, so that if the check valves were to fail open while the RCS was at pressure, a break could occur. As in the previous case, the loss of coolant could be stopped by closure of the isolation valve.

The DHR suction line presents several opportunities for potential interfacing-systems LOCAs. The most obvious is the potential for failure of both motor-operated or both manual valves. In the event of hardware failures of these valves, the break could occur in a portion of the low-pressure piping that could not be isolated. Thus hardware failure of the valves is

Table 1-1
Survey of Penetrations Relative to Potential for Interfacing-Systems LOCAs

Penetration Number	Design Pressure (psig)	System and Service	Qualitative Assessment
3, 4	150	Component cooling water supply for seal and letdown coolers, and return line	RCS pipes are small, with significant flow resistance. Would require failure of heat exchanger to expose system to RCS pressure. Automatic isolation valves are also provided.
14	150	Letdown line (to makeup and purification)	Pressure-reducing orifice would limit both potential for overpressurization outside containment and effective flow rate if a break occurred. Automatic containment isolation valves are also provided.
16	150	Drain to gaseous radwaste system	Small (1-inch) line, with significant pressure relief inside containment.
19, 20, 22, 50	1500	High pressure injection lines (four)	Portions of the system upstream from penetration are low pressure; isolation between high and low pressure provided by minimum of two check valves; detailed consideration desirable to address potential LOCAs.
27, 28	300	Low pressure injection lines (two)	Isolation between high and low pressure normally provided via two closed check valves; require detailed consideration.
29	300	Decay heat removal letdown line	Isolation via two normally-closed motor-operated valves in parallel with two closed manual valves; requires detailed consideration.
32	150	Miscellaneous drains to reactor coolant drain tank	Small line with large flow resistance; significant pressure relief inside containment.
39, 40	1050	Main steam lines	Addressed explicitly within the context of steam generator tube rupture.
41, 48	150	Quench tank recirculation line (in and out)	Adequate pressure relief inside containment via quench tank rupture disk.
44A, 47A, 47B, 71C	400	Core flood tank fill, drain, and vent lines	Small lines, normally isolated via closed block valves and injection check valves. Adequate pressure relief inside containment.
52 - 56	1500	Reactor coolant pump seal injection (four) and return (one) lines	Injection lines are designed for high pressure. Return lines are small, limiting effective break flow; they also contain automatic isolation valves.
74C	300	Auxiliary pressurizer spray	Multiple closed isolation valves in small line with large flow resistance.



(a) Injection lines for the HPI system.

(b) Injection line for the LPI system (typical of two lines).

(c) DHR suction line.

Figure 1-1. Simplified Diagrams of the Potential Pathways for Interfacing-Systems LOCAs

retained as one possible initiating event. There is also some potential that the suction line could be left open during startup following a cold shutdown. It would be nearly impossible to heat up the RCS with the valves left open, especially to a pressure sufficient to threaten the low-pressure piping. Furthermore, a break in this case could be isolated by closing one of the valves that had been left open. This specific possibility was examined in NUREG/CR-5604 and found to have a very small frequency. Therefore, it is not developed further. Finally, it has been postulated that the operating crew might open the suction valves in a premature attempt to initiate shutdown cooling, while the RCS was being cooled down but pressure was still high enough to threaten the integrity of the DHR system. Because of physical interlocks and administrative controls, this would seem to be a very remote possibility. It received substantial attention in NUREG/CR-5604, however, and consequently is retained as a possible initiating event.

To summarize, the following interfacing-systems LOCAs were selected for detailed assessment in this study:

- A break upstream of an HPI pump due to reverse flow through the isolation check valves, designated as event V_H ;
- A break in the LPI piping due to reverse flow through the isolation check valves in that system, designated as event V_L ;
- A break in the DHR piping due to hardware failures of the suction valves, designated as event V_D ; and
- A break in the DHR system due to premature opening of the suction valves while progressing to cold shutdown, designated as event V_S .

Table 1-2 summarizes how the events evaluated in NUREG/CR-5604 were treated in this study. As the table indicates, all of the events previously evaluated to be of any potential significance were included in this assessment. For completeness, event V_D was also evaluated in this study, although it was not addressed in NUREG/CR-5604.

Reactor Vessel Rupture

The potential exists for a rupture to occur in the reactor pressure vessel that would lead directly to core damage. This could occur if the break were large enough that the demand for makeup would exceed the capacity of the emergency core cooling systems, or if the break location would cause flow from these systems not to reach and cool the core. In general, three potential causes of failure were postulated:

- Overpressurization caused by excessive heat generation (e.g., during a failure to scram) or insufficient heat removal with inadequate pressure relief. These overpressurization events were modeled explicitly in the sequence logic where appropriate.
- Spontaneous failure of the reactor vessel due to "random" causes, such as the existence of an undetected flaw that grows due to normal stresses until a rupture develops. Despite the very low frequency of such events, the potential is retained for consideration in this analysis.

Table 1-2
Summary of IPE Treatment of Interfacing-Systems LOCAs
from NUREG/CR-5604

NUREG/CR-5604 Sequence	Description of Scenario	Treatment in IPE
MU&P (1)	Break upstream of HPI pump when isolation check valves in line used for normal makeup fail to close	Evaluated explicitly in the context of event V_H
MU&P (2)	Break in piping to BWST when test recirculation valves left open and isolation check valves in line used for normal makeup fail to close	Not explicitly considered due to additional multiple failures required; extremely low frequency assessed in NUREG/CR-5604
HPI (1)	Break upstream of HPI pump when isolation check valves in other injection lines fail to close	Evaluated explicitly in the context of event V_H
HPI (2)	Break in piping to BWST when test recirculation valves left open and isolation check valves in other injection lines fail to close	Not explicitly considered due to additional multiple failures required; extremely low frequency assessed in NUREG/CR-5604
DHR-SU	Break in DHR system due to failure to close DHR suction valves during plant heatup	Not explicitly considered due to difficulty in achieving heatup with valves open; very low frequency assessed in NUREG/CR-5604
DHR-SD	Break in DHR system due to opening of suction valves during cooldown while RCS pressure still high	Evaluated explicitly in the context of event V_S
LPI	Break in DHR system due to reverse flow through isolation check valves in injection line	Evaluated explicitly in the context of event V_L
Not analyzed	Break in DHR suction piping due to hardware failure of suction isolation valves	Evaluated explicitly as event V_D due to potential for comparable or higher frequency than some events that were evaluated in detail in NUREG/CR-5604

- Pressurized thermal shock, which could lead to brittle fracture of the vessel. Based on previous analyses (Refs. 7 and 8), the frequency of such an event can be conservatively estimated to be on the order of 5×10^{-7} per year. It is therefore judged to be adequate to subsume the potential for failure by this mode into the general category of reactor vessel failure due to all causes.

Gross failure of the reactor vessel is therefore retained as a separate initiating event. It is designated as event A_v in this study.

Summary of LOCA Initiators

Nine initiating events involving breaches of RCS integrity were identified for consideration in this analysis. The selection of these events was compared to the sets of LOCAs included in the three other available PRAs of Babcock & Wilcox plants. The comparison is summarized in Table 1-3. The comparison illustrates that the treatment of LOCAs for Davis-Besse is generally consistent with that for other plants, although there are some differences.

The updated Oconee PRA (Ref. 2) included an analysis of three general LOCAs, large, medium, and small. The functional definitions of these breaks are equivalent to those used in the Davis-Besse IPE, although there are some differences in specific break sizes that result from different designs and capacities for the injection systems.

The Crystal River-3 PRA (Ref. 4) used the breakdown from the original Oconee PRA (Ref. 9), which included only the large and small LOCA categories. This breakdown was based on the judgment that the unique success criteria for a medium LOCA (i.e., requiring a combination of high and low pressure injection and a core flood tank), which were drawn from licensing-basis calculations, were conservative. Because of this, and because the frequency was judged to be bounded by that for large LOCAs, a separate initiating event was not defined. In this analysis for Davis-Besse, however, it was judged to be prudent to retain the separate category for the insights that might be obtained.

The ANO-1 IREP (Ref. 3) considered six general categories of LOCAs, in contrast to the two evaluated originally for Oconee and for Crystal River-3, and the three included in this study and in the updated Oconee PRA. The very small category (breaks less than 0.008 ft² equivalent diameter) was distinguished by the requirement for only one of three HPI pumps for makeup, plus either operation of a pressurizer safety/relief valve (PSV) or availability of emergency feedwater (EFW) for heat removal. It was assumed that recirculation from the sump was not needed provided the reactor could be cooled down using EFW to the point at which shutdown cooling via the DHR system could be established. As is discussed later in Section 2.2, the makeup and HPI systems are of a different design for Davis-Besse, and the success criteria are therefore different as well. The small category (0.008 to 0.015 ft²) for ANO-1 corresponds more closely to the small category for Davis-Besse. A slightly larger category (0.015 to 0.087 ft²) was also defined, with success criteria less restrictive than either smaller or larger breaks. As noted earlier, this break was subsumed into the medium category for Davis-Besse. The next larger break range for ANO-1 (0.087 to 0.55 ft²) is functionally

**Table 1-3
Treatment of Loss-of-Coolant Accidents in Relevant PRAs**

Event	Oconee PRA	ANO-1 IREP	Crystal River-3 PRA	Davis-Besse IPE
Large LOCA	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree (event A)
Large intermediate LOCA	Not analyzed separately; included with large LOCA	Analyzed explicitly using separate event tree	Not analyzed separately; included with large LOCA	Not analyzed separately; included with large LOCA
Medium LOCA	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree	Not analyzed separately; included with large LOCA	Analyzed explicitly using separate event tree (event M)
Small intermediate LOCA	Not analyzed separately; included with small LOCA	Analyzed explicitly using separate event tree	Not analyzed separately; included with small LOCA	Not analyzed separately; included with intermediate LOCA
Small LOCA	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree (event S)
Very small LOCA	Not analyzed separately; included with small LOCA	Analyzed explicitly using separate event tree	Not analyzed separately; included with small LOCA	Not analyzed separately; included with small LOCA
Steam generator tube rupture	Analyzed explicitly using separate event tree	Not explicitly considered	Analyzed explicitly using separate event tree	Analyzed explicitly using separate event tree (event R)
Reactor vessel rupture	Screening analysis of initiating frequency	Not explicitly considered	Results from analysis in Oconee PRA adapted	Limited-scope analysis of event frequency (event Av)
Interfacing-systems LOCA	Detailed analysis of initiating frequency	Detailed analysis of initiating frequency	Assessed qualitatively to be a small contributor to core-damage frequency	Analyzed explicitly (events V _H , V _L , V _S , and V _D)
Instrument tube LOCA	Not considered	Not considered	Scoping analysis with some quantification	Screened out by scoping analysis

equivalent to the medium break for Davis-Besse. Another intermediate break size was defined for ANO-1 (0.55 to 1.0 ft²). The only difference between this event and the large LOCA was that only one of two core flood tanks was needed for the smaller size, rather than two for the large LOCA. Because the core flood tanks comprise a reliable passive system, it was judged to be unnecessary to subdivide the large LOCA to account for the more specific success criteria.

With regard to the special categories of events, nearly all of the studies included at least some consideration of a SGTR, a reactor vessel rupture, and interfacing-systems LOCAs. It seems evident that these events should be evaluated for purposes of completeness, particularly in a study that addresses the potential for offsite releases. The potential for an in-core instrument tube LOCA has been considered in the past only for Crystal River-3, and in that case only in a screening assessment with limited quantification. As noted previously, an evaluation was made that indicated that treatment of an in-core instrument tube break separate from other small LOCAs was not warranted for Davis-Besse.

With regard to special locations, the potential was identified for LOCAs that involved the lines dedicated to the safety injection systems. Specific initiating events to address these lines were not defined separately. Instead, specific events to address the effects of such LOCAs were included in the fault-tree models for the systems that could be affected (HPI, LPI, and the core flood tanks). These events represent failures of the applicable portions of the systems conditional on the occurrence of the more general LOCA categories that are relevant.

In summary, it is judged that the definition of LOCAs as initiating events is adequately comprehensive for the Davis-Besse IPE, based on a review of other relevant PRAs and an examination of the specific features of the plant design.

1.1.2 Transient Initiators

Transients are events that lead to a plant trip but that do not directly cause a breach in the integrity of the RCS. A separate transient initiating event was defined for each case in which there was cause for a reactor trip (either automatically or due to anticipated human action), and there was a unique effect on the ability of the plant systems to respond. The initiating events described in this section are actually classes of events that include a variety of plant upsets. The upset events for each group have the same general effects on the availability of plant systems, and hence are grouped together for the convenience of the analysis.

As was the case for LOCAs, the first step was to identify the transient initiators considered in PRAs for other Babcock & Wilcox plants and to evaluate their applicability to Davis-Besse. This is a particularly valuable first step, since these PRAs have already considered the applicability of "generic" initiators as they are defined in other sources, such as the broad spectrum of events covered in the Electric Power Research Institute (EPRI) report NP-2230 (Ref. 10). After identifying the relevance of these events for Davis-Besse, a system-by-system review was made, with particular emphasis on support systems, to identify events

unique or specific to Davis-Besse. Finally, the list of transients selected for analysis was reviewed against actual operating experience at Davis-Besse and against the extensive list of events in NP-2230, as well as other generic summaries of operating experience to ensure that no significant events were overlooked.

Transients with Direct Effects on Plant Operation

The transient initiators considered in the three available PRAs that were judged to be most relevant to Davis-Besse were reviewed relative to Davis-Besse system configurations and plant response. The results for transients other than those involving support systems are summarized in Table 1-4. The relevance of each event for Davis-Besse is discussed below.

Reactor/turbine trip. The first event considered represents a broad range of transients that lead to a reactor trip, but that have no direct or unique impact on the need for or the availability of systems that must respond to maintain core cooling. It is generally not necessary to distinguish between a reactor trip and a turbine trip as the initiating event, since a turbine trip will initiate an automatic reactor trip via the anticipatory reactor trip system (ARTS) whenever the plant is operating above 40% full power (Ref. 11). Therefore, a reactor and turbine trip occur nearly simultaneously, irrespective of which occurred first. Following the trip, main feedwater (MFW) would generally continue to maintain level in the steam generators, with heat transferred from the RCS then removed to the main condenser via the turbine bypass valves. This event is addressed explicitly and is referred to as event T₁.

Loss of main feedwater. Loss of MFW encompasses all events in which the ability to maintain cooling by supplying MFW to the steam generators is lost as a direct result of the initiating event, but no other systems needed following the reactor trip are affected. For Davis-Besse, this event includes failures within the MFW system itself; control-system faults that only affect MFW; failures affecting the condensate pumps; and loss of condenser vacuum, which would cause both a turbine trip and tripping of the MFW pumps. If the auxiliary feedwater (AFW) system is available, the event would generally progress in much the same manner as other reactor or turbine trips. This initiator is included as event T₂. In the original Oconee PRA (Ref. 9), a separate initiating event was included to reflect the potential that an upset could occur within the MFW system that would lead to a plant trip, but that (barring additional failures), sufficient MFW flow could continue to be available to maintain core cooling. In that study, a detailed fault tree representing failure of the MFW system following a plant trip was constructed. An initiating event reflecting partial loss of the system was defined to allow the increased conditional unavailability of the system under such conditions to be accounted for properly. For Davis-Besse, the unavailability of MFW following a plant trip was estimated based on plant-specific, system-level experience. Because this unavailability reflects all causes of loss of MFW, it is not necessary to account separately for trips that initially involve partial losses, after which the system fails completely. This is consistent with the practice in the updated Oconee PRA (Ref. 2) as well, in which no separate initiator was included. A separate initiator is therefore not defined for Davis-Besse.

**Table 1-4
Comparison of Plant Transients from Other Relevant PRAs**

Event	Oconee PRA	ANO-1 IREP	Crystal River-3 PRA	Davis-Besse IPE
Reactor/turbine trip	Analyzed explicitly	Analyzed as trip with all systems available	Analyzed explicitly	Analyzed explicitly (event T ₁)
Total loss of feedwater	Analyzed explicitly	Analyzed explicitly	Analyzed explicitly as loss of PCS	Analyzed explicitly (event T ₂)
Partial loss of feedwater	Analyzed explicitly in original; deleted in update	Included with reactor/turbine trip	Included with reactor/turbine trip	Included in reactor/turbine trip
Loss of condenser vacuum	Analyzed explicitly	Included with loss of feedwater	Included with loss of PCS	Included with loss of feedwater
Loss of offsite power	Analyzed explicitly	Analyzed explicitly	Analyzed explicitly	Analyzed explicitly (event T ₃)
Spurious engineered safeguards signal	Analyzed explicitly	Not explicitly considered	Analyzed explicitly	Analyzed explicitly (event T ₄)
Excessive feedwater	Analyzed explicitly	Included in loss of PCS	Analyzed explicitly	Included with loss of feedwater
Feedwater line break	Analyzed explicitly	Not explicitly considered	Analyzed explicitly	Analyzed explicitly (event T ₅)
Steam line break	Analyzed explicitly	Considered and eliminated	Included with excessive feedwater	Included with feedwater line breaks
Spurious low pressurizer pressure signal	Analyzed explicitly in original; deleted in update	Not explicitly considered	Analyzed explicitly	Considered and eliminated
Loss of power to reactor control systems	Loss of power for integrated control system (ICS) analyzed explicitly	Considered and eliminated	Considered and eliminated	Analyzed explicitly for key power supplies (events T ₇ , T ₈ , and T ₉)

Loss of condenser vacuum. Loss of condenser vacuum was evaluated as a separate initiating event for the Oconee PRA, since such an event would prevent using the turbine-bypass valves to transfer decay heat to the main condenser (in addition to causing the loss of main feedwater). For Babcock & Wilcox plants other than Oconee, however, there are both main steam relief valves and automatic atmospheric vent valves that permit rejection of steam. This event has therefore not been analyzed separately for other plants. The only event for which heat removal via the condenser is potentially important is a SGTR. Loss of condenser vacuum is therefore grouped with the loss of MFW initiator, and is not modeled separately.

Loss of offsite power. Loss of offsite power is a potentially important initiating event, because it renders main feedwater and many other non-safety systems unavailable. It also creates a demand for the emergency diesel generators to supply power for safety systems. A corresponding initiator is included in all of the PRAs. In the Oconee PRA, three separate initiators involving loss of offsite power were included to reflect site-specific aspects of the emergency power configuration (i.e., one pathway for emergency power, which is provided by hydro-electric units at Oconee, is through a main switchyard) and to account for differences in recovery potential. The loss of offsite power is included in this study as event T₃. In estimating the frequency and recovery potential for loss of offsite power, the initiator is further broken down into three primary types of losses: plant-centered (i.e., due to failures of the switchyard, transformers, etc.), grid-centered, and weather-related. These three causes are all considered within the context of the single initiating event T₃.

Spurious engineered safeguards signal. For all operating Babcock & Wilcox plants except Davis-Besse, the HPI system is also the system used for normal makeup to the RCS. The HPI pumps at those plants therefore have a shutoff head well above the normal RCS operating pressure. A spurious actuation in the safety injection mode could cause the HPI system to fill the pressurizer and raise RCS pressure to the setpoints for the pressurizer relief valves. The potential that this could lead to a small LOCA was the primary motivation for including the spurious signal as an initiating event.

For Davis-Besse, the HPI system is separate from the makeup system. The shutoff head for the HPI pumps is 1600 psig, so that even if the HPI system were to be actuated spuriously, there would be no direct effect on the RCS. Other effects of a spurious initiation of the safety features actuation system (SFAS) could, however, be of interest for Davis-Besse. Upon SFAS actuation, portions of the service water and component cooling water (CCW) systems would be reconfigured. The flow of CCW to the thermal barrier coolers for the seals in the reactor coolant pumps (RCPs) would also be isolated, which could increase the potential for a seal LOCA. A unique initiating event was therefore retained for spurious SFAS initiation, and it is designated as event T₄.

Excessive feedwater. The potential for a plant trip due to excessive feedwater was included for some PRAs for much the same reason as was the spurious actuation of the engineered safeguards systems: the potential existed for the resulting overcooling to cause

RCS pressure to drop to the setpoint for initiating HPI, which could then repressurize the system to the setpoints for the relief valves. For Davis-Besse, the overcooling would not typically be significant enough to depressurize the RCS below the setpoint for the SFAS system before a loss of MFW resulted. Moreover, as noted previously, the same concern does not exist with respect to pressurizing the RCS by HPI flow. Excessive feedwater was therefore included with the loss of MFW category, and not treated as a separate initiating event.

Feedwater and steam line breaks. Breaks in the feedwater or main steam lines were included as initiating events in some previous PRAs for Babcock & Wilcox plants due to a variety of plant-specific considerations. For Davis-Besse, several effects were of potential interest with regard to such breaks:

- A break in either the feedwater or main steam line could render one of the two steam generators unavailable.
- The steam/feedwater rupture control system (SFRCS) would actuate, causing the affected steam generator to be isolated, and reconfiguring the AFW system to feed only the intact generator.
- Depending on the nature of any additional failures, it is possible that the steam supplies for the two turbine-driven AFW pumps could be affected.

Because the effects of overcooling events do not, for the reasons outlined above, present a particularly serious concern for Davis-Besse, the unavailability of one or both of the steam generators is of primary interest with respect to a line break. Since a break in either a feedwater line or a steam line has similar consequences with respect to the availability of the steam generators, it was decided to combine the two types of breaks into one initiating event category. Because of the near symmetry of the plant systems, the model was developed assuming steam generator 1 was the affected generator. The initiator is defined as event T₅.

Loss of RCS makeup. During normal operation, a makeup pump operates to provide inventory control for the RCS, purification of reactor coolant, and seal injection for the RCPs. A standby pump is provided in the event the operating pump is unable to provide flow. If flow were not available from either of these pumps, the procedures instruct the operators to initiate a plant shutdown (Ref. 12). A reactor trip (prior to the controlled shutdown) would not occur unless RCS leakage was sufficiently large to make it impossible to maintain pressurizer level.

The makeup pumps also provide the means for accomplishing feed-and-bleed cooling in the event that there is a total loss of feedwater to the steam generators. Because of this, and because of the potential importance of a LOCA due to failure of cooling for the RCP seals, it was concluded that loss of makeup should be included as an initiating event. This initiator is designated as event T₆. The assumption was made that the loss of makeup would lead to a reactor trip. Since the systems that must function to preserve decay heat removal following a controlled shutdown with no makeup are sufficiently similar to those that must

operate following a plant trip with no makeup, this assumption is conservative, and is justified because of the degree of simplification it permits in the modeling process.

The need to address an event that involved only a loss of seal injection was considered. If the makeup system itself remained available (e.g., to respond to a possible seal LOCA if CCW subsequently failed), the loss of seal injection alone would have minimal impact on plant safety. It was judged, therefore, that the effects of such an event would be less important than the total loss of RCS makeup reflected by event T₆, and a separate initiator was not defined.

Spurious low pressurizer pressure signal. The Oconee PRA also included a unique failure within the integrated control system (ICS) that could have the effect of making the pilot-operated relief valve (PORV) unavailable for automatic pressure relief at the same time that it caused the pressurizer heaters to energize, the main feedwater system to run back, and the control rod drive system to attempt to withdraw the control rods. Such an event could lead to a reactor trip on high RCS pressure, and it was judged that there would be an increased likelihood of challenging the PSVs, with the resulting potential for inducing a small LOCA.

Subsequently, however, more careful investigation was made of the plant response to such an event. The pressurization would occur very slowly, and there would be significant opportunity for operator intervention, either before the reactor tripped or before the setpoint for the PSVs was reached. In addition, the frequency for such an event would be significantly less than that of more severe challenges, such as the loss of MFW. Therefore, this event has not been included in the updated Oconee PRA. For the same reasons, an analogous event was not addressed explicitly for Davis-Besse.

Loss of power to the integrated control system. Various losses of power to the ICS and non-nuclear instrumentation (NNI) were considered as potential initiating events. This evaluation benefited from a failure modes and effects analysis (FMEA) completed previously for Davis-Besse (Ref. 13).

With respect to the power supplies for the ICS itself, the only failures of significant interest with respect to the IPE would be the loss of MFW. It was therefore judged that it was not necessary to model loss of either the ac or the dc supply for the ICS as a separate initiator.

Failures affecting the NNI could have more critical effects. The most important effect of a loss of ac power for NNI-X would be for the controllers for normal makeup and for seal injection to fail "as-is". Operating procedures instruct the operators to trip the reactor and to initiate AFW to ensure that adequate secondary heat removal is sustained. Loss of ac power for NNI-Y would result primarily in the unavailability of certain control indications associated with the makeup system. It would therefore appear to be of more interest to model the effects of loss of NNI-X ac power.

For a loss of ac power to either NNI-X or NNI-Y to occur, however, a unique set of events would have to take place. Power is supplied to the NNI system from either of two

buses, YAU and YBU. An automatic transfer switch is provided to select the alternative source in the event that the one being used is lost. Loss of ac power would therefore occur only if there were a fault within the transfer switch itself, or if there were a fault in one of the ac loads and its associated fuse failed to function. On the other hand, loss of either YAU or YBU would have effects on systems beyond the NNI. It is therefore judged to be of more interest to evaluate the loss of each of these buses as separate initiating events, rather than the less likely loss of NNI ac power. The losses of these two buses are designated as events T7 and T8, respectively.

Loss of dc power for NNI-X would cause the loss of automatic pressure control for the RCS (via the pressurizer sprays and heaters and the PORV), and would have additional effects within the makeup system. It was therefore decided to treat this event as a unique initiator, denoted by event T9. Loss of dc power for NNI-Y would not have important effects on the systems required for core cooling, and was therefore not selected to be an initiating event.

The primary effect of loss of either ac or dc power to the ICS itself would be to supply inadequate MFW to the steam generators. These failures are therefore subsumed into event T2.

Support-System Initiators

A careful review was made of the support systems that are needed during plant operation and that serve as important auxiliaries following plant trips to identify any that could constitute a unique initiating event for Davis-Besse. Support-system initiators that have been addressed in earlier studies of Babcock & Wilcox plants include the following:

- Loss of service water,
- Loss of power to a major ac bus,
- Loss of a dc power bus, and
- Loss of instrument air.

Additional support systems that could be of interest are the heating, ventilating, and air conditioning (HVAC) systems and CCW. With the prior treatment of these events as background information, a system-by-system review was made to determine the need for including specific events. This review is summarized below.

Loss of service water. At Davis-Besse, two trains of service water are normally operating. These are designated as "primary" and "secondary" and have the following major loads:

Primary service water loop

- The heat exchanger in the operating CCW train. This system is, in turn, responsible for cooling a variety of important loads, including the seals for

the RCPs, motors and bearings for a number of important pumps, and, if they are started, the emergency diesel generators.

- The room coolers for two of the rooms housing ECCS equipment.
- One of the two normally-operating containment air coolers.

Secondary service water loop

- The heat exchangers for the turbine plant cooling water (TPCW) system, which provides auxiliary cooling for the feedwater and condensate systems, the main turbine-generator, etc.
- The additional ECCS room coolers.
- The other normally-operating containment air cooler.

If service water flow were to be lost to the CCW heat exchanger (i.e., the primary loop), the following chain of events would occur (Ref. 14):

- Attempts would be made to restore service water to the affected loop, by restarting the pump if it had tripped, or by aligning the third service water pump or the separate backup service water pump to supply flow.
- The affected train of CCW would begin to heat up, until the pump tripped on high temperature.
- Upon tripping of the operating CCW pump, a second CCW pump would start, and the non-essential loads would be automatically shifted to this second pump.
- The additional flow required of train 2 of service water to cool the new CCW load could be sufficient to cause service water header pressure to drop below 50 psig; at this point, the non-essential service water loads (i.e., TPCW) would be transferred to the circulating water system.

Therefore, the loss of the primary loop would not necessarily lead to a plant trip. If the TPCW loads continued to be cooled by circulating water and if the second CCW train provided cooling of the non-essential loads, plant operation would not be interrupted. Failure of either of these functions, however, would result in a plant trip with one train of service water unavailable. If the second CCW train were to fail, a trip would be required due to the loss of cooling to such components as the reactor coolant pumps and the control rod drive. If the TPCW system were to lose cooling from service water and circulating water failed to provide automatic backup cooling, a turbine trip and loss of main feedwater could result.

To account for these potential failures, and to ensure that dependencies were tracked properly, the effects of a plant trip that could result from loss of the primary train of service water were incorporated into the fault trees for appropriate systems by a small logic model, rather than by a single primary event as is the case for most initiators. The logic model is comprised of the following elements:

Plant trip due to loss of primary train of service water = loss of primary train of service water AND failure to swap cooling to the standby train of CCW OR failure of circulating water to provide backup cooling to TPCW

Loss of the primary train of service water is quantified as if it were an initiating event, although it does not ensure that there will be a plant trip. It is identified in the fault trees and sequences as event T₁₀. The two additional failures represented in the expression above are developed further in the fault-tree models. This treatment ensures that the potential for a plant trip is properly reflected in the sequence cut sets.

Loss of the secondary loop of service water flow could lead to a similar attempt at restoration, and possibly to a trip if cooling could not be restored to the TPCW system by either service water or condenser circulating water. There would be no immediate impact on the CCW system, although in the event of a subsequent failure of the operating CCW train, the backup train would not be available without realignment by the operators.

The loss of the secondary service water loop is therefore included as an initiating event as well, designated as event T₁₁. As for the loss of the primary train, no trip should occur if TPCW continues to be cooled by circulating water. An analogous model was therefore developed, with a plant trip occurring if the secondary loop of service water is lost and circulating water fails to provide backup cooling to TPCW.

A total loss of service water would cause a plant trip if flow could not be restored in a timely manner. The restoration efforts would focus on using the third service water pump or the backup service water pump; isolating any breaks in the system; and using the circulating water system as an alternative means of cooling the secondary loads. Although there are several options for the operators to restore service water flow, it is expected that a plant trip would usually occur before recovery could be accomplished. The loss of both normally-operating trains of service water is therefore included as an initiating event as well.

Consistent with normal operating practices, it is assumed that train 1 of service water is normally serving the primary loads (via pump 1-3) with train 2 supplying the secondary loop (using pump 1-2). As indicated above, losses of the respective trains are modeled as events T₁₀ and T₁₁. Event T₁₂ was included to reflect the potential for a total loss of service water, defined as loss of flow from both normally-operating trains.

Loss of component cooling water. As noted above, CCW provides cooling for several important loads. If the operating pump trips, a standby pump should start automatically and assume its loads. The operators are instructed to ensure that the non-essential loads required for normal operation are cooled and are isolated from the loop in which flow has been lost (Ref. 15). They are also instructed to isolate the essential loads associated with the lost loop, to ensure that adequate flow is available from the second CCW

pump. Cross-connections may be used to supply individual essential loads in the opposite division if their operation is necessary.

If the standby pump started properly, the CCW heat load would be shifted to the service water loop that had previously been cooling the secondary loads. The effect would be similar to a loss of the primary service water loop; the additional service water flow required to cool the CCW heat exchanger could lead to isolating the cooling water to the TPCW system and a demand for cooling from the circulating water system. If cooling were not available, the plant would trip. Loss of the operating train of CCW is therefore considered as a distinct initiating event. In the fault-tree models, the failure of circulating water to provide cooling to the TPCW system is also included (as was the case for service water initiator T₁₁), since if cooling succeeded there would be no plant trip. The loss of cooling in the normally-operating loop (assumed for the analysis to be train 1) is designated as event T₁₃.

The total loss of CCW flow would lead to a manual reactor trip, and tripping of the RCPs and makeup pumps (Ref. 15). After ensuring that cooling was available to the steam generators, the focus would be on restoring component cooling water. The total loss of CCW was modeled as event T₁₄.

Loss of turbine-plant cooling water. Cooling for the main turbine and main feedwater system is provided by TPCW. TPCW also provides cooling for some of the air compressors needed to sustain plant operation. A loss of TPCW would therefore lead to a plant trip. The effects, however, would generally be subsumed by a loss of instrument air. A separate initiating event for loss of TPCW is therefore not needed.

Loss of power to a major ac bus. A fault on an important 4160 vac bus could lead to a plant trip and the unavailability of all of the equipment normally supplied from that bus. Buses C1 and D1 supply the safety-related loads for Davis-Besse. During normal operation, each of these buses typically supplies different loads (e.g., bus C1 may supply the operating CCW pump, while bus D1 may supply the pump providing makeup to the RCS). Therefore, failure of each bus was modeled by a separate initiating event. The losses of bus C1 and bus D1 are designated as events T₁₅ and T₁₆, respectively.

Loss of dc power bus. The loss of a vital dc bus could also lead to a plant trip and to the loss of power to important loads (such as the closing power for 4160 vac breakers needed to start major system pumps). There are four safety-related 125 vdc buses (D1P, D1N, D2P, and D2N) serving the two safety divisions. The loss of either bus D1P or bus D2P would have the most significant effect on plant systems. Among the effects of losses of these buses are those listed below (Refs. 16 and 17):

Loss of bus D1P

- Two of three condensate pumps will trip due to deenergization of the auxiliary relays for the condenser low-level switch; this may cause a loss of main feedwater.

- If AFW is actuated, the valve controlling level for steam generator 1 will fail fully open, causing overcooling of the RCS. Remote control (from the control room) of the turbine for the AFW pump feeding this generator will also be lost; if the operators take no action, overfilling of the steam generator could lead to carryover of water that could affect operation of both turbine-driven AFW pumps.
- Breakers will fail as-is for a number of pumps, including the loop 1 CCW and service water pumps, and makeup pump 1, and for several buses.
- Emergency diesel generator 1 will be unavailable unless control power is transferred to another source.
- Seal injection will be lost to two of the four RCPs.

Loss of bus D2P

- The main turbine will trip.
- Seal return for the RCPs will be isolated. If the RCPs are not tripped, it is assumed that a seal LOCA may result. Tripping of two of the RCPs would require local operation of their breakers, since control power would not be available to permit operation from the control room.
- Control valves for AFW to steam generator 2 will fail open as described for loss of bus D1P.
- Breakers will fail as-is for the pumps and buses analogous to those described for loss of bus D1P.
- Emergency diesel generator 2 will be unavailable unless control power is transferred to another source.
- Seal injection will be lost to two of the four RCPs.

The losses of buses D1N and D2N have far less significant effects on plant operation (Refs. 18 and 19). Losses of bus D1P and of bus D2P were therefore selected as initiating events that merited specific treatment. They are designated as events T₁₇ and T₁₈, respectively.

Loss of instrument air. Several systems of interest with respect to core cooling use air-operated valves for isolation and control purposes. Based on consideration of the design of the instrument air system and on a review of previous analyses of air-system problems (Ref. 20), it was judged that three types of upset events were of potential concern:

- Rapid loss of pressure in the instrument air system, so that valves and instruments would tend to go to their failed positions.
- Slow loss of instrument air pressure. This could be important with respect to air-operated valves for which dedicated backup accumulators are available. Normally in such cases, the instrument air system is isolated from the accumulator by a check valve, so that if there is a reduction in air-system pressure, the check valve will seat and pressure will be maintained by the accumulator. If the depressurization occurs slowly enough, however, the check valve may not seat completely, allowing the

compressed gas in the accumulator to bleed back into the instrument air system. The use of the air-operated valve may therefore be lost.

- Contamination in the instrument air system. This is a potentially important cause for loss of instrument air, because there have been experiences at other plants in which the contaminant has caused at least some of the air-operated valves to fail "as-is" in positions other than those intended by design to be the failed state.

A survey was made of the air-operated valves in the systems important with respect to core cooling. With regard to the potential for a total loss of pressure, several important effects would be realized. Loss of instrument air pressure would lead to a loss of MFW. Most significant among the other effects would be the loss of seal return, which would necessitate tripping the RCPs to avoid a failure of the seals. Opening of the valves associated with the decay heat coolers could also be important, depending on the status of the DHR system. If the cooler outlet valves failed fully open, it is possible that the CCW pumps could experience runout conditions (although the valves are equipped with mechanical stops to prevent them from going more than 45% open upon loss of air). The same type of concern could arise for the service water supply to the CCW heat exchangers, if the isolation valve for the non-essential header should fail to close. It is apparent that an event representing loss of instrument air should be evaluated; such an event is denoted as event T19.

With respect to slow depressurization of the instrument air system, a relatively small number of valves are equipped with backup accumulators. The most important effect would be to lose the ability to control steam pressure using the atmospheric vent valves. This is important, however, only for sequences involving a steam generator tube rupture; otherwise, steaming through the spring-loaded main steam relief valves is an acceptable means of heat removal. Moreover, the atmospheric vent valves and turbine bypass valves are equipped with handwheels to permit them to be operated manually. Therefore, separate modeling for this failure mode does not appear to be warranted.

The question of the potential for contamination to lead to a loss of pressure while causing valves to remain in their pre-transient states is less clear. It is important to note that relatively few air-operated valves are required to change state to satisfy safety functions. Moreover, although contamination has led to the failure of multiple valves in past experience at other plants, it does not appear that events widespread enough to cause failure of large numbers of valves or valves in widely separated areas of the plant have occurred. It appears to be most appropriate to consider contamination as one possible cause of common-cause failure of the valves, and not to include a separate initiating event.

Loss of HVAC. Maintaining the proper room environment is necessary for certain types of equipment to continue to function. A review of the critical areas at Davis-Besse indicated that cooling for particular rooms is typically redundant, and that the HVAC systems are distributed (i.e., there is not a single cooling system or chilled-water system that provides critical cooling for large sections of the plant). The principle areas requiring HVAC are summarized in the following discussion.

- **Main control room.** The control room is served by a normal HVAC system, with backup by the control room emergency ventilation system. In the event that there is insufficient cooling available, procedures explicitly describe steps to take to reduce the heat load in the room and, when necessary, to achieve an orderly shutdown. Because of the redundant systems and the presence of operators to detect and correct an abnormal situation almost immediately, loss of HVAC to this area does not merit treatment as a separate initiating event.
- **ECCS pump rooms.** In the event of a demand for function of the high or low pressure injection pumps, increased heat load in the rooms housing the pumps would create a demand for room cooling. Room cooling is supplied by heat exchangers, with service water flowing continuously through the coils, and fans to provide circulation and forced flow across the cooling coils (the fans are normally in standby and are actuated on high room temperature). A loss of ECCS room cooling would not initiate a plant trip, although it could render the systems incapable of responding to other initiating events. Failures associated with room cooling are therefore developed in the fault-tree logic for the systems, but they do not constitute separate initiating events.
- **Makeup pump room.** The room housing the makeup pumps is served by a dedicated cooling system. Failure of room cooling is explicitly modeled as a cause of failure for the makeup system when operation of two makeup pumps is required (e.g., for makeup/HPI cooling). The heat load when only one pump is operating (e.g., during normal operation) is such that room cooling is not needed. Therefore, failure of room cooling is not included as a cause of loss of makeup as an initiating event.
- **High-voltage switchgear rooms.** The rooms housing the 4 kv switchgear are served by a normal HVAC system. Failures of the buses in these rooms themselves are considered as initiating events, but it is not expected that a loss of HVAC would lead to failures that would deenergize the bus. Moreover, HVAC is not required to function following a plant trip. Therefore, HVAC is not modeled for these rooms.
- **Low-voltage switchgear rooms.** The rooms housing low-voltage electrical equipment (low-voltage ac and dc buses, inverters, etc.) are served by separate normal and standby HVAC systems. For a plant trip to result from failure of cooling in one of these rooms, both systems would have to fail. Both systems are included in the model for failures of the relevant loads in the room. The most important causes of failure of the normal system include loss of offsite power and loss of instrument air. Both of these are already included as initiating events, and failure of the standby system is modeled for all relevant events. The effects of loss of both systems are also separately reflected by the initiating events for loss of a 4 kv ac bus and by the failures of the dc buses. Therefore, separate initiating events for the ventilation systems themselves are not required.
- **Service water pump room.** The three service water pumps are located in a room that is supplied by a dedicated ventilation system. Failures of this system that could affect availability of service water flow, including failures that could initiate a plant trip, are explicitly modeled as part of the service water system.
- **Component cooling water pump room.** The room in which the CCW pumps and heat exchangers are located is supplied by a ventilation system

similar to that for the service water pump room, as well as by a separate, non-safety system. As for the service water pump room, failures of ventilation are explicitly modeled both for unavailability of the CCW system and for potential losses of CCW leading to a plant trip.

Thus, the potential for HVAC failures to cause unavailability of plant systems to respond to an initiating event is explicitly reflected in the system fault trees. In addition, failures of HVAC contribute to initiating events involving the CCW and service water systems. No initiating events exclusively involving losses of HVAC were identified that merited consideration as separate initiating events.

Summary of Transient Initiating Events

Nineteen initiating events were identified to represent the transients that could be important for Davis-Besse. These events reflect both consideration of previous PRAs for similar plants and a system-by-system review for Davis-Besse. As a check on the adequacy of the set of events selected, three additional reviews were made.

The first of these reviews involved mapping the detailed breakdown of events from NP-2230 (Ref. 10) into the categories selected for Davis-Besse. This mapping is illustrated in Table 1-5. No events that would have unique effects on plant response sufficient to warrant inclusion as separate initiators were identified. Next, a review was made of events that have been identified as potential precursors to more severe accidents. These precursors are described and evaluated in a series of reports (Refs. 21 through 27), and include events that involved significant initiators or unique system failure modes. The events outlined in these reports were examined both with respect to the potential for initiators that had not otherwise been considered in the IPE, and as an additional means to check the degree of completeness of individual system models. No new initiating events were added based on this review.

The third review involved examining the reactor trip reports for Davis-Besse to ensure that none indicated the need to model an additional initiating event. As discussed in Section 3.1, the reactor trips were each assigned to one of the categories of initiating events, and this information was used in estimating frequencies for many of the transients.

1.1.3 Internal Floods

Flooding events have occurred at many nuclear plants, and some of those incidents have indicated the potential for more serious scenarios involving flood-induced failures of safety equipment (Refs. 28 and 29). Analytical studies have also identified plant-specific susceptibilities to flood damage. The Oconee PRA (Ref. 9) identified the frequency of core damage due to turbine building flooding as the primary contributor to core-damage frequency. Based on that study, numerous design and operational changes were adopted to reduce the estimated frequency of core damage due to these types of events. Other risk assessments that have examined flooding have found that the importance of flooding is very dependent on specific aspects of the plant design. Therefore, a comprehensive effort was made to characterize the hazard associated with internal floods at Davis-Besse. The full analysis of

**Table 1-5
Cross-Reference of Transient Initiators to NP-2230**

Event from NP-2230	Relevant Event for Davis-Besse IPE
1. Loss of RCS flow (1 loop)	Reactor/turbine trip (T ₁)
2. Uncontrolled rod withdrawal	Reactor/turbine trip (T ₁)
3. Control rod drive problems and/or rod drop	Reactor/turbine trip (T ₁)
4. Leakage from control rods	Reactor/turbine trip (T ₁)
5. Leakage from primary system	Reactor/turbine trip (T ₁), up to rate for small LOCA
6. Low pressurizer pressure	Reactor/turbine trip (T ₁)
7. Pressurizer leakage	Reactor/turbine trip (T ₁), up to rate for small LOCA
8. High pressurizer pressure	Reactor/turbine trip (T ₁)
9. Inadvertent safety injection	Spurious actuation of safety features (T ₄)
10. Containment pressure problems	Reactor/turbine trip (T ₁)
11. Chemical and volume control system malfunction/boron dilution	Loss of RCS makeup (T ₆)
12. Pressure/temperature/power imbalance—rod position error	Reactor/turbine trip (T ₁)
13. Startup of inactive coolant pump	Reactor/turbine trip (T ₁) (not relevant at full power)
14. Total loss of RCS flow	Reactor/turbine trip (T ₁); note that loss of offsite power (T ₃) is judged to be the most likely cause
15. Loss or reduction in feedwater flow (one loop)	Reactor/turbine trip (T ₁)
16. Total loss of feedwater flow (all loops)	Loss of main feedwater (T ₂)
17. Full or partial closure of main steam isolation valve (one loop)	Reactor/turbine trip (T ₁)
18. Closure of all main steam isolation valves	Loss of main feedwater (T ₂)
19. Increase in feedwater flow (one loop)	Reactor/turbine trip (T ₁)
20. Increase in feedwater flow (all loops)	Loss of main feedwater (T ₂)
21. Feedwater flow instability—operator error (during startup or shutdown)	Loss of main feedwater (T ₂)
22. Feedwater flow instability—miscellaneous mechanical causes	Loss of main feedwater (T ₂)
23. Loss of condensate pumps (one loop)	Reactor/turbine trip (T ₁)

Table 1-5 (continued)
Cross-Reference of Transient Initiators to NP-2230

Event from NP-2230	Relevant Event for Davis-Besse IPE
24. Loss of condensate pumps (all loops)	Loss of main feedwater (T ₂)
25. Loss of condenser vacuum	Loss of main feedwater (T ₂)
26. Steam generator leakage	Reactor/turbine trip (T ₁) or steam generator unavailable due to feedwater or steam line break (T ₅), depending on severity
27. Condenser leakage	Loss of main feedwater (T ₂)
28. Miscellaneous leakage in secondary system	Reactor/turbine trip (T ₁) or steam generator unavailable due to feedwater or steam line break (T ₅), depending on severity and location of leak
29. Sudden opening of steam relief valves	Loss of main feedwater (T ₂) or feedwater/steam line break (T ₅)
30. Loss of circulating water	Loss of main feedwater (T ₂)
31. Loss of component cooling	Loss of train 1-1 of component cooling water (T ₁₃) or total loss of component cooling water (T ₁₄)
32. Loss of service water	Loss of train 1 of service water (T ₁₀), loss of train 2 of service water (T ₁₁), or total loss of service water (T ₁₂)
33. Turbine trip, throttle valve closure, electrohydraulic control problems	Reactor/turbine trip (T ₁)
34. Generator trip or generator-caused faults	Reactor/turbine trip (T ₁)
35. Total loss of offsite power	Loss of offsite power (T ₃)
36. Pressurizer spray failure	Reactor/turbine trip (T ₁)
37. Loss of power to necessary plant systems	Loss of power from bus YAU (T ₇), loss of power from bus YBU (T ₈), loss of dc power supply for NNI-X (T ₉), loss of power from a 4160 vac bus (T ₁₅ or T ₁₆), and loss of a dc power bus (T ₁₇ or T ₁₈)
38. Spurious trips—cause unknown	Reactor/turbine trip (T ₁)
39. Auto trip—no transient condition	Reactor/turbine trip (T ₁)
40. Manual trip—no transient condition	Reactor/turbine trip (T ₁)
41. Fire within plant	Reserved for separate consideration as an external event

potential initiators is documented in a separate report (Ref. 30). The general process for selecting the initiators and the results of that process are briefly summarized in this section.

The assessment of flood hazard involved first a general screening of buildings to determine those that both contained equipment that might be important to safety and were potentially subject to flooding from sources within the plant. For each of the buildings that was found to be of interest, a more detailed screening was performed. The process employed in this second screening, which was supported by extensive system walkdowns, entailed applying the following criteria to determine whether a room could be removed from consideration:

- A room could be screened out if it contained no significant flood sources and did not have the potential to be flooded due to propagation from other areas.
- A room could also be screened out if it was incapable of retaining significant quantities of water (e.g., due to large openings in the floor) and if equipment in the room would not otherwise be affected (e.g., due to spray effects). Note, however, that the potential for the room to serve as a source of flooding to other rooms was further considered.
- A room that might be subject to flooding could be screened out if the flood would be incapable of affecting multiple trains of a system or trains of redundant systems, either directly or through propagation to other areas.

Based on these considerations, it was possible to screen out most of the areas in the plant; only a few were found to merit more detailed analysis. For each of these areas, the potential sources of flooding were examined in sufficient detail to determine those that had unique effects on the availability of important equipment, and to permit estimation of their frequencies. A small set of initiating events was then defined. Each event encompasses a broad range of possible failures that could all lead to similar effects on the plant systems. The areas that were examined in detail and the initiating events that were identified for detailed assessment are described in the following sections.

ECCS Pump Rooms

Each of two rooms at elevation 545 in the auxiliary building houses the pumps for one train of the high and low pressure injection and containment spray systems. Between them is located a room that contains the decay heat coolers for both trains and associated valves. The three rooms are isolated from each other by 10-ft flood walls. The rooms contain possible sources of flooding sufficient to exceed the flood barriers (most notably from the BWST), and, because they are low in the auxiliary building and have openings to upper elevations, are potentially subject to floods draining from other areas. Therefore, they merited detailed consideration.

The detailed evaluation of these rooms resulted in the definition of three initiating events that were explicitly considered in the IPE:

- A flood in the ECCS pump room for train 1, or in the room adjacent to it (separated from it by a non-watertight door) that could directly cause loss of one full train of ECCS and also failure of the motor-control centers required for operation of ECCS pump room cooling for both trains. The source of flooding could be any area in the auxiliary building that drained to that pump room. All of these sources were considered within a single initiator designated as event FE1.
- A flood originating in any of the rooms and propagating to the others due to failure of a BWST line. All such floods were considered in the context of event FE2.
- Flooding of both pump rooms from sources higher in the auxiliary building that drain to them. These types of floods were evaluated via an initiator designated as event FE3.

Service Water Rooms

The three service water pumps are located in a single room at the intake structure. Adjacent to the pump room, at a lower level, is a valve room that connects to a pipe tunnel leading to the main plant buildings. Floods in the pump room can cause loss of all three service water pumps, although a backup pump (the dilution pump) located in another area may be capable of sustaining service water flow. Flooding could originate from the service water system itself, from the cooling tower makeup system (whose pumps are located in the same pump room), or from portions of the fire suppression system. Because the pump room drains to the sumps in the valve room, flooding in the valve room could, over an extended period of time, back up into the pump room. This flooding could occur due to failures in the service water supply lines, the service water return lines, or the cooling tower makeup lines. In the event of such a flood, the valving required to make use of the backup pump would not be accessible to the operators. Detailed evaluation of these areas led to the development of two initiating events involving flooding of the service water pumps:

- Flooding originating in the service water pump room (or the room next door, housing the pumps for the fire suppression system), causing failure of all three service water pumps. In this case, recovery via the dilution pump would be a possible option. Floods that could have this effect are considered in the context of event FS1.
- Flooding originating in the valve room that could rise sufficiently to back up through the pump room drains and cause loss of the pumps. In this case, as noted above, use of the dilution pump would not be an option. This scenario is assessed by an initiator designated as event FS2.

Component Cooling Water Pump Room

Like the service water pumps, the three CCW pumps are located in a single room in the turbine building. The room also contains the CCW heat exchangers, which are cooled by the service water system. Failures of service water piping in the room could therefore produce relatively severe flooding that could threaten the CCW system.

A single initiating event was defined to encompass the potential for a flood in the CCW pump room. It is designated as event F_C . Although the most significant source of flooding is the service water system, there is also the potential for failure of the piping for the fire suppression system to cause flooding in the room.

1.1.4 Summary of Initiating Events

In total, 34 initiating events were identified for assessment in the Davis-Besse IPE. These events encompass a broad range of LOCAs, many different transients that do not lead directly to LOCAs, and potentially-important sources of flooding within the plant buildings. This is considered to be adequately representative of the types of events that could uniquely affect the ability of the plant systems to respond, and of the overall frequencies of events that could challenge plant safety. The events are summarized in Table 1-6.

1.2 DEFINITION OF CORE-DAMAGE SEQUENCES

After defining the set of unique initiating events to be considered, the next step is to identify the sequences of events that could lead to core damage for each. This was done by first defining the safety functions that must be achieved to prevent core damage. These safety functions were then related to plant systems that must function to accomplish them. The minimum criteria for success of each of these systems were determined from available information, supplemented with specific calculations when necessary. Event trees were then constructed to delineate the core-damage sequences. The top events for these event trees were usually represented in terms of the safety functions. The failure to accomplish each of these safety functions was then developed through fault-tree logic at a high level to denote the corresponding system-level failures, and to represent the functional interrelationships among the systems. These system failures were further developed through detailed fault trees. Taken together, the event trees, supporting logic, and system-level fault trees comprise an integrated model of the core-damage sequences.

The set of safety functions may be formulated in a variety of ways. A formulation that was found to be complete and convenient for use in the Davis-Besse IPE is that defined in Table 1-7. It can be seen that these safety functions are strongly interrelated; these interrelationships must be carefully represented in the core-damage event trees. Where it was necessary to the modeling process or aided in understanding the sequences better, the safety functions were sometimes broken down into more specific representations according to time phases of the accident or other relevant aspects.

End states were selected for the event-tree development based on the minimum stable conditions that needed to be achieved to ensure that core cooling could be sustained in the long term. For LOCAs, successful long-term cooling typically entailed recirculation from the containment sump, with heat removed via the DHR heat exchangers. For SGTRs, the mode of long-term cooling that would be considered successful depended on the status of the affected steam generator and of the RCS. If the affected steam generator could be isolated

**Table 1-6
Summary of Initiating Events for Davis-Besse**

Event	Designator	Mean Annual Frequency*
<u>Loss-of-Coolant Accidents</u>		
Large LOCA	A	1.0×10^{-4}
Medium LOCA	M	3.0×10^{-4}
Small LOCA	S	3.6×10^{-3}
Steam generator tube rupture	R	9.0×10^{-3}
Interfacing-systems LOCA via high pressure injection line	V _H	1.7×10^{-6}
Interfacing-systems LOCA via low pressure injection line	V _L	2.9×10^{-6}
Interfacing-systems LOCA via failure of isolation in decay heat removal letdown line	V _D	3.2×10^{-7}
Interfacing-systems LOCA due to premature opening of decay heat removal letdown line	V _S	1.8×10^{-5}
Reactor vessel rupture	A _V	5×10^{-7}
<u>Transients</u>		
Reactor/turbine trip	T ₁	6.0
Loss of main feedwater	T ₂	1.7
Loss of offsite power	T ₃	3.5×10^{-2}
Spurious safety features actuation	T ₄	1.3×10^{-2}
Steam generator 1 unavailable due to break in feedwater or steam line	T ₅	3.6×10^{-3}
Loss of makeup to the reactor coolant system	T ₆	5.8×10^{-2}
Loss of power from bus YAU	T ₇	0.17
Loss of power from bus YBU	T ₈	0.17
Loss of dc power supply for NNI-X	T ₉	1.8×10^{-2}
Loss of primary loop of service water**	T ₁₀	0.16
Loss of secondary loop of service water**	T ₁₁	0.16
Total loss of service water	T ₁₂	6.5×10^{-4}

**Table 1-6 (continued)
Summary of Initiating Events for Davis-Besse**

Event	Designator	Mean Annual Frequency*
<u>Transients (continued)</u>		
Loss of operating train of component cooling water**	T ₁₃	0.34
Total loss of component cooling water	T ₁₄	5.2 x 10 ⁻⁴
Loss of power from 4160 vac bus C1	T ₁₅	8.6 x 10 ⁻³
Loss of power from 4160 vac bus D1	T ₁₆	8.6 x 10 ⁻³
Loss of dc power from bus D1P	T ₁₇	1.1 x 10 ⁻²
Loss of dc power from bus D2P	T ₁₈	1.1 x 10 ⁻²
Loss of instrument air	T ₁₉	0.11
<u>Internal Floods</u>		
Flood from auxiliary building drainage to ECCS pump room for train 1	FE ₁	4.1 x 10 ⁻³
Flood of ECCS pump rooms due to failure of a line from the BWST	FE ₂	8.6 x 10 ⁻⁵
Flood of ECCS pump rooms due to drainage from auxiliary building	FE ₃	1.3 x 10 ⁻³
Flood in service water pump room	FS ₁	7.5 x 10 ⁻⁴
Flood from service water valve room	FS ₂	3.8 x 10 ⁻⁵
Flood in component cooling water pump and heat exchanger room	FC	3.5 x 10 ⁻⁴

* The mean annual frequency is reported for each event for convenient reference and to provide perspective in following the sequence development through the remainder of this section. For further discussion of the development of these frequencies, refer to Section 3.1.

**These events do not necessarily lead directly to a plant trip, but present the potential for a trip if additional system failures occur. The additional failures are modeled explicitly in the appropriate portions of the system fault trees.

Table 1-7
Safety Functions for Preventing Core Damage

Function	Description
Reactivity control	Termination or control of the neutronic chain reaction so that power generation in the core is limited, as necessary, to levels that can safely be removed, depending on the status of plant systems.
Control of RCS pressure	Maintenance of RCS pressure within limits that will not challenge the integrity of the pressure boundary, either by causing relief valves to lift (with an opportunity to fail to reclose), or by exceeding the stress limits of an RCS component.
Control of RCS inventory	Provision for sufficient inventory of water in the RCS such that heat removal from the core can be sustained at a rate which will prevent overheating and consequential fuel damage. This entails either ensuring that RCS integrity is maintained, or providing sufficient makeup to the RCS to compensate for inventory lost from the system.
Decay heat removal	Transfer of heat from the core to the reactor coolant and from the reactor coolant to an ultimate heat sink. RCS heat may be removed by the steam generators, by the heat exchangers of the DHR system, or by transfer first to the containment and then to the atmosphere.

and heat removal were available to the unaffected steam generator, core cooling could be sustained by remaining, at a minimum, at hot conditions. If the affected steam generator could not be isolated, the need to cool down sufficiently to establish a satisfactory means of long-term heat removal was considered. For transients in which the RCS remained intact, it was generally assumed that establishing stable cooling at hot shutdown conditions would be sufficient. Depending on the number and severity of actual failures, the plant would typically be returned to power, maintained in hot shutdown until repairs could be effected, or placed in cold shutdown. The failure to achieve normal cold shutdown (under conditions when core damage could be averted by remaining at hot shutdown) is not within the scope of this study.

A nominal mission time of 24 hours was selected for most applications in the study. This mission time was used in two ways. The principal purpose of this mission time was for use in calculating the unreliability of components following an initiating event. For example, following a loss of main feedwater, it was assumed that the AFW pumps would have to operate for at least 24 hours. The unreliability for these pumps was therefore estimated as the product of the failure rate for failure to continue operating and the mission time of 24 hours.

The mission time was also used as a basis to judge the need to model actions that would have to be taken to maintain core cooling in the long term. If a substantial change in the mode of operation would be necessary to maintain core cooling, the potential for failures associated with accomplishing this change was modeled, even if it would not arise until later than 24 hours after the initiating event. On the other hand, if relatively minor actions would be required to keep a system functioning beyond 24 hours, they were usually not modeled explicitly. An example of the former case might be the need to switch from the injection mode to recirculation from the containment sump following some small LOCAs. It could be that the inventory of the borated water storage tank (BWST) might not be depleted within 24 hours for such an event. Because its depletion would lead to a substantially different mode of operation, however, it was judged to be necessary to model the failure to achieve recirculation. With regard to the second case, it might be determined that there was no need to model failure to make up to the condensate storage tanks (which could last for more than 24 hours) to maintain a suction source for the AFW pumps, if it was judged that the required actions could easily be accomplished, since a major reconfiguration of the AFW system would not be required.

In a few cases, a shorter time was used for a system if its function would not be required to last for 24 hours. For example, following some LOCAs the injection phase would last for substantially less than 24 hours, and the actual time could be used. The mission time for the equipment required for the recirculation phase would still be 24 hours. For each system, assumptions were documented regarding the modes and phases of system operation that required explicit modeling.

This mission time is consistent with common practice in virtually all recent PRAs. The selection of 24 hours reflects the fact that, at that time after a trip, the decay heat level would be only about 0.6% of the pre-trip power level. If core cooling had been maintained up to

that time, it could be interrupted for fairly long periods without leading to overheating of the core, allowing ample time for repair or the initiation of an alternative means of core cooling.

The event tree sequences fall into three general categories of outcomes: core damage, no core damage, and transfer to another event tree. Each sequence involving core damage is also assigned to a core-damage bin. These core-damage bins partially define the plant-damage states, which are described in Section 3 of Part 4, and which are used to characterize the sequences for consideration in the back-end analyses. The core-damage bins reflect the characteristics of the accident sequences, up to the point of the loss of core cooling, that could be important in determining differences in containment response. Each core-damage bin is comprised of the following elements:

- Type of initiating event—the size of breach in the RCS, and whether or not the event implies a bypassing of the containment;
- Status of emergency core cooling—whether emergency core cooling functioned in the injection or recirculation modes; and
- Availability of steam generator cooling—whether the inventory of fission products that could be released to the environment might be reduced by the presence of cool surfaces or scrubbing in the steam generators.

For reference purposes, the characteristics for each of these three elements are summarized in Table 1-8. They are described in substantially more detail in Section 3 of Part 4. Note that, in some cases, top events are incorporated into the event trees specifically to permit the sequences to be differentiated among the core-damage bins (i.e., such top events denote how, rather than whether, core damage could occur).

The sections that follow describe how the safety functions were assembled and related to system-level failures, and how the bin characteristics outlined above were incorporated, to define the core damage accidents for each class of initiating event.

1.2.1 Event Trees for Loss-of-Coolant Accidents

Separate event trees were developed for each of the LOCAs identified as initiators in Section 1.1.1. The event trees and success criteria are described in the sections that follow.

Large Loss-of-Coolant Accident

The large LOCA includes ruptures within the RCS pressure boundary with flow areas greater than 0.5 ft². Such a break is characterized by rapid blowdown to containment, until the pressure in the RCS essentially reaches equilibrium with that in the containment. As RCS pressure dropped, the core flood tanks would begin to inject, and they would reflood the core. The DHR system, operating in the LPI mode, would then keep the core covered and provide a means for transferring decay heat to the containment. The DHR system would continue to operate in this mode until the need to switch over to recirculation from the containment sump was signaled on low-low level in the BWST. Steam released to the containment would be suppressed early on by the containment spray system. In the longer term, heat would be

**Table 1-8
Summary of Characteristics for Core-Damage Bins**

Bin Element	Designator	Description
Type of initiating accident	A	Large LOCA
	M	Medium LOCA
	S	Small LOCA
	R	Steam generator tube rupture
	V	Bypass of containment (other than SGTR)
	T	Transient (intact RCS except for cycling relief valves)
Status of emergency core cooling	I	Failed in the injection phase
	R	Succeeded in injection but failed in recirculation
Availability of steam generator cooling	Y	Feedwater is available to the steam generators
	N	Feedwater is not available to the steam generators
	X	Availability of feedwater to the steam generators is not relevant

removed from the containment atmosphere by the containment air cooling (CAC) system and from the containment sump by low pressure recirculation.

The success criteria for the safety functions as they relate to a large LOCA are summarized in Table 1-9. As the table indicates, reactivity control would be accomplished as an inherent aspect of the event, owing to the formation of voiding that leads initially to neutronic shutdown, followed by the injection of borated water. Control of RCS pressure would be precluded by the initiating event because of the large breach in the RCS. RCS inventory would be maintained if at least one train of the DHR system functioned in both the injection and recirculation phases. In the longer term, RCS inventory would continue to boil off into the containment, where it would be condensed. To maintain an appropriate long-term supply of water for recirculation to the reactor vessel, the water would need to be cooled by the heat exchangers in the DHR system.

The success criteria are derived primarily from the safety analyses presented in the USAR (Ref. 1). For large LOCAs, those analyses generally assume that both core flood tanks would inject to provide early reflooding of the core to limit the peak clad temperature. In the initial assessment of core-damage sequences for Davis-Besse, successful early response was assumed to require function of both core flood tanks. Subsequently, realistic thermal-hydraulic calculations were performed using RELAP5 (Ref. 31). These calculations showed that, even if both core flood tanks failed to provide flow, the integrity of the fuel would not be threatened. Therefore, the requirement for the core flood tanks to inject was removed from the success criteria.

Note also that containment cooling by either the containment spray or CAC systems is not reflected in this set of success criteria. Calculations have been performed to assess the effects of a total loss of heat removal (Ref. 32). These calculations indicate that even if the containment were to be overpressurized due to the continued buildup of steam, sufficient subcooled water would remain in the containment sump to support recirculation. In the long term, it would eventually be necessary to add some water to make up for evaporative losses (or to establish normal shutdown cooling). It was judged that the likelihood of failure to accomplish such long-term actions was negligible compared to other failure modes, provided that the DHR system functioned in both the injection and recirculation modes.

The event tree for sequences that could result from a large LOCA is provided in Figure 1-2. The event tree is made up of two top events. Both events encompass elements of both control of RCS inventory and decay heat removal. The first, early injection for core heat removal, refers to the phase of the accident when the DHR systems injects water to restore RCS inventory and to remove decay heat to the containment. The second event, coolant recirculation for long-term cooling, accounts for the change in operating state for the DHR system when it enters low pressure recirculation, and when decay heat is removed via the CCW system. These two events reflect the need to determine (for purposes of understanding the subsequent containment response) whether core damage ensued as a result of failure to inject water into the reactor vessel, or only after a substantial portion of the volume in the BWST had been injected.

**Table 1-9
Success Criteria for Large LOCA**

Safety Function	Success Criteria	Comments
Reactivity control	<ul style="list-style-type: none"> • None. 	Voiding in the core provides sufficient negative reactivity feedback to achieve initial shutdown. Injection of borated water, as required for core cooling, ensures control of reactivity (Ref. 1).
Control of RCS pressure	<ul style="list-style-type: none"> • None. 	Precluded due to the nature of the initiating event.
Control of RCS inventory	<ul style="list-style-type: none"> • Injection by one of two DHR pumps, drawing suction from the BWST and providing flow to its associated reactor vessel nozzle <p align="center">and</p> <ul style="list-style-type: none"> • Continued injection to the RCS by one of two DHR pumps, with the suction source switched to the containment sump prior to depleting the BWST inventory. 	Success criteria are based on analyses reported in the USAR, supplemented by more realistic calculations (Refs. 1 and 31).
Decay heat removal	<ul style="list-style-type: none"> • Continued supply of cooling water to at least one train of the DHR system operating in the low pressure recirculation mode. 	Decay heat is removed to the containment via the water injected to the reactor vessel. Heat removal is required during the recirculation phase to maintain sump water in a condition suitable for pumping by the DHR system and for effective core cooling.

LARGE LOCA	EARLY COOLANT INJECTION	LONG-TERM CORE COOLING	SEQUENCE DESCRIPTION	CORE-DAMAGE BIN
A	UA	XA		
A		XA01	A	NCD
	UA01		A/XA	ARX
			A/UA	AIX

Figure 1-2. Event Tree for Sequences Initiated by a Large LOCA

Based on the success criteria outlined in Table 1-9, these top events were then related to system-level failures through supporting fault-tree logic. The supporting logic explicitly defines the relationship between the functional events comprising the event tree and the top events for the system fault trees. The two top events that comprise this event tree are described below.

Event U_A: coolant injection for early core heat removal. Event U_A defines the need to provide injection to maintain adequate inventory in the reactor vessel, and to provide for core heat removal. As indicated in Table 1-9, this would be accomplished initially by injection from at least one of the two trains of the DHR system. Thus, the failure to achieve this safety function relates directly to the top event for failure of the DHR system to operate in the LPI mode. The simple corresponding logic is shown in Figure 1-3.

Event X_A: coolant recirculation for long-term cooling. Following depletion of the inventory contained in the BWST, it would be necessary to switch the suction source for the DHR pumps to the containment sump. This is reflected in the event tree by event X_A. The corresponding failure logic is shown in Figure 1-3. Failure to accomplish this function could result either from failure of the operating staff to perform the switchover properly and in a timely manner, or because both trains of the DHR system failed to operate in the recirculation mode. The compelling indication of the need to switch suction sources (the alarm on low-low level in the BWST) would be received within about 35 minutes after the initiating LOCA, although the operators would be aware of this impending condition before that time. Calculations indicate that water would be available in the BWST to support injection flow for about an additional 9 minutes after the alarm was received, during which time the DHR system would be reconfigured for recirculation (Ref. 33).

Summary of sequences initiated by a large LOCA. The event tree illustrates three functional sequences that could result from a large LOCA and identifies the outcomes for each. The first outcome, in which both early injection and late recirculation succeed, indicates no core damage (NCD). The two core-damage sequences are as follows:

- Sequence AX_A*. This sequence involves successful injection by the DHR system, but failure of low pressure recirculation (event X_A). It is assigned to core-damage bin ARX, which reflects the fact that, although there would be insufficient cooling available to prevent core damage, a substantial amount of water would have been injected through the reactor vessel and into the containment before core damage started.
- Sequence AU_A. This sequence is for large LOCAs in which cooling fails in the injection phase, either because at least one core flood tank did not function or because both trains of LPI failed (event U_A). Sequence AU_A is therefore assigned to bin AIX.

*The core-damage sequences are defined by the events whose downward branches are followed. Note that in Figure 1-2, as well as in all of the other event trees, slashes are used in the sequence designators to separate the top events. The slashes do not indicate complement events, as they are sometimes used in PRA.

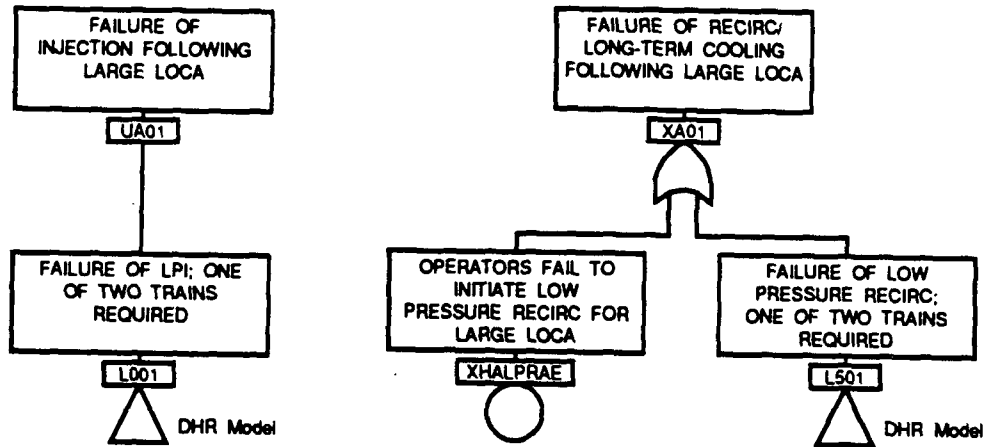


Figure 1-3. Supporting Logic for Top Events U_A and X_A of the Large LOCA Event Tree

Note that if early injection is unsuccessful, long-term cooling is irrelevant; hence, no branch point is provided for event X_A for the failure branch of event U_A . It should also be noted that the success of event U_A is implied in the definition of sequence AX_A . The appropriate success states are accounted for in the process of generating sequence-level cut sets, as described in Section 3.4. Finally, the status of cooling for the steam generators is not specified for these sequences. The physical processes associated with the core-melt progression and containment response for a large LOCA are not sufficiently sensitive to this condition to warrant explicit modeling of feedwater.

Medium Loss-of-Coolant Accident

Medium breaks are smaller than the range represented by the large category, but still provide a flow path sufficient to remove decay heat. The blowdown to containment would be slower than for a large LOCA, and makeup from the HPI system would be required to avoid uncovering the core. As RCS pressure continued to drop, the core flood tanks would discharge, and injection would eventually be provided by the DHR system in the LPI mode. In the longer term, the DHR system would be needed to recirculate water from the containment sump, just as in the case of the large LOCA.

The success criteria for the safety functions that are relevant for a medium LOCA are summarized in Table 1-10. As was the case for the large LOCA, the ability to control RCS pressure is precluded by the nature of the initiating event. The need for reactivity control via reactor trip is considered, since the voiding caused by the break may not produce sufficient negative reactivity to cause immediate shutdown. Because of the smaller rate of blowdown and correspondingly slower rate of depressurization relative to the large LOCA, core heat removal is accomplished if at least one train each of the HPI and DHR systems provide safety injection. In the longer term, low-pressure recirculation by the DHR system is adequate to maintain core cooling, as was the case for a large LOCA.

As for the large LOCA, the success criteria are based primarily on analyses reported in the USAR (Ref. 1). In the USAR analyses, at least one core flood tank was assumed to be available. Consistent with the large LOCA, however, more realistic calculations indicate that operation of the core flood tanks is not required to prevent core damage for LOCAs in the medium range as well. Therefore, only active injection was assumed to be needed.

It should be noted that the break range that defines the medium LOCA includes the potential for a complete rupture of the core flood/LPI line to the reactor vessel. Analyses of such a break have been performed and, for that break, flow from only the HPI system and the remaining core flood tank is required (Ref. 1). As noted in Section 1.1.1, this case was not analyzed separately, but was folded into the medium LOCA, with its slightly more conservative success criteria.

The event tree for sequences initiated by a medium LOCA is shown in Figure 1-4. The structure of the event tree is very similar to that for the large LOCA, except that an event has been added to consider the function of reactivity control. Both of the remaining events

**Table 1-10
Success Criteria for Medium LOCA**

Safety Function	Success Criteria	Comments
Reactivity control	<ul style="list-style-type: none"> • Insertion of two of seven rod groups by actuation of reactor protection system (RPS) or diverse scram system (DSS). 	<p>Medium LOCA may not directly produce the voiding required to achieve initial shutdown, before boration by emergency coolant injection (Ref. 1). Success criteria are based on input from Babcock & Wilcox (Ref. 34).</p>
Control of RCS pressure	<ul style="list-style-type: none"> • None. 	<p>Precluded due to the nature of the initiating event.</p>
Control of RCS inventory	<ul style="list-style-type: none"> • Injection by one of two HPI pumps, drawing suction from the BWST and providing flow to its associated reactor vessel nozzle <p align="center">and</p> • Injection by one of two DHR pumps, drawing suction from the BWST and providing flow to its associated reactor vessel nozzle <p align="center">and</p> • Continued injection to the RCS by one of two DHR pumps, with the suction source switched to the containment sump prior to depleting the BWST inventory. 	<p>Success criteria are based on analyses reported in the USAR, supplemented by more realistic calculations (Refs. 1 and 31).</p>
Decay heat removal	<ul style="list-style-type: none"> • Continued supply of cooling water to at least one train of the DHR system operating in the low pressure recirculation mode. 	<p>Decay heat is removed to the containment via the water injected to the reactor vessel. Heat removal is required during the recirculation phase to maintain sump water in a condition suitable for pumping by the DHR system and for effective core cooling.</p>

MEDIUM LOCA	REACTOR TRIP	EARLY COOLANT INJECTION	LONG-TERM CORE COOLING	SEQUENCE DESCRIPTION	CORE-DAMAGE BIN
M	K	UM	XM		
M	K		XM01	M	NCD
		UM01		M/XM	MRX
				M/UM	MIX
		TRANSFER		M/K	FAILURE TO SCRAM

MEDIUM.TRE 2-11-93

Figure 1-4. Event Tree for Sequences Initiated by a Medium LOCA

encompass aspects of controlling coolant inventory and maintaining decay heat removal. The three top events are described below.

Event K: reactor trip. As noted earlier, a medium LOCA will not lead to the degree of void formation associated with a large LOCA, so that early reactor trip is, in theory, required. Event K refers directly to failure of the reactor to trip.

Event U_M: coolant injection for early core heat removal. Event U_M defines the need to provide injection to maintain adequate inventory in the reactor vessel, and to provide for early decay heat removal. As indicated in Table 1-10, this is accomplished initially by injection from at least one of the two trains of the HPI system and at least one train of the DHR system. The supporting logic corresponding to the failure of event U_M is illustrated in Figure 1-5.

Event X_M: coolant recirculation for long-term cooling. Event X_M reflects the need to switch the suction source for the DHR pumps to the containment sump following depletion of the inventory contained in the BWST. At that point, the RCS would have reached a pressure low enough that continued injection by the HPI system would no longer be required. As shown in Figure 1-6, failure to accomplish this function could result either from failure of the operating staff to perform the switchover correctly at the proper time, or because of failure of both trains of the DHR system to function in the recirculation mode. With full injection flow (including containment spray), the time at which a signal to begin the switchover operation would be received is estimated to be about 80 minutes; it must be completed within about an additional 20 minutes (Ref. 33).

Summary of sequences for a medium LOCA. The event tree in Figure 1-4 illustrates the functional sequences that could result from a medium LOCA, and identifies the outcomes for each. The sequences other than the first, which does not lead to core damage, include the following:

- Sequence MX_M. This sequence involves successful injection by the HPI and DHR systems, but failure of low pressure recirculation (event X_M). It was assigned to core-damage bin MRX, since a substantial amount of water would have been discharged to the containment during the injection phase.
- Sequence MU_M. This sequence is for medium LOCAs in which cooling fails in the injection phase, due to the failure of HPI or DHR (event U_M). Sequence MU_M was assigned to bin MDX.
- Sequence MK. This sequence refers to the failure to trip following a medium LOCA (event K). The sequence does not lead directly to core damage, although that potential exists if there is insufficient injection of borated water to achieve shutdown. Detailed treatment of such a sequence is not needed, however, since failure of injection results in core damage irrespective of the status of reactivity control. Moreover, the frequency of a medium LOCA combined with a failure to trip would be very low. The

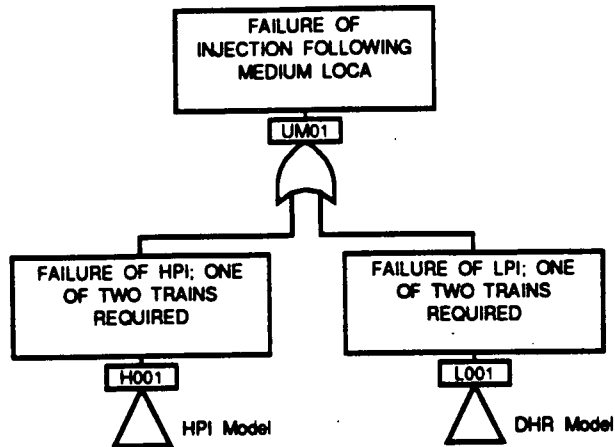


Figure 1-5. Supporting Logic for Top Event U_M of the Medium LOCA Event Tree

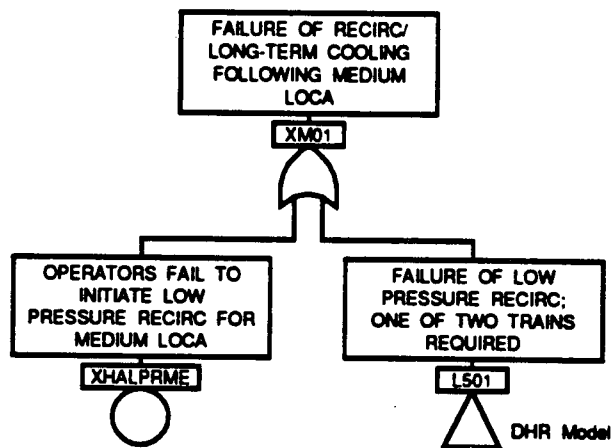


Figure 1-6. Supporting Logic for Top Event X_M of the Medium LOCA Event Tree

sequence is therefore illustrated for purposes of completeness, but is not developed (nor is its frequency quantified) further in this study.

Small Loss-of-Coolant Accident

By definition, a break corresponding to a small LOCA would be too large for normal makeup to maintain RCS inventory, but would be insufficient to provide for full removal of decay heat by itself, at least initially. A small LOCA would lead to a reactor trip (probably on low RCS pressure), and the continued decrease in RCS pressure would lead to automatic actuation of the HPI system to maintain coolant inventory. Subsequent pressure response would be a function of the size and location of the break. At the larger end of the break spectrum, the initial pressure drop could be relatively rapid, until the RCS reached saturation conditions. Pressure would continue to decrease until it stabilized at about the saturation pressure for the steam generators. Smaller breaks could cause an initial pressure drop; depending on the specific size of the break and the amount of makeup flow available, the RCS could then repressurize, or pressure could oscillate as the plant entered a boiler-condenser mode of cooling via the steam generators.

Breaks at the larger end of the spectrum (i.e., about 0.02 ft²) would discharge reactor coolant at the most rapid rate. For such a break, more than an hour would be available to initiate HPI flow to ensure that the core remained covered (Ref. 35). Smaller breaks would generally require even longer times, so one hour is used as representative in the analysis. In the longer term, it would typically be expected that the operators would cool down the plant and, depending on timing and on the specific location of the break, enter into shutdown cooling using the DHR system or into recirculation cooling from the containment sump, again using the DHR system. If the operators were unable to or chose not to cool down, high pressure recirculation could be initiated upon depletion of the BWST inventory.

Although main feedwater would not be lost as a direct result of the LOCA, the degree to which it would be effective in a boiler-condenser mode of steam-generator cooling is not known. Only the AFW system, with the higher thermal center it can create in the steam generators, is credited for providing cooling. If the AFW system failed to supply feedwater flow to the steam generators, the initial pressure drop caused by the LOCA and by the reactor trip would stop. Because the break that characterizes this LOCA range would not be large enough to remove decay heat fully, the RCS would repressurize. To ensure adequate core cooling, it would be necessary for the operators to augment high pressure injection with flow from the makeup pumps.

The success criteria for the safety functions that are relevant for a small LOCA are summarized in Table 1-11. Tripping of the reactor is needed to limit the rate of heat production. If steam-generator cooling continues to be available, RCS inventory could be maintained by injection from at least one of the two trains of HPI. As a backup to the HPI system, adequate injection could also be made available if both trains of makeup function. The operators could cool down using turbine bypass or the atmospheric vent valves, and shutdown cooling could be established using the DHR system. If cooldown could not be

**Table 1-11
Success Criteria for Small LOCA**

Safety Function	Success Criteria	Comments
Reactivity control	<ul style="list-style-type: none"> • Insertion of two of seven rod groups by actuation of RPS or DSS. 	Shutdown is required to limit heat production early in the accident (Ref. 34).
Control of RCS pressure	<ul style="list-style-type: none"> • RCS heat removal via AFW (as below for decay heat removal) <p align="center">OR</p> <ul style="list-style-type: none"> • PORV opens to relieve pressure <p align="center">OR</p> <ul style="list-style-type: none"> • One of two PSVs opens to relieve pressure. 	If feedwater is unavailable, one of the pressurizer relief valves may be required to open to prevent overpressurization of the RCS.
Control of RCS inventory	<ul style="list-style-type: none"> • Injection by one of two HPI pumps, drawing suction from the BWST and providing flow to its associated reactor vessel nozzle <p align="center">OR</p> <ul style="list-style-type: none"> • Injection by two of two makeup pumps within about one hour, drawing suction from the BWST and providing flow to the RCS <p>AND</p> <ul style="list-style-type: none"> • Establishment of shutdown cooling via DHR <p align="center">OR</p> <ul style="list-style-type: none"> • Continued injection to the RCS by one of two HPI pumps, supplied from the DHR pumps, with the suction source switched to the containment sump prior to depleting the BWST inventory. 	Success criterion for HPI is based on analyses reported in the USAR (Ref. 1). As backup to HPI, it is assumed that two makeup pumps must operate to provide sufficient injection at the pressures of interest (Ref. 36).

**Table 1-11 (continued)
Success Criteria for Small LOCA**

Safety Function	Success Criteria	Comments
Decay heat removal	<ul style="list-style-type: none"> • Flow from at least one of three AFW pumps to at least one of two steam generators within 30 minutes <li align="center">and • Cooldown to DHR entry conditions using at least one turbine bypass valve or atmospheric vent valve and establishment of shutdown cooling via one of two trains of DHR prior to depleting the inventory in the BWST or • Continued injection to the RCS by one of two HPI pumps, supplied from the DHR pumps, with the suction source switched to the containment sump prior to depleting the BWST inventory, and with cooling water available to the DHR heat exchanger in the operating train <p>OR</p> <ul style="list-style-type: none"> • Establishment of makeup/HPI cooling <li align="center">and • Continued injection to the RCS by one of two HPI pumps, supplied from the DHR pumps, with the suction source switched to the containment sump prior to depleting the BWST inventory, and with cooling water available to the DHR heat exchanger in the operating train. 	<p>To ensure that the core remains covered, AFW flow must be initiated within 30 min of the loss of MFW (Refs. 37 & 38). If heat removal is available, the reactor can be cooled down to DHR entry conditions and shutdown cooling can be established. If shutdown cooling fails or the RCS is not cooled down, high pressure recirculation can maintain long-term cooling.</p> <p>If cooling via the steam generators is not available, makeup/HPI cooling would need to be initiated. The success criteria for this mode of cooling are detailed in Section 1.2.2. Without feedwater available, it would also not be possible to cool down to DHR entry conditions prior to depleting the BWST, so it would be necessary to establish high pressure recirculation.</p>

accomplished, high pressure recirculation would have to be initiated before the BWST was depleted.

Decay heat removal could be accomplished via the steam generators by the initiation of AFW flow from at least one of the three pumps within about 30 minutes. A pathway for relieving steam from the steam generators must also be available. Because of the many pathways that could be made available (i.e., main condenser via the turbine bypass valves, or to the atmosphere via the atmospheric vent valves or main steam safety valves), no specific criteria are defined for this function.

If heat removal by the steam generators were not available, the RCS could repressurize above the shutoff head for the HPI pumps, since the break alone might not fully remove decay heat (at least initially). Under these circumstances, it is assumed that it would be necessary to establish makeup/HPI cooling. In addition to preserving RCS inventory, adequate makeup flow would be needed to remove decay heat. Because the total loss of feedwater following a small LOCA was anticipated to be a relatively low-frequency sequence compared to transients involving total loss of feedwater, success of this function was conservatively assumed to require the same set of equipment as for makeup/HPI cooling following a transient. This entails opening of the PORV or at least one of the PSVs to provide an additional pathway for the removal of decay heat, with injection provided by one or more of the makeup pumps. The success criteria for this function are described in more detail in Section 1.2.2.

It should be borne in mind that the small LOCA is characterized by a break that would not be adequate to remove decay heat fully soon after a reactor trip. In fact, however, many of the breaks in this range would be adequate to prevent the RCS from repressurizing, and establishing an additional bleed path or use of makeup would probably not be required. Because, as noted above, the frequency of this sequence was expected to be small, it was judged to be acceptable to maintain the relatively conservative criteria, rather than introducing further complexity via a finer discrimination of the break sizes.

In the long term, it would generally not be possible to cool down to DHR entry conditions if steam generator cooling were unavailable. Instead, high pressure recirculation would be required both to maintain RCS inventory and to provide for decay heat removal.

It should be noted that the operators are instructed to trip the RCPs in the event that subcooling margin is lost. This instruction stems from thermal-hydraulics calculations that have been performed using licensing-basis assumptions and parameters. These calculations indicate that operation of the RCPs after subcooling margin is lost could prolong the time during which there would be liquid flow through the break. RCP operation would therefore effectively increase the mass lost from the RCS, and it is possible that, if the RCPs were lost later in the event, the collapsed level in the RCS would be below the top of the active fuel in the core. This condition has not been explicitly modeled, primarily because it was judged that this phenomenon is a product of conservative calculations, and that loss of the RCPs would not actually constitute a serious threat to core cooling, provided that adequate makeup flow

was available. Even if untimely loss of the RCPs could threaten core cooling following a small LOCA, the following events would have to take place for core damage to ensue:

- The operators would have to fail to trip the RCPs upon loss of subcooling margin, and this step is clearly laid out at appropriate points in the emergency procedures (Ref. 39);
- There would have to be a failure within the HPI system, so that less than full HPI flow was available, leading to a delay in restoring RCS inventory;
- The RCPs would have to fail to continue operating for some reason within a time window when RCS inventory was at a minimum, leading to uncovering of the core; and
- After having been cooled for some time, the core would have to remain uncovered long enough to permit damage to begin.

Thus, even if there were a potential for loss of the RCPs to lead to uncovering of the core, the frequency of such a scenario would be very small. It was judged that the complexity in modeling that would be required to treat the specific sequence of events was not warranted, especially in light of the high likelihood that the potential for core damage is not real. Therefore, no success criteria were defined relating to the tripping of the RCPs. This practice is also consistent with the treatment of small LOCAs for other Babcock & Wilcox plants (e.g., Refs. 1 through 3).

The event tree for sequences initiated by a small LOCA is shown in Figure 1-7. The first event in the event tree corresponds to the function of reactivity control. Decay heat removal via the steam generators is reflected in the second event. It is placed early in the event tree because of its impact on the functions of inventory control and long-term heat removal. The final two events are analogous to those for the other LOCA categories, and include consideration of both injection and decay heat removal.

A separate top event was not defined for failure of RCS pressure control in the event that RCS heat removal was unavailable. Since use of the relief valves is assumed to be required for successful cooling under event U₅ if feedwater is not available, the pressure-relief function is subsumed into this event. The top events in the event tree are described below.

Event K: reactor trip. Reactor trip is required to limit the reactor to the generation of decay heat. Event K corresponds to failure of the reactor to trip, and sequences including this event are developed further within the context of the event tree for transients without scram (see Section 1.2.2).

Event B_s: decay heat removal via steam generators. Event B_s refers to the need to maintain a supply of feedwater to the steam generators, since the small LOCA alone is insufficient to remove decay heat fully. Only the AFW system is considered as a possible means to cool the steam generators, since MFW flow may not be able to support the boiler-condenser mode. The supporting logic for this event is illustrated in Figure 1-8. Successful AFW requires at least one of the two turbine-driven pumps to start and provide flow, or for

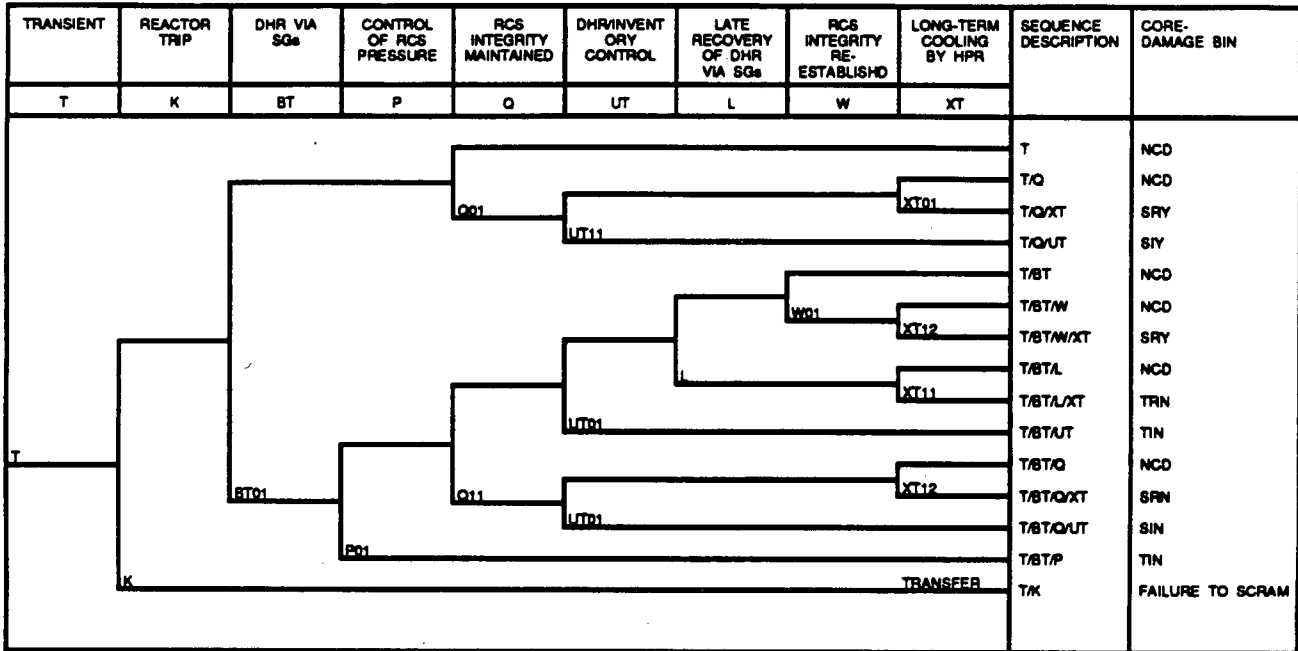


Figure 1-7. Event Tree for Sequences Initiated by a Small LOCA

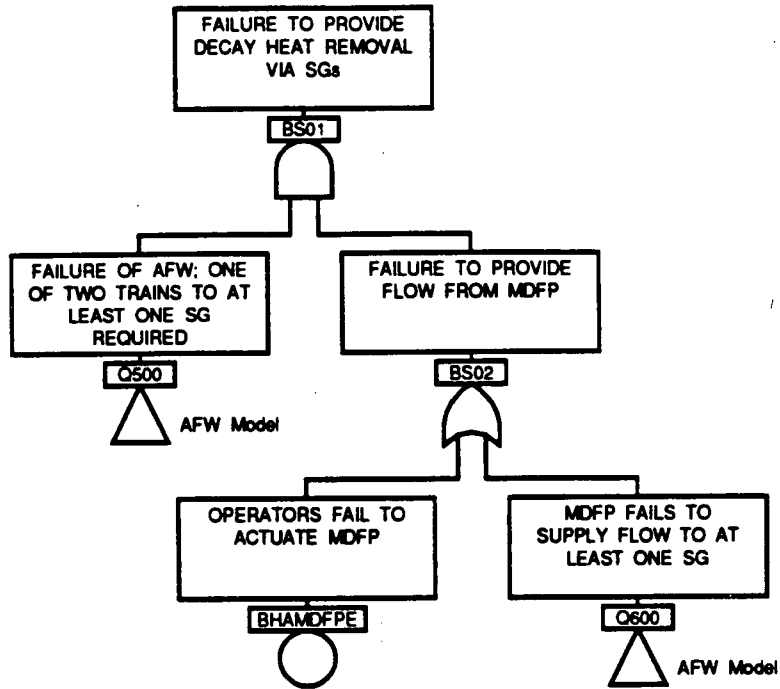


Figure 1-8. Supporting Logic for Top Event Bs of the Small LOCA Event Tree

the operators to actuate the motor-driven pump. Feedwater must be provided to at least one of the two steam generators.

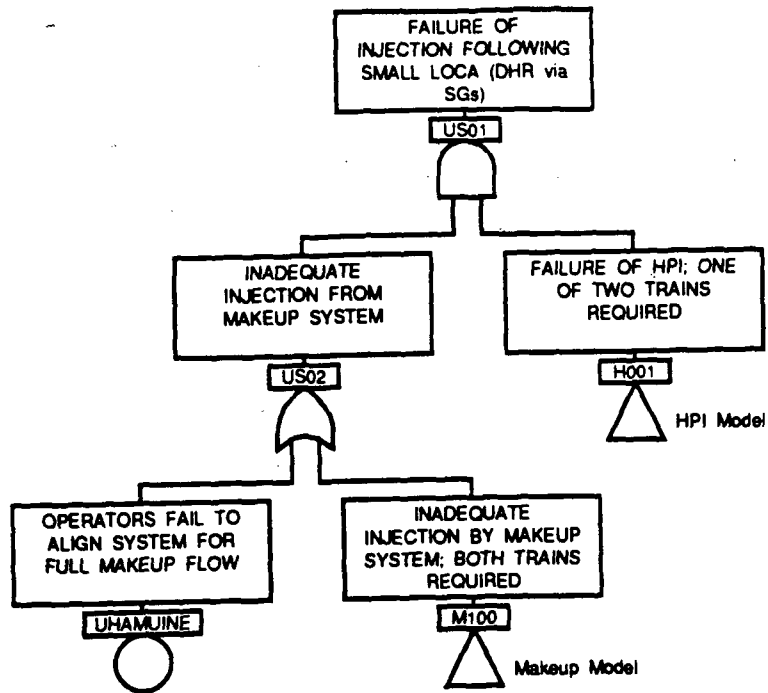
Event U_S: coolant injection for early core heat removal. Event U_S encompasses both the need for injection to maintain adequate inventory in the RCS and the provision for makeup/HPI cooling in the event that DHR via the steam generators is not available. Thus, failure for event U_S is represented by two different top events in the supporting logic, depending on the specific sequence. The logic is shown in Figure 1-9.

With RCS heat removal available (success for event B_S), the HPI system would be actuated, and one of two pumps could provide adequate flow to make up for the coolant lost through the break. Adequate inventory could also be supplied if the operators align both makeup pumps to provide injection. The logic for failure to provide sufficient injection with heat removal available is reflected in Figure 1-9 in the top event corresponding to gate US01.

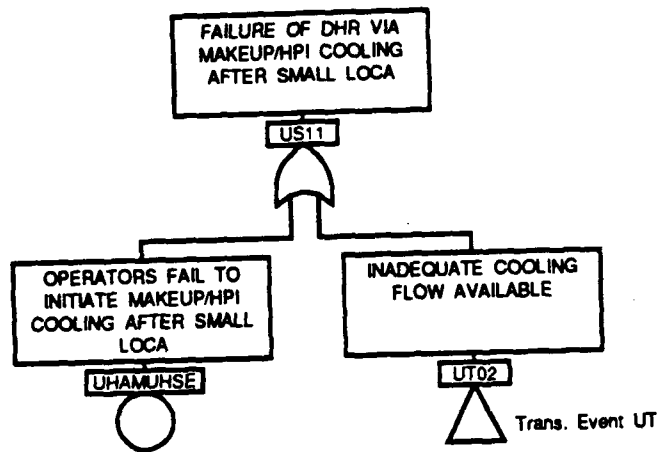
If RCS heat removal is not available (i.e., event B_S fails), it will be necessary to provide sufficient injection by the makeup system both to maintain RCS inventory and to remove decay heat. As outlined previously, it is conservatively assumed that the requirements for a path for the removal of decay heat and for the provision of sufficient makeup flow are the same as for makeup/HPI cooling in the event of a transient with total loss of feedwater. The failure to accomplish this function is depicted by gate US11 in Figure 1-9. Because the logic is identical to that for event U_T of the transient event tree, it is developed and described in more detail in the discussion of that event in Section 1.2.2.

Event X_S: long-term core heat removal. Prior to depleting the inventory in the BWST, it would be necessary to establish some mode of long-term cooling. As noted previously, it is likely that, if feedwater is available to the steam generators, the operators will cool the RCS down to the entry conditions for normal shutdown cooling. If they are unable to do so before the BWST is depleted, it will be necessary to establish recirculation cooling from the sump, using the DHR pumps to provide adequate suction head to the HPI system. These options are represented in the event tree by event X_S.

As was case for event U_S, two separate top gates are used in the development of the failure logic for event X_S, as shown in Figure 1-10. Gate XS01 is used for sequences in which event B_S is successful (i.e., removal of heat via the steam generators may permit cooldown to cold shutdown conditions). Under gate XS01, long-term cooling fails if both cooldown to enable use of shutdown cooling (gate XS02) and high pressure recirculation (gate XS12) are unsuccessful. It is assumed that cooldown can be accomplished if feedwater is available to at least one steam generator, and if at least one steam-line valve on the same generator can be controlled by the operators. If cooldown succeeds, the DHR system is considered for shutdown cooling. It should be noted that, if shutdown cooling failed because the suction valves from the RCS were unavailable, the operators would still be able to use low pressure recirculation from the containment sump. Both options are reflected under gate XS10.

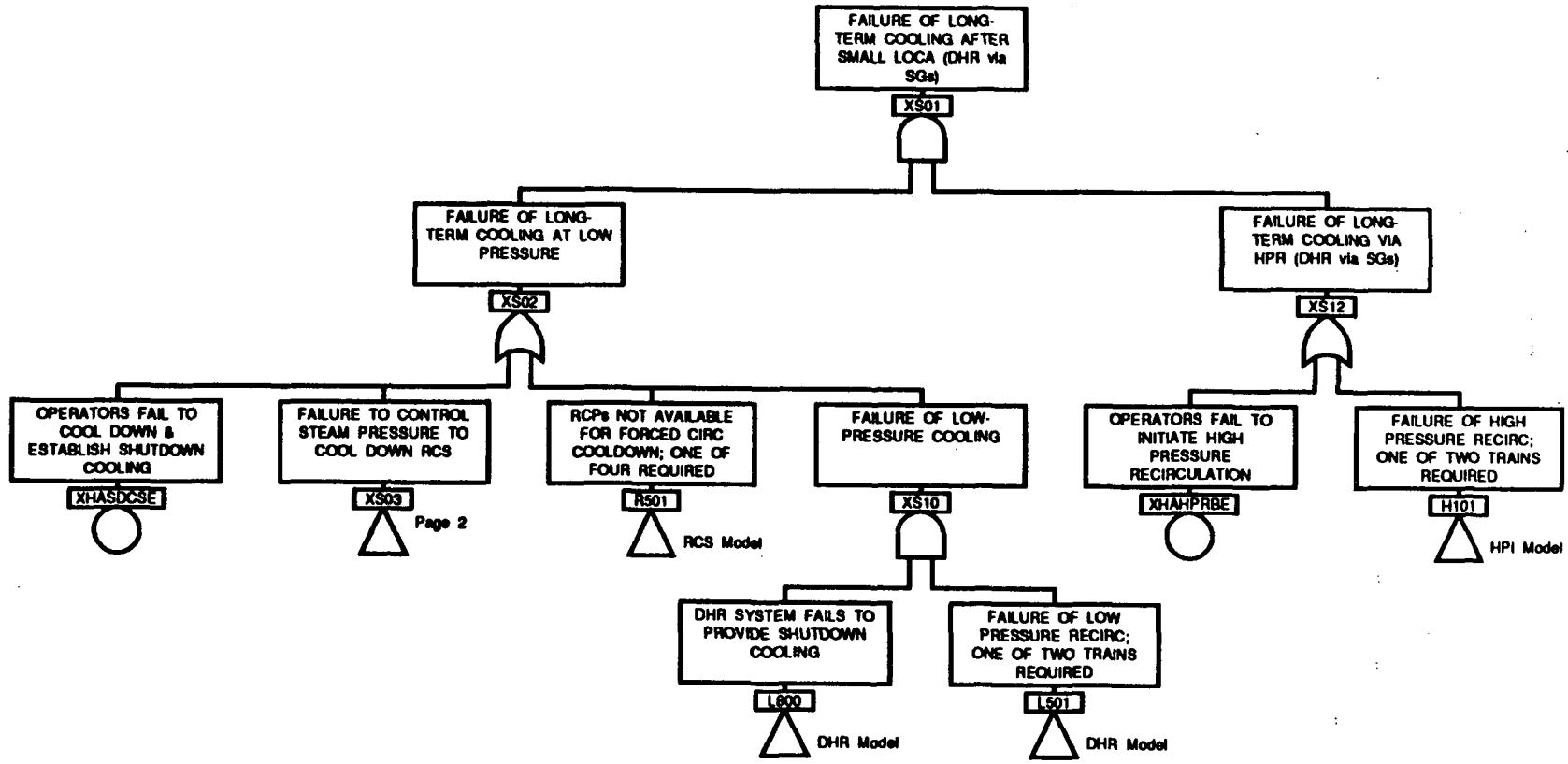


(a) With Decay Heat Removal Via Steam Generators



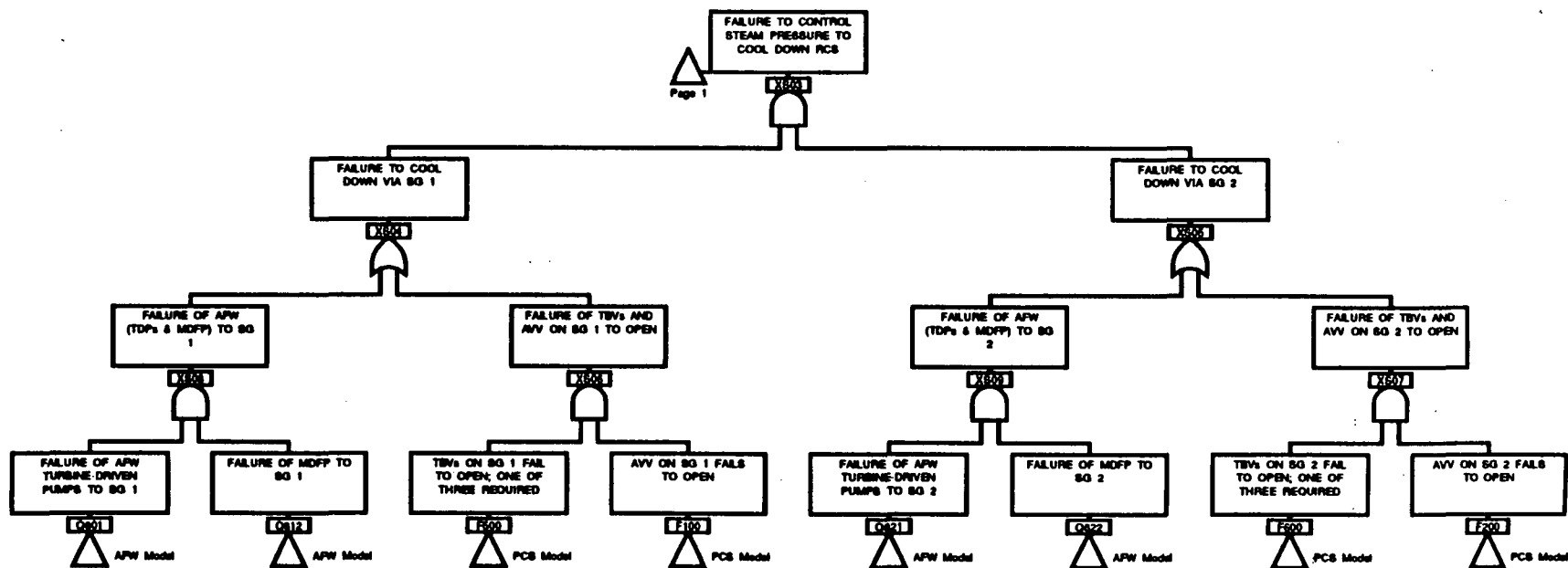
(b) Without Decay Heat Removal Via Steam Generators

Figure 1-9. Supporting Logic for Top Event U_S of the Small LOCA Event Tree



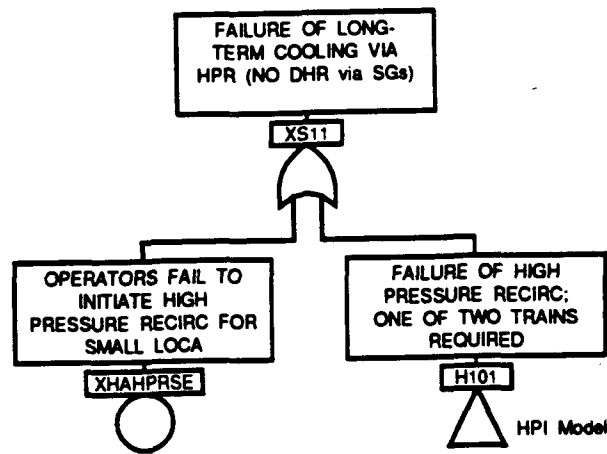
(a) With DHR Via Steam Generators (page 1 of 2)

Figure 1-10. Supporting Logic for Top Event X_S of the Steam Generator Tube Rupture Event Tree



(a) With DHR Via Steam Generators (page 2 of 2)

Figure 1-10 (continued). Supporting Logic for Top Event X₅ of the Steam Generator Tube Rupture Event Tree



(b) Without Decay Heat Removal Via Steam Generators

Figure 1-10. Supporting Logic for Top Event X_S of the Small LOCA Event Tree

For the case of failure of event B_S, gate XS11 applies. In this case, it would not be possible to cool down to DHR entry conditions because cooling via the steam generators was not available. The only option considered for long-term cooling for this case is high pressure recirculation from the emergency sump.

Summary of sequences for the small LOCA. The sequences comprised of successes and failures of the safety functions that come into play following a small LOCA are identified in Figure 1-7. The sequences other than the first, in which all relevant functions succeed, are as follows:

- Sequence SX_S. This sequence involves successful decay heat removal via the AFW system and injection by the HPI or makeup systems. The ability to maintain core cooling is lost due to failure to cool down and establish shutdown cooling or to initiate high pressure recirculation when the BWST is depleted (event X_S). This sequence is assigned to core-damage bin SRY, which reflects the fact that it involves loss of core cooling after successful injection of the BWST contents, so that a substantial amount of water will have been injected into the containment, and that feedwater is available to the steam generators.
- Sequence SU_S. This sequence also reflects successful decay heat removal via the AFW system, but uncovering of the core results from failure to supply adequate injection from the HPI or makeup systems (event U_S). It is assigned to core-damage bin SIY, indicating that the BWST contents would not be available to the containment via the injection systems, but that cooling would be available in the steam generators.
- Sequence SB_S. This sequence involves failure to maintain decay heat removal via the AFW system (event B_S), but the makeup system maintains heat removal and provides adequate injection. High pressure recirculation also succeeds, so that core damage is averted.
- Sequence SB_SX_S. This sequence is similar to sequence SX_S, except that feedwater is unavailable to the steam generators. Decay heat removal is accomplished via the makeup system early, but it fails when the BWST is depleted and high pressure recirculation is not initiated. This sequence is assigned to bin SRN.
- Sequence SB_SU_S. This sequence also involves failure of decay heat removal by the steam generators, and cooling using makeup also fails. This results in core damage earlier than would be the case for the preceding sequence. The outcome corresponds to core-damage bin SIN.
- Sequence SK. This sequence refers to the failure to trip following a small LOCA. The sequence does not lead directly to core damage, but is developed further via transfer to the event tree for transients without scram.

Steam Generator Tube Rupture

The SGTR is a special case of a small LOCA, in which the RCS inventory is lost to the steam generator (and, in most cases, eventually to the atmosphere), instead of retained within the containment. The event is therefore of particular interest because (1) without operator

action, the BWST supply available to make up for that lost through the break will eventually be depleted and lost from containment so that recirculation from the containment sump will not be possible; and (2) there is the potential for a release from the RCS to the atmosphere that could bypass the containment.

As noted in Section 1.1.1, for purposes of this analysis the SGTR was defined to be the complete rupture of a single tube. This would produce an initial leak rate of approximately 400 gpm (Ref. 40). As reactor coolant was lost through the break, pressurizer level would decrease, as would RCS pressure. Alarms on high radiation in the main steam lines would provide clear and unique indication to the operators, distinguishing this event from a small LOCA. Because of the relatively small leakage rate (compared to other LOCAs considered in this study), it is likely that the operators would have time to attempt to gain control of the RCS by lining up the makeup pumps to draw suction from the BWST and maintain pressurizer level. They would then initiate a controlled shutdown of the reactor. Otherwise, an automatic reactor trip would eventually be initiated on low RCS pressure. If RCS pressure continued to decrease, the HPI system would be actuated to help maintain RCS inventory.

Once adequate inventory control was achieved, the primary objective of the operators would be to isolate the steam generator containing the ruptured tube. To accomplish this would require depressurizing the RCS below about 1000 psig, to terminate leakage through the main steam safety valves (MSSVs) on the affected steam generator. The operators would cool down initially using both steam generators, if they were available. Once RCS pressure was reduced to about 1000 psig, they would cease steaming the generator containing the ruptured tube and attempt to isolate that generator. They would then continue the cooldown using the unaffected generator.

With the affected steam generator isolated, additional options could be available to the operators to maintain core cooling. The preferred path would be for the operators to establish normal shutdown cooling using the DHR system. If the plant could not be cooled down to the proper conditions for using the DHR system, it would be possible to continue to remove heat from the RCS using the intact steam generator. With the break isolated, the need for makeup would be essentially terminated. If the steam generator containing the ruptured tube could not be isolated (e.g., due to failure of a MSSV to close), there would be some additional leakage to the atmosphere. It was initially assumed that, unless cold shutdown conditions could be attained, this would lead to depletion of the BWST inventory and eventually to core damage. Calculations performed using MAAP, however, indicate that, if the cooldown were continued, the leakage rate would be decreased to the point that it would take a period of two or more days to deplete the BWST. During this time, additional measures could be taken to ensure a long-term supply of inventory or to isolate the leak. Therefore, if injection flow is available and if the operators are able to cool down using the unaffected steam generator, it is assumed that long-term cooling would be successful.

If the unaffected steam generator were not available, the operators would still cool down to about 1000 psig using the generator with the ruptured tube. At that point, they

would then open the PORV and initiate makeup/HPI cooling to continue the cooldown. The affected generator would be isolated, as in the case of cooldown using the intact generator. In this case, it might not be possible to reach cold shutdown conditions before the BWST inventory was depleted. With the ruptured tube effectively isolated, however, there would be adequate inventory in the containment emergency sump to support recirculation for long-term cooling.

If cooling were not available via the steam generators, the operators would be called upon to establish makeup/HPI cooling. Without restoration of feedwater, however, the RCS would remain at high pressure for some period of time, and it is expected that there would be inadequate inventory available to support sump recirculation when the BWST was depleted. Therefore, makeup/HPI cooling in the absence of feedwater is assessed to be successful only in the relatively short term; recovery of feedwater is assumed to be necessary to achieve successful long-term cooling.

The success criteria for sequences initiated by a SGTR are summarized in Table 1-12. Because of the different end states that could come into play, depending on the ability to cool down and to isolate the affected steam generator, the success criteria are somewhat more complex than for most other events. The requirements for reactor scram are assumed to be similar to those for a small LOCA. The availability of reactor scram is again represented by event K in the event tree for SGTRs, which is shown in Figure 1-11. As noted above, the normal course of action would be for the operators to initiate an early, controlled shutdown, so that reactor trip would not be necessary. The analysis was simplified somewhat by assuming that there would be a demand for a trip; this slight conservatism did not result in overstating the importance of any core-damage sequences involving SGTRs.

Control of RCS pressure for a tube rupture goes beyond the need to prevent overpressurization; RCS pressure must also be reduced so that the leakage through the ruptured tube can be terminated. The potential for overpressurization due to loss of all feedwater and failure of the PORV or at least one of the PSVs to open was neglected due to its very low frequency. Control of steam pressure to reduce RCS pressure is reflected in events C_R and C_U . Conditional on the status of heat removal by the steam generators, the availability of RCS pressure control is modeled in event P_R .

The control of RCS inventory is strongly dependent on control of RCS pressure, since it may be possible to terminate the leakage relatively early on. If this is not the case, injection to the RCS is considered in event U_R , which also accommodates makeup/HPI cooling for cases in which feedwater is lost early in the transient. The ability to prevent the further loss of RCS inventory by essentially extending the RCS pressure boundary to include the secondary side of the affected steam generator is considered in the context of event I in the event tree.

Events B_U and B_R encompass the ability to remove decay heat via the supply of feedwater to the steam generators. Feedwater is, of course, required to support cooldown as well. As noted above, if feedwater is available to neither steam generator, makeup/HPI cooling must be established until feedwater can be restored.

Table 1-12
Success Criteria for a Steam Generator Tube Rupture

Safety Function	Success Criteria	Comments
Reactivity control	<ul style="list-style-type: none"> • Insertion of two of seven rod groups by actuation of RPS or DSS. 	Shutdown is required to limit heat production early in the accident (Ref. 34).
Control of RCS pressure	<ul style="list-style-type: none"> • RCS heat removal via MFW or AFW (as below for decay heat removal) <p>AND</p> <ul style="list-style-type: none"> • Cooldown to at least 1000 psig using at least one turbine bypass valve or one atmospheric vent valve (if leak can be terminated) <p align="center">OR</p> <ul style="list-style-type: none"> • Continued cooldown using at least one steam valve on the unaffected steam generator and • Availability of at least one RCP to support forced circulation cooling and • Pressurizer spray valve or PORV opened to reduce RCS pressure. 	<p>For adequate control of RCS pressure, feedwater must be available initially or must be restored.</p> <p>Initial cooldown via one of the steam valves may permit isolation of the steam generator. Otherwise, continued cooldown is required to limit the loss of inventory through the broken tube.</p>
Control of RCS inventory	<ul style="list-style-type: none"> • Isolation of ruptured tube, permitted by cooldown to 1000 psig via the unaffected steam generator (as above) and • Closure of nine of nine MSSVs on the affected steam generator and • Closure of the main steam isolation valve on the affected steam generator <p>OR</p> <ul style="list-style-type: none"> • Injection by one of two HPI pumps, drawing suction from the BWST or • Flow from two of two makeup pumps within about one hour, drawing suction from the BWST and injecting to the RCS <p align="center">and</p> <ul style="list-style-type: none"> • Continued cooldown using the unaffected steam generator to minimize the effective leakage, as above or • Opening of PORV for cooldown and recirculation from the containment sump by one of two HPI pumps, supplied from the DHR pumps. 	<p>If the leak can be stopped initially by cooling down using the unaffected steam generator, makeup to the RCS may not be needed to prevent uncovering of the core. This requires both control of steam pressure and isolation of the steam generator containing the ruptured tube.</p> <p>For all other cases, injection is required as for a small LOCA (Refs. 1 and 36).</p> <p>In addition to makeup flow, leakage through the broken tube must be minimized to preserve a source of injection. This entails further cooldown on the unaffected steam generator, or depressurization using the PORV.</p>

Table 1-12 (continued)
Success Criteria for a Steam Generator Tube Rupture

Safety Function	Success Criteria	Comments
Decay heat removal	<ul style="list-style-type: none"> • Continued flow from MFW to at least one steam generator <li align="center">or • Flow from at least one of three AFW pumps to at least one of two steam generators within 30 minutes <li align="center">or • Establishment of makeup/HPI cooling, <u>and</u> eventual restoration of feedwater. 	<p>Adequate heat removal requires cooling by at least one steam generator. In the short term, makeup/HPI cooling can sustain decay heat removal, but the eventual depletion of the BWST inventory will necessitate restoration of feedwater for satisfactory long-term cooling.</p>

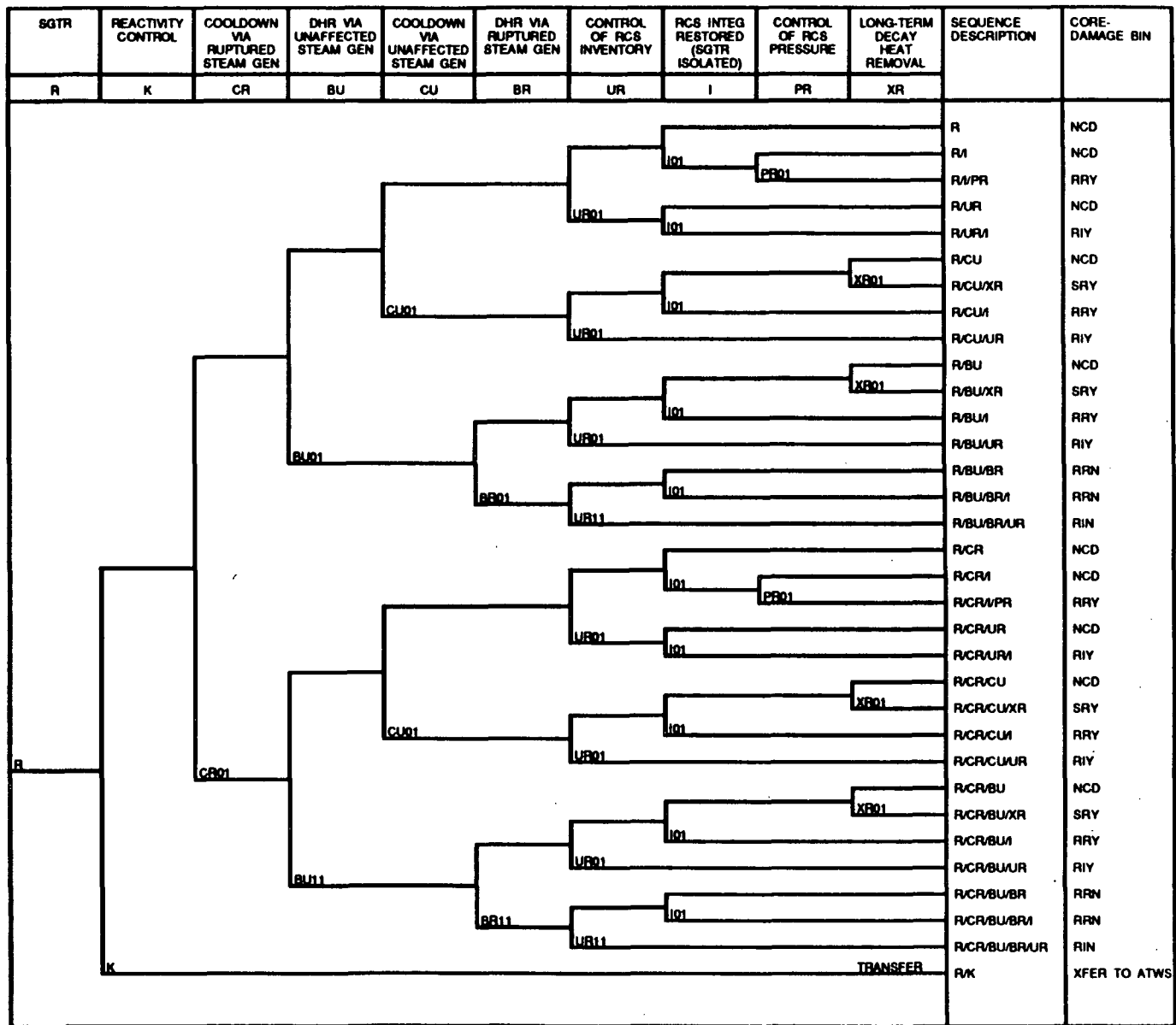


Figure 1-11. Event Tree for Sequences Initiated by a Steam Generator Tube Rupture

Successful long-term cooling is implied if the leakage can be terminated or minimized and if feedwater is available to the unaffected steam generator. If the unaffected generator could not be used for decay heat removal and/or cooldown, the operators would need to establish cooldown using makeup/HPI cooling. This can be successful in the long term if the affected steam generator is isolated and recirculation from the containment sump can be established. The events in the event tree and the sequences corresponding to their successes and failures are described below.

Event K: reactor trip. The operators have about 11 minutes to establish adequate makeup and control of plant conditions to prevent an automatic reactor trip (Ref. 40). Therefore, in most cases it would be expected that a reactor trip would not be required. To simplify the analysis, however, it is conservatively assumed that there would be a demand for an automatic trip, requiring function of the RPS. Event K corresponds to failure of the RPS, and is considered further within the context of the event tree for transients without scram (see Section 1.2.2).

Event CR: cooldown via steam generator with ruptured tube. The initial response to a SGTR would entail an attempt to cool down using both steam generators, until the pressure in the RCS could be reduced to below about 1000 psig so that the leakage through the tube could be stopped. If the steam generator containing the ruptured tube cannot be steamed, it is conservatively assumed that its level would rise sufficiently to cause main feedwater to be isolated. Because this affects heat removal from both steam generators, event CR is included first (after reactor trip) in the event tree. The logic for event CR, including failure of both the turbine bypass and atmospheric vent valves, is shown in Figure 1-12.

Event BU: heat removal via unaffected steam generator. The implications of achieving RCS heat removal via the unaffected steam generator are different from those if the generator containing the ruptured tube must be used. If the intact generator is available, the operators can cool down the RCS and isolate the affected generator. Once RCS pressure is reduced sufficiently to isolate the affected generator, the leak is effectively terminated. If adequate makeup has been made available to the RCS to maintain a medium for core cooling, core damage would be averted. If the affected steam generator must be used, however, the RCS must be cooled down further and a different mode of long-term cooling must be established. For convenience in the modeling process, therefore, the two steam generators are considered in different top events in the event tree.

The supporting logic corresponding to event BU is shown in Figure 1-13. Note that there are two top events, conditional on the status of event CR: if event CR is successful, failure for event BU requires loss of both main and auxiliary feedwater (gate BU01). Otherwise, only auxiliary feedwater (including the motor-driven feed pump) is assumed to be potentially available for heat removal (gate BU11).

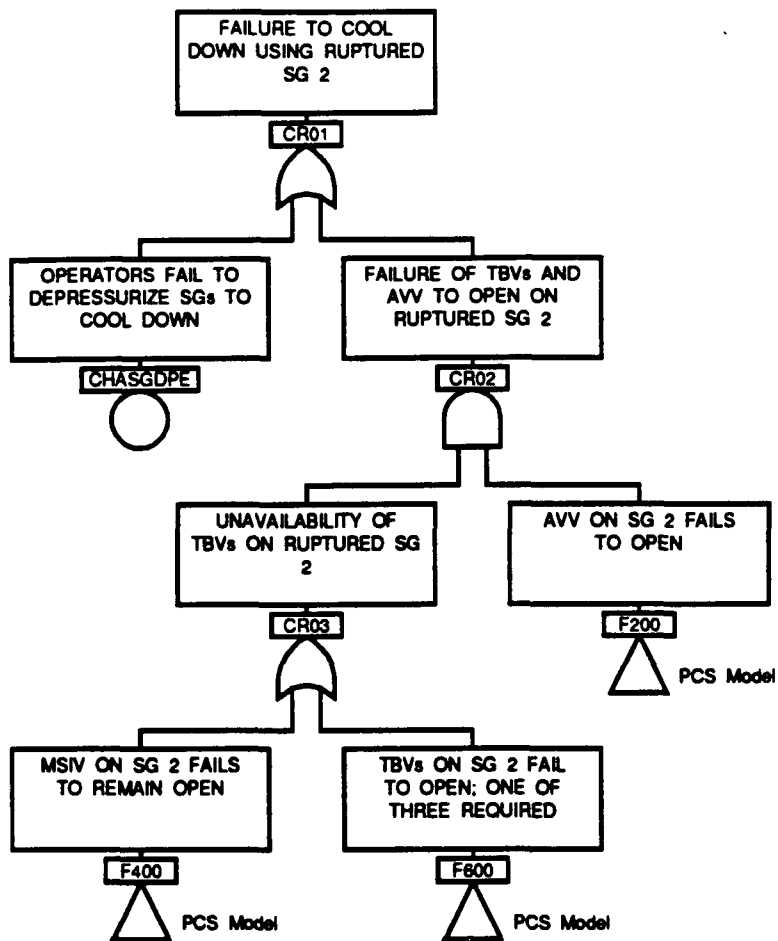
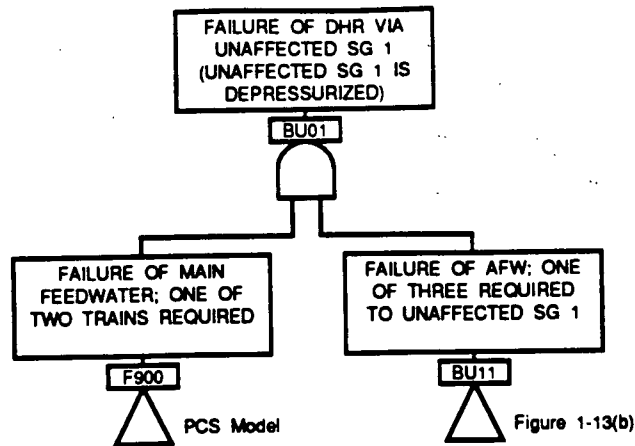
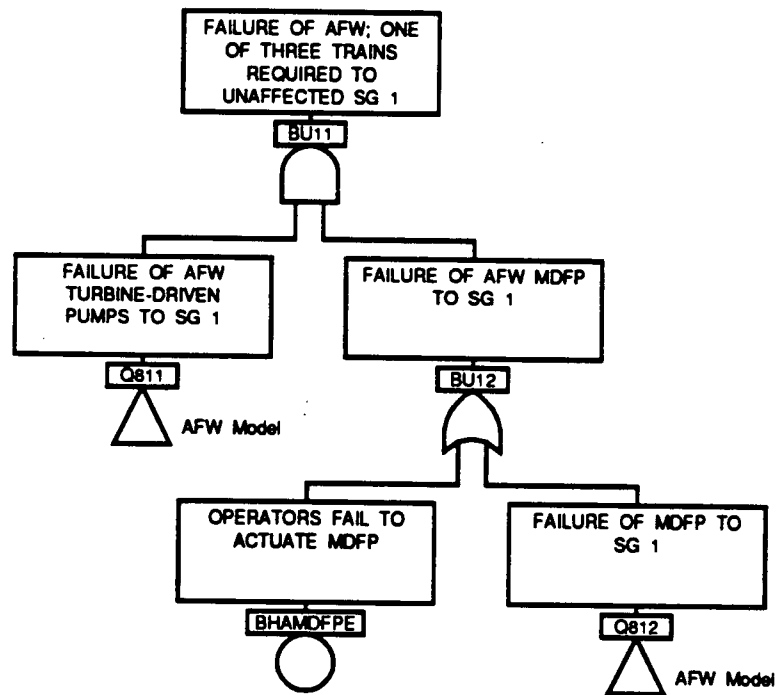


Figure 1-12. Supporting Logic for Top Event CR of the Steam Generator Tube Rupture Event Tree



(a) With Success of Event C_R



(b) With Failure of Event C_R

Figure 1-13. Supporting Logic for Top Event B_U of the Steam Generator Tube Rupture Event Tree

Event C_U: cooldown via unaffected steam generator. Continued cooldown using the unaffected steam generator is the preferred response to a SGTR. As the event tree depicts, if event C_U is successful, RCS pressure should be reduced to below the setpoints for the MSSVs well before the BWST inventory is depleted. If the generator containing the ruptured tube can be isolated, the leak will stop, and long-term core cooling can be maintained whether or not cold shutdown is achieved. The logic for failure to cool down the RCS using the unaffected steam generator is analogous to that for event C_R, and is shown in Figure 1-14.

Event B_R: heat removal via steam generator with ruptured tube. The unaffected steam generator is the preferred path for removal of heat from the RCS. If it is not available, however, the operators will use the generator with the ruptured tube to cool down the RCS initially. The failure logic for this event, developed under gates BR01 and BR11, is analogous to that for event B_U, and is depicted in Figure 1-15.

Event U_R: coolant injection for early core heat removal. As was the case for the small LOCA, the need for coolant injection is dependent in part on whether or not cooling is available via at least one of the steam generators. The failure to provide sufficient injection for the various modes of interest is reflected in the supporting logic for event U_R, shown in Figure 1-16.

If the RCS can be cooled down relatively quickly to below 1000 psig and the broken tube can be isolated, high pressure injection may not be needed. Otherwise, provided feedwater is available to at least one steam generator, this event is very similar to event U_S; adequate makeup can be provided by either the HPI or makeup systems, taking suction from the BWST (gate UR01 in Figure 1-16).

If neither steam generator is available to provide RCS heat removal, makeup/HPI cooling would be used to maintain core heat removal until a more permanent mode of cooling can be established. In this case, the options are somewhat more restricted than for a small LOCA. It is assumed that feedwater must eventually be restored to permit further cooldown of the RCS so that the leakage can be terminated before sufficient inventory is lost through the break to prevent successful recirculation from the containment sump. The logic for failure of makeup/HPI cooling for a SGTR is modeled under gate UR11.

If the unaffected steam generator could not be used to support cooldown but feedwater were available to the generator with the broken tube, the operators would cool the RCS partially and then isolate the ruptured generator. Cooldown would then proceed via makeup/HPI cooling, using the PORV as a path for heat removal. Failure to provide adequate cooling in this mode is developed under gate UR21.

Event I: isolation of steam generator containing ruptured tube. Whether or not the affected steam generator can effectively be isolated determines in large measure the options available to the operators to establish a means of long-term core cooling. If the RCS can be cooled down below the setpoints for the MSSVs and the affected steam generator can be isolated, the leak flow may be essentially stopped, and the operators can continue an

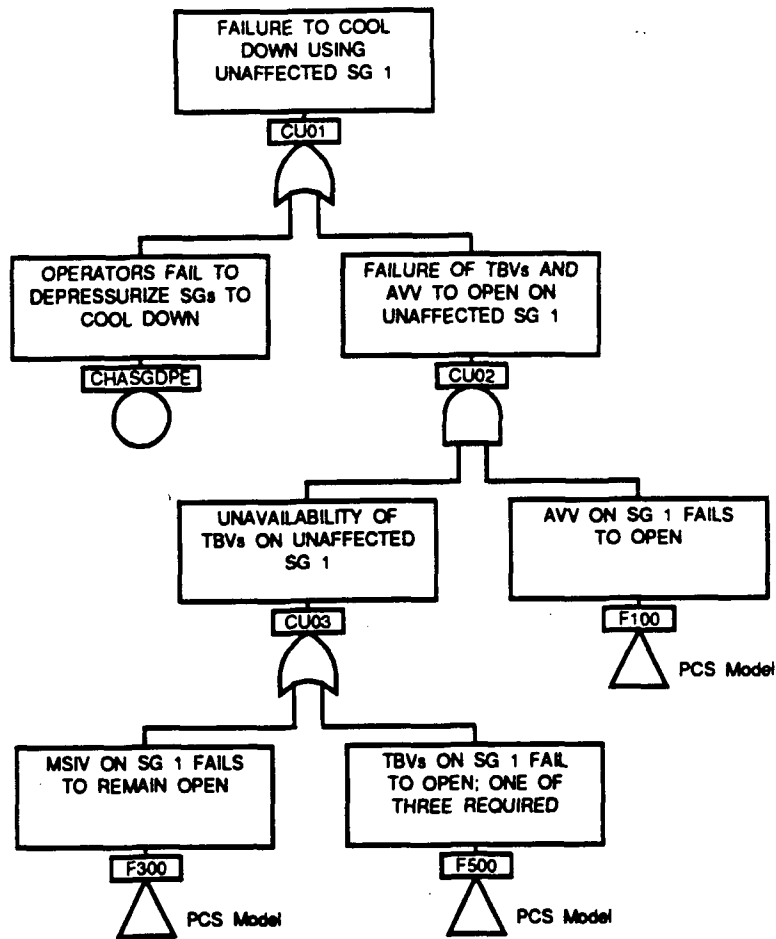
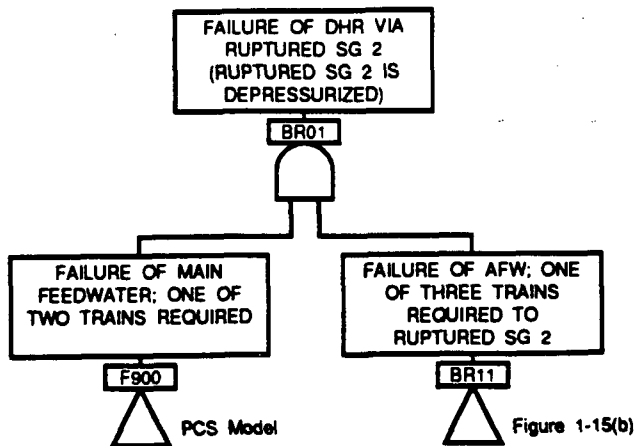
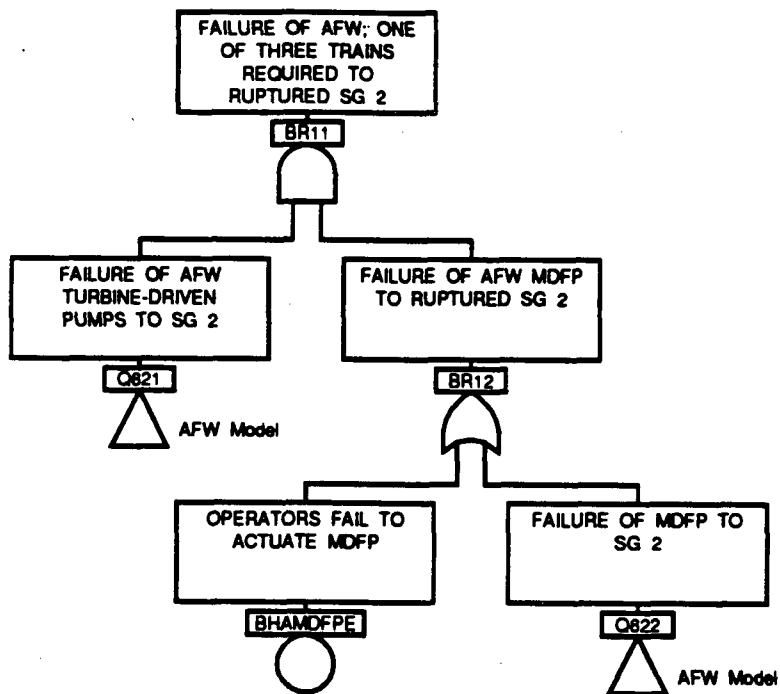


Figure 1-14. Supporting Logic for Top Event C_U of the Steam Generator Tube Rupture Event Tree

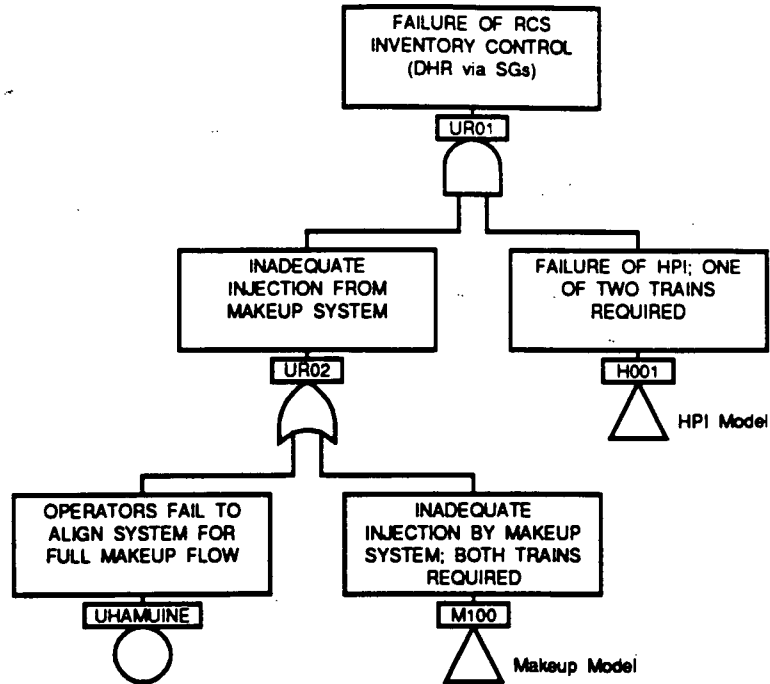


(a) With Success of Event Cr

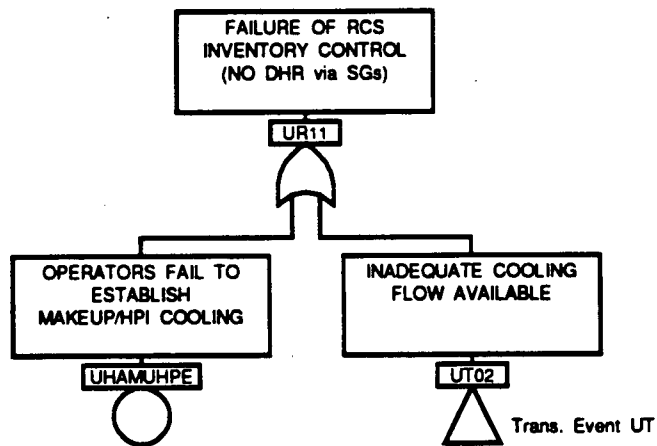


(b) With Failure of Event Cr

Figure 1-15. Supporting Logic for Top Event B_R of the Steam Generator Tube Rupture Event Tree



(a) With Cooldown Available Via the Unaffected Steam Generator



(b) Without Heat Removal Available Via Steam Generators

Figure 1-16. Supporting Logic for Top Event U_R of the Steam Generator Tube Rupture Event Tree

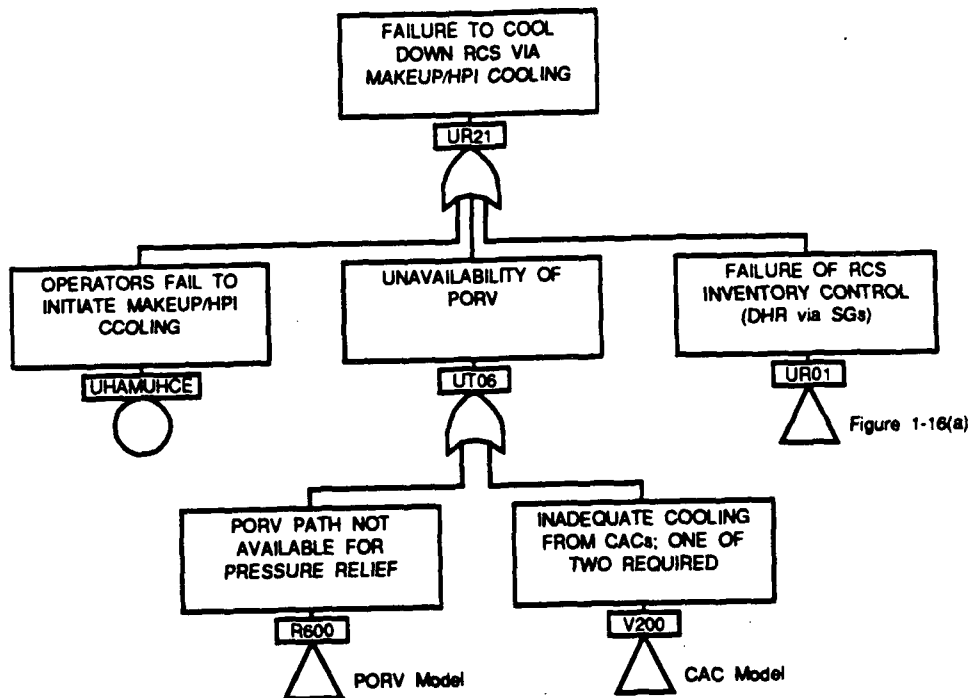


Figure 1-16(a)

(c) With Cooldown Not Available Via the Unaffected Steam Generator

Figure 1-16 (continued). Supporting Logic for Top Event U_R of the Steam Generator Tube Rupture Event Tree

orderly cooldown to enter shutdown cooling via the DHR system. They can also maintain core cooling by remaining at higher pressure, with heat removed via the intact steam generator. If leakage from the affected steam generator cannot be terminated, however, the operators must achieve cold shutdown conditions to establish stable long-term cooling. The logic for failure to isolate the steam generator containing the ruptured tube is depicted in Figure 1-17.

If the operators take control soon after the rupture occurs by increasing makeup flow and controlling the steam system, they can avoid an automatic reactor trip. By pursuing an orderly shutdown, the potential to open the MSSVs can also be avoided. A number of complications can be introduced in this scenario, however, and it is difficult to be certain that the reactor will not be tripped while still at relatively high power. As the logic in Figure 1-17 shows, it is therefore conservatively assumed that the MSSVs will be challenged by a SGTR, with the potential for one or more to stick open. It is also assumed that the MSIV for the affected generator must eventually be closed to provide isolation.

Event P_R: control of RCS for cooldown. To a significant extent, RCS pressure would be dependent on the pressure in the steam generators, since the leak itself would afford a limited means for depressurization. If the steam generator containing the ruptured tube could not be isolated (e.g., due to a stuck-open MSSV), it could be necessary to cool down the RCS to near cold shutdown conditions. Otherwise, leakage through the break would continue at a rate that might cause the BWST inventory to be depleted, with insufficient water collected in the containment to support recirculation from the containment sump.

For cooldown to this extent within the time frame for which the BWST inventory could be assured to be available, it is assumed that forced circulation of reactor coolant using the RCPs would be required. Pressure control could be accomplished using either the pressurizer spray (the preferred means), or by intermittent operation of the PORV. The logic for failure of event P_R is shown in Figure 1-18.

Note that this event is not challenged in the event tree for those cases in which the PORV might be needed to support cooldown via makeup/HPI cooling (i.e., when the unaffected steam generator could not be used to cool down the RCS). MAAP calculations show that, even if the PORV could not be opened, the leakage rate could be reduced sufficiently so that the BWST inventory would last for at least a few days. Therefore, failure to open the PORV is not assessed to lead to core damage.

Event X_R: long-term cooling via recirculation. In the event that the PORV is opened to support cooldown when the unaffected steam generator is not available, the BWST inventory may eventually be depleted. It is uncertain whether conditions would be reached that would permit the initiation of cold shutdown prior to that time. Therefore, it is assumed that high pressure recirculation from the containment sump would be required. The logic for failure of this mode is, as shown in Figure 1-19, identical to that for a small LOCA for cases in which high pressure recirculation was required.

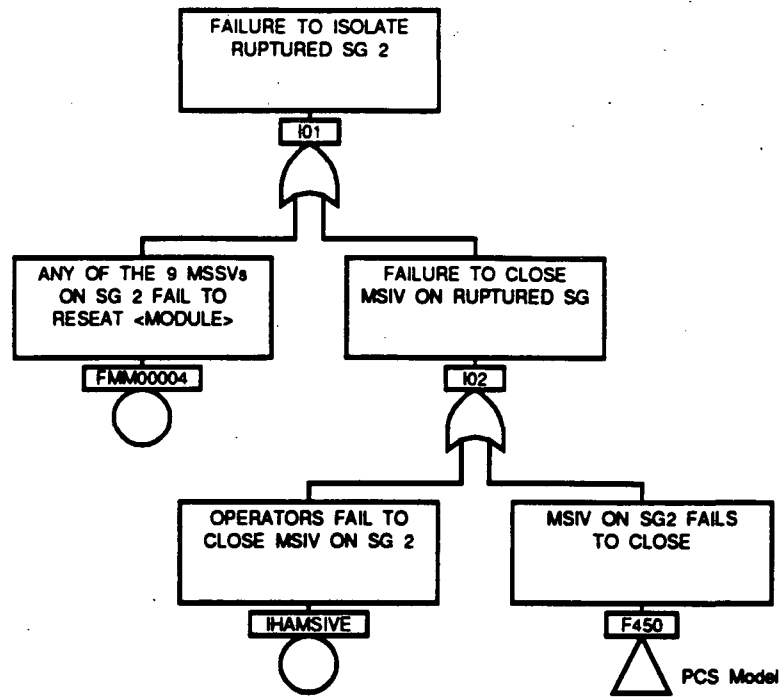


Figure 1-17. Supporting Logic for Top Event I of the Steam Generator Tube Rupture Event Tree

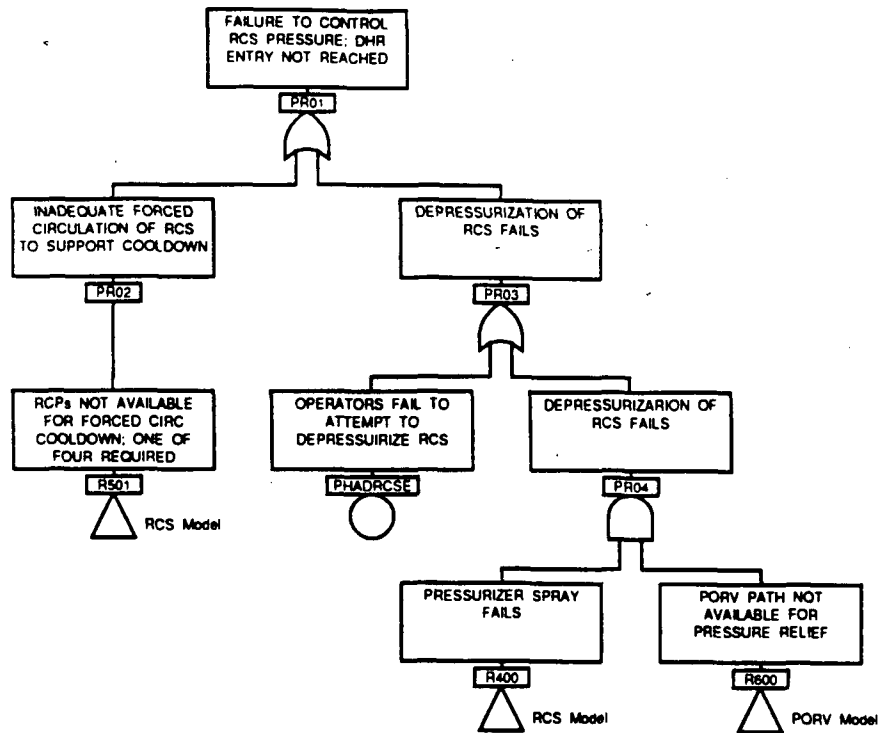


Figure 1-18. Supporting Logic for Top Event PR of the Steam Generator Tube Rupture Event Tree

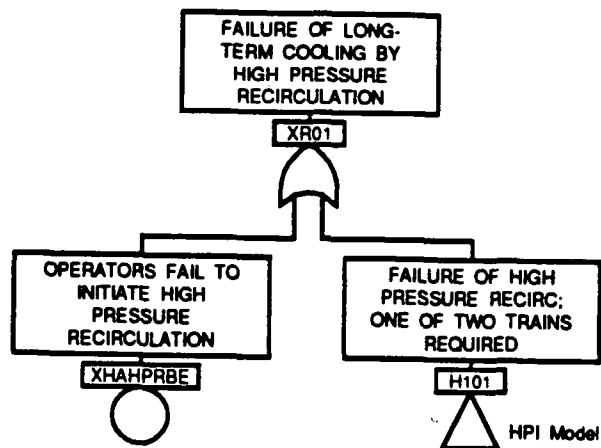


Figure 1-19. Supporting Logic for Top Event XR of the Steam Generator Tube Rupture Event Tree

Summary of sequences for a SGTR. The event tree shown in Figure 1-11 illustrates the functional sequences that could occur as a result of a SGTR. These sequences are described in the following discussion.

- Sequence R. In the first sequence, the reactor successfully trips, and the unaffected steam generator can be used to cool down the RCS. Injection succeeds, and the ability to cool down the RCS while isolating the broken generator will effectively stop the leak. Core damage does not occur.
- Sequence RI. In sequence RI, heat removal is available by both steam generators, but in this case the affected steam generator cannot be isolated (event I). Cooldown to cold shutdown conditions is achieved well before the BWST is depleted, and the leak is reduced to a very small amount. Core damage is therefore avoided.
- Sequence RIP_R. In sequence RIP_R, the steam generator containing the ruptured tube again fails to be isolated, and RCS pressure cannot be controlled sufficiently (event P_R) to minimize the leakage rate through the broken tube. The BWST inventory is eventually depleted, and core damage results. This sequence is assigned to core-damage bin RRY. Note that replenishment of the inventory in the BWST is a potential recovery option for cases in which the cooldown proceeded too slowly as a result of failure of forced circulation. This possibility was considered on a case-by-case basis during the quantification of the sequence frequencies.
- Sequence RUR. In sequence RUR, the unaffected steam generator is used for cooldown, but injection flow is not available (event U_R). The cooldown of the RCS enables the ruptured steam generator to be isolated and the leak terminated before the core is uncovered. Therefore, no core damage results.
- Sequence RUR_I. Sequence RUR_I is essentially the same as sequence RUR, except that the ruptured steam generator fails to be isolated. RCS inventory therefore continues to be lost to the atmosphere, and uncovering of the core would eventually result without injection. This sequence is assigned to core-damage bin RIY.
- Sequence RC_U. In sequence RC_U, the unaffected steam generator cannot be used to cool down the RCS (event C_U). The RCS is cooled down to about 1000 psig, at which time steaming of the generator containing the ruptured tube is terminated. Cooldown then continues using the PORV and cold injection by makeup or HPI. Note that even if the PORV could not be opened, the leakage rate through the break would be very small, so that the ability to maintain injection would not be threatened.
- Sequence RC_UX_R. As in the previous sequence, in sequence RC_UX_R the unaffected steam generator cannot be used to cool down the RCS to cold shutdown conditions. Therefore, it is assumed that the cooldown using the other steam generator is terminated and the PORV is opened to continue the cooldown. When the BWST is depleted, the transfer to recirculation from the containment sump fails (event X_R). This sequence is assigned to bin SRY, since it is most like a small LOCA with failure of recirculation (the leak through the broken tube was long since terminated).
- Sequence RC_UI. This sequence entails failure to cool down using the unaffected steam generator, so that cooldown using injection flow and the

PORV is required. The steam generator containing the ruptured tube cannot be isolated, so that inventory continues to be lost through the break. When the BWST is depleted, there is insufficient inventory in the containment sump to support recirculation. This sequence is assigned to bin RRY, since it is a late failure with feedwater available.

- Sequence RC_UU_R. In sequence RC_UU_R, the unaffected steam generator could not be used to cool down. Therefore, the leakage cannot be terminated without using the PORV to cool down. Injection from HPI or makeup is not available, so that the core is eventually uncovered. This sequence is assigned to bin RIY.
- Sequence RB_U. In sequence RB_U, the unaffected steam generator is not available to provide RCS heat removal (event B_U), but partial cooldown is accomplished using the steam generator containing the ruptured tube. That generator is then isolated, and the cooldown continues using the PORV. Therefore, core damage does not occur.
- Sequence RB_UX_R. This sequence is initially the same as sequence RB_U, but transfer to recirculation from the containment sump fails when the BWST is depleted. This sequence is assigned to bin SRY.
- Sequence RB_UI. Sequence RB_UI involves failure of heat removal via the unaffected steam generator, but with cooldown initially available using the steam generator containing the ruptured tube. The operators initiate cooldown using the PORV when the RCS is depressurized to about 1000 psig, but the affected generator cannot be isolated. Leakage continues at a rate that causes insufficient inventory to be available for recirculation from the containment sump, and the core is eventually uncovered. This sequence is assigned to bin RRY.
- Sequence RB_UU_R. In sequence RB_UU_R, leakage cannot be terminated completely because feedwater is not available to the unaffected steam generator. Injection is unavailable from makeup and HPI, so that the core eventually uncovers. This corresponds to core-damage bin RIY.
- Sequence RB_UB_R. In sequence RB_UB_R, neither steam generator is available to provide decay heat removal. The RCS cannot be cooled down to stop the leakage. Decay heat is initially removed via makeup/HPI cooling, but insufficient inventory is available to maintain recirculation from the containment sump when the BWST is depleted. The sequence is assigned to core-damage bin RRN. Note that, because of the long time available for action, restoration of feedwater and establishment of stable long-term cooling can be considered on a case-by-case basis during the sequence quantification process.
- Sequence RB_UB_RI. This sequence is similar to sequence RB_UB_R, except that the generator containing the broken tube fails to be isolated. Like the previous sequence, this one is assigned to core-damage bin RRN. Restoration of feedwater alone may not be sufficient to permit achieving stable long-term cooling, as was the case for sequence RB_UB_R.
- Sequence RB_UB_RU_R. In this sequence, there is again a total loss of feedwater, and the operators are not able to establish makeup/HPI cooling to prevent core damage. The sequence is assigned to bin RIN.
- Sequence RC_R. In this sequence, the ruptured steam generator cannot be steamed (event C_R). The unaffected steam generator is used to cool down

the RCS. The ruptured steam generator is then isolated, and the leak is terminated.

- Sequence RC_{RI} . This sequence is similar to sequence RC_R , except that the ruptured steam generator cannot be isolated. Cooldown of the RCS succeeds, however, so that the leak is reduced to a very small amount, and core damage does not occur.
- Sequence RC_{RIPR} . This sequence is similar to sequence RC_{RI} , except that RCS pressure cannot be reduced sufficiently to minimize the leakage through the ruptured tube. Therefore, there is eventually insufficient inventory available, and the core uncovers. This sequence is assigned to core-damage bin RRY.
- Sequence RC_{RUR} . In this sequence, the ruptured steam generator cannot be steamed, but cooldown is initiated using the unaffected generator. High pressure injection fails, but the leak is terminated before sufficient inventory is lost through the ruptured tube to lead to uncovering of the core.
- Sequence RC_{RURI} . This sequence is similar to the preceding one, except that the ruptured steam generator cannot be isolated. Because of the continued leakage of reactor coolant, the core is eventually uncovered. The sequence is assigned to core-damage bin RIY.
- Sequence RC_{RCU} . In this sequence, neither generator can be used for controlled cooldown of the RCS due to the failure of steam pressure control. The RCS pressure would be reduced more slowly to about 1000 psig, permitting isolation of the generator containing the ruptured tube. From that point, the PORV would be used to support continued cooldown.
- Sequence RC_{RCUXR} . This sequence is similar to the previous sequence, except that, when the BWST is depleted, recirculation from the containment sump is not available. This sequence is assigned to bin SRY, since the leak through the ruptured tube is effectively terminated.
- Sequence RC_{RCUI} . In this sequence, cooldown using the PORV is initiated after the RCS is depressurized to about 1000 psig. Leakage through the affected generator continues because of an isolation failure. Eventually, there would be insufficient inventory available to support recirculation from the sump, and core damage would result. This sequence is assigned to bin RRY.
- Sequence RC_{RCUUR} . Sequence RC_{RCUUR} involves failure to cool down using either steam generator and failure of high pressure injection. Leakage cannot be eliminated, so that the core will eventually be uncovered. This sequence is assigned to bin RIY.
- Sequence RC_{RBU} . In this sequence, the ruptured steam generator cannot be steamed to cool down the RCS, and feedwater is unavailable to the unaffected steam generator. RCS pressure would eventually be reduced to 1000 psig, and the cooldown would be continued using the PORV. In the long term, recirculation could be provided from the containment sump.
- Sequence RC_{RBUXR} . This sequence is similar to sequence RC_{RBU} , except that recirculation from the containment sump would not be available. The sequence is assigned to bin SRY.
- Sequence RC_{RBUI} . This sequence is similar to sequence RC_{RBU} , except that the ruptured steam generator cannot be isolated. Depletion of the

BWST inventory would cause eventual failure of high pressure injection. The sequence is assigned to core-damage bin RRY.

- Sequence RCRBUUR. Sequence RCRBUUR involves failure of RCS heat removal via the unaffected steam generator, and failure to cool down using the ruptured generator. Therefore, the leakage cannot be terminated. High pressure injection is unavailable, so that the core will eventually be uncovered. This sequence is assigned to bin RIY.
- Sequence RCRBUBR. In this sequence, the ruptured steam generator cannot be steamed, and feedwater is not available to either generator. RCS pressure will remain high, so that leakage will continue through the broken generator at a significant rate. Makeup/HPI cooling succeeds in the short term, but there would be insufficient inventory available to permit recirculation from the containment sump. This sequence is assigned to bin RRN. Note that long-term restoration of feedwater could prevent core damage, and is considered on a case-by-case basis in the quantification process.
- Sequence RCRBUBRI. This sequence is similar to the preceding one, except that the steam generator containing the ruptured tube fails to be isolated. This sequence is also assigned to bin RRN.
- Sequence RCRBUBRUR. In this sequence, there is a total loss of feedwater, and makeup/HPI cooling fails. This sequence is assigned to core-damage bin RIN.
- Sequence RK. This is a tube rupture followed by failure of the reactor to trip. It is considered further in the context of the special event tree constructed for sequences involving failure to scram, as described in Section 1.2.2.

Interfacing-Systems LOCAs

Interfacing-systems LOCAs are, by definition, events that have the potential to lead to both core damage and a bypassing of containment. The four initiating events defined in Section 1.1 account for the occurrence of an interfacing-systems LOCA. Because these events were assessed to be quite low in frequency, the potential that the ECCS would fail other than due to the effects of the break itself were neglected. The only question with respect to whether or not they lead to core damage is, therefore, the possibility that the breaks could be isolated before the ECCS would be lost. Therefore, no event trees were constructed for these events. Instead, the isolation measures are described below for each initiating event.

Event IH: failure to isolate a break due to reverse flow in a HPI injection line. Various combinations of component failures were considered that could lead to a break upstream from one of the HPI pumps. The breaks were assessed to occur at the time of quarterly stroke-testing of one of the motor-operated valves in the injection lines, and the same valve could be reclosed to isolate the break. In NUREG/CR-5604 (Ref. 6), a period of several hours was estimated to be available in which isolation of the break would prevent eventual uncovering of the core. The logic corresponding to failure to close the isolation valve (assumed for purposes of the analysis to be valve HP2A) is shown in Figure 1-20. Note that the human interaction corresponds, in the naming convention for basic events, to a non-

recovery action. This is because the isolation action would rely on diagnosis and decision-making that is not covered explicitly by plant procedures.

Event I₁: failure to isolate a break due to reverse flow in a LPI injection line. A second scenario for an interfacing-systems LOCA was assessed to be the potential for rupture of the check valves in the injection lines to the RCS for the DHR system. Similar to the preceding event, the break flow could be terminated by closure of the normally-open isolation valve in the affected injection line. In NUREG/CR-5604 (Ref. 6), a period of somewhat over an hour was estimated to be available in which isolation of the break would prevent eventual uncovering of the core. The logic corresponding to failure to close the isolation valve (assumed for purposes of the analysis to be valve DH1A) is shown in Figure 1-21. As in the previous case, the human interaction corresponds to a non-recovery event.

Event I₂: failure to isolate a break due to hardware failure of the DHR suction valves. The potential for an interfacing-systems LOCA was also considered in the event of hardware failures (e.g., disk ruptures) of the series motor-operated valves isolating the DHR system from RCS pressure during normal operation. In this case, it is possible that the break could occur in a location that could not be isolated. Otherwise, closure of a manual valve (valves DH10 or DH26) would stop the leak flow. Based on the analyses in NUREG/CR-5604 (Ref. 6), it is estimated that a period of several hours would be available in which isolation of the break would prevent eventual uncovering of the core. The logic for failure of the break to be isolated is shown in Figure 1-22.

Event I₃: failure to isolate a break due to premature opening of valves DH11 and DH12. The fourth scenario considered as a possible interfacing-systems LOCA entailed opening of the suction valves from the RCS to enter into cold shutdown at a time when the pressure in the RCS was still well above normal entry conditions. This could lead to a break in the lower-pressure DHR piping. Reclosure of either valve DH11 or valve DH12 would terminate the leakage. Once again, based on the analyses reported in NUREG/CR-5604 (Ref. 6), it is estimated that a period of several hours would be available in which isolation of the break would prevent eventual uncovering of the core. The logic for failure of the break to be isolated is shown in Figure 1-23.

Reactor Vessel Rupture

Event A_v represents a catastrophic failure of the reactor vessel such that the injection systems would be incapable of keeping the core covered. No event tree is required, since the initiator is assumed to lead directly to core damage. The vessel failure is judged to be most like a large LOCA with failure of recirculation, since it is very likely that the injection systems would function to provide water to the containment, even if they could not prevent the core from being damaged. Therefore, it is included in core-damage bin ARX.

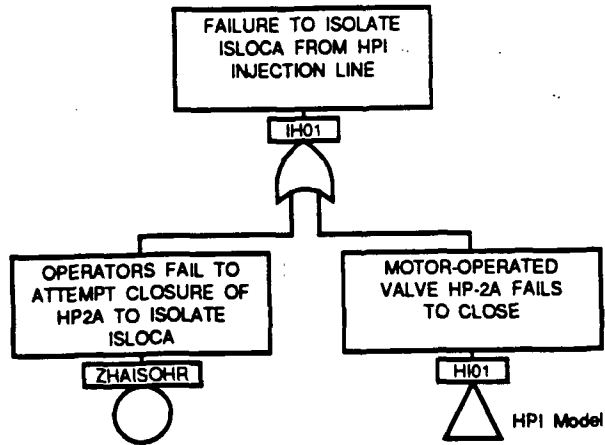


Figure 1-20. Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_H

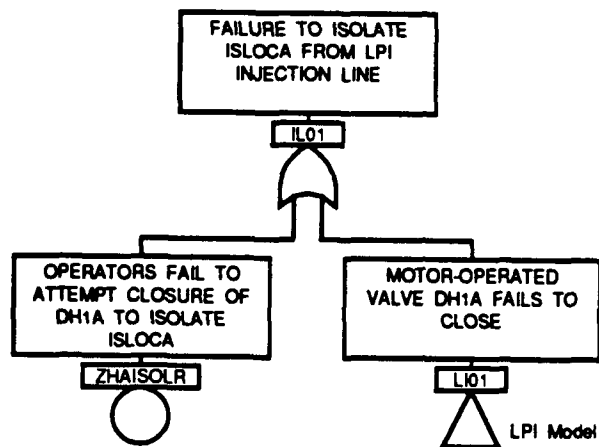


Figure 1-21. Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_L

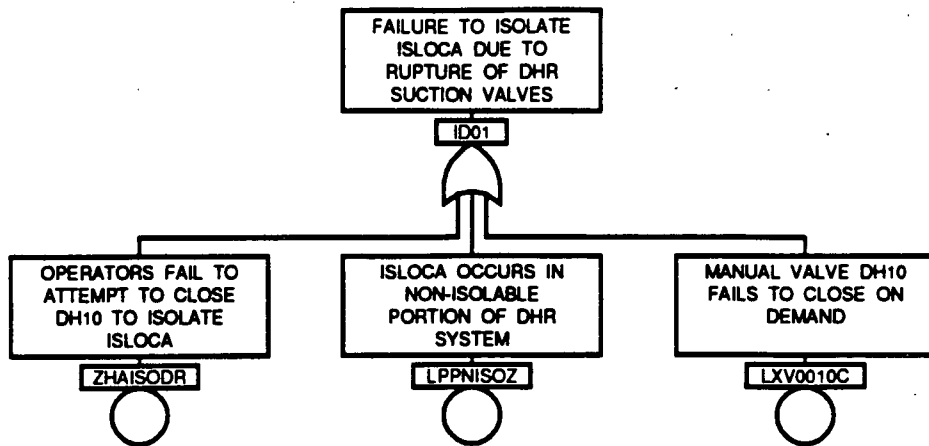


Figure 1-22. Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_p

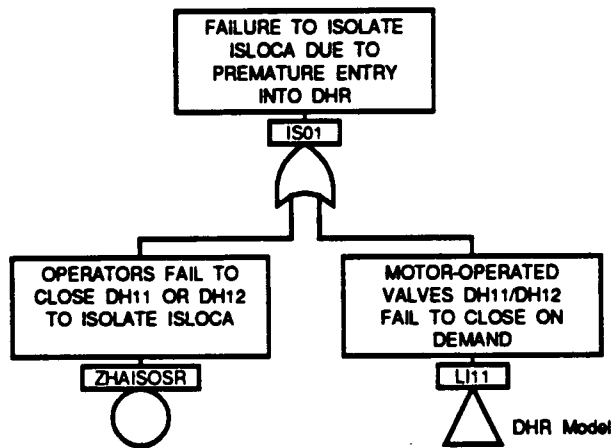


Figure 1-23. Supporting Logic for Failure of Isolation for Interfacing-Systems LOCA V_s

1.2.2 Event Trees for Transient Initiators

Events other than LOCAs that create a demand for a reactor trip are grouped under the general category of transients. Because the functions that must be achieved following all transients are generally the same, a single event tree has been constructed to consider all initiating events. The specific effects of the various initiators on the availability of systems needed to maintain core cooling are accommodated through appropriate events in the supporting logic for the top events in the event tree and through the system-level fault trees. A separate event tree was also constructed to consider the special conditions imposed by a failure of the reactor to trip given occurrence of a transient.

Transient Event Tree

Following most transients, there would be a demand for a reactor trip (either automatically, or manually in anticipation of an eventual automatic actuation). The core would continue to be cooled by circulation of reactor coolant, by forced circulation if the RCPs continue to operate, or by natural circulation otherwise, with heat removed via the steam generators. Main feedwater would usually continue to supply the steam generators, but AFW flow would be made available if main feedwater were lost. Decay heat could be transferred to the main condenser if the turbine bypass valves were available. Otherwise, the generators could steam to the atmosphere via the MSSVs or the atmospheric vent valves. Provided there was no breach in the pressure boundary for the RCS, core cooling could be maintained for an extended period of time without other major system operations. The plant could be cooled down to make repairs if needed, or returned to power operation if the source of the trip could be readily identified and corrected.

If no feedwater were available to the steam generators, the operators would realign the makeup system to provide increased flow and would open the PORV to establish makeup/HPI cooling (Ref. 39). This mode of direct core cooling could be maintained until the inventory in the BWST was depleted. Prior to that time, either steam generator cooling would need to be restored, or high pressure recirculation from the containment sump would have to be established.

Other possibilities for interrupting core cooling could result if transient conditions led to the loss of RCS integrity. If RCS heat removal via the steam generators were to be lost, the reactor coolant pressure would increase to the point that the PORV and/or pressurizer safety valves were challenged. If none of the three valves (there are two safety valves) were to open, or if they opened at a pressure that was too high, the RCS pressure boundary could be damaged, or RCS pressure might remain too high to permit adequate injection of makeup water to remove decay heat. If the valves were opened properly, one or more could also fail to reclose, creating the equivalent of a small LOCA. A small LOCA could also result if interruption of seal cooling led to loss of the pressure boundary normally sustained by the RCP seals.

The safety functions as they relate to these scenarios are summarized in Table 1-13, relative to the success criteria for the systems needed to accomplish them. These safety

**Table 1-13
Success Criteria for Transients**

Safety Function	Success Criteria	Comments
Reactivity control	<ul style="list-style-type: none"> • Insertion of two of seven rod groups by actuation of RPS or DSS. 	Shutdown is required to limit heat production early in the transient (Ref. 34).
Control of RCS pressure	<ul style="list-style-type: none"> • Decay heat removal via steam generators (as described below) <p align="center">OR</p> <ul style="list-style-type: none"> • PORV opens to relieve pressure <p align="center">OR</p> <ul style="list-style-type: none"> • One of two pressurizer PSVs opens to relieve pressure. 	If feedwater is unavailable, one of the pressurizer relief valves may be required to open to prevent overpressurization of the RCS.
Control of RCS inventory	<ul style="list-style-type: none"> • Seal cooling maintained for RCPs, as detailed for event Q <p align="center">and</p> <ul style="list-style-type: none"> • RCS pressure controlled below relief valve setpoints, as above, OR • Relief valves reclose, if opened <p>OR</p> <ul style="list-style-type: none"> • Injection by HPI or makeup adequate for small LOCA, as per Table 1-11. 	<p>In the absence of adequate seal cooling, seal failure may result in a small LOCA.</p> <p>If the PORV or one of the PSVs were to stick open, a small LOCA would result.</p> <p>If a seal LOCA occurs or if a relief valve sticks open, a transient-induced LOCA results, requiring injection in the same way as for initiating small LOCAs.</p>
Decay heat removal	<ul style="list-style-type: none"> • Continued flow from at least one MFW pump to at least one of two steam generators <p>OR</p> <ul style="list-style-type: none"> • Flow from at least one of three AFW pumps to at least one steam generator <p>OR</p> <ul style="list-style-type: none"> • Initiation of makeup/HPI cooling, as detailed in Table 1-14 <p align="center">and</p> <ul style="list-style-type: none"> • Restoration of feedwater to at least one steam generator prior to depleting the BWST inventory OR • Initiation of high pressure recirculation from the containment sump prior to depleting the BWST inventory, with cooling water supplied to the associated decay heat cooler. 	<p>A continued supply of MFW flow to the steam generators can maintain adequate RCS heat removal.</p> <p>If MFW flow is lost, flow from one of the three AFW pumps within about 4 min to prevent RCS pressure from increasing to the PORV setpoint, within about 10-12 minutes to prevent lifting the pressurizer PSVs, and within about 30 min to ensure that the core remains covered (Refs. 37 & 38).</p> <p>With no feedwater available, makeup/HPI cooling using the makeup system must be initiated. In the long term, either feedwater must be restored, or makeup/HPI cooling must be maintained, with recirculation from the containment sump.</p>

functions were used to construct the event tree shown in Figure 1-24. Note that the initiator in this event tree is identified as event "T". This is a placeholder for all of the transient initiating events, since the single event tree is used for all of them.

In Figure 1-24, reactivity control is represented by event K. Decay heat removal via the steam generators is explicitly considered in the context of events B_T and L. Event B_T refers to the availability of feedwater to maintain core cooling. If heat removal via the steam generators is not available (i.e., event B_T fails), the need for control of RCS pressure is considered in event P. Loss of heat removal followed by failure to provide adequate pressure relief is assumed to lead to core damage.

Event Q represents the maintenance of RCS integrity, and reflects both the possibility that a small LOCA might result from the failure of seal cooling for the RCPs, and the potential that a relief valve might stick open if it were challenged. Event U_T reflects both the ability to provide backup decay heat removal via makeup/HPI cooling if steam generator cooling is unavailable (failure of event B_T), and maintenance of RCS inventory in the event of a transient-induced LOCA (failure for event Q). If makeup/HPI cooling is initiated, the potential that feedwater might be recovered before the inventory in the BWST is depleted is considered in event L. If feedwater is recovered (success for event L), the possibility that it might not be possible to close the pressurizer relief valves to permit restoration of RCS integrity is considered in event W.

Success for events L and W results in a stable mode of long-term cooling with heat removal via the steam generators. If there is a transient-induced LOCA (failure of event Q or event W), the need for establishing recirculation from the containment sump is accounted for by event X_T. Recirculation from the sump, as reflected in event X_T, would also be required if cooling via the steam generators remained unavailable, and makeup/HPI cooling had to be sustained as the mode for long-term cooling.

Each of the top events is discussed below, followed by a summary of the specific functional sequences that result.

Event K: reactor trip. As was the case for small LOCAs and SGTRs, event K refers to the need to trip the reactor to limit core heat production following the initial transient. Depending on the nature of the transient, the failure to trip the reactor can place demands on the core cooling systems that are substantially different from those that result when the reactor successfully trips. To simplify the transient event tree, these conditions are considered separately in the context of an event tree developed specifically for transients with failure to trip. The event tree shown in Figure 1-24 indicates a transfer to this event tree, which is discussed later in this section.

Event B_T: decay heat removal via the steam generators. Decay heat removal using the steam generators requires both a supply of feedwater and a path for the rejection of steam, to either the main condenser or the atmosphere. Unless the nature of the transient itself causes an interruption of main feedwater flow, it should continue automatically

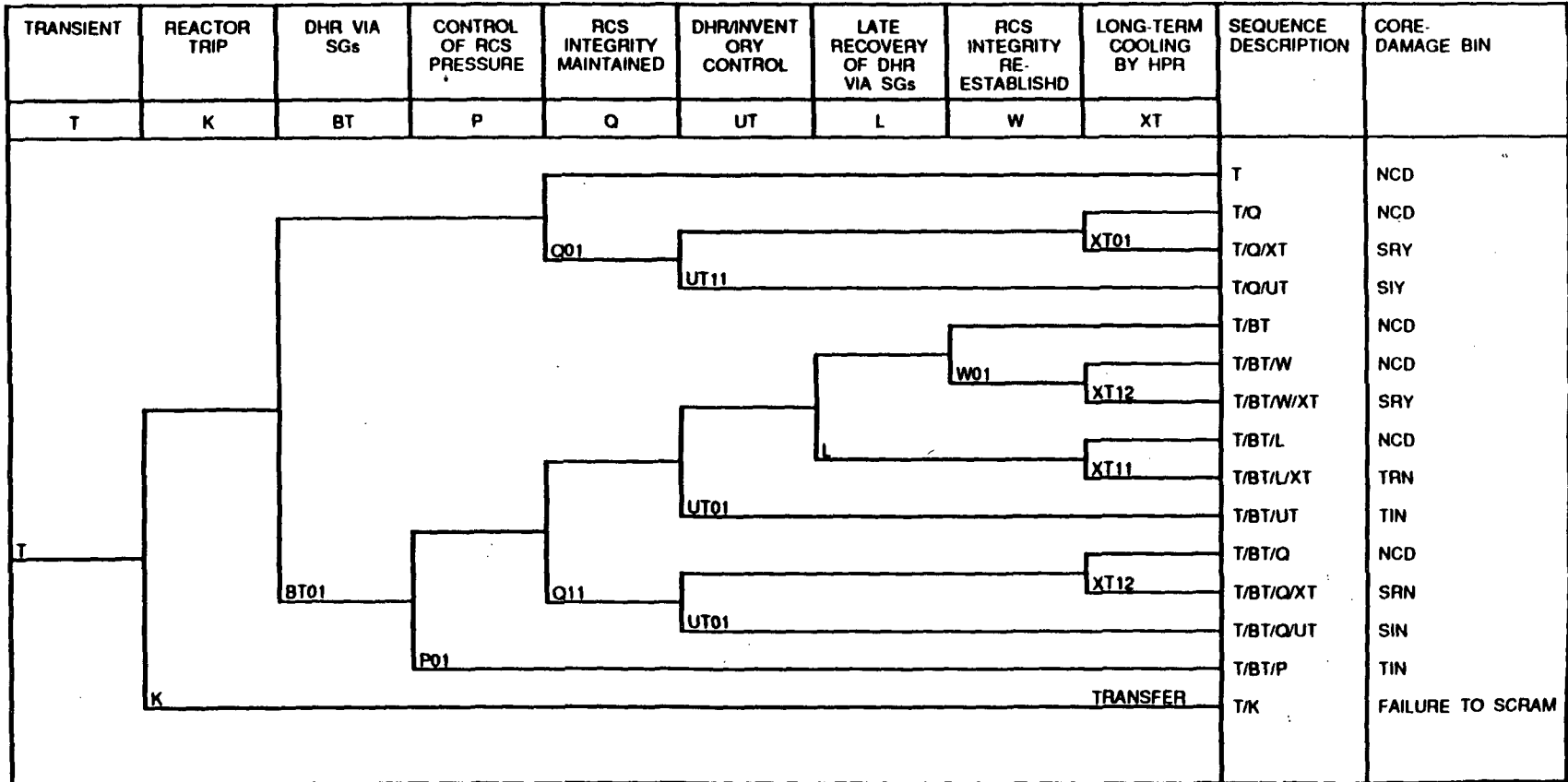


Figure 1-24. Event Tree for Sequences Initiated by a Transient

to supply the steam generators at a rate that would match the decreased level of heat production in the reactor. If the main feedwater system were lost, the turbine-driven AFW pumps would be started automatically, and flow from at least one of them would be sufficient to provide decay heat removal. If either or both of these pumps were to fail, the operators could start the motor-driven feedwater pump.

There are several options for steaming from the generators. Initially following tripping of the main turbine, some combination of the turbine bypass valves, atmospheric vent valves, and MSSVs would typically function to remove the steam that was being produced. The steam generation would decrease rapidly following tripping of the reactor. After that point, only one of these valves on a steam generator receiving feedwater would be needed to support decay heat removal. Because of the redundancy and diversity of the components provided to accomplish this function, it is not modeled explicitly in the context of failure of event B_T.

The logic corresponding to failure of event B_T is shown in Figure 1-25. A number of the initiating events considered in the study have the potential to cause a loss of main feedwater directly (e.g., a loss of offsite power would cause loss of the main feedwater flow). The supporting logic illustrates the effects of these events. If main feedwater is unavailable, the logic indicates that either of the turbine-driven pumps or the motor-driven pump (started by operator action) could provide adequate auxiliary feedwater. The timing of the action to start the motor-driven pump (given loss of main feedwater and failure of both of the turbine-driven pumps) affects downstream events in the event tree. If the operators start the pump within a few minutes, cooling can be reestablished before the PORV setpoint is reached. If starting of the pump is accomplished within 10-12 minutes, the PORV may open, but the pressurizer PSVs would not be challenged. Failure to start the pump within about 30 minutes would lead to uncovering of the core, if makeup/HPI cooling had not been established previously. These aspects were accounted for in the appropriate sequence cut sets during the quantification process.

Event P: control of RCS pressure. If heat removal via the steam generators is lost, RCS pressure will increase as decay heat is stored in the reactor coolant. The setpoint for the PORV will be reached first. Because cycling of the PORV will not provide relief adequate to remove decay heat fully immediately after a reactor trip, pressure will continue to increase until the PSVs are opened. The most likely outcome would be that at least one of the relief valves would open at a higher pressure. This pressure could be too high to permit the injection of cold water by the makeup system as a means of removing decay heat. Because of the relatively small frequency of this sequence, failure of event P following failure of event B_T is assumed to lead to core damage. This somewhat conservative assumption is made to avoid the need to model the sequence in more detail, and is reflected in the event tree in Figure 1-24. Figure 1-26 illustrates the fault-tree logic for failure of event P.

Event Q: maintenance of RCS integrity. Preservation or restoration of RCS heat removal via the steam generators is sufficient to ensure continued core cooling only if the integrity of the RCS pressure boundary is maintained. Small LOCAs that initiate a reactor trip

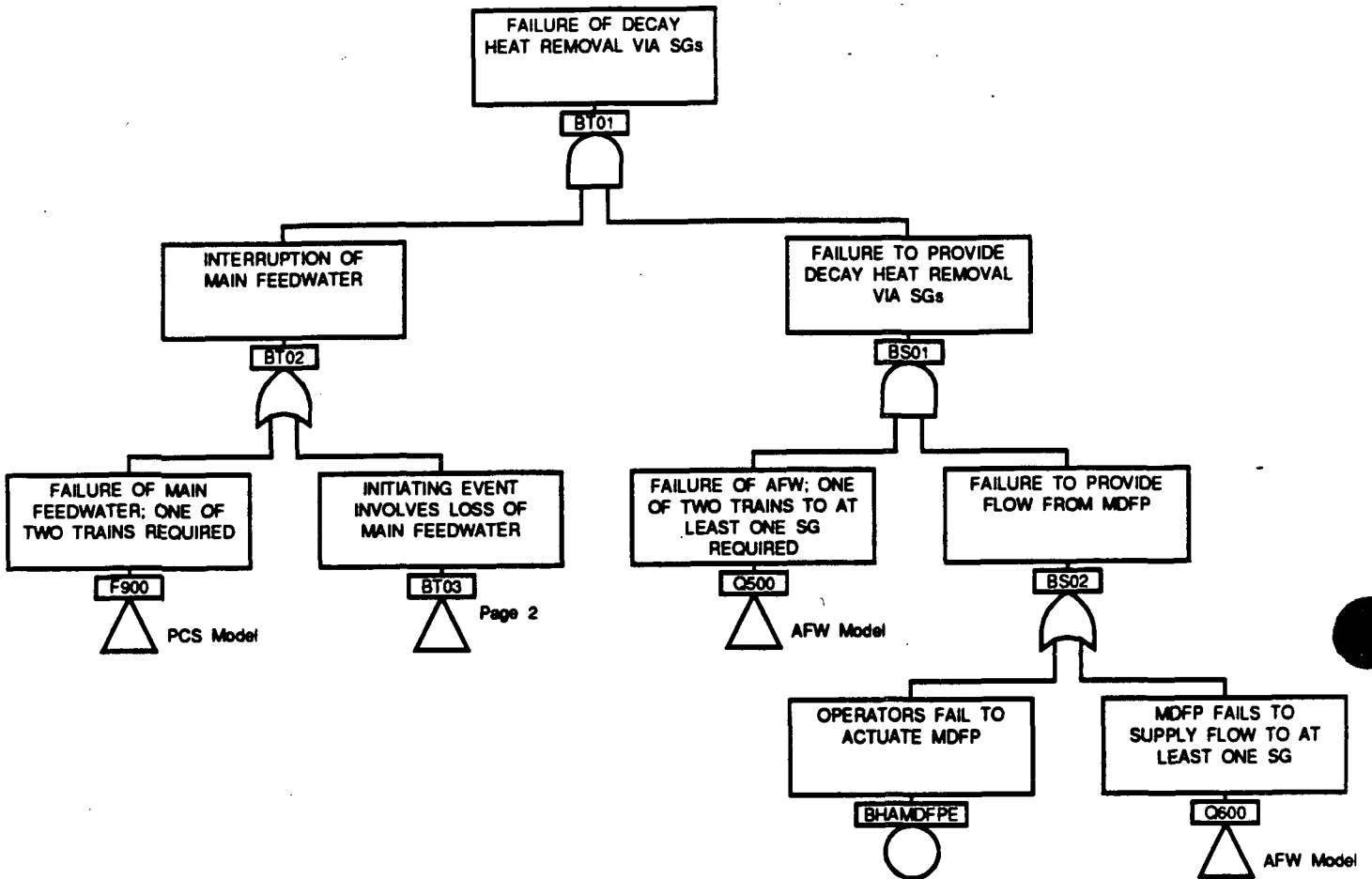


Figure 1-25. Supporting Logic for Top Event B_T of the Transient Event Tree (page 1)

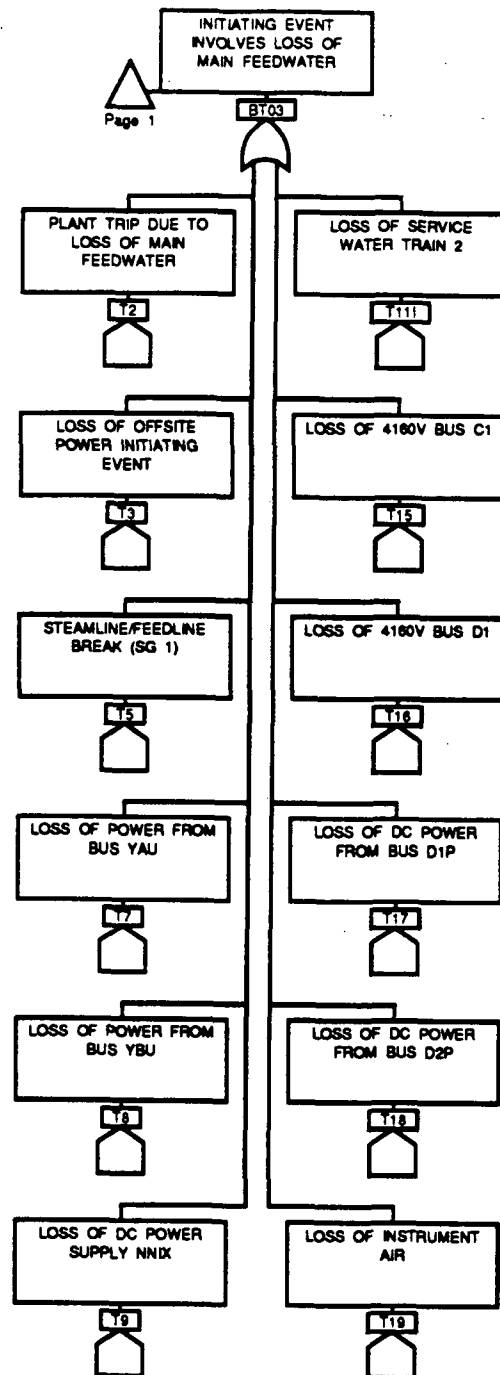


Figure 1-25. Supporting Logic for Top Event B_T of the Transient Event Tree (page 2)

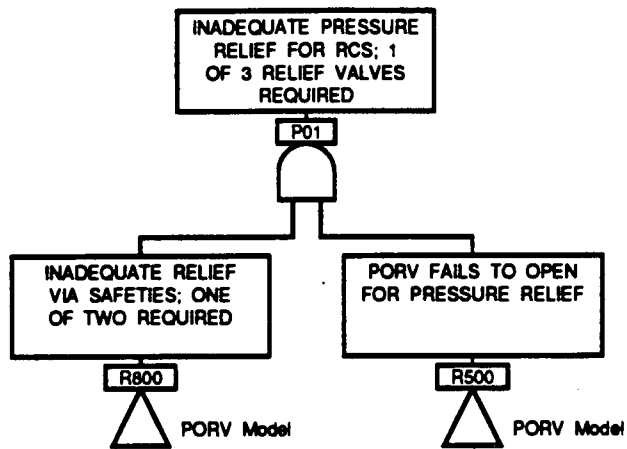


Figure 1-26. Supporting Logic for Top Event P of the Transient Event Tree

are considered separately as initiating events, as described in Section 1.2.1. Small LOCAs that could result from transient upsets fall primarily into two categories: stuck-open pressurizer relief valves, and failures of the RCP seals.

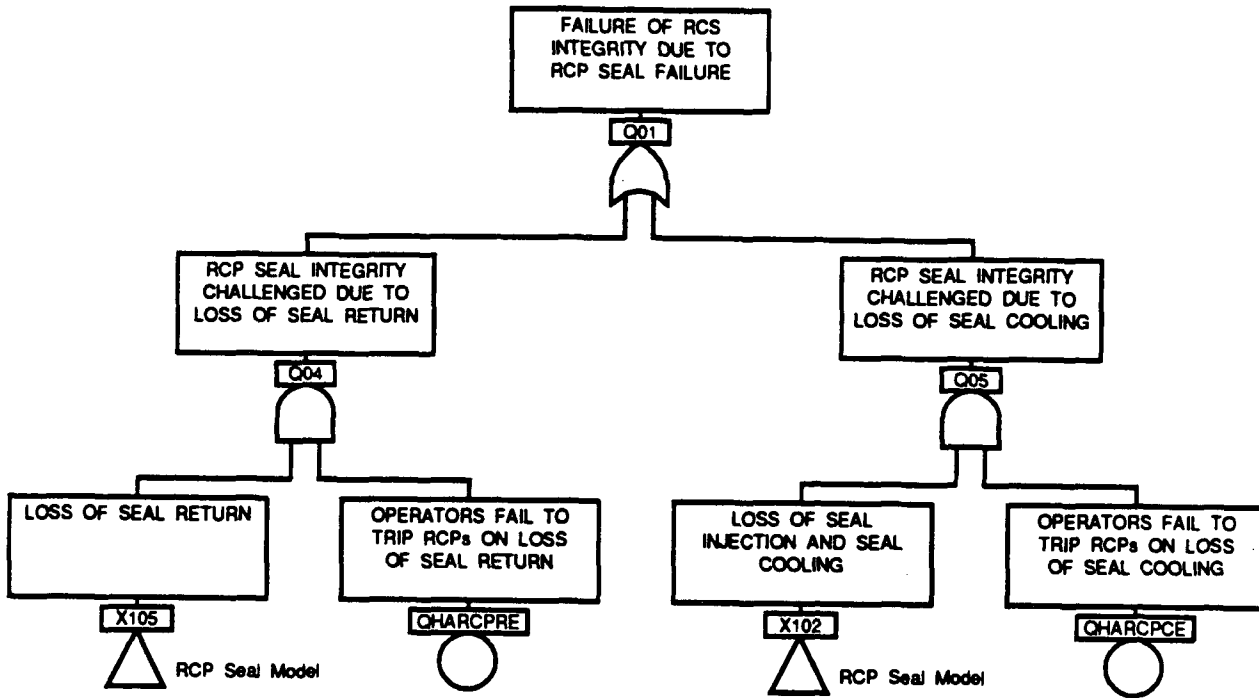
The most important mechanism for a stuck-open relief valve to occur as a result of a transient is for there to be at least a temporary total loss of feedwater. Thus, if RCS heat removal fails initially (i.e., event B_T) but pressure relief succeeds (event P), there is the potential that one of the relief valves that opened will fail to reclose. Whether or not RCS heat removal is interrupted, there is the potential that a failure of the RCP seals could occur as a consequence of loss of seal cooling.

Consideration of the loss of RCS integrity therefore depends on prior event B_T. If decay heat removal is available in the context of event B_T, it is assumed that the only significant potential for loss of integrity would result from a loss of seal cooling. This is shown in the supporting logic provided in Figure 1-27 (represented by top gate Q01).

The effects of various losses of cooling for the RCP seals have been evaluated in response to Generic Issue 23 (Ref. 41). As part of the response to that issue, Davis-Besse, which uses RCPs supplied by Byron-Jackson, now employs a new seal design (designated model N-9000). These seals employ three stages, each of which is designed to withstand differential pressure equivalent to full RCS pressure. Extensive testing and engineering evaluations have been performed for the seals, as described in Section 4.4. Based on this information, the potential for failure of RCP seals leading to a small LOCA is assumed to exist under either of the following conditions (Ref. 42):

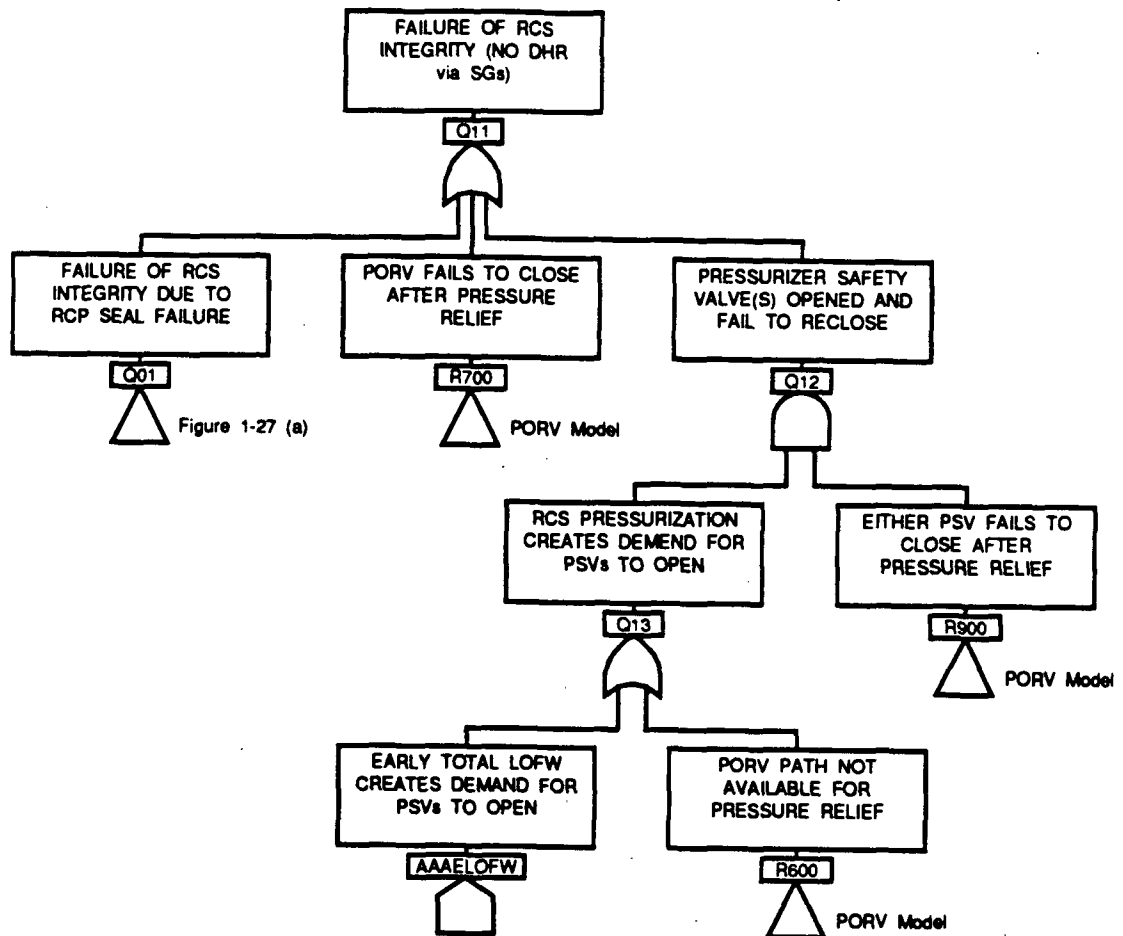
- (1) If seal return is isolated and the RCPs are not tripped within about 30 minutes, or
- (2) If both seal injection and cooling to the pumps' thermal barriers are lost and the pumps are not tripped within about 10 minutes.

As Figure 1-27 shows, in the case of a loss of decay heat removal via the steam generators, loss of RCS integrity can result either because of a stuck-open relief valve or failure of the RCP seals (gate Q11). If there were a sustained loss of feedwater to the steam generators, the pressurizer PORV would be challenged to open. Whether RCS pressure continued to rise to the setpoints for the PSVs would depend on the availability of the PORV and the decay-heat load at the time that of the loss of feedwater. Even if the PORV opened properly, if feedwater were lost at the time of the plant trip, it is likely that its cycling would not be sufficient to prevent the increase in RCS pressure to the setpoints for the PSVs. Because some of the most important failure modes for the AFW system involve operation for a period of hours before failure, the case in which the PORV would be able to provide relief sufficient to prevent opening the PSVs was also considered. This is reflected in the logic by the use of a flag (event AAAELOFW) that permits the timing of loss of feedwater to be addressed for individual sequence cut sets.



(a) With Heat Removal Via the Steam Generators

Figure 1-27. Supporting Logic for Top Event Q of the Transient Event Tree



(b) Without Heat Removal Via the Steam Generators

Figure 1-27. Supporting Logic for Top Event Q of the Transient Event Tree

Note also that, later in the event tree (in event W), an additional chance is given for the relief valves to fail to reclose. This arises as a result of the late restoration of RCS heat removal after makeup/HPI cooling has been established and used for some time.

Event U_T: coolant injection for DHR or inventory control. Event U_T relates to using the makeup and/or HPI systems to maintain core heat removal under conditions of either a total loss of RCS heat removal or a transient-induced small LOCA.

Following a total loss of RCS heat removal via the steam generators, the operators are instructed to reconfigure the makeup system to provide full flow from both pumps when RCS temperature reaches 600°F, and to open the PORV to provide a path for the removal of decay heat (Ref. 39). Calculations indicate that the operators have a minimum of 11 minutes after the total loss of feedwater to establish this mode of core cooling, if all feedwater is lost at the time of the reactor trip (Ref. 37). As noted in the success criteria outlined in Table 1-14, there are primarily two ways in which makeup/HPI cooling can succeed:

- If the PORV can be opened and left open, RCS pressure will shortly begin to decrease, such that adequate flow can be achieved using only one makeup pump (in the piggyback mode, taking suction from the discharge of the associated DHR pump).
- If the PORV cannot be opened, RCS pressure will remain at about 2500 psig as the PSVs cycle. At this higher pressure, flow from both makeup pumps would be needed to remove decay heat.

In the longer term, the success criteria are somewhat reduced, as indicated in Table 1-14. The logic corresponding to failure to establish makeup/HPI cooling is shown in Figure 1-28 (under gate UT01). Based on the timing of the loss of feedwater, the need for the PORV was evaluated on case-by-case basis during the quantification process.

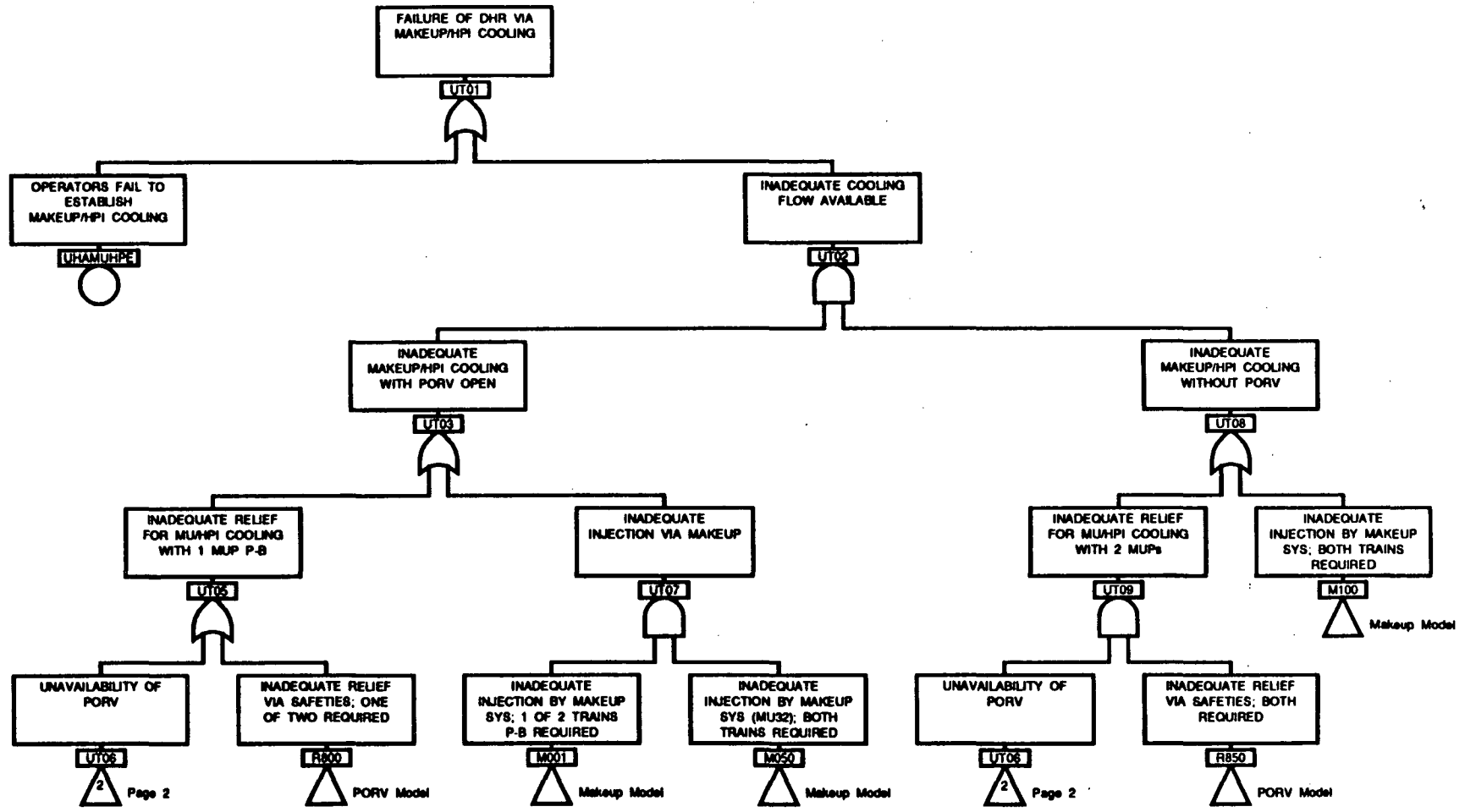
Figure 1-28 also addresses the logic for the failure of safety injection in the event of a transient-induced LOCA (i.e., failure for event Q). This logic, as indicated by gate UT11, is identical to the logic for failure of injection for the small LOCA event tree, as discussed in Section 1.2.1.

Event L: late restoration of decay heat removal via the steam generators. In the event of a sustained loss of RCS heat removal, makeup/HPI cooling could provide core cooling as long as the inventory of water in the BWST was available. Prior to depletion of the BWST inventory, either feedwater would have to be restored, or high pressure recirculation would have to be established. Event L is included in the event tree to provide a means to consider the available options for restoration of feedwater to the steam generators.

It has been estimated that the BWST inventory would reach the setpoint at which the operators would be instructed to initiate high pressure recirculation at about 20 hours after makeup/HPI cooling started (Ref. 33). Depending on the reasons for the early failures of main and auxiliary feedwater, this provides a substantial amount of time for at least some

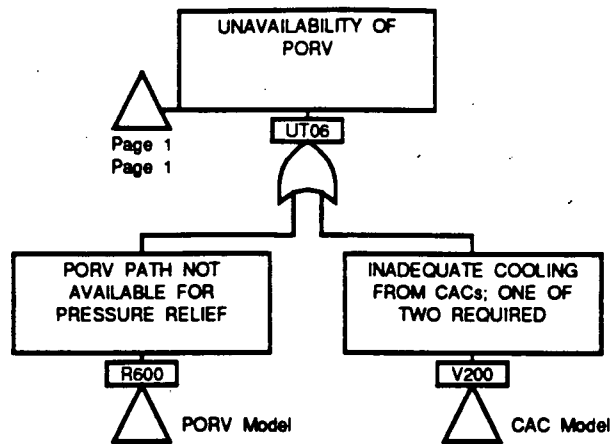
Table 1-14
Specific Success Criteria for Makeup/HPI Cooling

Success Criteria	Comment
<u>With initial, total loss of feedwater:</u>	
<ul style="list-style-type: none"> • Opening of the PORV within about 11 min to provide a bleed path and • Opening of at least one PSV to provide additional relief and • Injection by one of two makeup pumps drawing suction from the discharge of an LPI pump in the piggy-back mode and providing flow to the RCS via both injection lines, with pump mini-recirculation lines and letdown isolated or • Injection by two of two makeup pumps drawing suction from the BWST and providing flow to the RCS via both injection lines or via the normal makeup line, with pump mini-recirculation lines or letdown isolated 	<p>Without RCS heat removal via the steam generators, direct core heat removal must be established by opening a relief path to the containment and initiating makeup flow to remove decay heat (Refs. 37 and 43). The operators are instructed to initiate makeup/HPI cooling at any time when RCS temperature reaches 600°F, irrespective of attempts to recover feedwater or take other recovery actions (Ref. 39). They are instructed to establish flow from both makeup pumps and open the PORV. To provide adequate injection, isolation of mini-recirculation and/or letdown may be required.</p>
<u>OR</u>	
<ul style="list-style-type: none"> • Opening of two of two PSVs to provide relief and • Injection by two of two makeup pumps within about 11 min, drawing suction from the BWST and providing flow to the RCS via both injection lines, with pump mini-recirculation lines or letdown isolated 	
<u>With loss of feedwater delayed (about 4 hr):</u>	
<ul style="list-style-type: none"> • Opening of the PORV within about 30 min to provide a bleed path or • Opening of at least one PSV to provide relief and • Injection by one of two makeup pumps drawing suction from the discharge of an LPI pump in the piggy-back mode or directly from the BWST. 	<p>The PORV is needed for up to about 4 hr (Ref. 44). After that time, because of the absence of the initial large heat load and the significantly reduced decay heat level, a single PSV could serve as an adequate path for the removal of decay heat, even with only one makeup pump providing injection.</p>

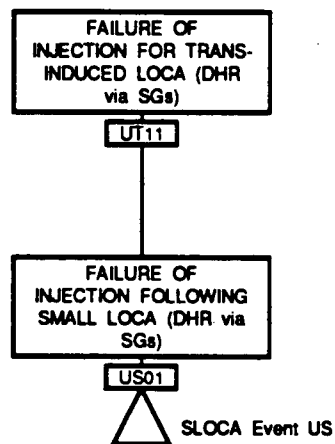


(a) Following Total Loss of Feedwater (page 1)

Figure 1-28. Supporting Logic for Top Event U_T of the Transient Event Tree



(a) Following Total Loss of Feedwater (page 2)
Figure 1-28. Supporting Logic for Top Event U_T of the Transient Event Tree



(b) Injection with Feedwater Available
Figure 1-28. Supporting Logic for Top Event U_T of the Transient Event Tree

cooling to be made available to the steam generators. No explicit logic corresponding to the failure of this event has been constructed. The event is used to define the sequences of interest; restoration of feedwater is considered on a case-by-case basis for the cut sets associated with the sequence up to that point.

Event W: late restoration of RCS integrity. If RCS heat removal were restored after makeup/HPI cooling had been established, core cooling could be maintained if the integrity of the RCS could be restored as well. This would entail closing the relief valve or valves used during makeup/HPI cooling.

The logic corresponding to failure of event W is shown in Figure 1-29. If the PORV had been used for makeup/HPI cooling, the PSVs would not be challenged further to open and therefore be given the opportunity to fail to reclose (failure to reclose during the early pressurization, before establishment of makeup/HPI cooling, is considered in the context of event Q). If the PORV were not available, it is assumed that both PSVs would have been cycling during makeup/HPI operations. Note that assessment of failure to reclose for these valves reflects the judgment that, after extended operation for relieving subcooled or two-phase flow, the PSVs may not close as reliably as they would for short-term pressure transients.

Event X_T: long-term cooling. If feedwater could not be restored, or if a transient-induced LOCA occurred, it would be necessary to establish a means of long-term cooling before the BWST inventory is depleted. The logic for failure of long-term cooling is shown in Figure 1-30. For the case of a loss of RCS integrity (failure of event Q) but with heat removal available via the steam generators (success for event B_T), the logic is identical to that for the analogous event X_S (under gate XS01) for the small LOCA. Failure in this case, indicated by gate XT01, takes into account the options of cooling down the RCS and establishing shutdown cooling or low pressure recirculation using the DHR system, or remaining at pressure and performing high pressure recirculation.

If makeup/HPI cooling had been initiated as a consequence of a total loss of feedwater, it might not be possible to cool down sufficiently to use the DHR system before the BWST inventory was depleted. It would be necessary for the operators to provide suction to the HPI pumps from the discharge of the DHR pumps, which would draw from the containment emergency sump. Earlier, makeup/HPI cooling could have succeeded with the RCS pressure near the setpoints for the PSVs if the PORV were not available, because of the high shutoff head of the makeup pumps. Procedures warn against using the makeup system to recirculate water from the containment sump, however, so that only use of the HPI pumps is considered. The shutoff head for the HPI pumps is well below the setpoint for the PSVs (2500 psig). Therefore, the PORV would have to be opened to support high pressure recirculation, if it had not already been opened for makeup/HPI cooling. This logic is developed under gate XT11.

In the event that there is a transient-induced LOCA as well as a total loss of feedwater, high pressure recirculation is again assessed to be the only option for long-term cooling that

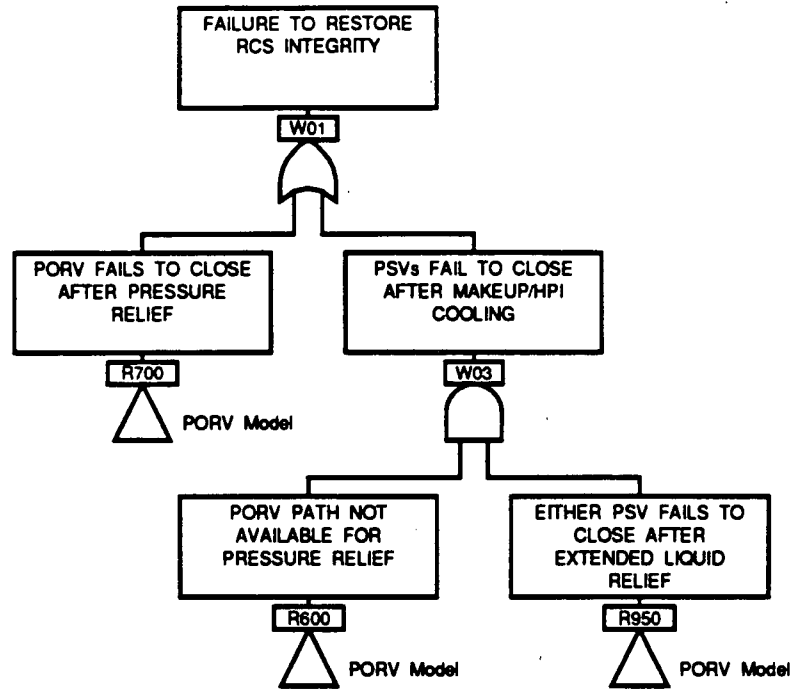
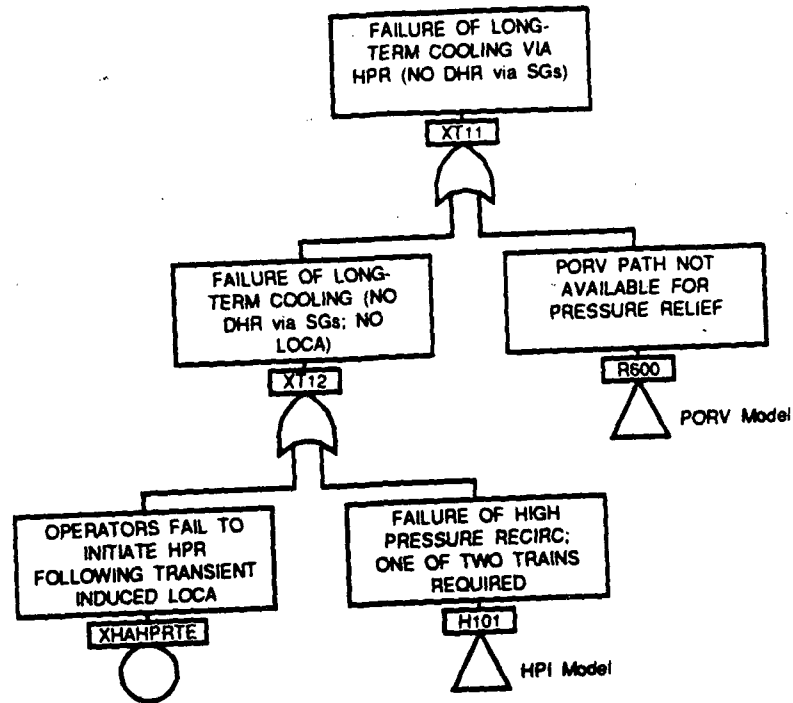
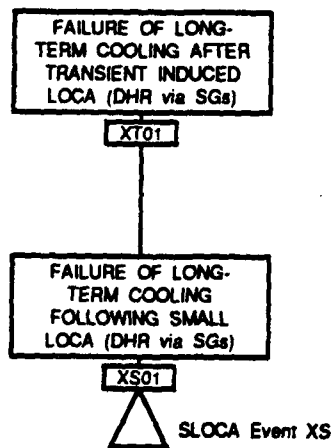


Figure 1-29. Supporting Logic for Top Event W of the Transient Event Tree



(a) Without Feedwater Available

Figure 1-30. Supporting Logic for Event Top XT of the Transient Event Tree



(b) With Feedwater Available

Figure 1-30. Supporting Logic for Top Event XT of the Transient Event Tree

could be established before the BWST inventory was depleted. In this case, the PORV would not be needed, so only gate XT12 (under gate XT11) is used in the quantification process.

Summary of sequences for the transient event tree. The transient event tree (Figure 1-24) illustrates the functional-level sequences that could result from a transient initiating event. These sequences are as follows:

- Sequence T. In this sequence, the reactor trips successfully, decay heat removal is provided by the steam generators, and RCS integrity is maintained. Core cooling is therefore successful.
- Sequence TQ. Unlike the previous sequence, sequence TQ involves a loss of RCS integrity (event Q) due to failure of the RCP seals (since RCS heat removal was not interrupted). Adequate makeup was available in both the injection and recirculation phases, however, and core damage was averted.
- Sequence TQX_T. Sequence TQX_T involves a transient-induced LOCA, as in the previous sequence. In this case, although injection succeeds, core damage results from the failure to establish long-term cooling (event X_T). This sequence is assigned to core-damage bin SRY, since the RCS pressure and release rate to the containment would correspond to a small LOCA; the failure would occur after successful injection; and feedwater would be available to at least one of the steam generators.
- Sequence TQU_T. In sequence TQU_T there is a transient-induced LOCA, and core cooling is lost as a result of failure to provide adequate safety injection (event U_T). This sequence is assigned to bin SIY.
- Sequence TB_T. Sequence TB_T is a transient with a total loss of feedwater (event B_T). Makeup/HPI cooling succeeds in the short term, and feedwater is restored before the BWST inventory is depleted. The operators are able to reestablish RCS integrity, and core cooling is successful.
- Sequence TB_TW. This sequence is similar to the preceding sequence, except that, when feedwater is eventually restored, at least one of the relief valves used to support makeup/HPI cooling does not reclose (event W). High pressure recirculation succeeds, averting core damage.
- Sequence TB_TWX_T. In sequence TB_TL₁WX_T, as in the previous sequence, heat removal via the steam generators is regained, but it is not possible to reestablish RCS integrity. Core damage results because of failure of high pressure recirculation. This sequence is assigned to bin SRY, since feedwater is available and core cooling was lost after an extended period of successful injection.
- Sequence TB_TL. Sequence TB_TL involves total loss of feedwater, and feedwater fails to be restored before the BWST is depleted during makeup/HPI cooling (event L). High pressure recirculation succeeds, so that core damage does not occur.
- Sequence TB_TLX_T. Sequence TB_TLX_T is similar to the previous sequence, except that high pressure recirculation fails, resulting in core damage. This sequence is assigned to core-damage bin TRN.

- Sequence $TB_T U_T$. Sequence $TB_T U_T$ involves a total loss of feedwater and failure to establish makeup/HPI cooling (event U_T). Since this is a failure of injection, the sequence is assigned to bin TIN.
- Sequence $TB_T Q$. This sequence also involves the interruption of feedwater, and there is a subsequent LOCA due to either a stuck-open relief valve or a failure of RCP seals. Injection and recirculation cooling succeed, however, averting core damage.
- Sequence $TB_T QX_T$. This sequence also involves a transient-induced LOCA coincident with a total loss of feedwater. Makeup/HPI cooling is successful early, but high pressure recirculation fails when the inventory of the BWST is depleted. It is assigned to bin SRN, since feedwater is not available.
- Sequence $TB_T QU_T$. Sequence $TB_T QU_T$ is a transient-induced LOCA after loss of all feedwater, with failure to provide adequate injection (event U_T) for inventory control and decay heat removal. The sequence corresponds to core-damage bin SIN.
- Sequence $TB_T P$. In this sequence, heat removal via the steam generators is lost, and the pressurizer relief valves fail to prevent overpressurization of the RCS (event P). Core damage is assumed to result. The sequence is assigned to bin TIN.
- Sequence TK. This is a transient with failure of the reactor to trip. The sequences that could result are developed further through a transfer to the event tree for failure to trip, described in detail in the next section.

Event Tree for Failure to Trip

Because the demands placed on the systems needed to maintain core cooling can be significantly different for transients with failure of the reactor to trip, a separate event tree for such sequences was developed. Two closely-related considerations are most important in evaluating the potential for core damage to result from a failure to trip: (1) the ability to remove heat from the core and the RCS at a rate sufficient to avoid disruption of the fuel cladding, and (2) the need to maintain RCS pressure at a level that would not result in serious damage to the RCS pressure boundary.

The most challenging sequences that result from the failure to trip would generally be those that involve the loss of main feedwater (Refs. 45 and 46). In such cases, the interruption of normal heat removal would lead to a rapid increase in RCS pressure as the heat generated by the core was stored in the reactor coolant, and to an insurge of coolant into the pressurizer. The RCS pressure would reach a maximum that would depend on many factors, the most important of which would include the following:

- The initial power level, which would determine in part the amount of heat that would continue to be generated;
- The time in core life, which would determine the amount of negative reactivity feedback based on the moderator-temperature coefficient (MTC);

- The amount and timing of heat removal provided by the steam generators; and
- The availability of pressure relief, and specifically of the pressurizer spray, the PORV, and the PSVs.

As the reactor coolant heated up, the moderator-temperature feedback would lead to a decrease in reactor power. If the RCS retained its integrity through the initial pressurization, reactor power would eventually stabilize at a point approximately equivalent to the heat removal capacity corresponding to the amount of main or auxiliary feedwater being supplied to the steam generators. During this period, the operators would continue to attempt to insert the control rods; failing that, they would begin boration of the RCS to achieve shutdown.

Because of the relatively low frequency of sequences involving failure to trip, it was appropriate to simplify the sequence analysis in some areas. The primary simplification was to eliminate from consideration potential core-damage sequences that did not directly result from the failure to trip. For example, the RCS pressure transient would lead to a demand for pressure relief, with a corresponding potential for one or more of the relief valves to fail to reclose. Such a sequence is clearly bounded by other transients that could lead to a small LOCA, and by the small LOCA initiating event itself. The success or failure of long-term cooling is also not explicitly modeled. If adequate heat removal is sustained early in the transient, and if neutronic shutdown is achieved, it is assumed that the frequency of core damage due to subsequent failures is low compared to other types of accidents.

The acceptance criteria that define whether or not core damage would be expected to occur for the LOCAs and transients presented in the preceding event trees do not apply directly to the case of failure to trip. For other sequences, the acceptance criteria and corresponding success criteria are predicated on the assumption that heat removal corresponding only to decay power levels is required. In this case, it is necessary to establish criteria for an adequate rate of heat removal, and for RCS pressure to remain within bounds that would indicate a serious rupture would not result.

With respect to the first of these areas, the ability to avoid serious disruption of the reactor fuel has generally not been found to be of concern, provided adequate heat removal via the steam generators can be maintained uninterrupted (Ref. 47). For purposes of this study, this is assumed to infer that, if main feedwater is lost, AFW must be supplied automatically by at least one of the two turbine-driven pumps.

It is somewhat more difficult to determine the actual pressure capacity of the RCS. Depending on how failure of the RCS is defined, gross rupture of the RCS pressure boundary would not be expected unless pressure far exceeded 5,000 psig. Leakage might occur at lower pressures. This would bring into question the operability of the valves that serve as the pressure boundary between the reactor vessel and the injection systems. If a large pressure spike could both create leakage and defeat the injection systems because the isolation check valves could not open, core damage might result. The potential for leakage at pressures above about 4,300 psig has not been investigated in detail, and therefore cannot be

immediately ruled out (Ref. 48). Based on the design pressures of the check valves, however, it is judged that they will remain operable when exposed to downstream pressures above 4,300 psig (Refs. 49 and 50). The actual pressures at which significant leakage might occur or the valves might fail to operate are not known. Because the frequency of a transient involving failure to trip is low, it is reasonable to select a relatively conservative acceptance criterion (such as 4,300 psig) so that effort required for detailed analysis can be devoted to more important scenarios.

The nominal peak pressure for a failure to trip following loss of main feedwater is estimated to be about 4,100 psig (Ref. 46). It is necessary, therefore, to define events that would cause this peak pressure to be substantially more than 200 psi higher than this value, assuming conservatively that such a condition could lead to core damage. Sensitivity studies have been performed on a number of parameters that could affect the peak pressure (Ref. 47). Among the results that could be relevant to this assessment are the following:

- Changes in initial power level are very important. A reduction in initial power of 5% would reduce the peak pressure by about 200 psi; a reduction of 15% would reduce the peak by about 500 psi. This is especially important because plant experience indicates a somewhat higher rate of trips involving loss of main feedwater that occur at lower power levels than while operating at nominal full power.
- The moderator-temperature coefficient can also be significant. A MTC that is less negative or more negative by 10% can cause the peak pressure to likewise increase or decrease by approximately 100 psi.
- The ability to provide adequate pressure relief is critical. A reduction of 10% in the relief capacity can cause the peak pressure to increase by as much as 200 psig.

A review was made of the trip experience at Davis-Besse. It was determined that most of the trips due to causes other than the loss of main feedwater occurred at or near full power. Accounting for the positive attributes of this minority of lower-power trips, therefore, would not have a significant effect on the frequency of overpressurization due to failure to trip. A more pronounced correlation was observed between power level and the likelihood of a trip coincident with loss of main feedwater. Of the ten such trips, four occurred at or near full power; the remainder occurred at power levels of 40% or less. It is estimated that a loss of feedwater occurring at these lower power levels would result in a peak RCS pressure lowered by over 1000 psi if the reactor failed to trip.

If either pressurizer safety valve failed to open, the total relief capacity (based on the ratio of flow areas) would be reduced by about 38% (Ref. 45). Because the PORV is smaller than a PSV, its failure would cause the pressure capacity to be reduced by about 24%. Failure of any of the three relief valves to open is therefore assumed to lead to an unacceptable peak pressure, unless the initial power level were low (i.e., less than about 40%) or the MTC were more negative.

A nominal value for MTC of $-1.04 \times 10^{-4} \Delta k/k/^\circ F$ was used in the base-case analyses of response to a failure to trip (Ref. 46). A distribution of the MTC value over a typical fuel cycle was reviewed, and it was determined that the MTC would be more negative than this value within four days of a 500-day cycle. During the first days, the MTC may be less negative, depending on the amount of critical boron. During this time, there is also significant testing, and the period at full power is likely to be limited. Because of uncertainties during this period, and because of the potential for changes in future refueling cycles, it was conservatively assumed that a failure to trip during the first 1% of the cycle could lead to a pressure rise that could threaten RCS integrity. On the other hand, the period of time during which the MTC might be sufficiently negative to offset the effects of a failure such as that of one of the relief valves to open would be relatively short. Hence, the potential benefit of such an MTC was neglected.

The considerations relating to the effects of power level, MTC, and the status of relief valves on the peak RCS pressure are summarized in Table 1-15 for reference purposes. The reduced set of success criteria for sequences involving failure to trip are therefore as summarized in Table 1-16.

The success criteria were incorporated into a simple event tree to delineate potential core-damage sequences that could result from a failure to trip. This event tree is illustrated in Figure 1-31. As in the case of the transient event tree, event T is a placeholder for all of the initiating events for which this event tree applies (i.e., small LOCA, SGTR, and all of the transients). Reactivity control is considered in events K_1 (early) and K_2 (late). RCS heat removal is considered separately for main feedwater (event B) and auxiliary feedwater (event L). Event P_K reflects the conditions that could lead to a failure of RCS pressure control and a consequential loss of RCS integrity. To preserve core heat removal, it is assumed that the reactor must eventually be shut down, as considered in event K_2 . Each of these events is described below.

Event K_1 : reactivity control early. Event K_1 represents the need for reactor trip at the outset of the transient. If the reactor trips, the remainder of this event tree does not apply. Failure of the reactor to trip, as discussed in Section 2.2, is modeled as a single basic event that reflects a common-cause mechanical failure of the control rods to insert into the core. Thus, failure for event K_1 implies that shutdown may later have to be achieved by emergency boration.

Event B: heat removal available via main feedwater. The availability of heat removal via the main feedwater system is broken out separately in this event tree because the loss of main feedwater has a very large impact on whether or not the subsequent peak pressure could challenge the integrity of the RCS or the operability of RCS components. If main feedwater continues to function following the demand for reactor trip, it is assumed that only emergency boration is necessary to prevent core damage. Otherwise, AFW must provide heat removal, and the additional conditions that could lead to an unacceptable pressure in the RCS must be considered.

Table 1-15
Assumed Effects of Relevant Factors for Failure to Trip After
Loss of Feedwater

Reactor Status		Impact on Peak RCS Pressure		
Initial power level	Moderator-temp. coefficient	All relief valves function	One relief valve fails to open	Two relief valves fail to open
High	more negative than 99% value	Acceptable peak	Unacceptable peak	Unacceptable peak
	less negative than 99% value	Unacceptable peak	Unacceptable peak	Unacceptable peak
Low	more negative than 99% value	Acceptable peak	Acceptable peak	Unacceptable peak
	less negative than 99% value	Acceptable peak	Unacceptable peak	Unacceptable peak

Table 1-16
Success Criteria Following Failure to Trip

Safety Function	Success Criteria	Comments
Reactivity control	<ul style="list-style-type: none"> • Insertion of two of seven rod groups by actuation of RPS or DSS <p align="center">OR</p> <ul style="list-style-type: none"> • Establishment of emergency boration by the makeup system within 1 hr. 	<p>If the control rods cannot be inserted, it will be necessary to borate using the makeup system. It is conservatively assumed that this must be initiated within one hour from the onset of the transient.</p>
Control of RCS pressure	<ul style="list-style-type: none"> • Continued RCS heat removal via MFW <p>OR</p> <p><u>If reactor power is initially high:</u></p> <ul style="list-style-type: none"> • MTC more negative than the 99% value <p align="center">and</p> <ul style="list-style-type: none"> • The PORV and both PSVs open for pressure relief <p><u>If reactor power is initially low:</u></p> <ul style="list-style-type: none"> • The PORV and both PSVs open for pressure relief <p align="center">OR</p> <ul style="list-style-type: none"> • At least two of three pressurizer relief valves open for pressure relief and • MTC more negative than the 99% value. 	<p>If main feedwater remains available, the peak pressure will be substantially lower than if feedwater is interrupted. Without main feedwater available, the peak pressure is assumed to exceed the capacity of the RCS under some conditions. These are broken out further in Table 1-14.</p>
Control of RCS inventory	<ul style="list-style-type: none"> • Assured if RCS pressure is controlled; precluded otherwise. 	<p>If the RCS pressure reaches an unacceptable peak, a large system rupture is assumed to occur.</p>
Heat removal	<ul style="list-style-type: none"> • Continued flow from at least one MFW pump to at least one of two steam generators <p align="center">OR</p> <ul style="list-style-type: none"> • Flow from at least one of two turbine-driven AFW pumps. 	<p>MFW would prevent excessive RCS pressure and ensure adequate heat removal until the reactor could be shut down. Without MFW, it is assumed that only the turbine-driven AFW pumps can deliver flow in time to prevent an unacceptably high peak pressure, since the motor-driven pump would be started manually.</p>

INITIATING EVENT	REACTIVITY CONTROL (EARLY)	RCS HEAT REMOVAL VIA MFW	RCS HEAT REMOVAL VIA AFW	RCS PRESSURE CONTROL LED WITHIN LIMITS	REACTIVITY CONTROL (LATE)	SEQUENCE DESIGNATOR	CORE-DAMAGE BIN
T	K1	B	L	PK	K2		
						T	NO FAILURE TO SCRAM
						T/K1	NCD
						T/K1/B01	NCD
						T/K1/B01/K201	TIY
						T/K1/B01/PK01	SIY
						T/K1/B01/L01	SIN

Figure 1-31. Event Tree for Sequences Involving Failure to Trip

The supporting logic for failure of event B is shown in Figure 1-32. The logic is straightforward, and indicates either failure of the main feedwater system to respond initially, or loss of main feedwater as a direct consequence of the initiating event.

Event L: heat removal available via auxiliary feedwater. If main feedwater is lost, AFW flow must be made available both to preserve core cooling and to prevent the RCS pressure from reaching a very high peak. It is assumed that a delay in actuating AFW would lead to unacceptable consequences; therefore, only automatic actuation is considered. This means that credit can be given only to flow from the turbine-driven pumps, since the motor-driven pump would require manual actuation. The supporting logic is comprised of the top event for the AFW system fault tree, and is also shown in Figure 1-32.

Event P_K: RCS integrity maintained by controlling RCS pressure. The conditions that could lead to overpressurization of the RCS are evaluated in the context of event P_K. These conditions are discussed earlier, and are summarized in Tables 1-14 and 1-15. The supporting logic for this event, shown in Figure 1-33, is a fault-tree representation of the information in the tables. Note that, as discussed earlier, only loss-of-feedwater initiators are considered as potential lower-power initiating events. This is based on a review of the plant-specific operating experience, which indicated that there was a higher likelihood that a trip involving a loss of feedwater would occur at power levels below about 40% than would be the case for other types of initiating events.

Event K₂: reactivity control late. Following the initial peak pressure, the RCS pressure at which some level of stability would be reached would depend on a wide variety of factors. For purposes of this analysis, it is assumed that the RCS pressure would remain near the setpoints for the pressurizer relief valves for an extended period. This would cause a demand for makeup to ensure that the core remained covered. It is assumed that the injection of borated water is required both to preserve RCS inventory and to bring about an eventual shutdown so that more stable conditions can be achieved. Because only mechanical failures of the RPS are considered in these sequences, the only way in which shutdown can be achieved is by the injection of borated water. As called for by the emergency procedure, it is assumed that this would require use of the makeup system, with the operators aligning suction to draw from the BWST (Ref. 39). The operators would also need to maintain letdown of reactor coolant so that the boron concentration of the RCS could be increased appropriately. The supporting logic for failure of this event is shown in Figure 1-34.

Summary of sequences involving transients without trip. The sequences that could result from a failure to trip are summarized below. Note that the first sequence in the event tree implies successful trip, and consequently is not discussed further.

- Sequence TK₁. Sequence TK₁ involves failure of the rods to insert due to a mechanical common-cause fault (event K₁). Main feedwater provides heat removal, and shutdown is achieved by emergency boration. Core damage therefore does not occur.

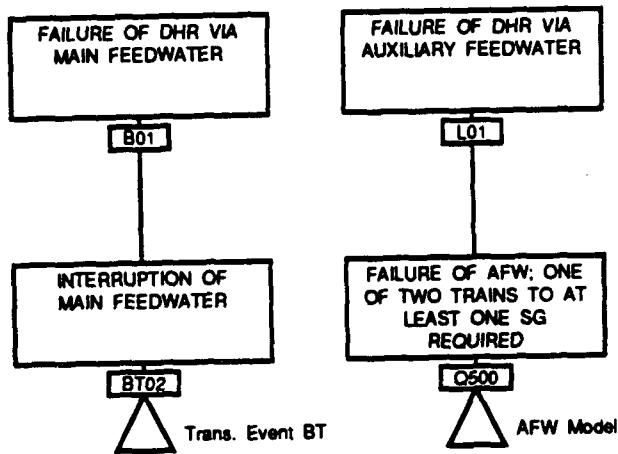


Figure 1-32. Supporting Logic for Top Events B and L of the Event Tree for Failure to Trip

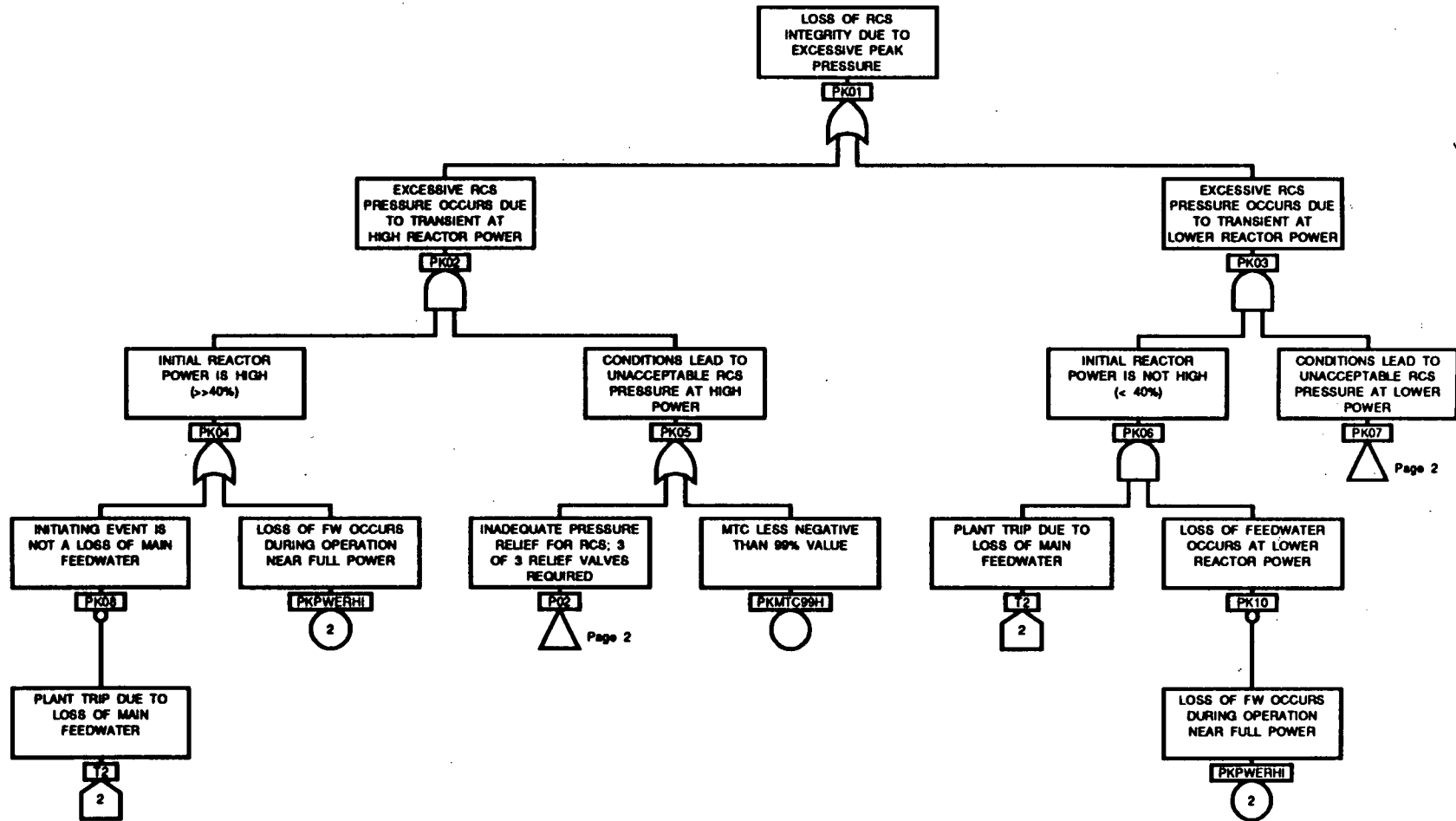


Figure 1-33. Supporting Logic for Top Event P_K of the Event Tree for Failure to Trip (page 1)

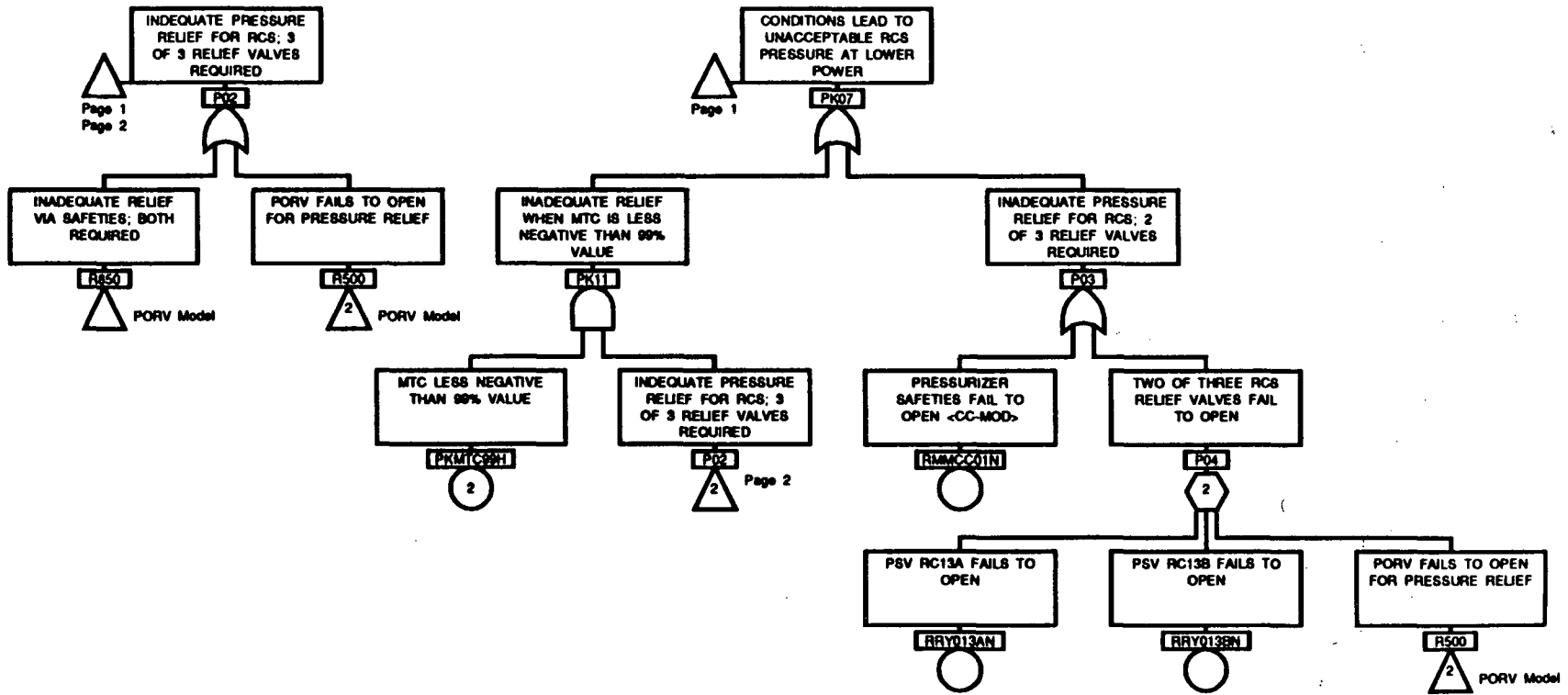


Figure 1-33. Supporting Logic for Top Event P_K of the Event Tree for Failure to Trip (page 2)

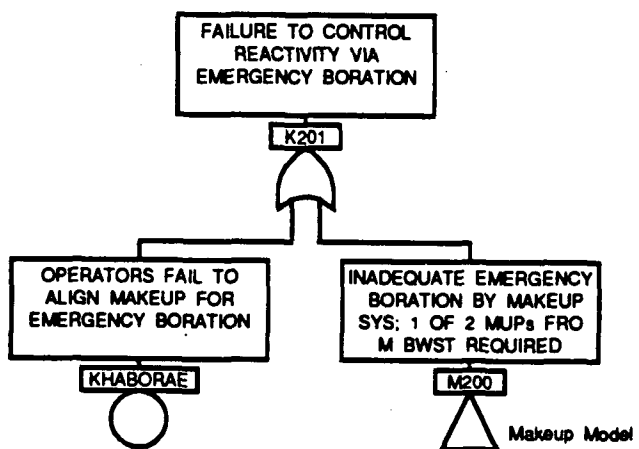


Figure 1-34. Supporting Logic for Top Event K₂ of the Event Tree for Failure to Trip

- Sequence TK₁K₂. In this sequence, main feedwater is again successful. Core damage occurs, however, due to the inability to provide injection of borated water (event K₂). This sequence is assumed to lead to core damage at high pressure, with feedwater available to the steam generators. It is therefore assigned to core-damage bin TTY.
- Sequence TK₁B. This sequence involves a failure to trip and loss of main feedwater (event B). Auxiliary feedwater provides RCS heat removal, however, and the reactor is successfully shut down.
- Sequence TK₁BP_K. Sequence TK₁BP_K involves a loss of main feedwater and failure to control RCS pressure, so that overpressurization occurs (event P_K). It is assumed that this sequence would lead to a major rupture in the RCS, and that the injection systems would not be able to provide flow (e.g., due to damage to the check valves comprising the RCS pressure boundary). The sequence is assigned to bin AIX.
- Sequence TK₁BL. This sequence involves a total loss of RCS heat removal. It is assumed that this sequence would also lead to a severe overpressurization of the RCS, and it is therefore assigned to bin AIX as well.

1.2.3 Event Trees for Internal Floods

In section 1.1.3, six initiating events involving internal floods were identified for analysis. All six of these events could lead to a reactor trip, either automatically, or manually as a precaution due to the amount of equipment affected. In all of these cases, the RCS would initially be intact (i.e., none leads directly to a LOCA). The floods therefore were accommodated by the event trees constructed for transient events. They were treated as transients, and their effects on plant equipment were modeled explicitly at the appropriate point in the system fault trees. No separate event trees were constructed for these initiators.

1.3 SEQUENCE GROUPING IN BACK-END ANALYSIS

As noted in Section 1.2, potentially important differences in the impact on subsequent containment response were incorporated into the definition of the core-damage sequences. This was accomplished through the definition of core-damage bins, which both define the conditions of interest and serve to permit sequences with similar characteristics to be grouped. The development of the core-damage bins and their role in the interface between the front-end and back-end analyses are described in Section 3 of Part 4. The sequences and their assignment to core-damage bins are summarized in Table 1-17.

**Table 1-17
Summary of Core-Damage Bins and Sequence Assignments**

Bin	Bin Description	Sequence	Sequence Description
AIX	Large LOCA leakage rate, failure of injection	AUA	Large LOCA initiating event with failure of low pressure injection
		TK ₁ BP _K	Any initiating event with failure to trip, loss of main feedwater, and failure to maintain RCS pressure within acceptable limits
		TK ₁ BL	Any initiating event with failure to trip and total loss of feedwater
ARX	Large LOCA leakage rate, failure of recirculation	AX _A	Large LOCA initiating event with failure of low pressure recirculation
		AV	Reactor vessel rupture initiating event
MIX	Medium LOCA leakage rate, failure of injection	MU _M	Medium LOCA initiating event with failure of high or low pressure injection
MRX	Medium LOCA leakage rate, failure of recirculation	MX _M	Medium LOCA initiating event with failure of low pressure recirculation
SIY	Small LOCA leakage rate, failure of injection, with feedwater available	SU _S	Small LOCA initiating event with failure of injection
		TQU _T	Transient or flood initiating event with RCP seal LOCA and failure of injection
SIN	Small LOCA leakage rate, failure of injection, with feedwater not available	SB _S U _S	Small LOCA initiating event with failure of feedwater and failure of makeup/HPI cooling
		TB _T QU _T	Transient or flood initiating event with total loss of feedwater, RCP seal LOCA or stuck-open relief valve, and failure of makeup/HPI cooling

Table 1-17 (continued)
Summary of Core-Damage Bins and Sequence Assignments

Bin	Bin Description	Sequence	Sequence Description
SRY	Small LOCA leakage rate, failure of recirculation, with feedwater available	SXS	Small LOCA initiating event with failure of long-term cooling via DHR or recirculation from sump
		RCUXR	SGTR with failure of cooldown via unaffected steam generator, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation
		RBUXR	SGTR with failure of feedwater to unaffected steam generator, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation
		RCRCUXR	SGTR with failure of cooldown by both steam generators, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation
		RCRBUXR	SGTR with failure of cooldown by ruptured steam generator, failure of feedwater to unaffected steam generator, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation
		TQXT	Transient or flood initiating event with RCP seal LOCA and failure of long-term cooling
		TBTWX_T	Transient or flood initiating event with total loss of feedwater early, successful makeup/HPI cooling, stuck-open relief valve when feedwater is restored, and failure of high pressure recirculation
SRN	Small LOCA leakage rate, failure of recirculation, with feedwater not available	SB_SX_S	Small LOCA initiating event with failure of feedwater and failure of high pressure recirculation
		TBTQXT	Transient or flood initiating event with total loss of feedwater early, successful makeup/HPI cooling, stuck-open relief valve or RCP seal LOCA, and failure of high pressure recirculation

Table 1-17 (continued)
Summary of Core-Damage Bins and Sequence Assignments

Bin	Bin Description	Sequence	Sequence Description
RIY	Bypass due to steam generator tube rupture, with failure of injection but availability of feedwater	RUR I	SGTR with failure of injection and failure to isolate generator containing ruptured tube
		RCUUR	SGTR with failure of cooldown via unaffected steam generator, failure of injection for cooldown via makeup/HPI cooling
		RBUR	SGTR with failure of feedwater to unaffected steam generator, failure of injection for cooldown via makeup/HPI cooling
		RCRUR I	SGTR with failure of cooldown via ruptured steam generator, failure to isolate that generator, and failure of injection
		RCRCUUR	SGTR with failure of cooldown using either steam generator and failure of injection
		RCRBUUR	SGTR with failure of cooldown using ruptured steam generator, failure of feedwater to unaffected steam generator, and failure of injection
RIN	Bypass due to steam generator tube rupture, with failure of injection and failure of all feedwater	RBURUR	SGTR with failure of feedwater to both steam generators and failure of makeup/HPI cooling
		RCRBUUR	SGTR with cooldown via ruptured steam generator not available, failure of feedwater to both steam generators, and failure of makeup/HPI cooling
RRY	Bypass due to steam generator tube rupture, with successful injection but failure of long-term cooling, with feedwater available	RIPR	SGTR with failure to isolate ruptured steam generator, failure to control RCS pressure to reach low pressure conditions
		RCUI	SGTR with failure to isolate ruptured steam generator, failure to cool down using unaffected steam generator

Table 1-17 (continued)
Summary of Core-Damage Bins and Sequence Assignments

Bin	Bin Description	Sequence	Sequence Description
RRY (continued)		RBUl	SGTR with failure to isolate ruptured steam generator, failure to provide feedwater to unaffected generator
		RC _R IP _R	SGTR with failure to cool down using ruptured steam generator, failure to isolate that generator, and failure to control RCS pressure to reach low pressure conditions
		RC _R CUl	SGTR with failure to cool down using either steam generator and failure to isolate the ruptured generator
		RC _R BUl	SGTR with failure to cool down using the ruptured steam generator, failure to isolate that generator, and failure of feedwater to the unaffected generator
RRN	Bypass due to steam generator tube rupture, with successful injection but failure of long-term cooling, with feedwater not available	RBU _B R	SGTR with failure of feedwater to both steam generators, successful makeup/HPI cooling, but failure to restore feedwater to achieve long-term cooling
		RBU _B RI	SGTR with failure of feedwater to both steam generators and failure to isolate the ruptured generator
		RC _R BU _B R	SGTR with failure to cool down using the ruptured steam generator, failure of feedwater to both steam generators, successful makeup/HPI cooling, but failure to restore feedwater to achieve long-term cooling
		RC _R BU _B RI	SGTR with failure to cool down using the ruptured steam generator, failure of feedwater to both steam generators and failure to isolate the ruptured generator
V	Bypass due to interfacing-systems LOCA	VHlH	Interfacing-systems LOCA due to failure in HPI injection line, failure to isolate break
		VLlL	Interfacing-systems LOCA due to failure in LPI injection line, failure to isolate break

Table 1-17 (continued)
Summary of Core-Damage Bins and Sequence Assignments

Bin	Bin Description	Sequence	Sequence Description
V (continued)		VDID	Interfacing-systems LOCA due to failure of DHR suction valves, failure to isolate break
		VSI _S	Interfacing-systems LOCA due to premature opening of DHR suction valves, failure to isolate break
TIN	Transient (i.e., no LOCA) with failure of feedwater and failure of injection	TBTUT	Transient or flood with total loss of feedwater and failure of makeup/HPI cooling
		TBTP	Transient or flood with total loss of feedwater and failure of pressurizer relief valves to open
TRN	Transient with failure of feedwater and failure of recirculation	TBTLXT	Transient or flood with extended total loss of feedwater and failure of high pressure recirculation
TIY	Transient with failure of injection, but feedwater available	TK ₁ BK ₂	Any initiating event with failure to trip, loss of main feedwater, and failure to provide borated makeup

Section 2 SYSTEMS ANALYSIS

In the preceding section, the systems that could play a role in preventing core damage were identified in the event trees and their supporting logic. This section describes the manner in which the possible failures of those systems were evaluated. For most systems, this was accomplished through the construction of detailed, coordinated fault-tree models. Section 2.1 provides an overview of the system modeling. It includes a discussion of the approach taken in developing the fault-tree models, including modeling assumptions, the role of human interactions, and a discussion of the failure modes modeled. Section 2.2 provides a description of each system modeled in the PRA. It discusses the system function, its design and operation, system dependencies, and how the system was integrated into the overall plant model. It is in this section that the overall system dependency matrix which describes the hard-wired, functional, spatial, and other dependencies can be found.

2.1 OVERVIEW OF SYSTEMS ANALYSIS

The systems analysis task had two principle objectives. The first was to develop an overall plant model that accurately depicts the design and operation of the systems required to respond to the initiating events identified in Section 1. The second was to solve the event trees by quantifying the integrated model to obtain the core-melt sequences and their frequencies.

The task of developing system models required coordination and iteration with several other tasks. The success criteria that defined the top events for the front-line systems (i.e., those directly involved in providing core cooling) were developed as part of the event sequence logic. As the modeling process yielded increased understanding of system operation and failure modes, appropriate modifications were made to the event trees and their supporting logic. Coordination with the assembly of the reliability data base was also important. It was necessary to develop the fault trees to a level of detail sufficient to identify all potentially important failure modes, and especially to ensure that dependencies were properly addressed. Failure rates and other data were needed for each of the primary events identified in this manner. On the other hand, it was also necessary to ensure that the modeling not be carried to such a fine level of detail that meaningful failure rates could not be derived from the available data bases. In some cases, failures were developed down to a fine level of detail to aid in understanding the system, but the low-level events were then combined into a single basic event for the application of data.

Close coordination was also required with the assessment of human reliability. As described in Section 3.2, events relating to human interactions before and in response to initiating events were included at appropriate points in the fault trees. Finally, the quantification process imposed some constraints on the modeling process. To facilitate the computer solution process, groups of independent basic events were, in some cases, combined

in modules. The use of modules effectively reduced the size of the fault trees for the solution process, without causing information to be lost. The modularization step is described further in Section 2.1.1.

The result of the systems analysis effort was the development of fault-tree models that describe the ways in which plant systems can fail and subsequently contribute to sequences that lead to core-damage. The determination of the systems for which modeling was required was based on the results of the initiating event and accident sequence analysis discussed in Section 1. The assessment of the relevant accident sequences culminated with the creation of event trees based on those safety functions that needed to be accomplished to prevent core damage, and the systems that fulfilled those functions. Systems that are directly involved in achieving the safety functions are referred to as front-line systems. Fault-tree models were developed for all such front-line systems. Models were subsequently developed for those systems which provide the needed support functions, such as electric power and cooling water for the front-line systems. Table 2-1 lists the system models developed and describes the extent of the analysis performed for each system. In some cases, a simplified model or system-level unavailability was used where it was determined that this was appropriate. For example, failure of main feedwater (MFW) following a reactor trip was developed through a simple fault tree in which all dependencies on other systems were identified, and faults within the MFW system itself were represented by a single basic event. The unavailability for this basic event was based on extensive plant experience, and it was judged that this would yield a more accurate representation of the system reliability than would be achieved by a detailed fault-tree analysis for the system.

2.1.1 System Modeling Guidance

The systems required to respond to an initiating event were identified through the accident sequence analysis. It was in this section that the functions necessary to maintain core cooling were defined. Fault-tree logic was used to translate the various core cooling functions into specific system requirements. This is referred to as the top logic, and it defined the top gates for the development of the system-level fault trees.

For the Davis-Besse IPE, models for the core-damage sequences consisted of sets of large fault trees that were linked together based upon the logic specified in the event trees. The fault trees incorporated all significant contributors to system failure, including front-line component failures, common-cause failures, support system failures, maintenance unavailabilities and operator errors where appropriate. Data for all events were applied to the fault-tree models, and the integrated model was solved to define the combinations of events that lead to core-melt. As such, the method used for determining the core-melt frequency was the "large fault tree, small event tree" approach.

Development of the fault-tree models was based on the guidelines outlined in the PRA Procedures Guide (Ref. 51). Emphasis was placed on choosing appropriate system boundaries, consistently treating component failures in the models, developing and applying a basic event naming scheme, and providing consistent documentation in each of the system

**Table 2-1
Systems Analysis Summary**

System Model	Analysis Method
Decay heat removal	Detailed fault-tree model for low pressure injection and recirculation and for shutdown cooling.
High pressure injection	Detailed fault-tree model for injection and recirculation.
Core flood	Detailed fault-tree model.
Makeup and purification	Detailed fault-tree model for seal injection, makeup/HPI cooling and emergency boration.
Reactor coolant	Detailed fault-tree models for pressurizer spray, the PORV, the primary safeties and the reactor coolant pumps and seals.
Power conversion	Detailed fault-tree models for the AVVs, MSIVs and TBV. Simplified fault-tree models for the condensate system and the circulating water system. Simplified fault-tree model based on plant data for the main feedwater system.
Auxiliary feedwater	Detailed fault-tree model including both turbine-driven pumps and the motor-driven pump.
Containment spray	Detailed fault-tree model for injection and recirculation.
Containment air cooling	Detailed fault-tree model.
ECCS room coolers	Detailed fault-tree model.
Containment isolation	Detailed fault-tree model.
Reactor trip	System-level failure assessment.
Safety features actuation system	Detailed fault-tree model for the various actuation levels.
Electric power	Detailed fault-tree models for various busses, MCCs, diesel generators, batteries and chargers.
Service water	Detailed fault-tree model for various service water loads.
Component cooling water	Detailed fault-tree model for various CCW loads.
Instrument air	Detailed fault-tree model for various headers.

notebooks. For each system, applicable design drawings, system descriptions, accident analysis, Technical Specifications, licensee event reports, electrical one-line drawings, logic diagrams and operating and maintenance procedures were collected and reviewed. Each system analyst became intimately familiar with the design and operation of the system prior to development of the system fault-tree model. System walk-downs were also used to aid in understanding integrated system operation. For purposes of this analysis, the fault trees were developed based on the system configurations and operating procedures as they existed on June 30, 1990. Because of the relatively few modifications made after June 1990, those implemented during the subsequent refueling outage, the seventh refueling outage, were also implemented. Therefore, the PRA models reflect the as-built configuration of the plant as of the end of the seventh refueling outage. (The eight refueling outage is scheduled to begin on March 1, 1993).

Based on a knowledge of the system and its role in the accident sequences, fault-tree models were developed for the system functions as they appeared in the top logic file. Top gates were defined in terms of major system trains or blocks (e.g., combinations of flow paths in the case of a fluid system). This approach simplified any subsequent changes to the fault trees to accommodate modified or added events as they were identified in the event sequence analysis and quantification tasks.

The following general rules were followed in the development of each fault-tree model:

- Top events for each fault tree were defined in terms of their function as identified in the core-damage sequence analysis. System success criteria were based on vendor information, supporting scoping calculations, and engineering judgment. In some instances, conservative assumptions were made to bound those cases for which limited information existed. Such assumptions were re-evaluated, as necessary, if they had a dominant effect on the results of the analysis.
- Each fault tree included failures which would interrupt a process flow path, divert flow from a process flow path, interrupt required support functions or cause loss of control of a process flow path. Failures in small lines which diverted flow away from a train or component but which had no significant impact on system function (usually a diversion of less than ten percent of the primary flowrate) were excluded.
- Fault-tree models were ultimately developed only to the level of detail at which appropriate failure data existed. For example, in reviewing plant records for pump failures, information to determine the specific failure mechanism (e.g., breaker fault, wiring fault, lube oil pump fault) was not always available. Consequently, a basic event for failure of the pump to start includes all such failures.
- Appropriate references to support systems were made through the use of transfer gate logic rather than developing the same support system model for several front-line systems. This ensured the same support system logic was applied to all applicable front-line systems. A set of system boundary conditions was employed to ensure that this linking was done correctly.

This approach assured that system interactions which arise due to functional dependencies between different systems were modeled explicitly.

- The effects of initiating events on the availability of a system were included in the fault tree to ensure that they were tracked properly. For example, the initiator referring to loss of power from dc bus D1P is included as one of the failure modes for the bus in the fault tree.
- Minimum recirculation paths were modeled if they were required for component operability during the mission specified for the sequence under consideration.
- Human error contributions to system unavailability were considered for each event in the fault trees. Human errors made prior to the initiating event were modeled at the component or train level. For each standby system, separate human failure events were modeled for each standby train in addition to one that applied to both trains. Operating procedures were used to determine post-initiator human interactions which were modeled at the highest level possible in the fault trees or logic supporting the event trees. As described in Section 3.2, high screening values were used for the human interactions in the quantification process. Events that were considered potentially important during the sequence quantification process were then evaluated in detail.
- Maintenance which could be performed while at power was included in the fault trees. Maintenance unavailability was generally modeled in terms of groups of components (trains) for each system.
- Testing which could be performed while at power was included in the fault-tree models. It should be noted, however, that testing was included only if it put the system in a configuration that would make the system unavailable to perform its safety function.
- Check valves were modeled for failure to remain open and failure to prevent reverse flow only if such a failure prevented the system or subsystem from performing its required function.
- Manual valves and other components with low failure probabilities were included for analysis completeness and to provide a mechanism for modeling reconfiguration to off-normal conditions. Manual valves in instrument lines (i.e., root valves) were typically not modeled. Manual valves which could affect multiple instruments and also had the potential to be misaligned because of testing or maintenance were modeled to ensure consideration of dependencies.
- Events which required numerous independent component failures in order to occur (i.e., several basic events below an AND gate) were excluded if their combination was of low probability and there were no dependencies involved.
- Pipe breaks within systems were typically not modeled, except in cases in which a pipe break had the potential to fail the entire system or more than one system.

After initial delineation of the system failure modes, the effective size of the fault trees was reduced to facilitate the quantification process. This was done through a process of combining independent basic events into groups, referred to as modules. The modules were

defined based on logical groupings of system faults (e.g., by including all of the basic faults associated with an individual pump train), rather than by creating the largest possible independent sub-trees, as has sometimes been done in past PRAs. In this way, it was possible to consolidate the fault trees significantly, without loss of the basic structure or understanding of the system reflected in the original fault trees.

The most important aspect of the modularization process was the need to ensure that any potentially dependent events were not incorporated. To that end, the following types of events were not permitted to be included in modules:

- Links to support systems,
- Human interactions,
- Common-cause events*,
- Maintenance unavailabilities, and
- Flags that defined conditions for the event-sequence analysis.

Once the modularized fault trees were developed, they became the basic system models for the analysis, and no attempt was made to maintain the detailed fault trees. Any changes to the logic were made for the modularized fault trees. When changes were made, however, care was still taken to ensure that dependencies were accounted for properly.

Fault trees form the basis for the analysis of all systems and sequences. It is through the solution of the fault trees that minimal cut sets are identified and the sequence frequencies estimated. Several sources of information were collected, reviewed and incorporated into the fault trees. It was essential for this information to be recorded in a consistent format such that it could be easily reviewed and readily modified if necessary. As such, each fault tree is documented in a system notebook that describes the system, its function, and operating and maintenance practices. Each system notebook also contains a copy of the system fault tree, applicable drawings, Technical Specifications, a summary of associated licensee event reports and any modeling assumptions. Figure 2-1 is the standard table of contents that was used in assembly of each system notebook to guide the development of the fault trees.

In an effort to develop a relatively straightforward model, some assumptions were made with regard to the overall plant configuration. For example, Davis-Besse has three service water pumps, one of which is normally lined up as the primary, a second as the secondary, and the third as a spare. The plant configuration chosen was based on normal operating configurations taking into consideration any additional equipment requirements (such as the additional breakers associated with the CD switchgear pumps). In this analysis, service water train 1 was modeled as the normally operating train serving primary loads via

* Each common-cause event itself was defined as a separate module that combined a basic component fault and the appropriate common-cause factor. This facilitated the process of updating events based on changes to the data bases. These events were never included in modules with other events.

Table of Contents

- 1.0 System Function
- 2.0 System Description
 - 2.1 Equipment Description
 - 2.2 System Testing and Maintenance
 - 2.3 Component Location in Plant
 - 2.4 System One-Line Diagram
- 3.0 System Operation
 - 3.1 Normal System Operation
 - 3.2 Accident Condition System Operation
 - 3.3 Applicable Technical Specification Limits
- 4.0 Support Systems
- 5.0 Operating Experience Review
- 6.0 Modeling Notes and Assumptions
 - 6.1 Modeling Assumptions
 - 6.2 Top Gates Modeled
 - 6.3 Flags Included in the Model
 - 6.4 Human Actions Included in the Model
 - 6.5 Common-Cause Failures Modeled
- 7.0 Modularized Fault tree
- 8.0 References

Figure 2-1. Typical Table of Contents for a System Notebook

pump 1-3, with train 2 normally operating supplying the secondary loop via pump 1-2. Similarly, CCW pump 1-2 was modeled as the normally operating pump with CCW pump 1-3 in standby. Both service water pump 1-1 and CCW pump 1-2 were modeled as spare pumps with their respective breakers racked out. Makeup pump 1-2 was modeled as the normally operating pump with pump 1-1 aligned as a backup. Other less significant configurations, such as non-essential motor-control center alignments, are discussed in the appropriate system notebooks.

A consistent naming convention was used throughout development of the models to identify uniquely each event in the study. All gates are made up of three or four characters and all basic events are made up of eight characters. The use of these characters is described below:

- **Gates.** Gates were designated as follows: sxxx(x), where s was used to designate the system to which the event applies and xxx(x) is a sequential number.
- **Basic events.** Basic events were identified as follows: stcxxxxf where s was used to designate the system to which the event applies, tc was used to designate the component type code (e.g., MV for motor-operated valve and TP for turbine-driven pump), xxxx was used by the analyst to denote the specific component and f was used to describe the failure mode (e.g., C for fails to close and F for fails to run). The component type code and failure mode provided a direct link to the data base, as described in Section 3.1.
- **Maintenance blocks.** Maintenance blocks were identified as follows: sMBxxxxx, where s was used to designate the system to which the event applies, "MB" was used to designate the event as a maintenance block, and xxxxx was used by the analyst to describe the effected component or group of components.
- **Modules.** Modules were identified as follows: sMMxxxxx where s was used to designate the system to which the event applies, "MM" was used to designate the event as a module and xxxxx was used by the analyst to describe the effected component or group of components.
- **Common-cause events.** Common-cause events were identified as follows: sMMCCxxx, where s was used to designate the system to which the event applies, "MMCC" was used to designate the event as a common-cause event and xxx was used by the analyst to describe the specific common-cause event. Common-cause events were developed as modules, hence the nomenclature "MMCC". The module included one event that described the component type code and failure mode and another event that provided the common-cause multiplier.
- **Flags.** Flags were identified as AAAXxxxx, where "AAA" identified the event as a flag and xxxxx was used by the analyst to denote the specific flag.
- **Human interactions.** Human interactions were identified as follows: sHAXxxxxt where s was used to designate the system to which the event applies, "HA" was used to designate the event as a human interaction, xxxx was used by the analyst to describe the event itself and t was used to

describe the type of human action: "L" for pre-initiator, "E" for post-initiator type CP, and "R" for post-initiator type CR events.

- **Recovery events.** Recovery events were identified as follows: Zrcxxxxy where "Z" was used to designate the event as a recovery, rc was used to identify the type of recovery, "HA" for human action, "OP" for offsite power recovery following a plant trip and "T3" for recovering offsite power following the loss of offsite power as the initiating event, xxxx was used by the analyst to describe the event itself and y was used to identify the type of recovery, "E" for type CP human interactions and "R" for type CR interactions or other recovery.

2.1.2 System Dependencies

One of the most important aspects of the development of the system fault trees was the proper treatment of dependencies. The types of dependencies that were considered include the following:

- Functional dependencies, in which the function or failure of one system affects the ability of another to function in the role called for by the system models. For example, high pressure recirculation following a small LOCA would require function of the DHR system in the low pressure recirculation mode. These functional failures were modeled explicitly in the fault trees.
- Spatial dependencies, which imply the potential for failure of multiple components due to common location. The assessment of spatial dependencies focused on the potential for adverse environments, and particularly on the need for ventilation, heating, or room cooling under various accident conditions, and these were modeled explicitly. Dependencies due to the effects of flooding from sources within the plant were also explicitly modeled, as summarized in Section 2.1.3.
- Hardwired dependencies, which include reliance on support systems. The links to support systems were also modeled explicitly throughout the logic.
- Human interactions, which could result in common failure of multiple trains or systems. These were included in the logic, as described in Section 3.2.
- Inter-component dependencies, involving failure of similar components due to a common cause.

The inter-system dependencies, including functional and hardwired dependencies, are summarized in the matrix provided as Table 2-2. Each of these dependencies is detailed further in conjunction with the system descriptions provided in Section 2.2.

Inter-component dependencies comprise the subset of dependent events referred to as common-cause failures. During the development of the fault trees, care was taken to identify groups of components that could be subject to common-cause failure. The types of events that were modeled include the following:

- Identical or similar pumps within the same system (failure to start or to run);

**Table 2-2
Overall System Dependency Matrix**

System	Support Systems												
	Ac Power	Dc Power	Service Water	CCW	IA	Room Cooling	BWST	SFAS	Main Steam	Con-denser	Circ. Water	TPCW	Makeup
DHR train 1/2	C1/D1	D1P/D2P		*		*	*	*					
HPI train 1/2	C1/D1	D1P/D2P		*		*	*	*					
CS train 1/2	E1/F1	D1P/D2P				*	*	*					
ECCS rm 105/115	E1/F1		*										
Makeup train 1/2	C1/D1	D1P/D2P		*	*	*	*						
PORV		D2N				*							
CAC 1-3/1-2	E1/F1		*		E1/F1			*					
Pressurizer spray	F1												
RCPs	*	*		*	*								*
Ctmt. isolation	E1 & F1												
Core flood													
SFAS													
EDG 1-1/1-2	Y1/Y2	D1P/D2P		*		*							
SBODG		*				*							
Dc Power	E1/F1					*							
Batteries						*							

**Table 2-2 (continued)
Overall System Dependency Matrix**

System	Support Systems												
	Ac Power	Dc Power	Service Water	CCW	IA	Room Cooling	BWST	SFAS	Main Steam	Con-denser	Circ. Water	TPCW	Makeup
Service wtr trn 1/2	C1/D1	D1P/D2P				*							
CCW train 1/2	C1/D1	D1P/D2P	*			*		*					
SAC 1-1	*	*											*
SAC 1-2	*												*
EIAC	*												
AFW train 1/2	*	*							*				
MDFP	*	*											
MFW train 1/2	E3/F3	*			*				*	*			*
TBVs	*	DBP			*					*	*		
AVV 11B/11A	Y1/Y2	D1P/D2P			*								
MSIV MS101/100	Y1/Y2	D1P/D2P			*								
Main condenser	*												*
Circ. water													
TPCW													

- Two or more valves which perform a similar function within a system, or are located in the same environment (failure to open, to close, or to control flow);
- Logic signals which perform redundant functions;
- Diesel generators (failure to start or to run);
- Batteries and chargers (no output);
- Bus-tie breakers (failure to open or to close);
- Identical or similar ventilation fans or room coolers within the same system (failure to start or to run);
- Air compressors (failure to start or to run);
- Pump strainers (failure to operate).

2.1.3 System Modeling for Internal Flood Analysis

A thorough evaluation was made of the potential for core damage due to the effects of internal flooding. A separate report documents in detail the assessment of the internal flood hazard (Ref. 30). The results presented in that report include the identification of a specific set of initiating events involving internal floods.

Basic events representing these initiating events were incorporated directly into the fault-tree logic at the point at which they would affect individual trains or whole systems, as appropriate. Where necessary, additional basic events representing failures to terminate the flooding prior to failure of additional equipment were also included in the fault trees. Thus, internal flooding is actually treated in the same manner as any other initiating event in quantifying the frequencies of the core-damage sequences.

2.2 SYSTEM DESCRIPTIONS

This section provides brief descriptions of the systems that were evaluated as part of the IPE. The information in this section is a summary of that compiled in the system notebooks. Each section provides an outline of the system function, an overview of its design and operation, further definition of the dependencies shared with other systems, and a description of its role in the core-damage sequences.

2.2.1 Decay Heat Removal

The decay heat removal (DHR) system operating in the low pressure injection (LPI) mode injects borated water to the RCS for emergency core cooling in the event of a LOCA. The DHR system also provides for long-term core cooling post-LOCA by recirculating water from the containment sump. In the decay heat removal mode, the system removes decay heat and sensible heat from the reactor during the latter stages of cooldown (i.e. after the steam generators reduce RCS temperature to approximately 280F) and during cold shutdown.

Design and Operation

As shown in Figure 2-2, the DHR system consists of two independent pumping trains which, in the LPI mode, take suction from the BWST and inject borated water into the RCS through the core flood lines. Both LPI suction headers are kept filled and ready for service at all times. When the borated water storage tank (BWST) level decreases to approximately 8 feet, the system is aligned to recirculate reactor coolant from the containment emergency sump in the low pressure recirculation (LPR) mode. For LOCAs in which RCS pressure is too high for adequate injection flow, the DHR pumps, taking suction from the BWST, can be aligned to provide suction to the high pressure injection (HPI) pumps in a "piggyback" operation. When the BWST reaches its low-low-level limit, the DHR pumps, taking suction from the sump, can also provide suction to the HPI pumps for high pressure recirculation (HPR). In the decay heat removal mode, the system takes suction from one of the RCS hot legs and returns flow through the DHR coolers to the RCS via the core flood lines.

The BWST is an insulated tank located outside the west end of the auxiliary building. The BWST contains a minimum volume of 482,778 gallons of borated water at a minimum boron concentration of 1800 ppm. The boron concentration is maintained at levels high enough to provide an adequate shutdown margin. Because the BWST is located outside, a recirculation system and a heating system are provided to prevent stratification of boron and freezing of the water. The temperature range for operability of the BWST is 35F to 90F. For control purposes, level and temperature indicators are provided.

The single outlet line from the BWST contains a manual valve that is normally locked open. This line is divided into separate suction lines for the two DHR trains. Each of these lines contains a motor-operated valve that is normally open (valves DH7A and DH7B). These valves are interlocked with the sump outlet valves (DH9A and DH9B) such that only one set can be opened at any one time.

The containment emergency sump is an open concrete structure with two motor-operated outlet valves, DH9A and DH9B. A wire mesh intake screen with 0.25 inch openings prevents large particles from getting into the recirculation lines and possibly obstructing flow or damaging the DHR pumps.

During decay heat removal operation, the pumps take suction from the RCS via the decay heat drop line, which is connected to the #2 hot leg. This line is normally isolated by two motor-operated valves in series, DH11 and DH12. If either valve is unavailable, bypass valves (DH21 and DH23) can be manually opened to establish a DHR flowpath. Downstream, the line branches into two paths where normally closed motor-operated valves (DH1517 and DH1518) are also opened for decay heat removal operation.

The DHR pumps are single-stage centrifugal pumps with a rated capacity of 3000 gpm each. The bearings are cooled and lubricated by oil which is moved by slinger rings and is, in turn, cooled by the component cooling water (CCW) system.

The DHR coolers are shell and tube, U-type heat exchangers. The discharge of the DHR pumps passes through the tube side of the coolers. The cooling water, which is CCW,

passes through the shell side. The DHR cooler and bypass valves DH14A and DH14B and DH13A and DH13B are solenoid-actuated, pneumatically operated butterfly valves. These valves are used to ensure maximum cooling in the LPI mode (necessary for pump protection during injection and at pump shutoff head) and control RCS temperature during the decay heat removal mode. Valves DH14A and DH14B are normally open and valves DH13A and DH13B are normally closed. This configuration ensures the system is aligned for maximum flow through the coolers while in the LPI mode. DH13A and DH13B may be manually throttled during shutdown cooling.

The DHR system is normally in a standby mode. During accident conditions, a safety features actuation system (SFAS) level 3 actuation signal starts both DHR pumps and provides confirmatory open signals to the DHR pump suction valves and DHR cooler outlet valves. A SFAS level 2 provides confirmatory open signals to the BWST outlet valves and also provides confirmatory close signals to the sump recirculation valves. A SFAS level 3 provides confirmatory close signals to the DHR cooler bypass valves. Upon low-low level in the BWST, a SFAS level 5 actuation signal provides a permissive signal to allow the operator to switch from BWST to sump suction.

Dependencies

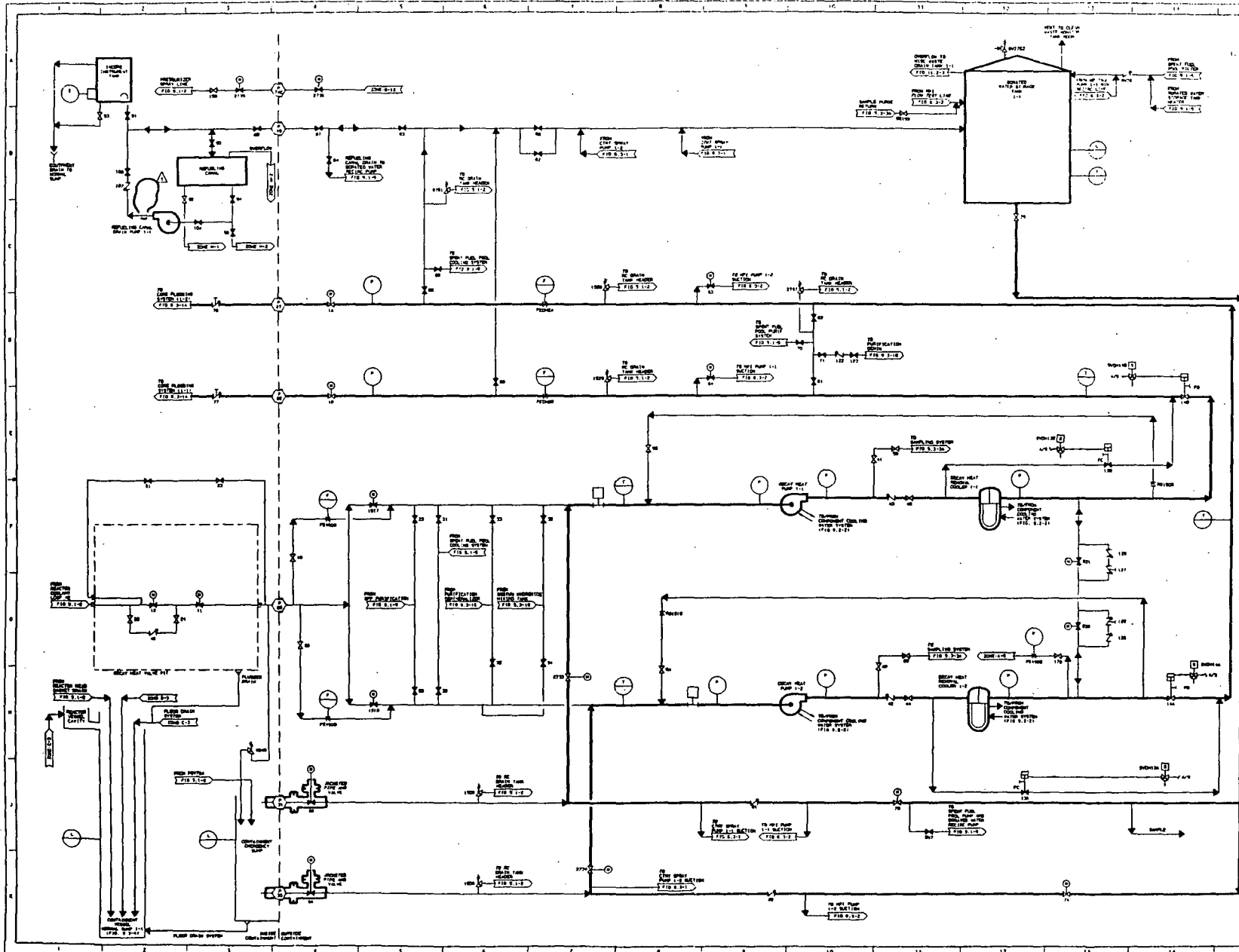
The DHR system requires the function of several auxiliary systems, as outlined in Figure 2-3. SFAS actuation signals are necessary for automatic starting and operation of equipment under accident conditions. Motive power for each of the pumps and motor-operated valves is received from the respective safety-related buses. Control power (dc) is necessary for operation of the larger power supply breakers. Heat generated by the pump bearings is removed by cooling water supplied by the CCW system. Room ventilation is provided to ensure adequate cooling and ventilation of the pump motors. The instrument air (IA) system is necessary for proper operation of the DHR cooler and bypass valves in regulating RCS temperature in the decay heat removal mode. It should be noted, however, that these valves fail safe upon loss of air, such that flow will still be maintained through the DHR coolers.

Role in the Sequence Models

The fault tree for the DHR system defines combinations of component failures that result in an inadequate flow of water to the RCS for two major modes of operation, injection and recirculation. Only one of two DHR trains is required for success in both the injection and recirculation phases. In the injection phase for both large and medium LOCAs, the DHR system is required to inject borated water from the BWST directly into the RCS to prevent uncovering the core. Failure of the system for these events is reflected in the event trees by events U_A and U_M , respectively. In the recirculation phase, water that has collected in the containment emergency sump is used as the suction source for the DHR pumps. Failure of LPR is reflected in events X_A and X_M for large and medium LOCAs, respectively. DHR is also necessary to establish long-term cooling for SGTR sequences at low RCS pressure which

NOTES

1. ALL VALVES ARE PROVIDED WITH TAGS UNLESS OTHERWISE NOTED.



DAVIS-BESSE NUCLEAR POWER STATION			
UNIT 1 AND 2			
THE TROOP GARDIAN COMPANY			
FUNCTIONAL DRAWING			
DECAY HEAT REMOVAL			
LOW PRESSURE INJECTION SYSTEM			
FIGURE 6.3-2A			
1			

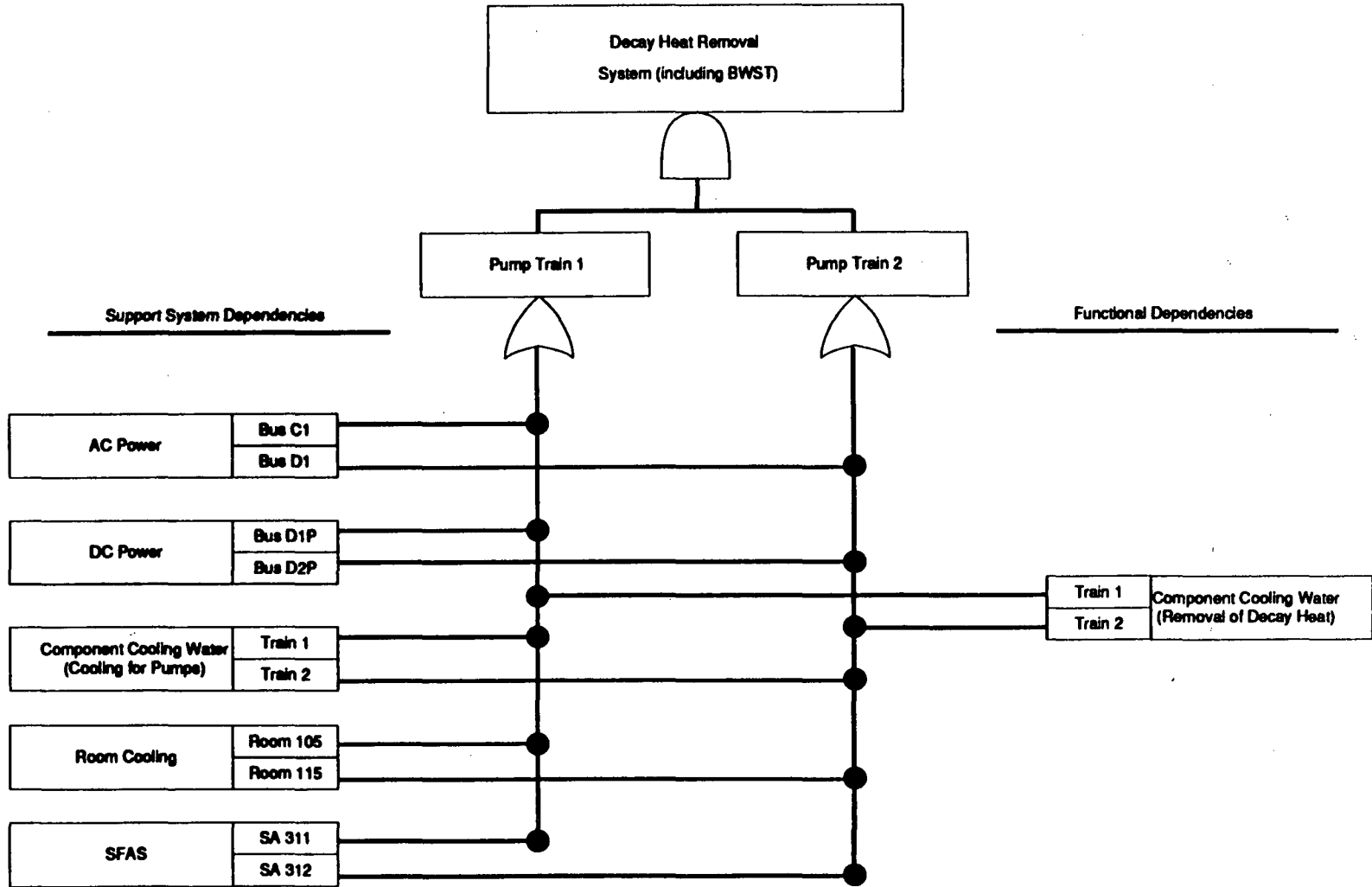


Figure 2-3. DHR System Dependencies

is contained in event X_R .

For small LOCAs (either as initiating events or induced by events such as loss of RCP seal cooling), the DHR system is called upon for long-term cooling in one of three modes. If the RCS can be cooled down using the steam generators, long-term cooling can be established by either the low pressure recirculation or shutdown-cooling modes. If the RCS is not cooled down, the DHR system must operate in the recirculation mode to support high pressure recirculation. Failure in these modes is developed under events X_S for the small LOCA event tree and event X_T for the transient event tree.

Support of high pressure recirculation may also be required for SGTRs in which it is not possible to cool down using the unaffected steam generator (event X_R), or for cases of long-term makeup/HPI cooling, as for transients with a sustained loss of feedwater (event X_T).

2.2.2 High Pressure Injection

The HPI system provides injection of borated water to the RCS to prevent uncovering the core following a small or medium LOCA.

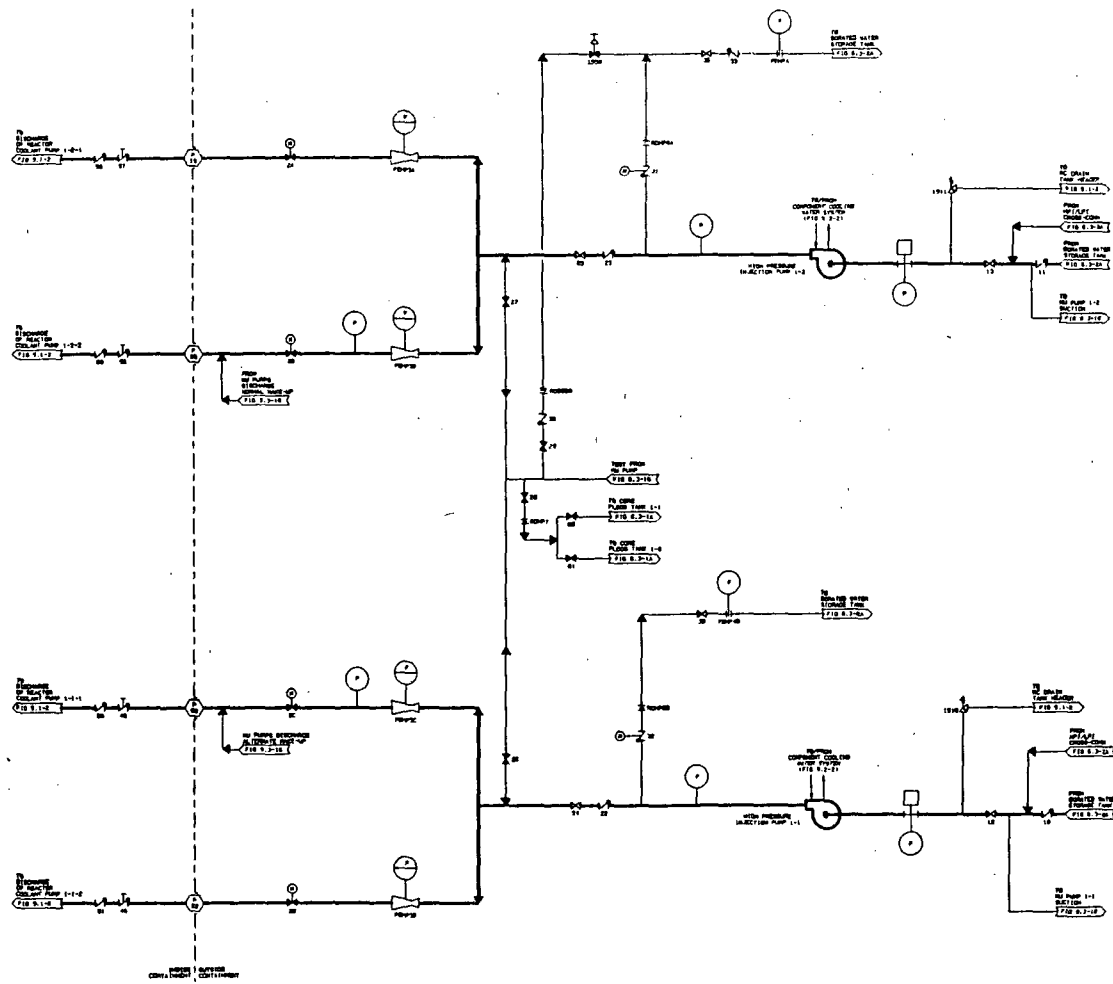
Design and Operation

As shown in Figure 2-4, the HPI system consists of two independent trains which initially take suction from the BWST and inject borated water into the RCS via two injection lines per train. The HPI pumps are capable of injecting BWST water into the RCS over the RCS pressure range of approximately 1650 psig to 0 psig, with a maximum capacity for one HPI pump of about 900 gpm. A normally open minimum flow recirculation line from each HPI pump to the BWST would protect the pumps if they were operating while RCS pressure exceeded the pump shutoff head. Both HPI suction headers are kept filled and ready for service at all times. For pipe breaks in which RCS pressure is too high for adequate flow, the HPI pumps can be aligned to take suction from the discharge of the DHR pumps. When the BWST is depleted, the DHR pumps can provide suction to the HPI pumps from the containment sump in the high pressure recirculation mode.

The HPI pumps are 11-stage centrifugal pumps capable of delivering 500 gpm at 1300 psig. Minimum recirculation of 35 gpm is provided through valves HP31 and HP32 to the BWST for protection of the HPI pumps. Lubrication and cooling for the thrust bearings of each pump are supplied by two lube oil pumps, one powered by 480 vac and the other powered by 125 vdc. Both oil pumps start when a pump start signal is received. When adequate oil pressure is developed, the dc pump will automatically stop and be placed in the standby mode. If oil system pressure should decrease, the dc oil pump would restart. Component cooling water is required for pump lube oil cooling. To prevent the pump motors from overheating, ventilation for the rooms housing the pumps is provided to ensure adequate cooling.

NOTES

1. ALL VALVES ARE PRELUBED WITH "MP" UNLESS OTHERWISE NOTED.



DAVIS-BESSE NUCLEAR POWER STATION
 UNIT NO. 1
 THE FALCON SERVICE COMPANY
 FUNCTIONAL DRAWING
 HIGH PRESSURE INJECTION SYSTEM

Cross-connect valves DH63 and DH64 are provided to supply HPI pump suction from the DHR system ("piggy-back" operation). This provides a means for long-term cooling by recirculation of sump water in the high pressure recirculation mode until pressure has been adequately decreased to allow low pressure recirculation via the DHR pumps alone.

The HPI system is normally in a standby mode, but upon a SFAS condition, a level 2 actuation signal starts both HPI pumps, opens the four HPI injection valves, and provides confirmatory open signals to the two BWST outlet valves. Following BWST depletion and for pressures too high for operation of low pressure recirculation, the HPI pumps are aligned to take suction from the discharge of the DHR pumps in the high pressure recirculation mode.

Dependencies

The HPI system requires the function of several auxiliary systems, as outlined in Figure 2-5. SFAS actuation signals are necessary for automatic start and operation of equipment under accident conditions. Motive power for each of the pumps and motor-operated valves is received from the respective safety-related buses. Control power (dc) is necessary for operation of the larger power supply breakers. Heat generated by the pump bearings is removed by cooling water supplied by the CCW system. Room ventilation is provided to remove excess heat generated by the pump motors. The respective train of DHR is required to supply the necessary suction head for high pressure recirculation operations.

Role in the Sequence Models

The HPI system model defines combinations of component failures that result in an inadequate flow of water to the RCS. Injection by the HPI system is required for small and medium LOCAs and SGTRs. Failure of the HPI system is reflected in the respective event trees by events U_S , U_M , and U_R . It is also reflected in event U_T for transient-induced LOCAs (e.g., RCP seal LOCAs). For cases in which the RCS cannot be cooled down to conditions at which the DHR system can be used, high pressure recirculation is considered for long-term cooling. Failure of high pressure recirculation is developed in events X_S , X_M , X_R , and X_T for the small and medium LOCA, SGTR, and transient event trees, respectively.

2.2.3 Makeup and Purification

The makeup and purification system operates continuously during all phases of RCS operation, including power operation and RCS heatup and cooldown. The makeup (MU) system draws (or lets down) coolant from the RCS and pumps it back to the RCS after it has gone through a purification process. The fault tree for the makeup system was developed for the following requirements: (1) RCP seal injection; (2) injection of borated water as a backup to the HPI system; and (3) injection for makeup/HPI cooling in the event of loss of cooling via the steam generators.

Design and Operation

The makeup and purification system, as shown in Figure 2-6, consists of two makeup

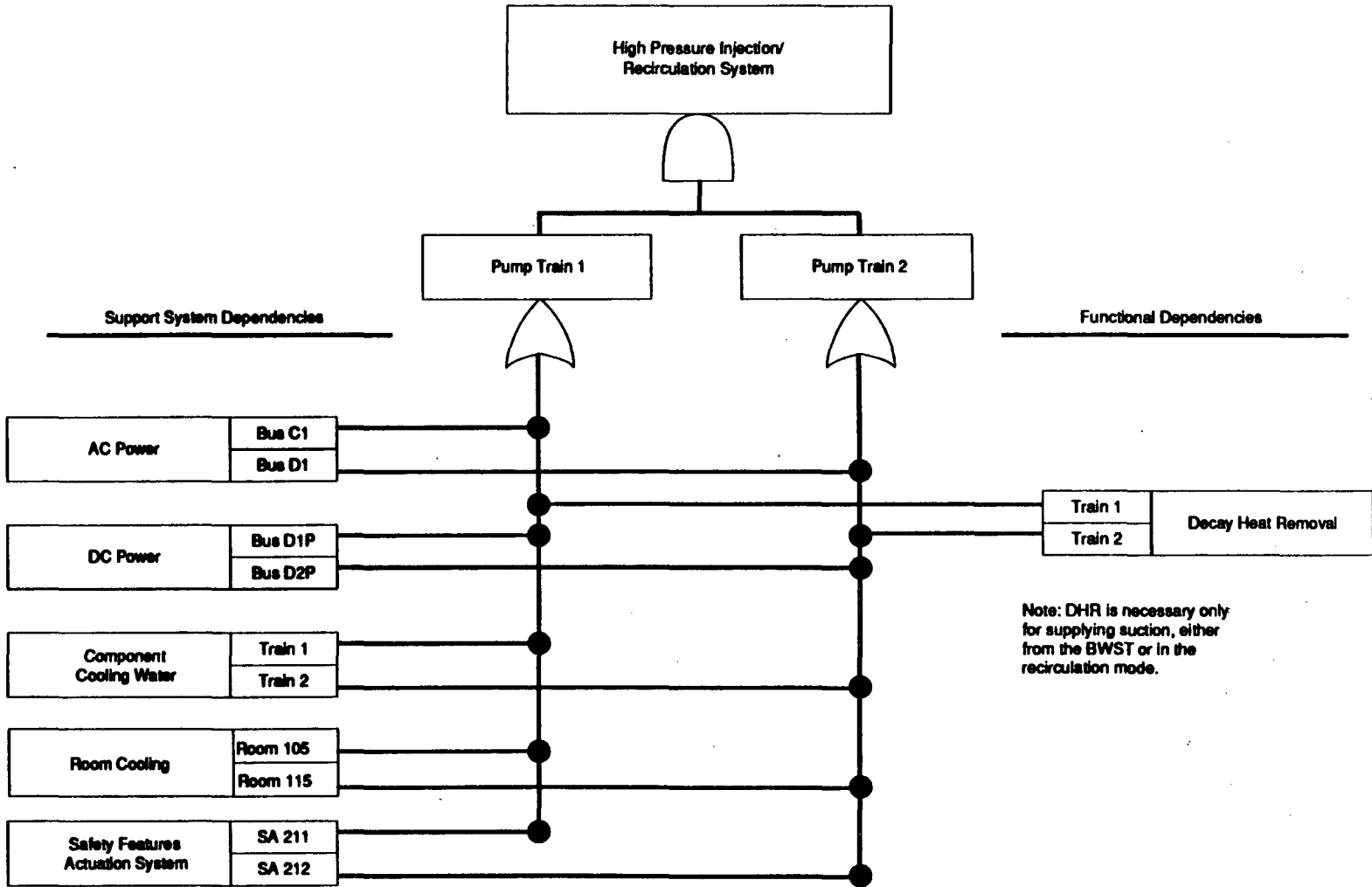
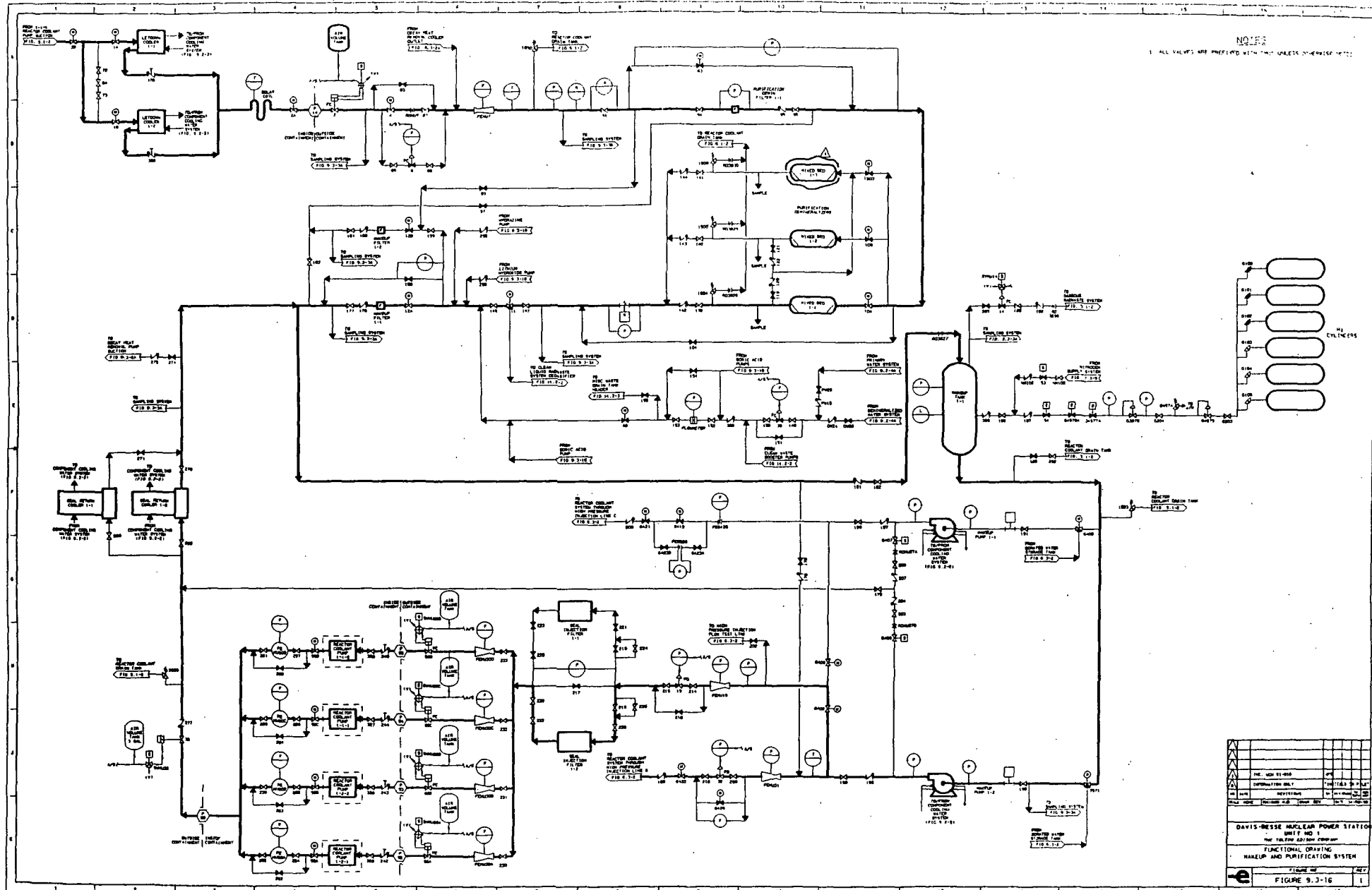


Figure 2-5. HPI System Dependencies



NOTES
 1 ALL VALVES ARE PROVIDED WITH TAGS UNLESS OTHERWISE NOTED

REV	NO.	DESCRIPTION	DATE

DAVIS-BESSE NUCLEAR POWER STATION
 UNIT NO. 1
 THE FUNCTIONAL DRAWING PROGRAM
 FUNCTIONAL DRAWING
 MAKEUP AND PURIFICATION SYSTEM
 FIGURE 9.3-16
 SHEET 1

pumps, two RCS injection lines and a RCP seal injection line. Normally, only one makeup pump is in operation with the other pump in standby. Consistent with normal plant operations, makeup pump 1-2 is modeled as the normally running pump while makeup pump 1-1 is in standby.

Each makeup pump is a horizontal, twelve-stage, variable speed centrifugal pump rated at 150 gpm at 2500 psig. Valve MU3971 (MU6405) is a three-way motor-operated valve which aligns the suction of makeup pump 1-2 (1-1) to either the makeup tank or the BWST. The valves are interlocked so that on a low makeup tank level, pump suction is automatically transferred to the BWST. If the valve does not transfer, the makeup pumps are automatically tripped after a 45 second time delay. On a high makeup tank level, pump suction is automatically transferred from the BWST back to the makeup tank. Lubrication for each pump is provided by both a dc and an ac oil pump. The dc pump aids in startup and serves as a backup to the main ac oil pump.

Normal makeup flow to the RCS is regulated by an air-operated control valve, MU32, which can operate automatically based on level signals from the pressurizer. Valve MU32 is designed to fail open upon loss of air.

The makeup system can be used to provide for RCS makeup in the event of a small LOCA. It can also be used for emergency boration following a transient without scram, and for makeup/HPI cooling in the event of a loss of all secondary side cooling. During an SFAS condition, a level 2 signal isolates the letdown line by shutting MU2A and MU3 and a level 3 signal isolates flow to all four RCP seal injection and return lines to help conserve RCS inventory.

Following the June 9, 1985 loss of feedwater, significant modifications were made to the makeup system to enhance makeup/HPI cooling. Success of makeup/HPI cooling is ensured through the redundancy in makeup pumps, of which only one is required for success, and the redundancy in RCS heat removal capability, through the PORV or the primary safeties.

Dependencies

For successful operation, the makeup and purification system requires the function of other plant systems as outlined in Figure 2-7. Motive power and control power for the pumps and motor-operated valves in each train are provided by their respective essential buses. The isolation valves for the minimum recirculation on each pump require dc power to close, thereby ensuring maximum flow during makeup/HPI cooling operations. Ac and dc power are required for each makeup pump's normal and backup oil pump, respectively. NNIX ac and dc power is also required for successful operation of control valve MU32. Control power (dc) for breaker operation is only required for makeup pump 1-1. Makeup pump 1-2 is normally in operation and, upon loss of offsite power, its associated power supply breaker remains shut, thereby requiring no dependence on dc power for breaker re-closure.

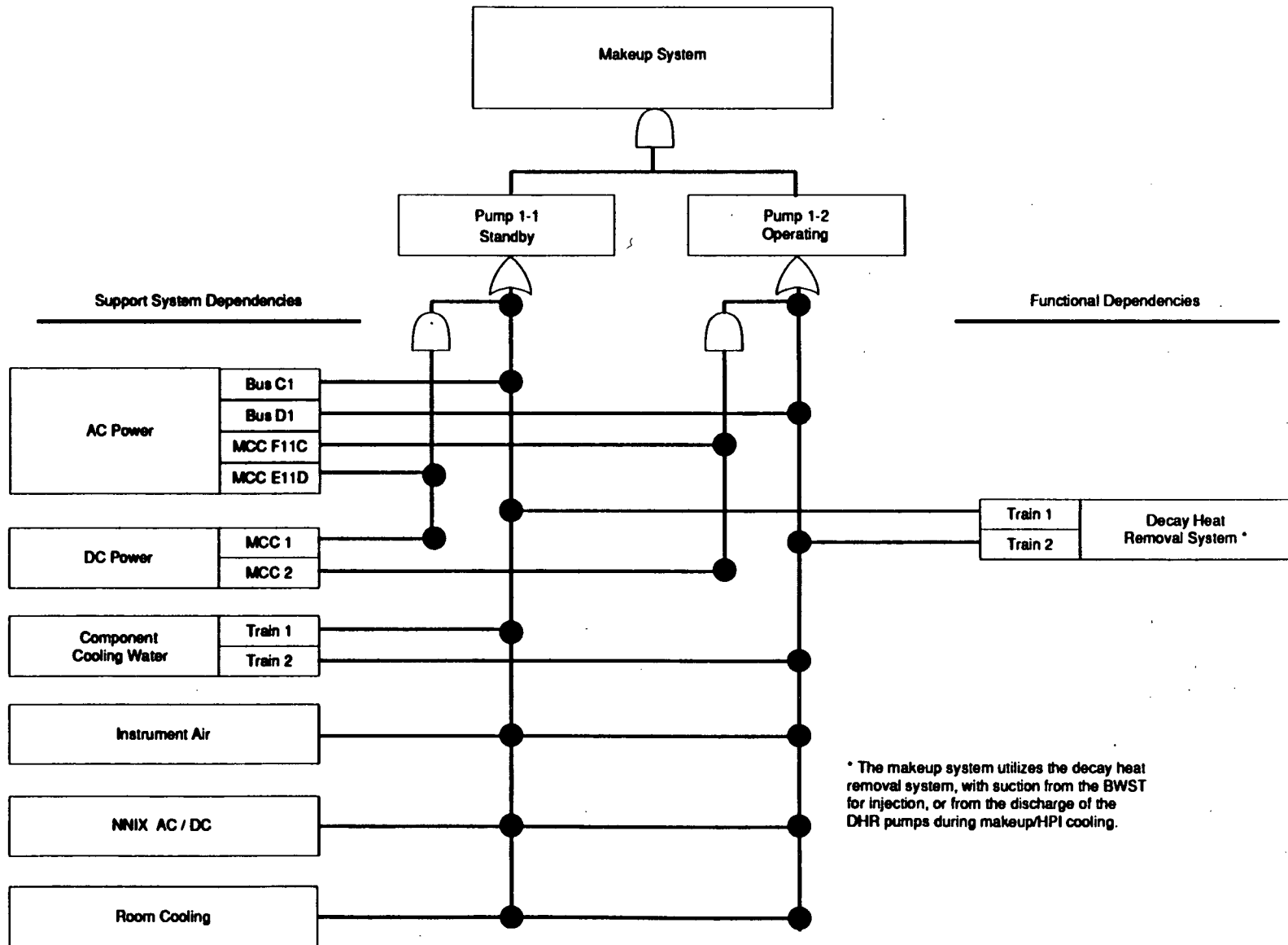


Figure 2-7. Makeup and Purification System Dependencies

The CCW system removes heat generated by the bearings of each makeup pump from the lubricating oil. Normally, the CCW pump supplying RCP seal cooling and the makeup pump supplying injection to the RCS are operated from opposite electrical buses to prevent a loss of both functions given a loss of a single 4160 vac bus.

Valve MU3, which fails shut upon loss of air, requires instrument air from the auxiliary building non-essential header in order to maintain flow through the RCS letdown line.

During makeup/HPI cooling, with the RCS at elevated pressures, the DHR pumps can be aligned to draw water from the BWST to supply the makeup pumps.

Makeup pump room cooling is necessary to remove heat generated by the pump motors if both makeup pumps are operating. It is provided by room coolers powered by a non-essential ac bus. However, if normal room cooling is lost, as would be the case during a loss of offsite power, adequate cooling can be ensured by opening the makeup pump room door.

Role in the Sequence Models

The makeup system plays an important role in transient, small LOCA, and SGTR sequences. Injection as a backup to HPI is reflected in events U_T , U_S , and U_R for cases in which there is a small LOCA or SGTR. These events also accommodate the need for makeup/HPI cooling in the event of a total loss of feedwater.

Use of borated makeup and letdown of reactor coolant are also modeled for cases in which there is a failure of the reactor to trip. The use of the makeup system for emergency boration is reflected in event K_2 of the event tree for failure to trip.

2.2.4 Core Flood

The core flood system is a passive engineered safety feature designed to inject borated water into the reactor vessel following a loss of RCS pressure. The core flood system is designed to operate during medium and large LOCAs. The core flood system requires no power to operate during a LOCA. The motor-operated isolation valves are always open during normal power operation. Two check valves in series for each line protect the core flood tanks from overpressure due to normal RCS operating pressures. During a medium or large LOCA, RCS pressure would decrease rapidly. The check valves would open at 600 psig, injecting borated water into the reactor vessel.

Design and Operation

As shown in Figure 2-8, the core flood system consists of two 1410 ft³ tanks, each with its own injection line. The normal operating level of the core flood tanks is 13 feet with a Technical Specification capacity requirement of 7555 to 8004 gallons. Boron concentration is required to be between 1800 and 3500 ppm to ensure sufficient shutdown margin. Nitrogen is used to keep the core flood tanks at a normal operating pressure of 600 psig. During plant startup, core flood isolation valves are opened by the operator when the RCS pressure reaches

650 to 700 psig. The motor operated isolation valves are equipped with two position switches. One position switch is a valve stem position switch while the other is a valve operator position switch. These switches prevent a single failure from giving an erroneous indication of valve position.

During normal power operation, the core flood system, as part of the emergency core cooling system (ECCS), is a passive system serving no function other than being in a standby mode. If a LOCA were to occur, borated water from the core flood tanks would be injected into the RCS when pressure dropped to 600 psig at the core flood nozzle. For a double-ended break of the piping at the RCP discharge, RCS pressure would reach 600 psig approximately 17 seconds after the break. The capacity of the core flood tanks would be depleted after approximately 40 seconds, requiring low pressure injection to prevent the core from being uncovered.

Dependencies

There are no support systems required for the core flood system to function properly during accident conditions.

Role in the Sequence Models

The success criteria originally developed for large and medium LOCAs were derived primarily from the licensing-based accident analyses for Davis-Besse. Subsequently, more realistic assessments were made using RELAP5 and MAAP. It was concluded that no significant overheating of the core would occur for large and medium LOCAs without injection by the core flood tanks, provided the other injection systems succeeded. Therefore, the core flood system is currently not reflected in any of the event trees.

2.2.5 Reactor Coolant

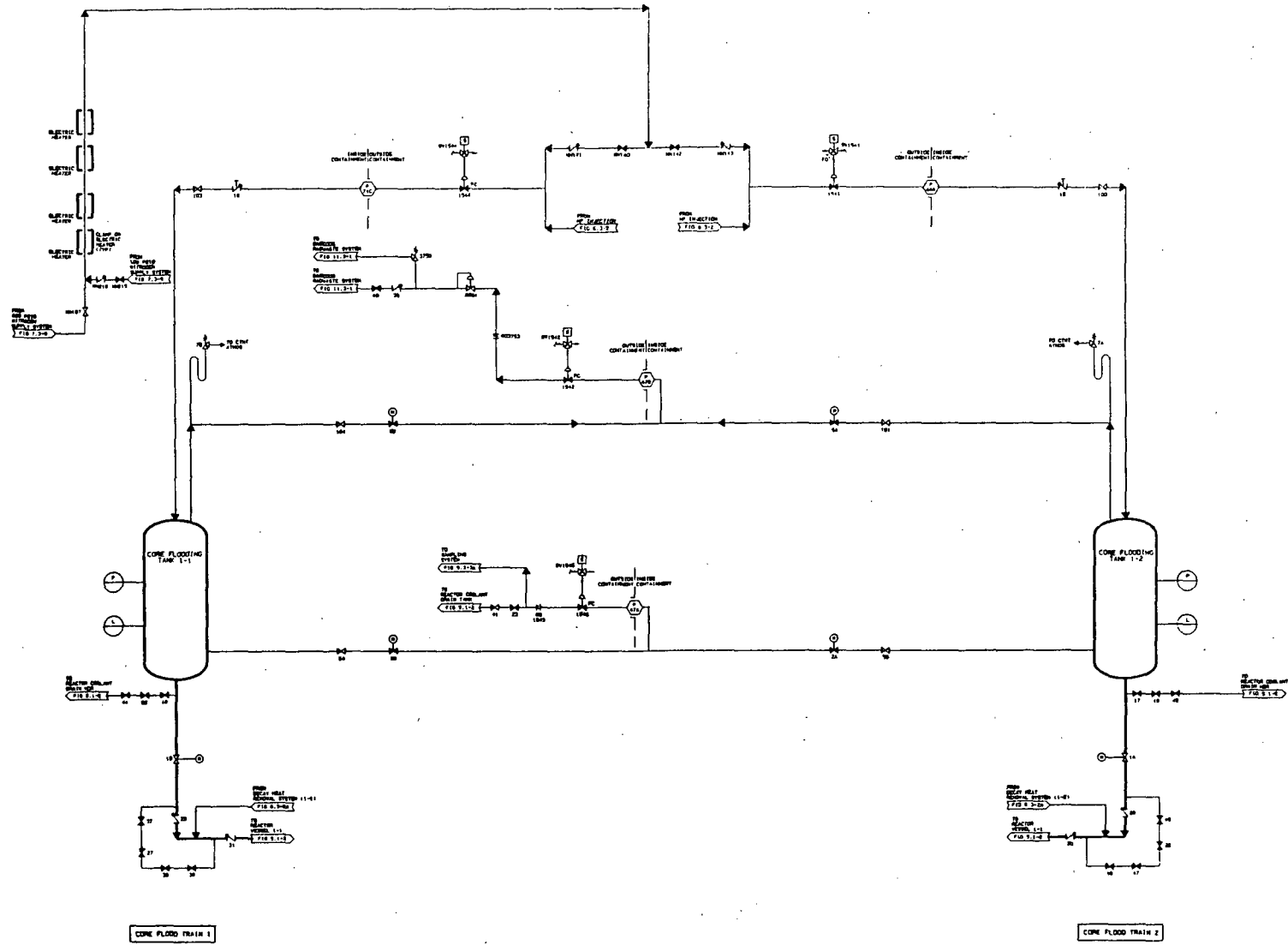
Components of interest for the IPE within the RCS include the pilot-operated relief valve (PORV), pressurizer safety relief valves (PSV), pressurizer spray, and reactor coolant pumps (RCP). The primary functions of these components with respect to this study are to provide a means of depressurization and forced-circulation cooldown following a postulated accident. The PORV and relief valves provide overpressure protection and also provides a means of removing decay heat from the RCS during makeup/HPI cooling. The pressurizer permits control of RCS pressure. Pressurizer spray can be used to reduce pressure in the RCS by spraying relatively cold water into the pressurizer steam space.

Design and Operation

A simplified drawing of the RCS including the PORV and PSVs is show in Figure 2-9. The RCS is a "raised-loop" design with the steam generators above the reactor core in order to allow an inventory of RCS coolant to flow back into the core in the event of a LOCA and to promote natural circulation of reactor coolant.

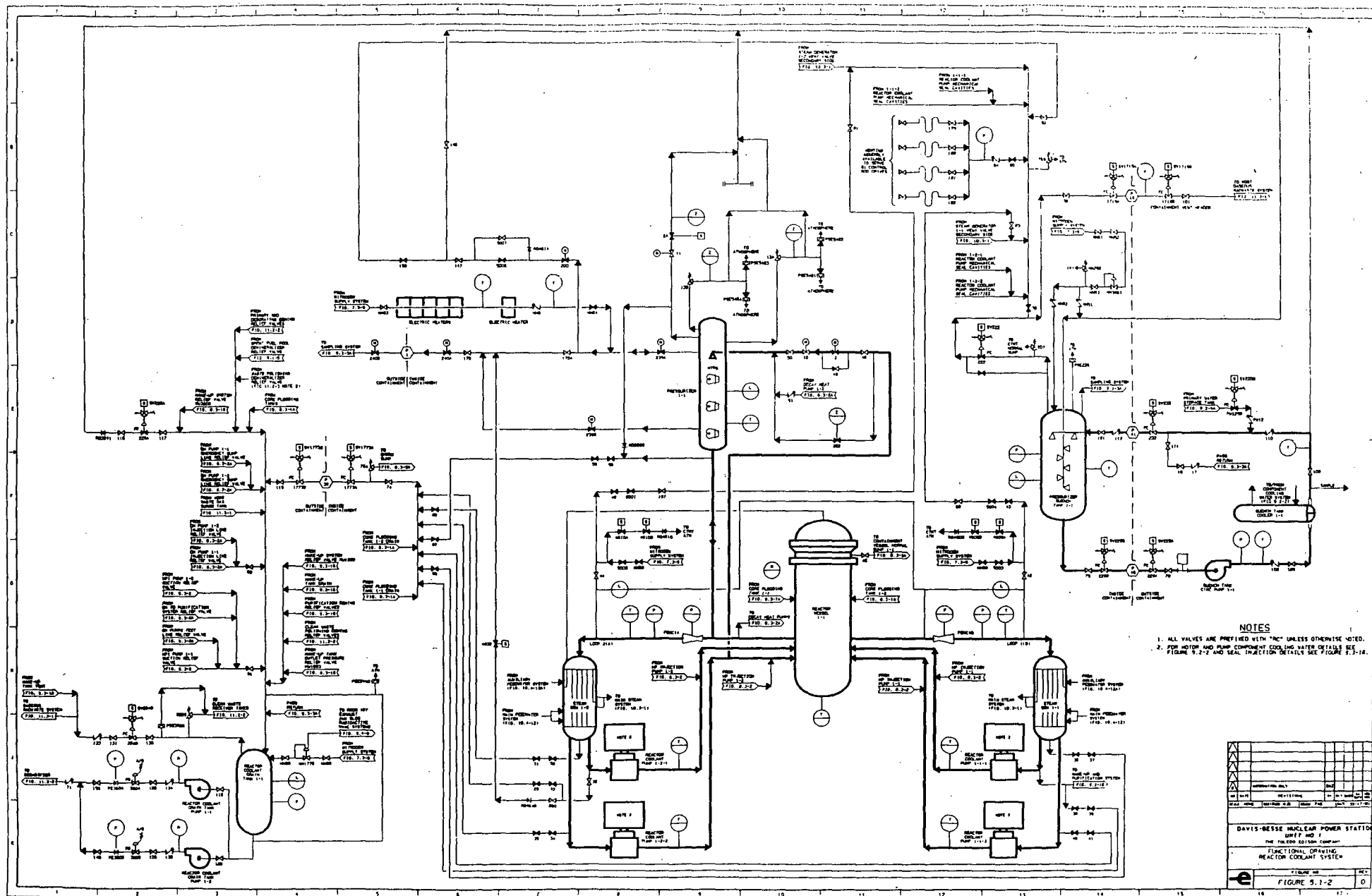
NOTES

1. ALL VALVES ARE PREFIXED WITH TEST UNLESS OTHERWISE NOTED



NO.	DATE	REVISIONS	BY	CHKD.	APP'D.
DAVIS-BESSE NUCLEAR POWER STATION					
SHEET NO. 1					
FUNCTIONAL DRAWING					
CORE FLOODING SYSTEM					
FIGURE NO. 6.3-1A					
REV. 0					

FIGURE 2-R



- NOTES
1. ALL VALVES ARE PROVIDED WITH "NC" UNLESS OTHERWISE NOTED.
 2. PWR MOTOR AND PUMP COMPONENT COOLING WATER DETAILS SEE FIGURE 5.1-2 AND SEAL INJECTION DETAILS SEE FIGURE 5.1-16.

NO.	DESCRIPTION	REV.
1	ISSUED FOR CONSTRUCTION	1
2	REVISED TO REFLECT CHANGES TO THE DESIGN	2
3	REVISED TO REFLECT CHANGES TO THE DESIGN	3
4	REVISED TO REFLECT CHANGES TO THE DESIGN	4
5	REVISED TO REFLECT CHANGES TO THE DESIGN	5
6	REVISED TO REFLECT CHANGES TO THE DESIGN	6
7	REVISED TO REFLECT CHANGES TO THE DESIGN	7
8	REVISED TO REFLECT CHANGES TO THE DESIGN	8
9	REVISED TO REFLECT CHANGES TO THE DESIGN	9
10	REVISED TO REFLECT CHANGES TO THE DESIGN	10
11	REVISED TO REFLECT CHANGES TO THE DESIGN	11
12	REVISED TO REFLECT CHANGES TO THE DESIGN	12
13	REVISED TO REFLECT CHANGES TO THE DESIGN	13
14	REVISED TO REFLECT CHANGES TO THE DESIGN	14
15	REVISED TO REFLECT CHANGES TO THE DESIGN	15
16	REVISED TO REFLECT CHANGES TO THE DESIGN	16
17	REVISED TO REFLECT CHANGES TO THE DESIGN	17
18	REVISED TO REFLECT CHANGES TO THE DESIGN	18
19	REVISED TO REFLECT CHANGES TO THE DESIGN	19
20	REVISED TO REFLECT CHANGES TO THE DESIGN	20

DAVIS-BESSE NUCLEAR POWER STATION
 SHEET 7 OF 8
 THE REACTOR COOLANT SYSTEM
 FUNCTIONAL OPERATING
 REACTOR COOLANT SYSTEM
 FIGURE 5.1-2
 REV. D

There are two RCPs per primary loop which provide for forced convective heat transfer in removing heat generated in the reactor core and transferring it to the steam generators. The RCPs are classified as diffused-flow, single-suction, vertical centrifugal pumps each designed with a rated capacity of 90,670 gpm at 358 ft. head. Each RCP motor is classified as a 13.2 kvac single speed, squirrel cage induction type motor with a maximum rating of 9,000 Hp.

The PORV (RC2A) is an electrically controlled pilot-operated relief valve. When the pilot valve is closed, the valve inlet pressure and the pressure under the valve disk are the same, allowing the disk spring to keep the PORV closed. When the pilot valve is open, the pressure under the valve disk is reduced, allowing the valve inlet pressure to push down on the valve disk and compress the disk spring to open the PORV. The PORV is set to open at 2450 psig and to reseal when RCS pressure drops to 2400 psig. One of two narrow range pressure transmitters located on each hot leg provides input for PORV control. The PORV discharges directly to the pressurizer quench tank, which, in the event of quench tank overpressurization, releases pressure to the containment through the tank's rupture disk. The PORV may also be operated manually by operators in the control room. The normally open, motor-operated PORV block valve (RC11) can be closed to isolate the PORV.

The two pressurizer code safety valves are sealed by means of a bellows assembly, balanced and spring loaded. The relief setpoint for these valves is 2500 psig, discharging to the containment atmosphere.

Pressurizer spray receives water from a line at the RCP 2-2 discharge. Spray flow is controlled by operation of motor-operated spray valve RC2. When in the automatic mode, the valve will open to 40% when RCS pressure increases to 2205 psig and close when the pressure decreases to 2155 psig. The valve can also be operated manually from the control room. A small flow is continuously maintained by a 1/2" bypass spray flow valve (RC49) to reduce thermal shock to the spray nozzle.

Three separate level transmitters provide indication of pressurizer level. One of these indications is selected in conjunction with one pressurizer temperature signal to develop a temperature-compensated pressurizer level signal which is used to control makeup to maintain a constant pressurizer level.

Dependencies

As outlined in Figures 2-10 through 2-12, the RCPs, PORV and PSVs are dependent on other auxiliary systems for successful operation. The RCPs are powered from their respective 13.8 kvac buses and also require the use of dc breaker control power. RCP seal injection, which ensures for proper operation of the pump seals, is provided by the makeup system. RCP seal injection also requires the use of instrument air and dc power for maintaining the isolation valves in the injection lines and common return header open. Either seal cooling from the CCW system or seal injection from the makeup system is required to prevent overheating of the RCP seals.

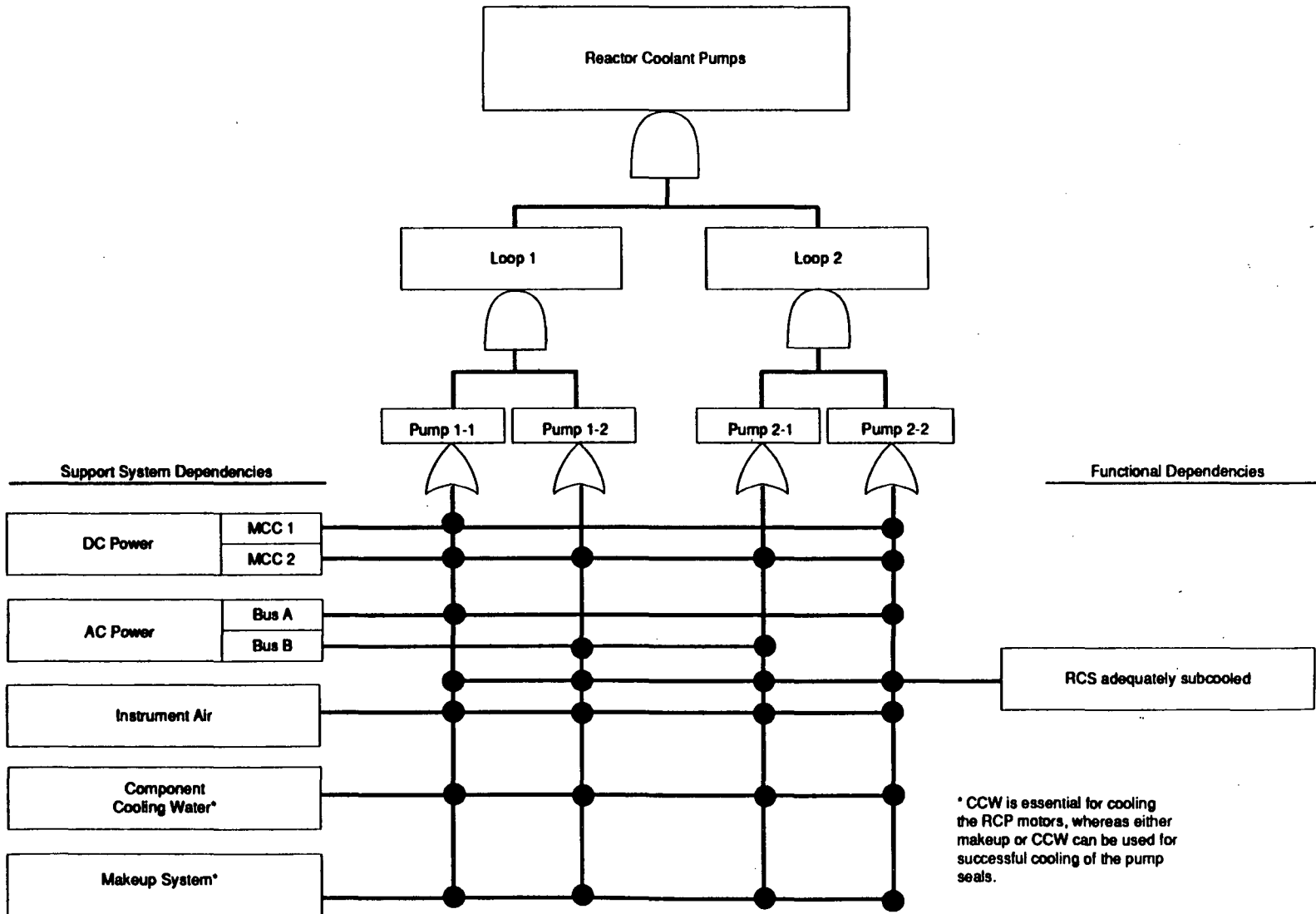
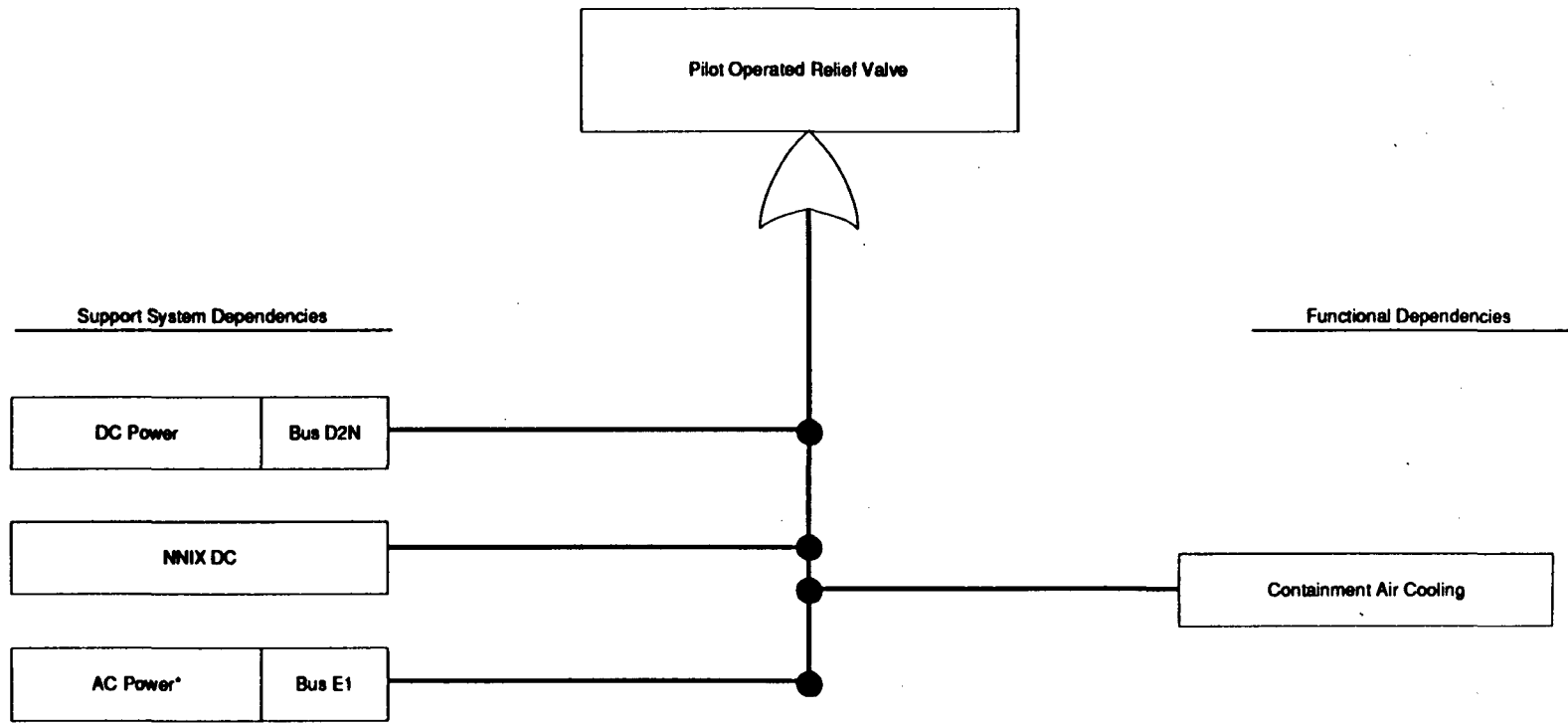


Figure 2-10. Reactor Coolant Pump Dependencies



* For operation with PORV block valve closed.

Figure 2-11. PORV Dependencies

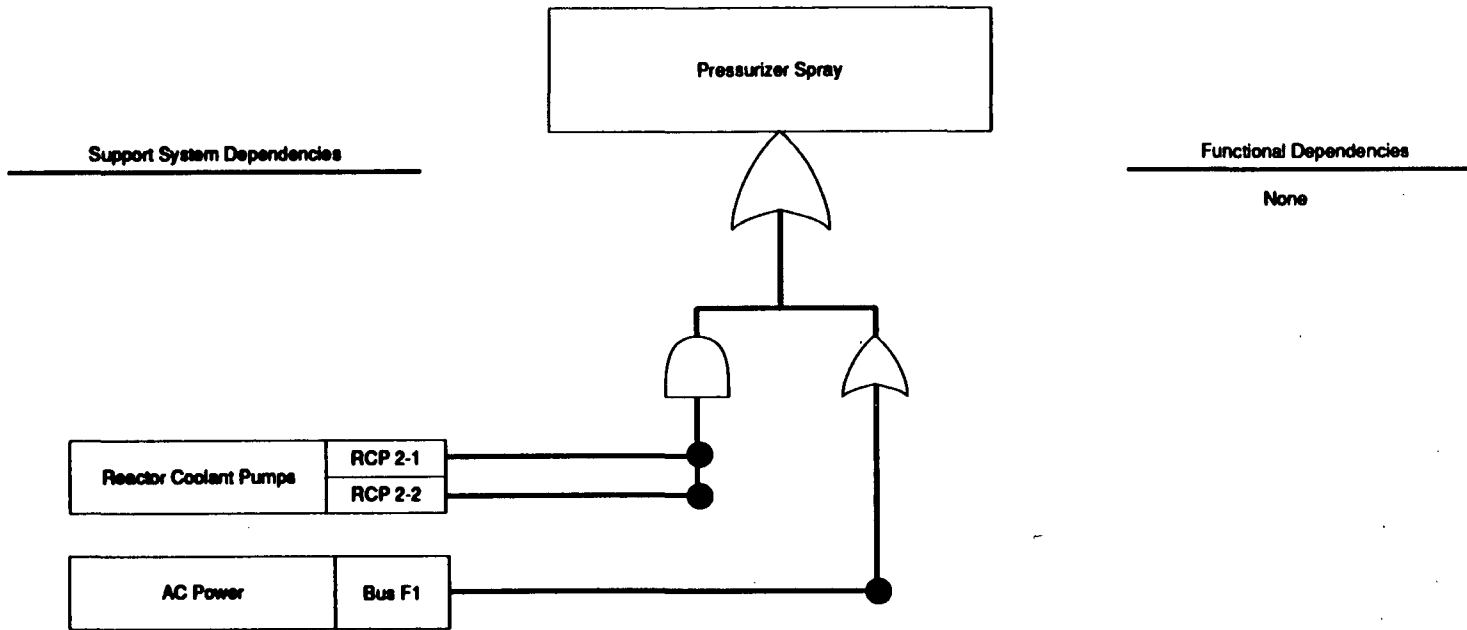


Figure 2-12. Pressurizer Spray Dependencies

The PORV block valve and pressurizer spray valve are both powered from essential 480 vac. The driving force for spray flow can be provided by either of the RCPs in loop 2. The PORV itself is controlled and operated by dc power, including NNIX dc. For the PORV to provide a means of cooling the primary, it is also required that the containment air coolers function properly. The code safety relief valves actuate based on actual RCS pressure and do not require support from other plant systems.

Role in the Sequence Models

The following RCS functions are utilized in the small LOCA, SGTR, ATWS, and transient sequences: (1) pressurizer spray, (2) PORV actuation and operation, (3) operation of RCPs, (4) PORV path for makeup/HPI cooling, and (5) actuation of code safety relief valves.

For the transient sequences, the PORV and safety relief valves are used under transient event P, control of RCS pressure. The PORV and/or safety relief valves are also required to provide a bleed path for reactor coolant during makeup/HPI cooling. This is modeled in events U_T , U_S , and U_R of the transient, small LOCA, and SGTR event trees, respectively. For extended operation of makeup/HPI cooling, it may be necessary to rely on the PORV alone to support high pressure recirculation from the containment sump. This is modeled in events X_T , X_S , and X_R of the respective event trees.

Failure of the PORV or safety relief valves to reclose after opening introduces the potential for a transient-induced LOCA. This potential is modeled under events Q and W of the transient event tree.

The availability of the RCPs is primarily of interest with respect to the need for cooldown of the RCS. For cases in which there is a small LOCA with heat removal available, events X_S and X_T consider cooldown to shutdown cooling conditions. Use of the RCPs both for forced circulation and to enable use of the pressurizer spray is considered in event P_R of the SGTR event tree.

For sequences involving failure to trip, the PORV and pressurizer safety relief valves play an essential role in controlling elevated RCS pressures under sequence event P_K , since RCS integrity could be compromised due to excessive peak pressure. Requirements for relief capacity depend on power level history and values of the moderator temperature coefficient.

2.2.6 Power Conversion

The power conversion system (PCS) includes main steam, main feedwater (MFW), the condenser and condensate system, turbine plant cooling water (TPCW), main steam safety valves (MSSV), atmospheric vent valves (AVV), main steam isolation valves (MSIV), turbine bypass valves (TBV), and the circulating water system. The overall function of the PCS is to transfer heat from the primary (in the form of steam) from the steam generators to the main condenser via the TBVs. Circulating water removes heat from the condenser and releases this heat to the atmosphere through the evaporative process in the cooling tower. As a backup to

the TBVs in the event the condenser is not available or the MSIVs are closed, control of the steam pressure will automatically transfer to the AVVs which release steam directly to the atmosphere. Overpressure protection of the steam generators is also provided by the MSSVs. Isolation of the steam generators is accomplished by closing the MSIVs. The TPCW system provides cooling for numerous secondary plant components, and the station air compressors. During normal power operation, feedwater is delivered to the steam generators by the main feedwater pumps from the condensate system via the deaerator storage tanks.

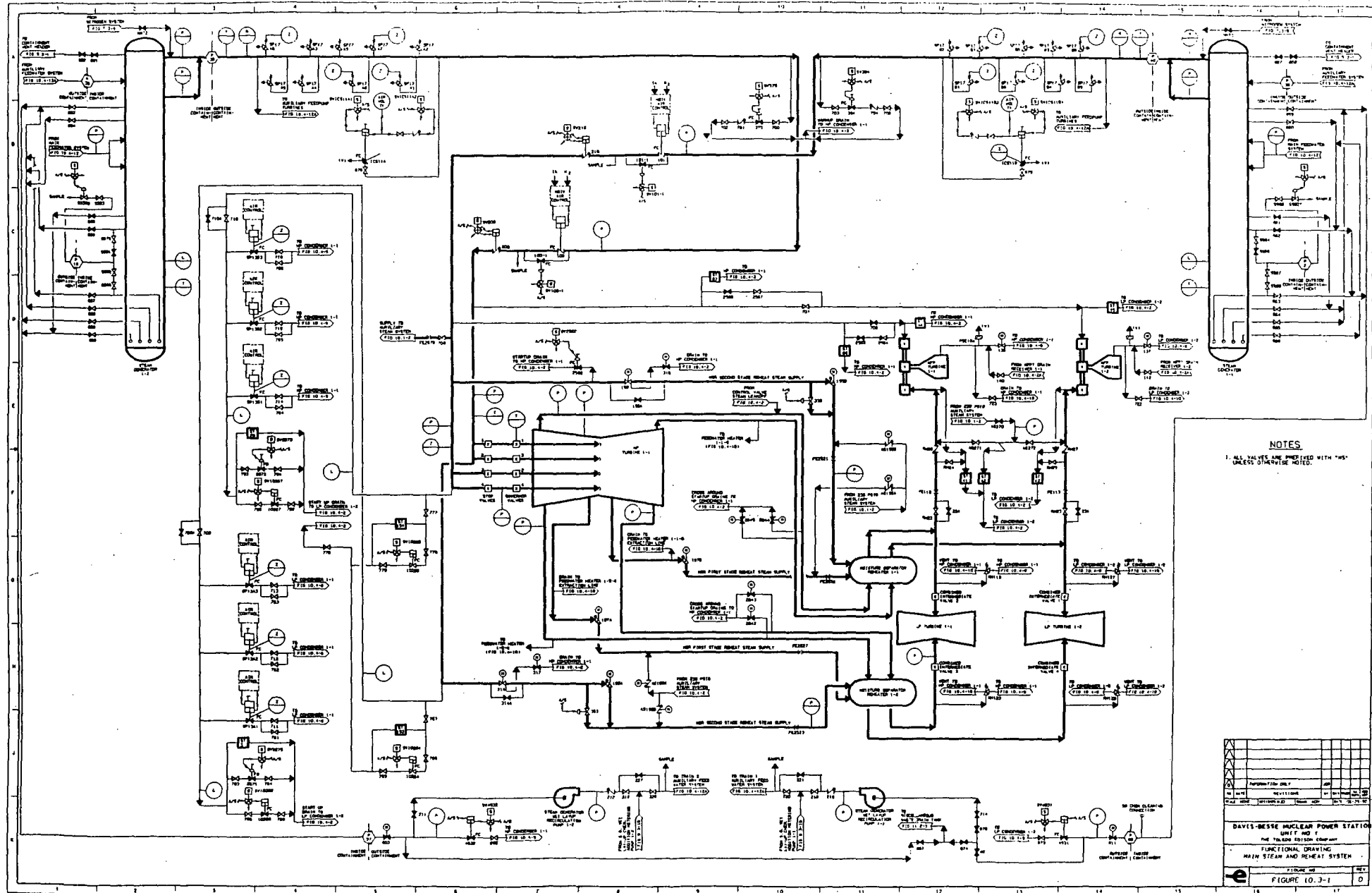
Design and Operation

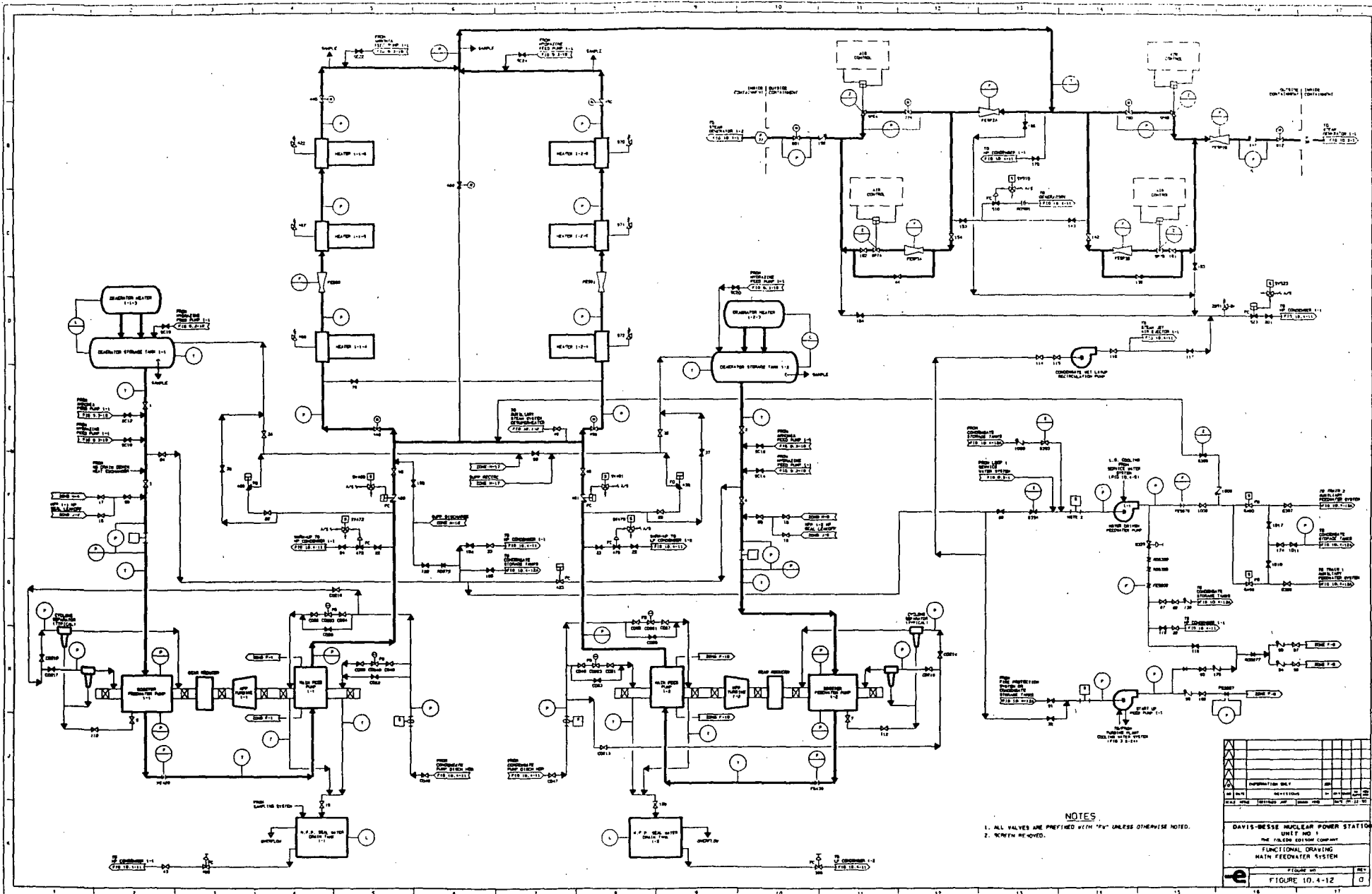
The main steam system, main feedwater system, and condensate system are depicted in Figures 2-13 through 2-15, respectively.

The flowpath for feedwater begins at the deaerator storage tanks, which receives water directly from the condensate system. The condensate system supplies water to the deaerators which are a suction source for the booster feed pumps and a seal water supply for both the booster and main feed pumps. The stored water is heated and deaerated using eighth-stage extraction steam from the main turbine. The two booster pumps are single-stage, double-suction centrifugal pumps driven by their respective main feed pump turbine through a reduction gear unit. The booster pumps increase the water pressure to provide the required NPSH for the main feed pumps. The two turbine-driven main feed pumps are single-stage, double-suction centrifugal pumps. Following a reactor trip not associated with a loss of MFW, the MFW system remains in operation delivering condensate from the deaerators to the steam generators for the removal of reactor decay heat.

The condenser is a twin-shell multi-pressure (high and low) condenser. It is designed to maintain a pressure of 2.7 inches Hg absolute on the high pressure side and 1.9 inches Hg absolute on the low pressure side. Cooling water is supplied by the circulating water system. The vacuum system removes air and non-condensable gases from the deaerating sections of the main condenser and discharges to the station vent. A steam jet air ejector is normally used; however an additional motor-driven mechanical vacuum hogger and a steam jet hogger can also be used. There are three constant speed, five-stage centrifugal condensate pumps. Following a reactor trip, only one condensate pump is required. Seal water is provided by each pump's own discharge. To protect the pumps when running at shutoff head, a minimum recirculation flowpath is provided.

Four, 25-percent capacity circulating water pumps take suction via individual supply lines from an open concrete channel from the cooling tower basin. Each pair of pumps discharges into separate loops passing first through the low pressure section and then through the high pressure section of the condenser. The heat transferred to the circulating water is then dissipated to the atmosphere via the cooling tower. Cooled water collects in the cooling tower basin and then flows via the open concrete channel to the suction lines of the circulating water pumps. The circulating water pumps are single-stage, double-suction centrifugal pumps. Oil lubrication is provided by slinger rings and seal water is provided by the clearwell



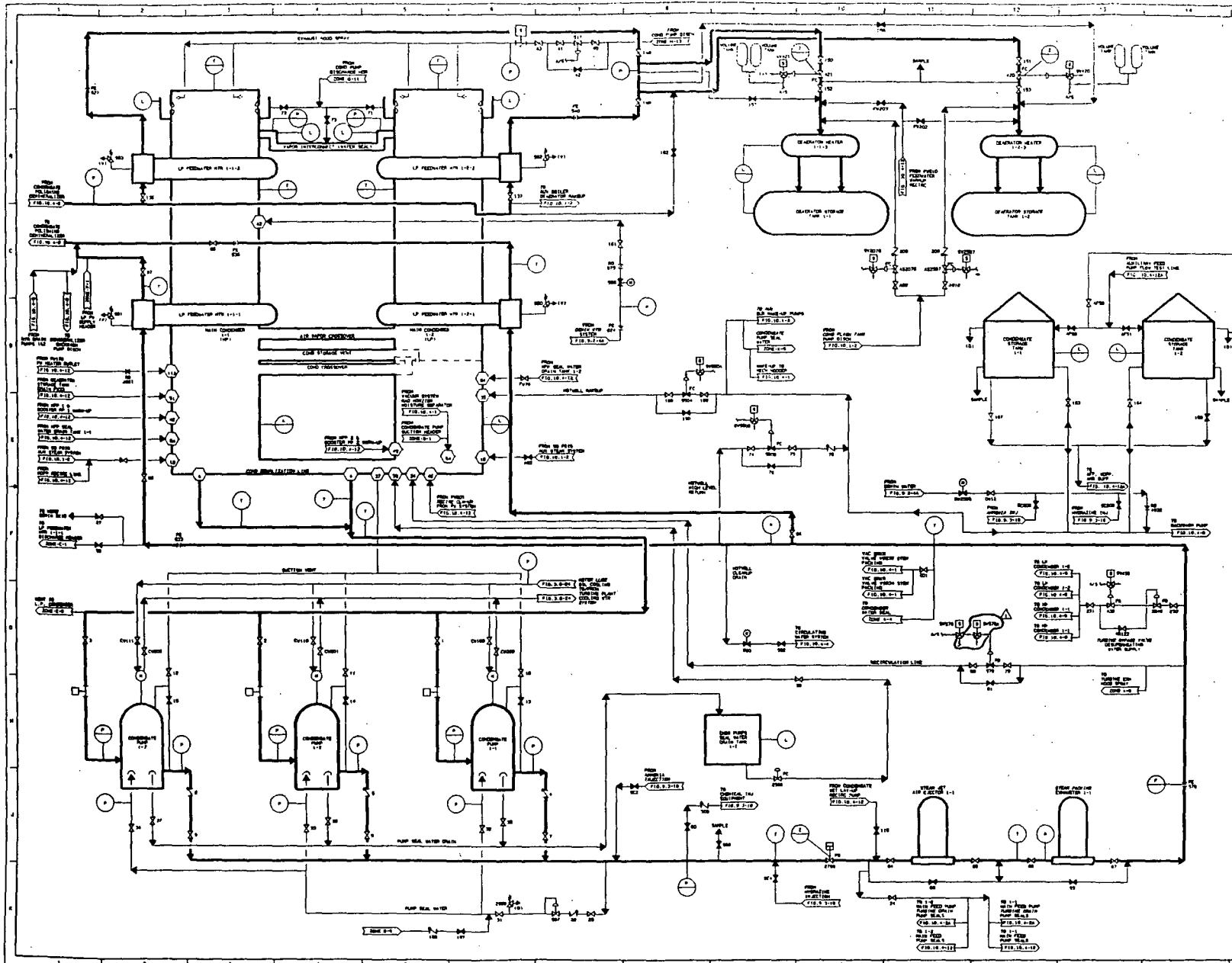


NOTES

1. ALL VALVES ARE PREFICTION WITH 'FV' UNLESS OTHERWISE NOTED.
2. WHEN REQUIRED.

NO.	REV.	DESCRIPTION	DATE
DAVIS-BESSE NUCLEAR POWER STATION UNIT #2 THE FOLEN DESIGN COMPANY FUNCTIONAL DRAWING MAIN FEEDWATER SYSTEM			
FIGURE NO. 10.4-12			

NOTES
 1. ALL VALVES ARE PROVIDED WITH TGT UNLESS OTHERWISE NOTED.



NO.	DATE	BY	CHKD.
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

DAVIS-BESSE NUCLEAR POWER STATION
 SHEET NO. 1
 THE FUEL OXIDATION COMPANY
 FUNCTIONAL DRAWING
 CONDENSATE SYSTEM
 FIGURE NO. 10.4-11
 1

transfer pumps. During normal power operation, all four circulating water pumps are required. Following a reactor trip, only one circulating water pump is required.

TPCW is a closed loop system. During normal operation, two of the three TPCW pumps are operating with one in standby. The operating pumps take suction from the low level cooling water tank and discharge through two of the three TPCW heat exchangers to the high level cooling water tank. The water from the high level cooling water tank gravity drains through each component served by TPCW. The TPCW pumps are vertical three-stage, motor-driven centrifugal pumps. The TPCW heat exchangers are normally cooled by service water but can be cooled by circulating water. During normal operation, two of the three heat exchangers are in operation and one is in standby. On a low service water discharge pressure or SFAS level 2 signal, the TPCW coolers are isolated from service water. When service water is not available, circulating water is automatically aligned to supply cooling for the TPCW heat exchangers.

There are nine, safety-related, spring-operated MSSVs per steam line. Each line has a total capacity equal to 120 percent of the rated steam flow. As system pressure increases above the safety valve setting, the pressure pushes the valve disc and stem up, compressing the spring and opening the valve. After the excess steam pressure is relieved, spring force drives the disc downward and the valve reseats.

The AVVs are stacked disc-drag angle valves with pneumatic controllers which receive signals from the integrated control system (ICS). There is one safety-related AVV per steam line. Each AVV is rated at 7.5 percent of steam flow for 100 percent rated power. The AVVs open at approximately 1025 psig. Each AVV is provided with a safety-related accumulator (air volume tank) to close the valve after a loss of air. Upon loss of air or control power, the AVVs can be controlled locally by use of the installed handwheel.

There is one safety-related, air-operated MSIV per steam line. The MSIVs are balanced-disc stop valves set in opposition to the normal flow direction. The valves use air pressure to open and spring force for closing. The MSIVs are controlled using air-operated three-way valves. When the solenoid valves are energized, the control air is admitted to the air-operator to provide air pressure in opening the MSIV.

There are three air-operated TBVs per steam line. Each TBV is provided with a nonsafety-related air accumulator to actuate the valve after a loss of air. The TBVs are controlled by the ICS. Each TBV is rated at approximately 5 percent of the rated steam flow at 100 percent power. Together, the six TBVs have a capacity of approximately 25 percent of the maximum rated steam flow.

Dependencies

Dependencies for the MFW system, AVVs, MSIVs, TBVs, and condensate system are shown in Figures 2-16 through 2-20 respectively. MFW dependencies include offsite power, non-essential 480 vac power, instrument air, TPCW, ac/dc NNIX and ICS power for control signals, and the condenser/condensate system for suction. The condenser/condensate system

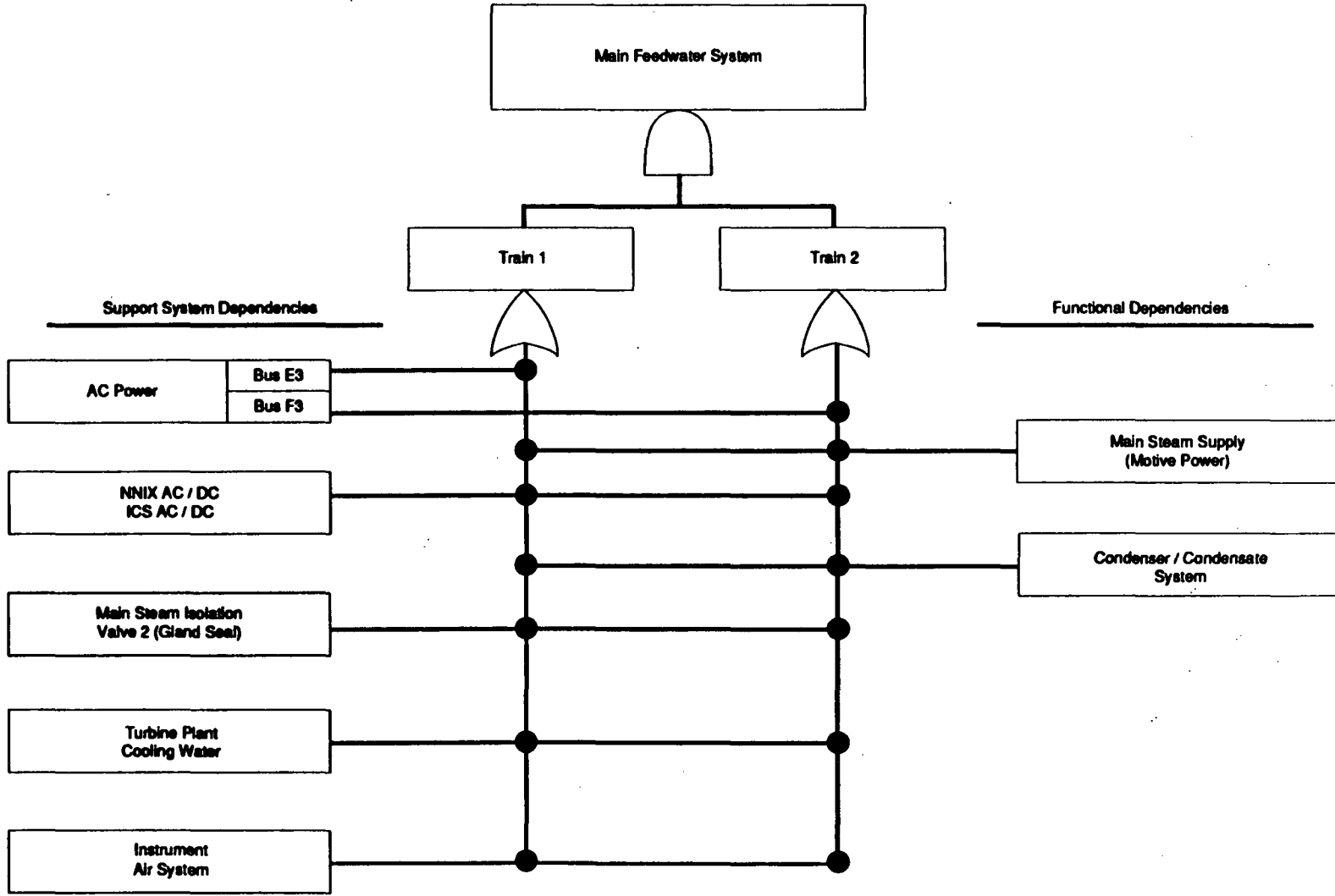
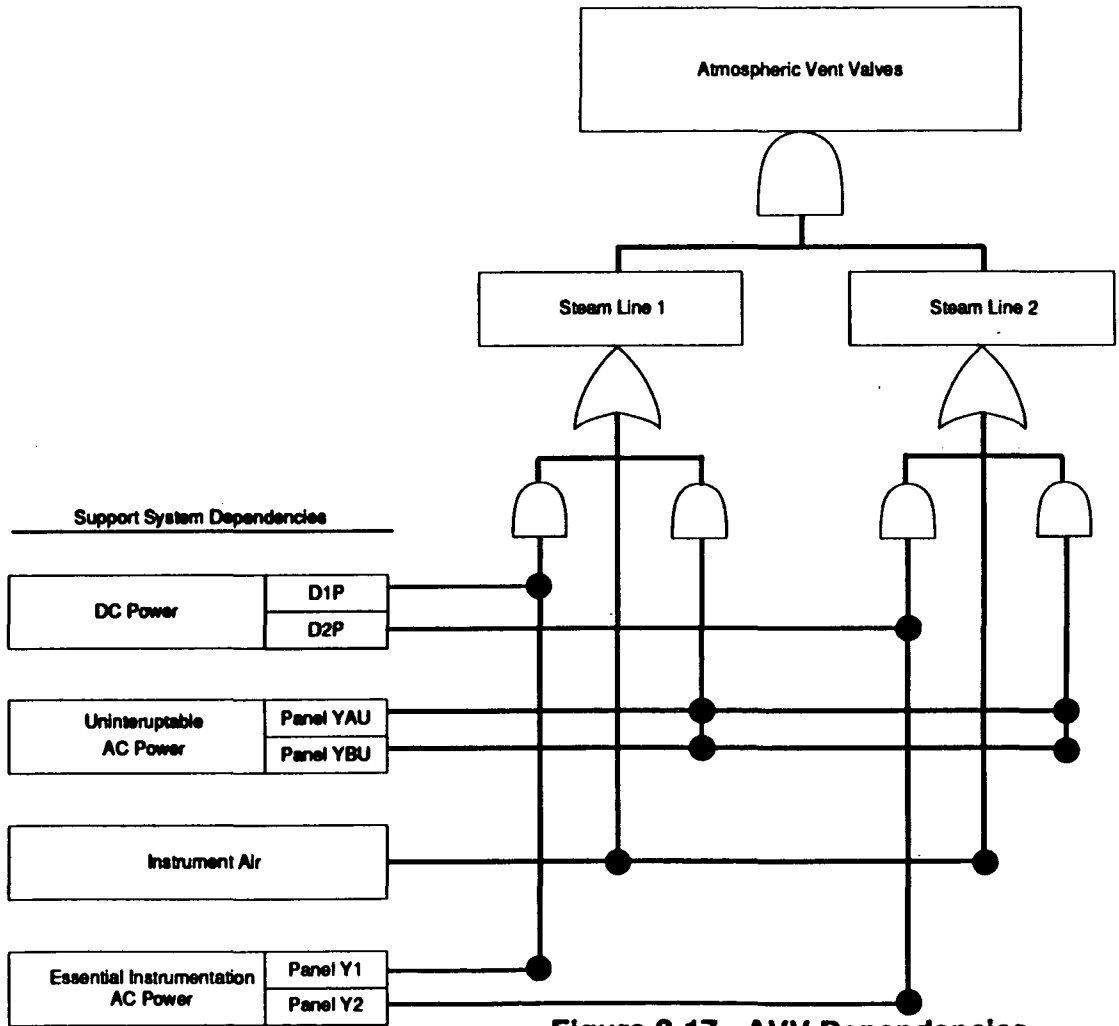


Figure 2-16. Main Feedwater System Dependencies



Support System Dependencies

DC Power	D1P	●
	D2P	●
Uninterruptible AC Power	Panel YAU	●
	Panel YBU	●
Instrument Air		●
Essential Instrumentation AC Power	Panel Y1	●
	Panel Y2	●

Functional Dependencies

None

Figure 2-17. AVV Dependencies

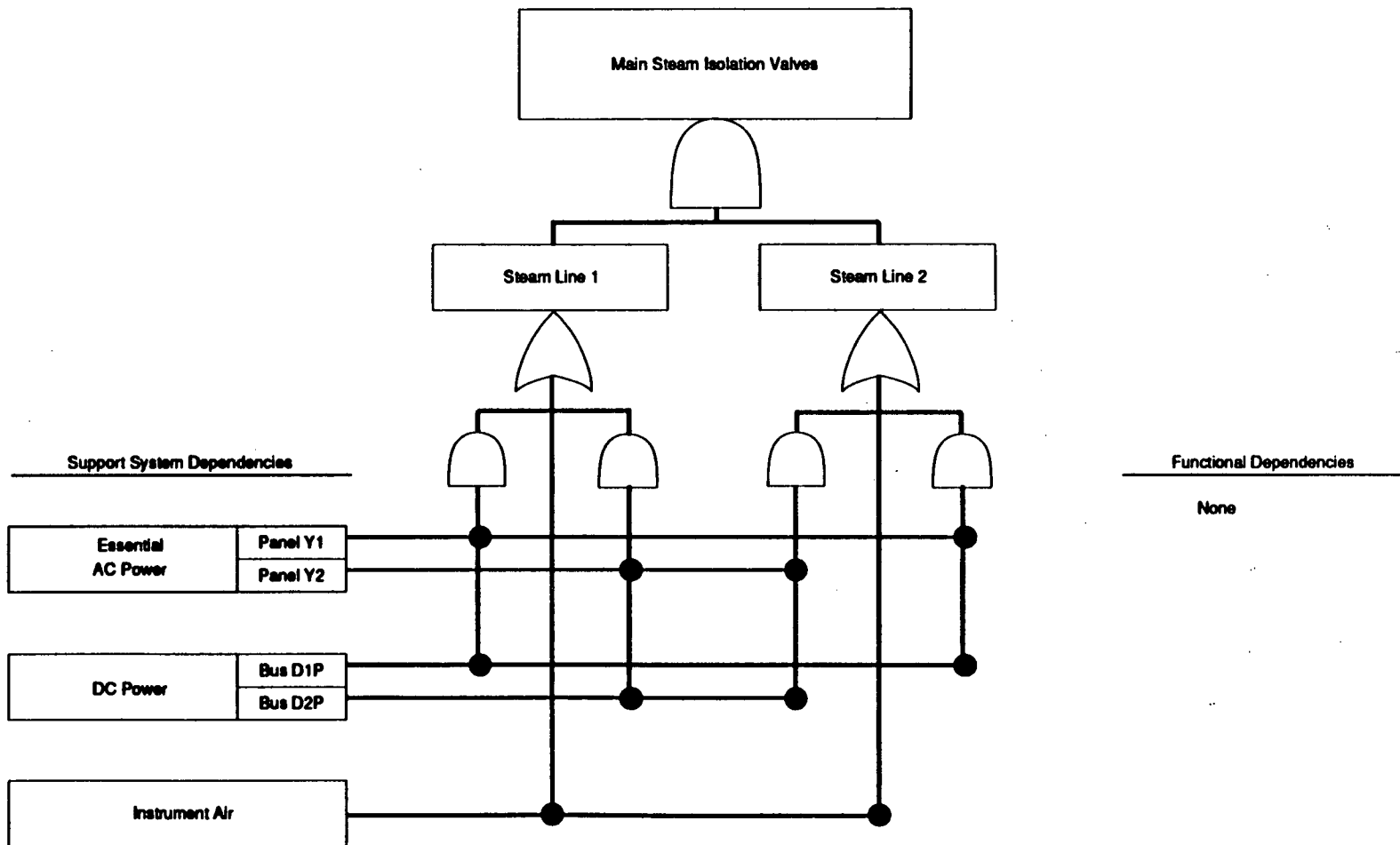


Figure 2-18. MSIV Dependencies

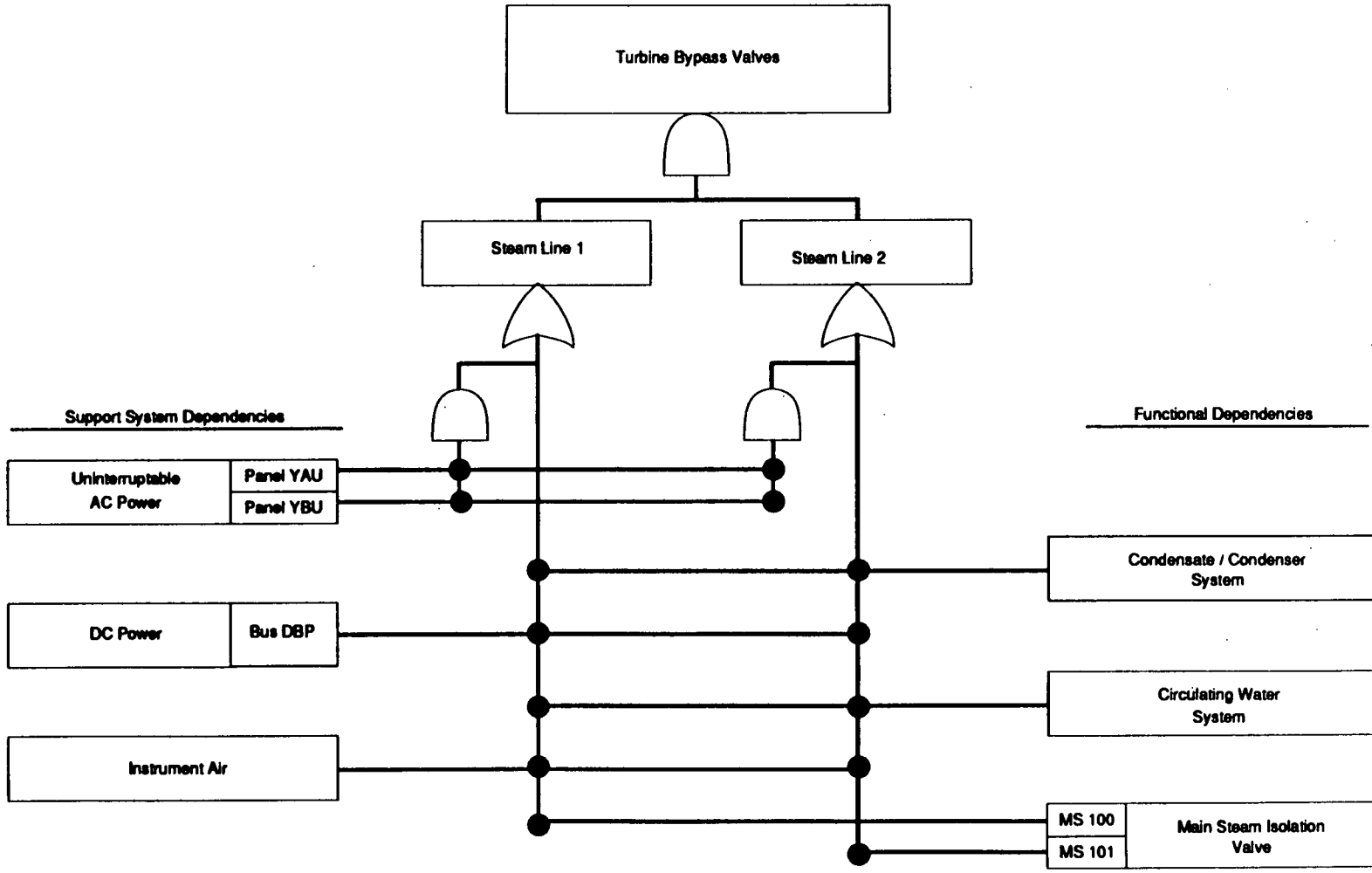


Figure 2-19. TBV Dependencies

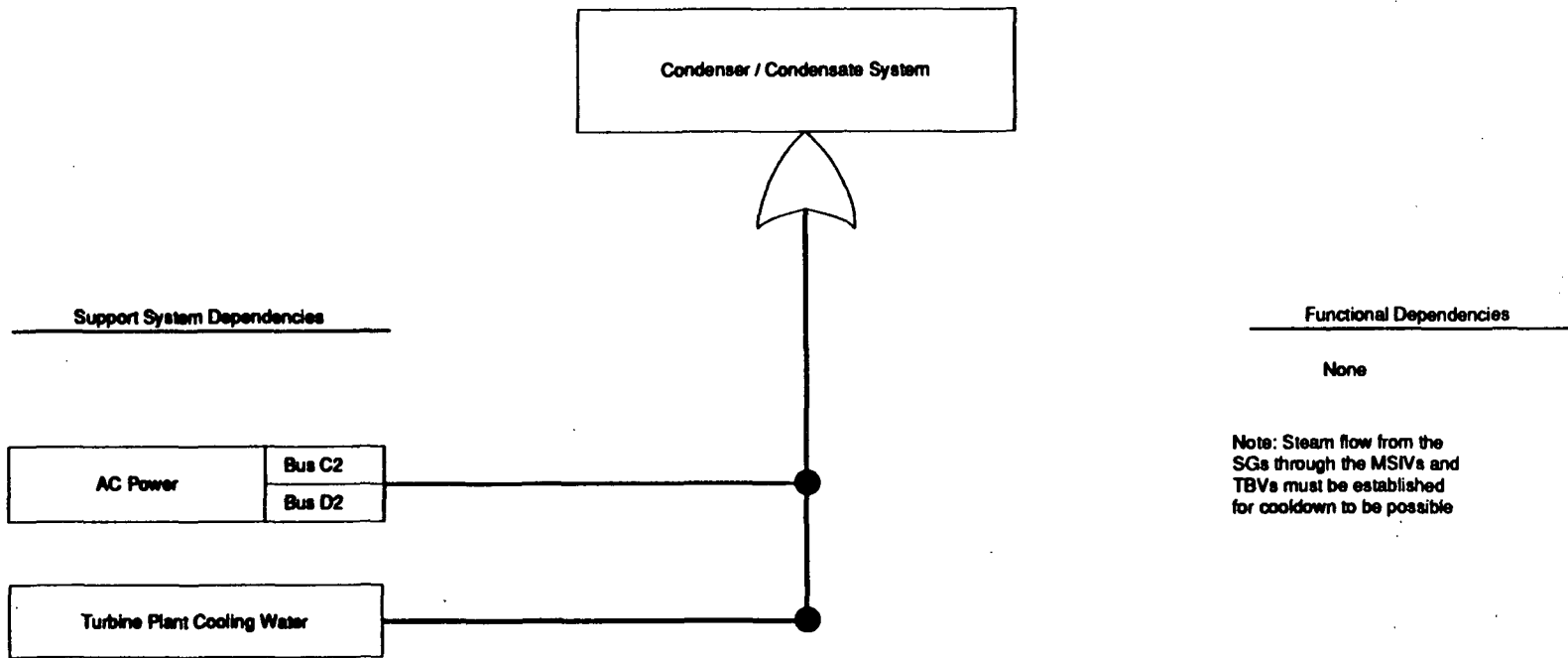


Figure 2-20. Condensate System Dependencies

requires non-essential 4160 vac power and TPCW. The circulating water system's only dependency is 13.8 kvac offsite power. Non-essential 4160 vac power and the service water system, with the circulating water system as a backup, are needed to support TPCW. For the AVVs, dependencies include instrument air, dc control power, and both essential and uninterruptable 120 vac power. The MSIVs depend on dc control power, essential ac power, and instrument air in order for them to function properly. Support dependencies for the TBVs include instrument air and dc and uninterruptable ac power. Other dependencies for the TBVs include the condenser/condensate system, circulating water system, and most importantly, whether or not the MSIVs are open. Since the MSSVs are mechanically actuated by steam pressure alone, there are no support systems for the MSSVs.

Role in the Sequence Models

The PCS system fault-tree model defines combinations of component failures that result in a failure for a particular function of each subsystem within the PCS.

The MFW system's major role in the sequences is to provide feedwater to the steam generators for the production of steam so that heat may be removed from the RCS. In all cases, only one train of MFW is necessary to provide adequate heat removal from the primary. Transient sequences utilize MFW under sequence event B_T, decay heat removal via steam generators. For sequences involving failure to trip, MFW is modeled under event B, RCS heat removal via MFW. SGTR sequences consider the availability of both the ruptured and intact steam generator in removing decay heat via MFW, represented by events B_R and B_U, respectively.

TPCW provides cooling for secondary plant components and serves as a support for the MFW system as well as the two station air compressors.

The module FMM00004 for the MSSVs accounts for any of the 9 MSSVs on SG1-2 failing to reseat and is used under SGTR event I, which represents the ability to isolate the ruptured steam generator.

The AVVs play a role in SGTR sequences in which they are used to cool down their respective steam generators by releasing steam to the atmosphere. In particular, they are included in the model for events C_U and C_R which describe cooldown using the unaffected and affected steam generator, respectively. For failure of long-term cooling following a small LOCA, including transient sequences which lead to a LOCA, the AVVs are modeled under events X_S and X_T, which both represent the ability to carry out long-term core cooling (assuming decay heat removal via steam generators).

The MSIVs play an important role in the SGTR model for both cooldown and isolation. The MSIVs directly impact the ability of the TBVs to be used in the cooldown process. Because the MSIVs are upstream of the TBVs, if they are shut the TBVs cannot be used for cooldown. Similar to the AVVs, the MSIVs are modeled under the sequence events C_U for the unaffected steam generator and event C_R for the ruptured steam generator. Isolation of the generator containing the ruptured tube involves being able to shut its MSIV.

Other systems which play a role in the sequence models are the TBVs, circulating water, and condenser/condensate system. As mentioned before, the TBVs are included in the SGTR model involving cooldown of either the affected or unaffected steam generator. Like the AVVs, the TBVs are used in events C_R and C_U respectively. Under emergency conditions, the circulating water system is used in support of the TPCW system when the normal service water flow for train 2 is diverted to the CCW system. The condenser/condensate system supports cooldown of the steam generators via the TBVs and the ability of MFW to feed the steam generators.

2.2.7 Auxiliary Feedwater

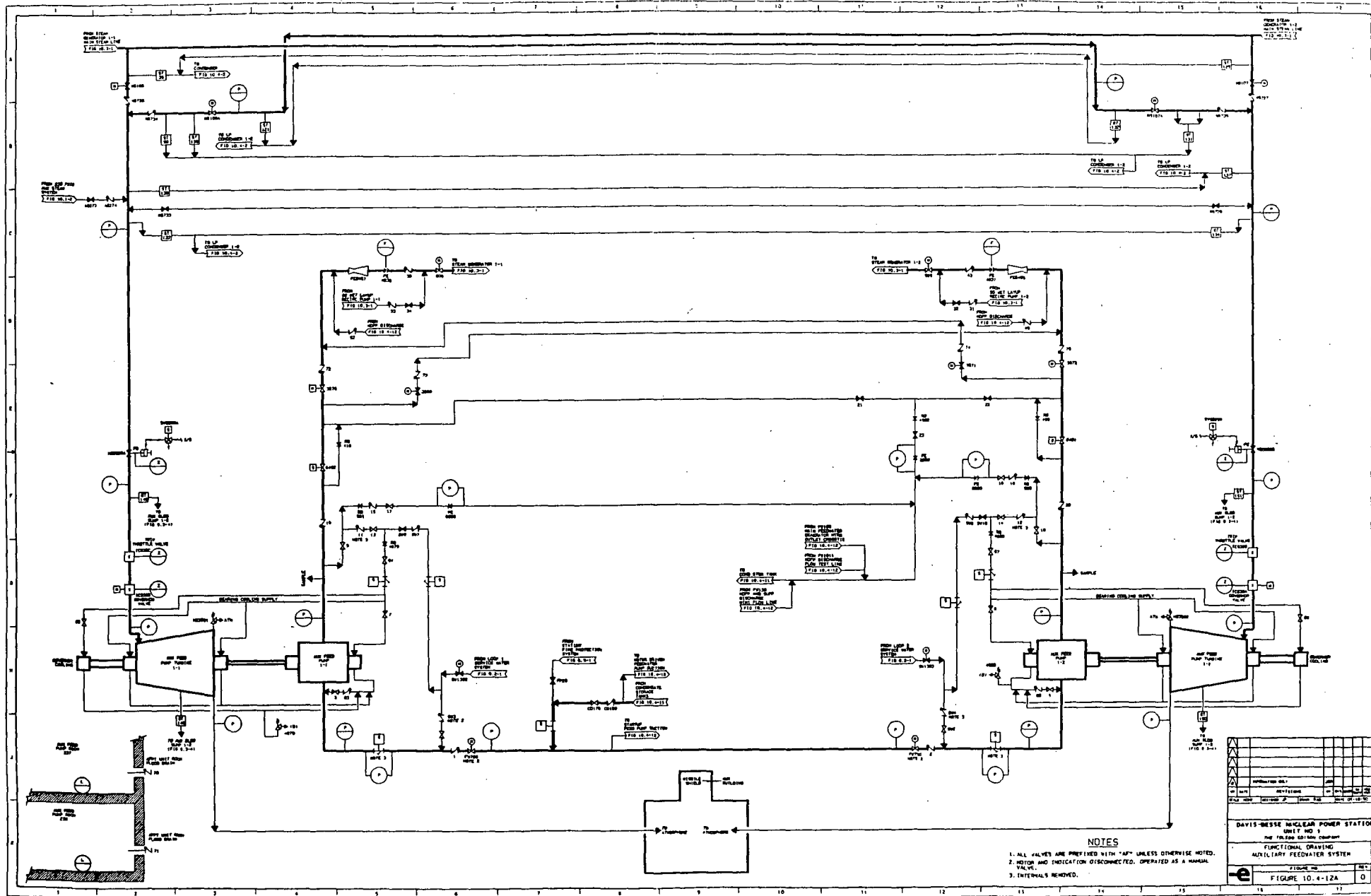
The Davis-Besse auxiliary feedwater (AFW) system is used to provide feedwater to the steam generators for the removal of reactor decay heat as a backup to main feedwater, and also to promote natural circulation in the event of a loss of all four reactor coolant pumps. The AFW system provides a sufficient secondary side heat sink to cool down the RCS following a reactor trip at full power to conditions at which the DHR system can be placed in operation.

Design and Operation

The major components of the AFW system are shown in Figure 2-21. During normal full power operation, the AFW system is in standby with both turbine-driven pumps available. The motor-driven feed pump (MDFP) is used for plant startup and then aligned as a backup auxiliary feed pump when reactor power is above 40 percent. The MDFP is started by operator action in the event of failure of either of the turbine-driven pumps.

The condensate storage tanks (CSTs) are the normal suction source for the turbine-driven auxiliary feed pumps and the MDFP. The two CSTs are normally cross-connected with one CST outlet valve open. The Technical Specification CST inventory requirement of at least 250,000 gallons ensures enough water is available to the AFW system to remove decay heat for 13 hours, with subsequent cooldown to 280F. The suction valve for each AFP is a motor-operated valve, but the power supply has been physically disconnected and is locked open. In the event the condensate storage tanks are unavailable, two low pressure switches, located upstream of each pump suction isolation valve, automatically open respective service water supply valves, thereby providing a backup suction source from the service water system.

The turbine-driven pumps are seven-stage centrifugal pumps each with a capacity of 1050 gpm at 1050 psig with the turbine operating at a maximum rated speed of 3600 rpm. One pump is sufficient to supply 600 gpm 40 seconds after a loss of MFW to meet decay heat removal requirements. To ensure pump protection, there is a two inch mini-recirculation line which taps off the discharge line just upstream of the Target Rock flow control valves. The AFW pump turbines are rated at 800 hp at a shaft speed of 3600 rpm, utilizing steam at 885 psig and 590F. The turbines are of the horizontal type having a split casing, solid wheel rotor



- NOTES**
1. ALL VALVES ARE PROVIDED WITH "AP" UNLESS OTHERWISE NOTED.
 2. MOTOR AND INDICATION DISCONNECTED, OPERATED AS A MANUAL VALVE.
 3. INTERNALS REMOVED.

REVISIONS	
NO.	DESCRIPTION

DAVIS-BESSE NUCLEAR POWER STATION	
UNIT NO. 3	
THE FEEDER SYSTEM DRAWING	
FUNCTIONAL DRAWING	
AUXILIARY FEEDWATER SYSTEM	
FIGURE NO.	
FIGURE 10.4-12A	0

with only one stage. Turbine overspeed protection is provided by a trip throttle valve actuated by a mechanical overspeed trip mechanism.

The MDFP is an eight-stage centrifugal pump with a design flow rate of 800 gpm at a discharge pressure of 1042 psig. The MDFP is powered by a 3600 rpm, 800 hp motor using 4160 vac power. A minimum flowrate of 180 gpm and a NPSH of 21 feet are required for pump protection. The MDFP is capable of taking suction from either the CST or the service water system while in the AFW mode. The MDFP can be manually started to provide feedwater in the event that either or both turbine-driven pumps fail. In the event offsite power is unavailable, the MDFP can be supplied from the station blackout diesel generator (SBODG) or by electrical realignment from either of the emergency diesel generators (EDG).

Valves on the main steam lines permit operating the AFW pump turbines with steam from either their respective or opposite steam generator. The valves to the AFW pumps from their respective steam generator (MS106 and MS107) are normally closed and the valves from the cross-connected steam generator (MS106A and MS107A) are normally open. Each turbine exhausts to the atmosphere. Low pressure switches at the turbine steam inlets will automatically isolate steam to the turbine should a low pressure condition exist, indicative of a steam line break.

The Target Rock flow control valves are dc-powered solenoid valves that are modulated to maintain the required steam generator level. They are interlocked with their respective steam admission valves such that when the steam admission valves are closed, control power to the flow control valves is removed and the valves fail fully open. When the steam admission valves leave their closed seat, control power is restored to the valves to maintain the required steam generator level.

The steam-feedwater rupture control system (SFRCS) provides protection against main steam and feedwater line breaks, steam generator overfill, steam generator low level, and loss of all four reactor coolant pumps. The SFRCS also provides for automatic start of the AFW system when it is needed for removing decay heat. SFRCS is divided into two actuation channels each comprised of two logic channels. Upon SFRCS actuation, each turbine-driven pump will feed its own steam generator while steam supply to both turbines is cross-connected from both steam generators. If SFRCS is actuated on either a steam generator 1-1 or steam generator 1-2 low pressure condition, the intact generator will be fed from both turbine-driven pumps with the depressurized steam generator being isolated. Steam to both turbines will be supplied from the intact generator.

Dependencies

As outlined in Figure 2-22, the AFW system requires various support systems for operation. As stated above, SFRCS provides for automatic initiation, with channels 1 and 3 providing input to AFW train 1 and channels 2 and 4 servicing train 2. Essential power from 480 vac and 120 vac as well as dc control power are required for control of isolation and throttle valves. Motive power for the turbine-driven pumps is supplied by steam from the

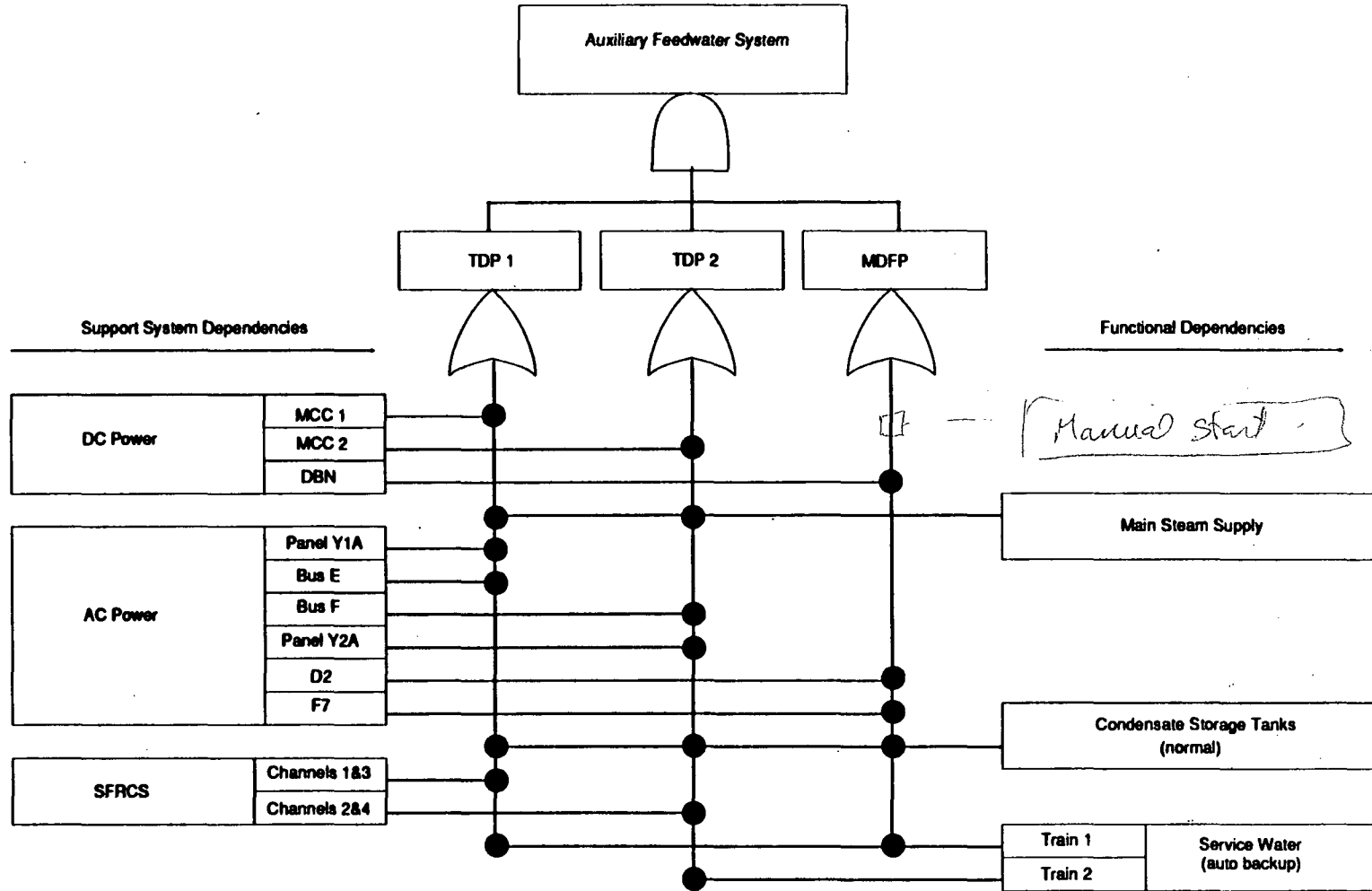


Figure 2-22. Auxilliary Feedwater System Dependencies

steam generators or the auxiliary steam system. The MDFP is powered by 4160 vac which can be supplied by the SBODG upon loss of offsite power. Power supplied from the 480 vac and dc systems are also required for successful operation of the MDFP. Service water is included as a backup suction source for AFW in the event the CSTs are unavailable. Room cooling is provided to ensure continued equipment operability.

Role in the Sequence Models

The AFW system plays a vital role in the removal of decay and sensible heat from the primary system in the event MFW is unavailable. AFW is used to cool down the RCS early in the sequence for small LOCAs, represented by sequence top gate B_S , failure to provide heat removal via steam generators. Similarly, for transient sequences the AFW system can be used for decay heat removal, represented by event B_T . Given an initial failure of AFW for the transient events, late recovery of heat removal via the steam generators is given credit depending on the type of AFW failure and available recovery actions.

When considering the role of the AFW system in SGTR sequences, both the turbine-driven pumps and the MDFP are considered for supplying feedwater to either the intact or ruptured steam generator for decay heat removal. This is represented by SGTR sequence events B_U , failure of heat removal via unaffected steam generator 1-1 and B_R , failure of decay heat removal via ruptured steam generator 1-2.

For sequences involving failure to trip, only the turbine-driven pumps are considered for providing RCS heat removal via the steam generators. The MDFP is excluded because the need for heat removal is immediate in mitigating the RCS pressure increase. Unlike the turbine-driven pumps, which are automatically started, the MDFP requires manual start by the control room operator. This event is designated by event L, failure of heat removal via auxiliary feedwater.

2.2.8 Containment Spray

The containment spray (CS) system provides cooling and pressure suppression to the containment vessel by spraying borated water into containment following a LOCA. The system also is effective in scrubbing some fission products from the containment atmosphere. One train of CS along with one containment air cooler (CAC) is designed to reduce pressure and remove the total post-LOCA heat energy released to the containment.

Design and Operation

As shown in Figure 2-23, the CS system consists of two possible suction paths; during injection from the BWST and during recirculation from the containment emergency sump. When the water in the BWST reaches a level of 8.0 feet, spray pump suction is transferred to the containment emergency sump for the recirculation phase of system operation.

There are two CS pumps rated at 1300 gpm which supply the spray ring headers with borated water, thereby cooling the containment following a LOCA. Each pump is a single-

stage, horizontal centrifugal pump powered by a 200 hp motor. The pump seals are cooled with water from the impeller.

Valves CS1530 and CS1531 are 8-inch motor-operated globe valves which are normally closed and serve as containment isolation valves during normal plant operation. In the event of a LOCA, the valves receive a SFAS signal to open to allow containment spray flow to the spray ring header. The valves are fully open during injection and are throttled to approximately 55 percent open during recirculation to protect the pump motors and to ensure a flow rate compatible with the available NPSH.

The spray nozzles spray borated water into the post-LOCA containment atmosphere. Ninety stainless steel nozzles are connected to each 8-inch spray ring header. The spray pattern of either of the two independent and redundant spray headers provides adequate volumetric coverage for fission-product removal.

The CS system is normally in standby with both trains available. A SFAS level 2 actuation signal opens both spray isolation valves, CS1530 and CS1531. A SFAS level 4 actuation signal at a containment pressure of approximately 24 psig starts both pumps. A SFAS level 5 actuation signal prompts the operator to manually transfer the containment spray water supply to the containment emergency sump by opening valves DH9A and DH9B.

Dependencies

As outlined in Figure 2-24, the CS system is dependent on the proper functioning of other plant support systems. SFAS actuation signals are necessary for automatic start and operation of equipment under accident conditions. Motive power for each of the pumps and motor-operated valves is provided by the respective safety-related buses. Control power (dc) is necessary for operation of the power supply breakers for the pumps and valves. To prevent overheating, ECCS room ventilation is provided to ensure adequate cooling and ventilation of the pump motors. The borated water supply is provided via portions of the DHR system in injection and recirculation.

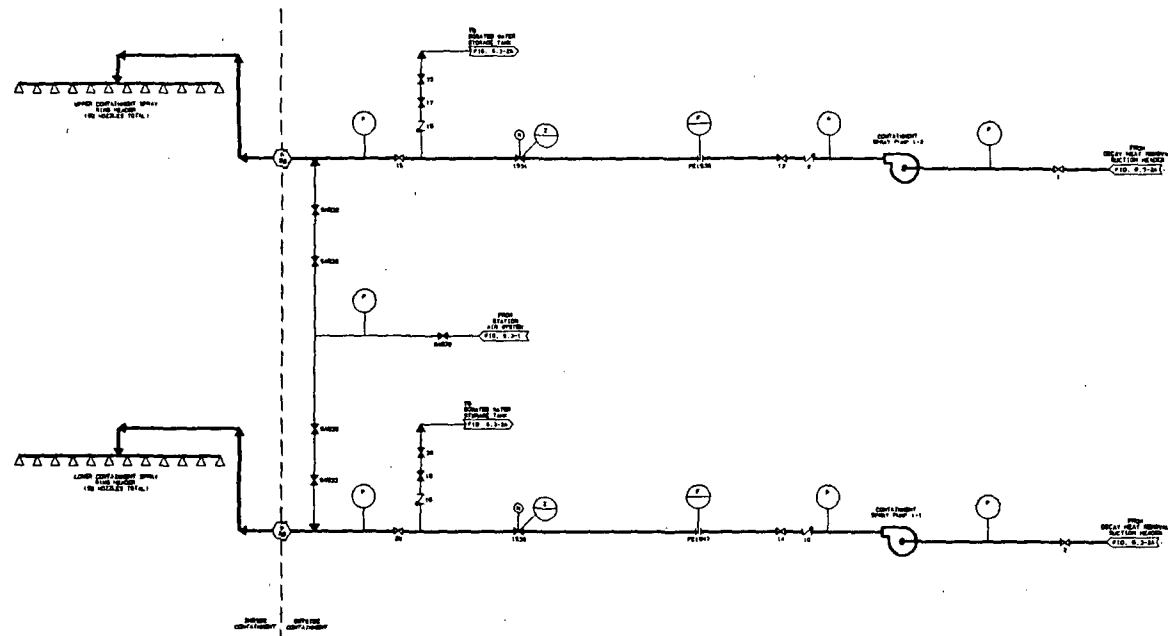
Role in the Sequence Models

There are two top gates for the CS system which play a role in the containment vessel's ability to contain fission products within its volume, preventing a post-accident release to the environment. Events G_1 (no flow to spray nozzles during injection) and G_2 (no flow to spray nozzles during recirculation) are used in the bridge event tree. A failure of both trains is required for failure of the CS system during both injection and recirculation modes of operation.

2.2.9 Containment Air Cooling

The containment air coolers (CACs) are used during normal operations and during accident conditions to cool the containment environment. The heat removed by the CACs

NOTES
 1. ALL VALVES ARE PROVIDED WITH TDS* UNLESS OTHERWISE NOTED.



DAVIS-BESSE NUCLEAR POWER STATION										
UNIT NO. 1										
THE FOLLOWING COMPART										
FUNCTIONAL DRAWING										
CONTAINMENT SPRAY SYSTEM										
FIGURE NO.										
FIGURE 6.3-1										
REV.										
0										

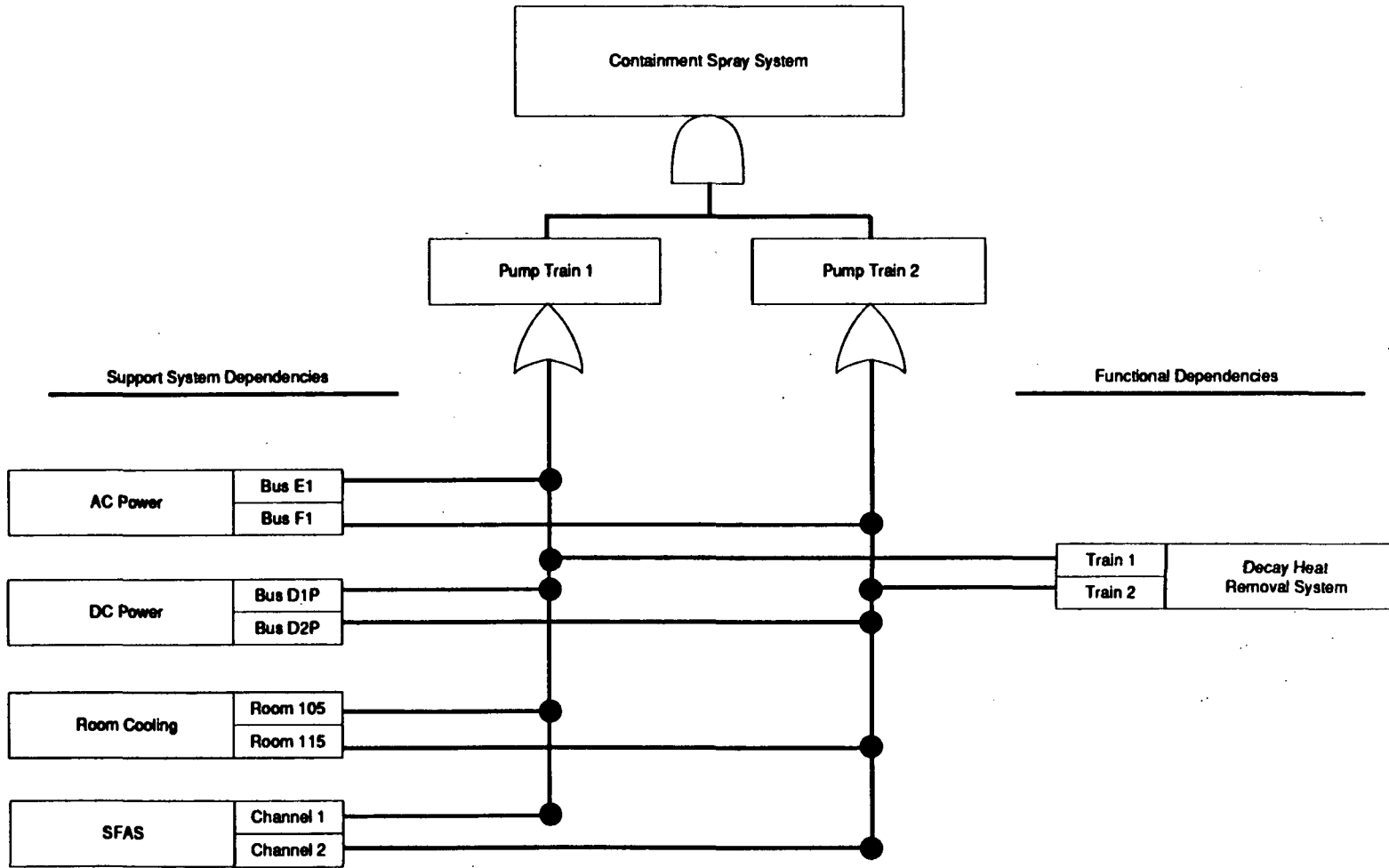


Figure 2-24. Containment Spray System Dependencies

mitigates the temperature and pressure increase following a LOCA and ensures operational integrity of the containment vessel and associated equipment.

Design and Operation

As shown in Figure 2-25, the CAC system is composed of three parallel trains, each with an air cooler unit, ductwork, and backdraft dampers. Each air cooler unit consists of a finned-tube cooling coil and a direct drive fan. The CAC fans draw air through the cooling coils where heat is transferred from the air to the cooling water in the tubes. Cooling water for the air cooler units is supplied by the service water system. Downstream from each CAC are fusible link dropout registers, and backdraft dampers which are provided to prevent backflow. The CAC trains then come together in a common supply header designed to distribute air to necessary equipment inside containment.

Service water is normally supplied to two CACs while the third CAC is in standby with its service water supply isolated to ensure adequate flow through the two operational CACs. The cooler fans operate in fast speed during normal plant operation in order to circulate the maximum volume of air inside containment. A temperature control valve in the CAC discharge line downstream from each CAC automatically regulates service water flow based on a signal from a temperature indicating controller, providing temperature control while the fan is in fast speed.

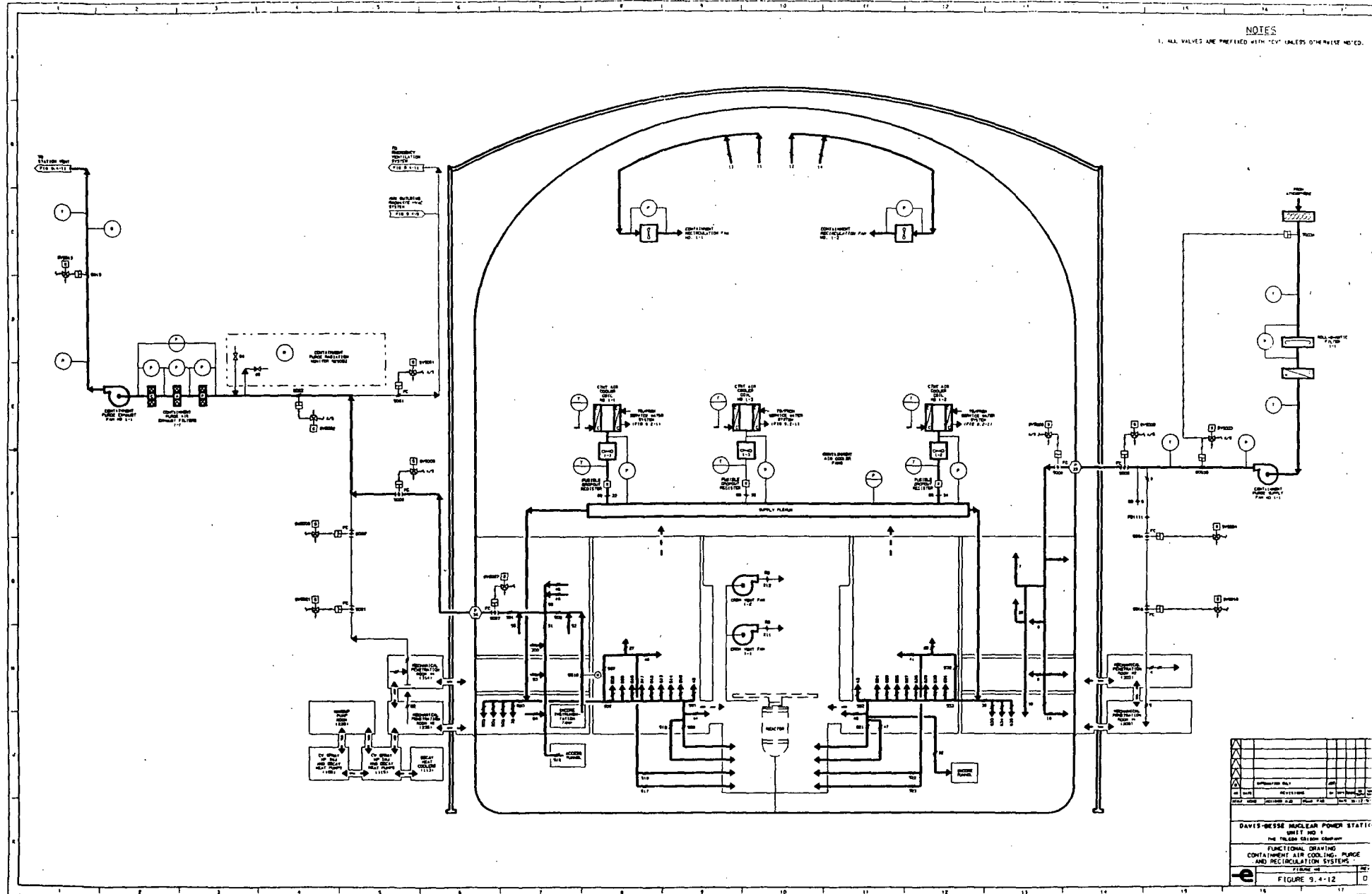
Upon receipt of a SFAS level 2 signal while in fast speed, the CAC fans are deenergized by interrupting control power to their fast speed circuitry. The fans will stop and then restart in slow speed five seconds later. Following an accident, the service water control valve in the CAC discharge header goes to the full open position to allow full flow through the in-service CAC coils, thereby maximizing cooling capacity. When temperature inside containment reaches 165F, the fusible links are designed to melt and cause the dropout registers to open. The CACs and containment spray work together in removing post-LOCA heat in order to maintain an adequate containment environment.

Dependencies

As outlined in Figure 2-26, various support systems are needed for successful operation of the CACs. The CAC fans require essential 480 vac power. SFAS level 2 is required for proper actuation of the CACs during post-LOCA conditions. Applicable portions of the service water system supply cooling to the operational CAC heat exchangers.

Role in the Sequence Models

The CACs serve an important role in both the front-end and back-end analyses. Operation of at least one CAC is required to maintain an environment that is suitable for long-term operation of the PORV during makeup/HPI cooling. Operation of at least one CAC can also provide for removal of decay heat from containment. This is reflected by event H in the bridge trees that link the core-damage event tree to the containment event tree.



NOTES
 1. ALL VALVES ARE PREFIRED WITH 'CV' UNLESS OTHERWISE NOTED.

DAVIS-BESSE NUCLEAR POWER STATION			
UNIT NO. 1		THE YELLOW CAJON SUBSTATION	
FUNCTIONAL DRAWING			
CONTAINMENT AIR COOLING, PURGE			
AND RECIRCULATION SYSTEMS			
FIGURE NO.			
FIGURE 9.4-12			
D			
REVISION NO.	DATE	BY	CHKD. BY

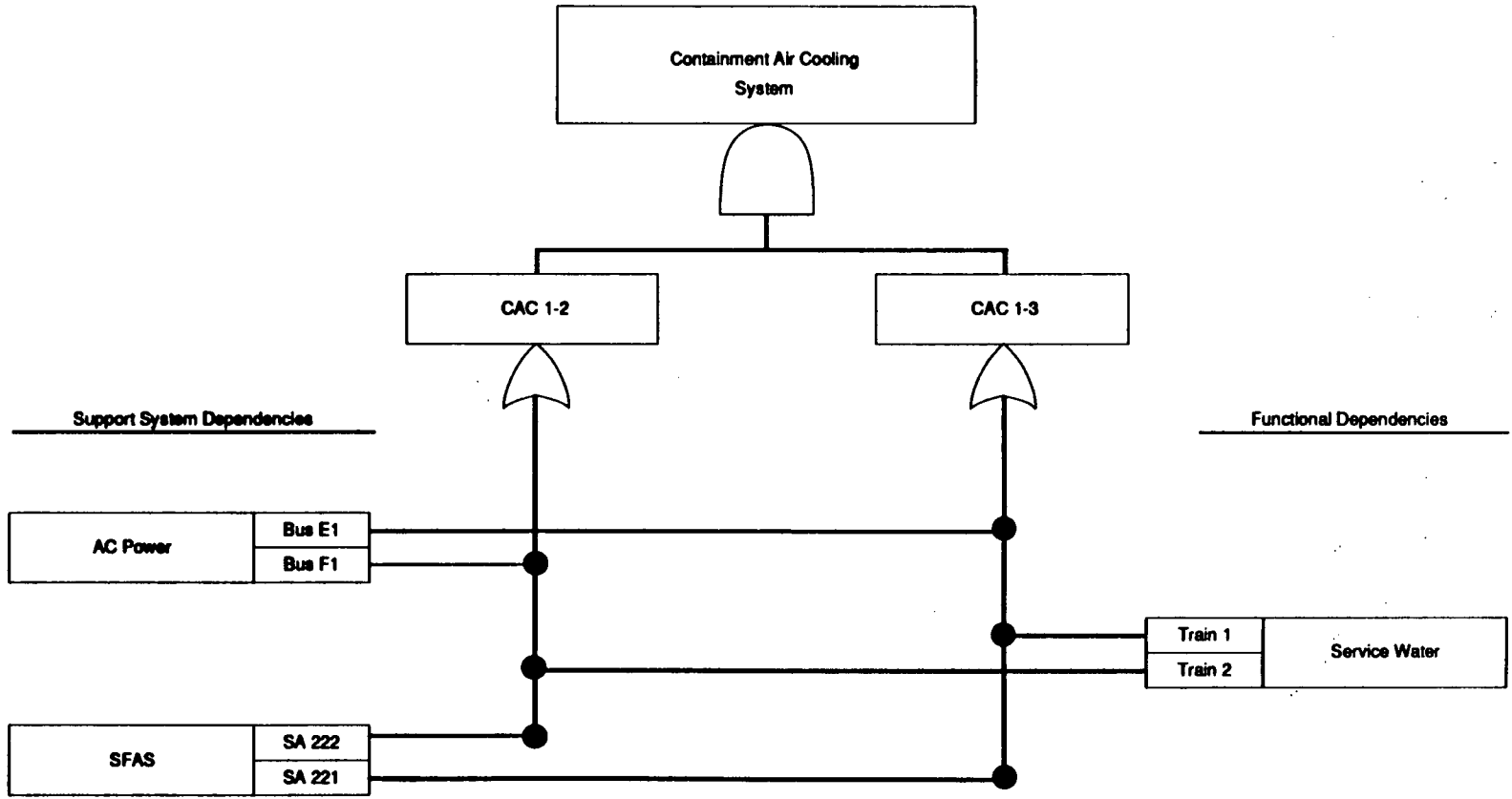


Figure 2-26. Containment Air Cooler Dependencies

2.2.10 Containment Isolation

The function of the containment isolation system is to isolate the containment vessel in the event of a radioactive release inside containment. This prevents the uncontrolled release of radioactive gases and/or liquids to the environment. The pressurization of the containment vessel is indicated by an SFAS level 2 actuation. The level 2 actuation initiates the closing of the containment isolation valves for the penetrations of the containment vessel.

Design and Operation

The containment isolation system is composed of valves from many systems that are used to seal the containment vessel penetrations in the event of a radioactive release inside containment. During normal power operation, the containment isolation valves are positioned according to the needs of the particular penetrations they isolate. The containment isolation valves included in this model are automatically closed upon receiving the required SFAS actuation signal. Those valves which would preclude operation of a nuclear safety system do not close on an SFAS state, but can be closed by the operators if that safety system is not in use or necessary.

Isolation of different penetrations is accomplished by a variety of combinations of valves; most combinations correspond to one of the following:

- One or more normally closed manual valves both inside and outside containment;
- Two check valves, one inside and one outside containment, that would close to block flow from inside containment;
- Two motor-operated valves or a motor-operated valve and an air-operated valve, with one valve inside containment and the other outside; these valves could be normally closed, or could be actuated to close automatically upon a SFAS signal;
- A combination of both a power-operated valve and check valve, such as used for the vacuum breaker lines.

Each of the penetrations was examined relative to a set of screening criteria to identify those that present the most serious challenge with respect to both the probability and severity of releases if isolation were to fail. Lines were eliminated from further consideration if they satisfied any of the following criteria:

- The line is a closed loop inside containment, such that a failure of the pressure boundary would be required for an isolation pathway to exist.
- The penetration is normally closed, and it is of such a nature that it would be impossible to overlook its being open. For example, if the refueling tubes were not isolated, the containment would be flooded from the spent fuel pool.
- The line is very small, such that if it were open it would tend to be plugged by aerosols. For purposes of this analysis, lines less than about 3/4" in diameter were excluded.

- The line would lead through a path that would be continuously full of water during and after the accident, such that there would be significant scrubbing of any release of radioactive isotopes. It must be confirmed that pressurization of the containment could not blow the water out from the downstream pathway, and that the water would not otherwise be drawn away during an accident.
- The probability of the pathway being open is clearly extremely small (e.g., the line contains a normally-closed valve and two automatic isolation valves). More specifically, the probability of non-isolation (given core damage) should be less than 10^{-3} for a line less than 2 inches in diameter, and less than 10^{-4} for one greater than or equal to 2 inches.

As a result of this screening process, only a few penetrations required more detailed analysis, and the probability of isolation failure was found to be dominated by the contributions from two types. The first is comprised of eight lines that protect the containment from collapse due to a negative pressure differential. Each of these 8-inch lines contains a vacuum breaker and a normally open motor-operated valve. The motor-operated valves are actuated to close upon a SFAS level 2 signal. The second type is the line from the containment normal sump. This line contains two 4-inch motor-operated gate valves in series, which are normally open and require an SFAS level 2 actuation signal for automatic isolation. The flow path for this line leads to the miscellaneous waste drain tank, which is vented to atmosphere via the station vent.

Dependencies

The isolation valves require essential 480 vac power for operation and a SFAS level 2 signal for automatic actuation in the event of a reactor accident. For the vacuum breaker lines, bus E1 is responsible for providing power to the three motor-operated valves in lines B through D and bus F1 for the five in lines F through J. SFAS level 2 from actuation channel 1 services those motor-operated valves in lines B through D and actuation channel 2 for those in lines F through J. For the containment sump, motor-operated valves DR2012A and DR2012B are powered by buses E1 and F1, respectively, with their respective SFAS level 2 signals from actuation channels 1 and 2.

Role in the Sequence Models

The containment isolation system plays a role in the containment vessel's ability to contain fission products within its volume, preventing a post-accident release to the environment. Event B, containment vessel fails to isolate, is used in the event trees which bridge the front-end analysis with the back-end analyses of the containment vessel. Failure to isolate the containment vessel will not only result in a post-accident release of fission products, but also give varying results for the pressure/temperature characteristics of the containment vessel atmosphere. Failure of any of the eight vacuum breaker lines to be isolated is assumed to correspond to a large isolation failure. The sump line would constitute a small leak if it were to fail to isolate.

2.2.11 Reactor Trip

The purpose of the reactor protection system (RPS) is to initiate a reactor trip when a sensed parameter (or group of parameters) exceeds a setpoint value indicating the approach to an unsafe condition. In this manner, the reactor core is protected from exceeding design limits and the reactor coolant system (RCS) is protected from overpressurization.

Design and Operation

The RPS consists of four identical protection channels which are redundant and independent. Each channel is served by its own independent sensors which are physically isolated from the sensors of the other protective channels. Each sensor supplies an input signal to one or more signal processing strings in the RPS channel. Each signal processing string terminates in a bistable which electronically compares the processed signal with trip setpoints. All bistable contacts are connected in series. In the normal untripped state, the contact associated with each bistable will be closed, thereby energizing the channel terminating relay. The RPS is set up such that when two out of four channels trip, each of the four RPS channels will cause their respective control rod drive mechanisms to de-energize and an automatic scram to occur.

There are eight trip bistables that are normally in series with the power supply to each of the protective channel trip relays. The trip bistables include the following conditions for which a scram can occur: (1) high RCS pressure, (2) low RCS pressure, (3) high RCS temperature trip, (4) variable low RCS pressure, which compares the RCS pressure to the temperature, (5) high reactor power, (6) power-to-flow ratio, (7) power imbalance vs. flow, and (8) high containment volume pressure. In addition, the RPS is designed to trip a channel upon loss of power or removal of any module required to perform a protective function.

As a backup to the RPS, the diverse scram system (DSS) is used to mitigate the consequences of an anticipated transient without scram event by tripping the reactor if the control rods fail to drop from an RPS trip due to high RCS pressure. The DSS is a two-out-of-two logic system which has no dedicated sensors, but instead continuously monitors the extended-range reactor coolant system pressure from the post-accident monitoring system. If the pressure exceeds the programmed setpoint, the DSS activates relays that remove power from the control rod drive (CRD) programmer lamps. When this power is removed, the control rods drop, thus tripping the reactor. The DSS will also actuate the "DSS trip" alarm to indicate that a CRD trip has been initiated. The DSS consists of six modules which combine to perform the intended function: two independent DSS control modules (channels 1 and 2); two system power supply modules; and two 24 vdc power supply modules.

Dependencies

Dependencies for the reactor trip system were not explicitly modeled, as described below.

Role in the Sequence Models

A detailed model was not developed for the RPS or DSS for the IPE. Based on previous detailed investigations which were reviewed earlier by the NRC, the reliability of the trip systems is expected to be very high (Ref. 80).

While the prior evaluation focused on the reliability of the trip signals and operation of system components, it did not specifically address the potential for common-cause failure of the control rod assemblies to insert due to mechanical binding. Given the very high reliability calculated for the system and the potential that the operators could back up failures of automatic trip signals, it was judged that the risk of failure to trip could be dominated by this non-recoverable mechanical failure mode.

Therefore, the failure of the RPS and DSS was reflected in the sequence logic by a single event representing common-cause failure of the control rod assemblies to insert following a trip signal. This single event corresponds to event K_1 in the event tree for sequences involving failure to trip. The probability of failure was estimated based on a review of PWR operating experience and treatment of this failure mode in other PRAs. As a result, an unavailability of 1×10^{-6} per demand was assessed for this failure mode.

2.2.12 Safety Features Actuation System

The function of the safety features actuation system (SFAS) is to automatically prevent or limit fission product and energy release from the core, to isolate the containment vessel, and to initiate operation of the engineered safety features in the event of a LOCA or fuel handling accident inside containment. The main goal is to localize, control, and mitigate such accidents and to maintain radiation exposure levels below applicable guidelines. SFAS also monitors the 4160 vac essential buses for the loss of offsite power and undervoltage to initiate sequencing of the safety loads on the emergency diesel generators on a loss of power coincident with a SFAS actuation.

Design and Operation

There are five incident levels of ESF actuation: (1) SFAS level 1 occurs when either a high containment radiation, a high containment pressure, or a low RCS pressure condition occurs; (2) SFAS level 2 occurs when either a high containment pressure or a low RCS pressure condition occurs; (3) SFAS level 3 occurs when either a high containment pressure or a low-low RCS pressure condition occurs; (4) SFAS level 4 occurs when a high-high containment pressure condition occurs; and (5) SFAS level 5 occurs when a BWST low-low level condition occurs.

SFAS consists of four identical and redundant sensing and logic channels (1 through 4), of which channels 1 and 3 are shown in Figure 2-27. The outputs of logic channels 1 and 3 combine to form SFAS actuation channel 1 while the outputs of logic channels 2 and 4 combine to form actuation channel 2. The sensing channels monitor redundant and independent process variables and initiate a trip when the monitored variable or parameter exceeds a set limit. Each of the four logic channels monitors the trip bistable of the

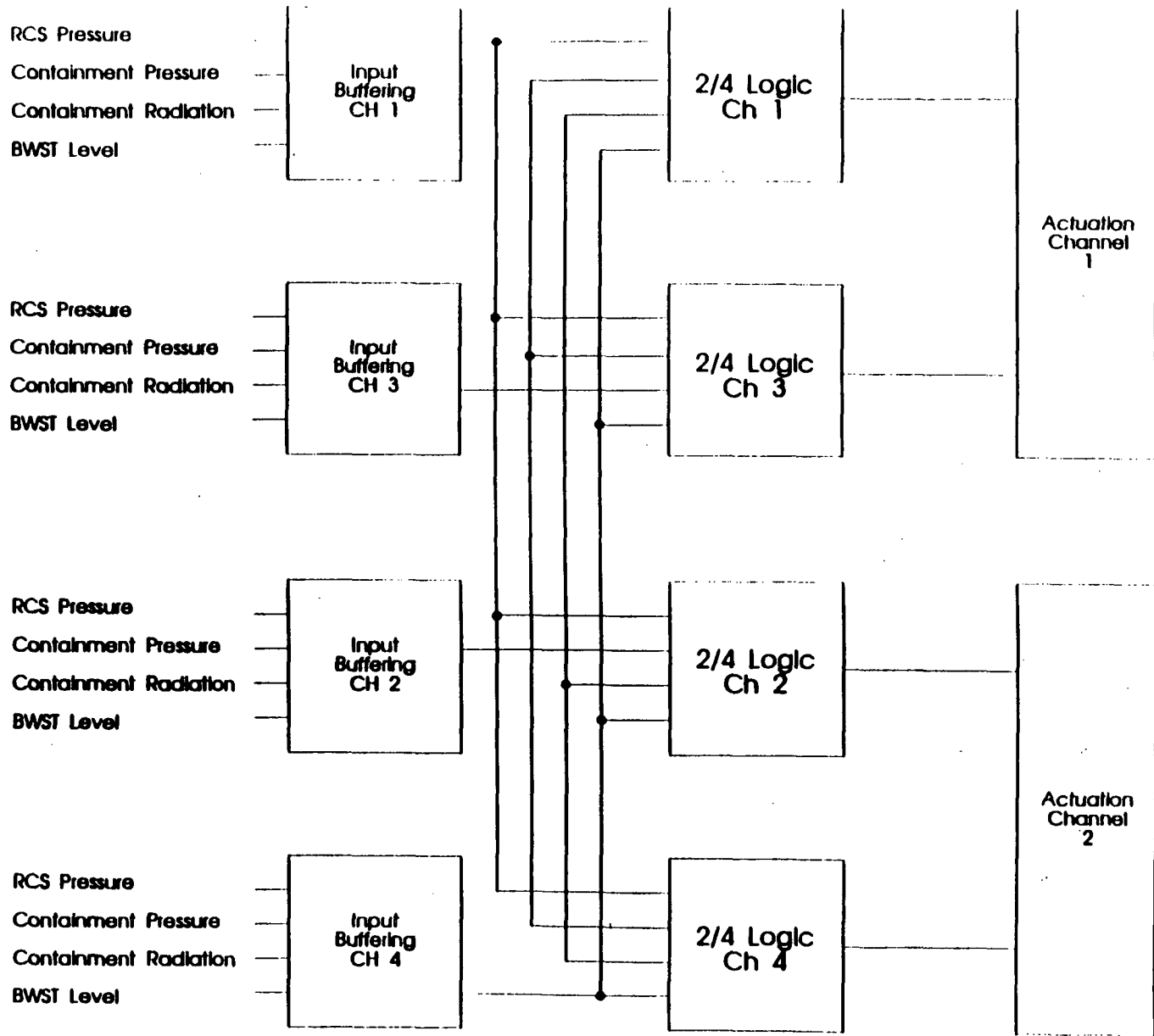


Figure 2-27. SFAS Functional Drawing

corresponding sensing channel and of the remaining three sensing channels through isolation devices. Input signals from the four bistables monitoring a given parameter are used to make up a two-out-of-four matrix logic. If any two out of four trip bistables monitoring a given station variable trip, the output modules for all four logic channels will indicate a tripped condition. The contacts of the output relays are configured to actuate the equipment needed to mitigate the consequences of the existing accident condition. The output contacts of logic channel 1 are interconnected to logic channel 3 to create actuation channel 1 and likewise for channels 2 and 4 for actuation channel 2. Both complementary logic channels of each actuation channel must actuate in order for a full SFAS actuation.

Dependencies

Since SFAS is designed as a fail-safe system, there are no support systems modeled for SFAS. That is, if electric power to an SFAS channel were lost, that channel would indicate a tripped condition.

Role in the Sequence Models

SFAS levels 1 through 4 play a primary role during accident sequences in automatically starting and operating the plant's emergency systems for accident mitigation. Automatic action helps ensure timely sequencing for operation of ECCS equipment in order to free the operator from the initial burden of quickly processing and analyzing numerous plant parameters. SFAS level 5 offers no automatic action other than to prompt the operator to switch from the injection mode to recirculation.

SFAS level 2 is an input to the following systems required for operation during emergency conditions: service water (for closure of SW1395), initiation of HPI, CCW (for start of the second pump), reconfiguration of the containment air coolers, closure of the appropriate containment isolation valves, and opening of the isolation valves for containment spray. Additionally, a SFAS level 2 state will result in isolation of RCS letdown in the makeup and purification system.

SFAS level 3 is an input to the CCW and DHR systems. SFAS level 3 is responsible for starting both DHR pumps in the LPI mode, initially taking suction from the BWST. CCW is reconfigured such that flow is provided to both DHR coolers and the non-essential header is isolated by shutting valve CC1460.

SFAS level 4 is an input to the containment spray system for automatic start of the spray pumps and also provides a signal for isolation of CCW to the letdown coolers and RCPs.

2.2.13 ECCS Room Ventilation

The ECCS room coolers are designed to maintain a suitable environment in the ECCS rooms to ensure continued operation of the equipment in the HPI, DHR, and containment spray systems.

Design and Operation

ECCS room coolers 1-4 and 1-5 service room 105 which contains HPI pump 1-1, DHR pump 1-1, and CS 1-1. ECCS room coolers 1-1 and 1-2 service room 115 which contains HPI pump 1-2, DHR pump 1-2, and CS pump 1-2.

Each cooling unit consists of a cooling coil and a fan. The supply air from the fan is cooled by the room cooling coil. Service water flows through the cooler tubes providing the cooling medium. A temperature control valve at the discharge of each cooler throttles service water flow to maintain room temperature within a desired band. When room temperature reaches 88F, the ECCS room cooler outlet motor-operated valves automatically open and the fans start. At 73F, the fans are deenergized. There is normally an open bypass valve around the motor-operated valves to maintain some flow through the coolers at all times.

During normal power operation, the ECCS equipment is not in operation and the ECCS room coolers are generally not in operation. Upon receiving a SFAS level 1 actuation signal, the ECCS room isolation dampers automatically shut to isolate the ECCS rooms. Room temperature is then controlled by the room coolers which automatically start when the temperature reaches 85F. For rooms 105 and 115, the cooling capacity is such that only one room cooler is necessary to maintain sufficient temperature conditions for each room.

Dependencies

As outlined in Figure 2-28, the ECCS system is dependent upon other plant systems for successful operation. Essential 480 vac from the respective safety-related buses is required for operation of the ECCS cooler fans and service water cooling is necessary for removal of heat generated by the ECCS equipment.

Role in the Sequence Models

As mentioned before, the ECCS room coolers support their respective ECCS train, consisting of the HPI, DHR, and containment spray systems. The two top events modeled in this system describe combinations of failures which result in the unavailability of room cooling for ECCS rooms 105 and 115. Lack of ECCS room cooling to either ECCS room is considered to fail that respective train of ECCS.

2.2.14 Integrated Control System

The function of the integrated control system (ICS) is to maintain a balance between reactor power, steam generator feedwater flow, and turbine-generator electric load. It provides automatic reactivity control during power operation by control rod insertion and withdrawal. It also provides for controlled core heat removal at power in lieu of utilizing safety systems, and decay heat removal after reactor trip by control of atmospheric vent valves (AVVs), turbine bypass valves (TBVs), main and startup feedwater valves, and main feedwater pumps.

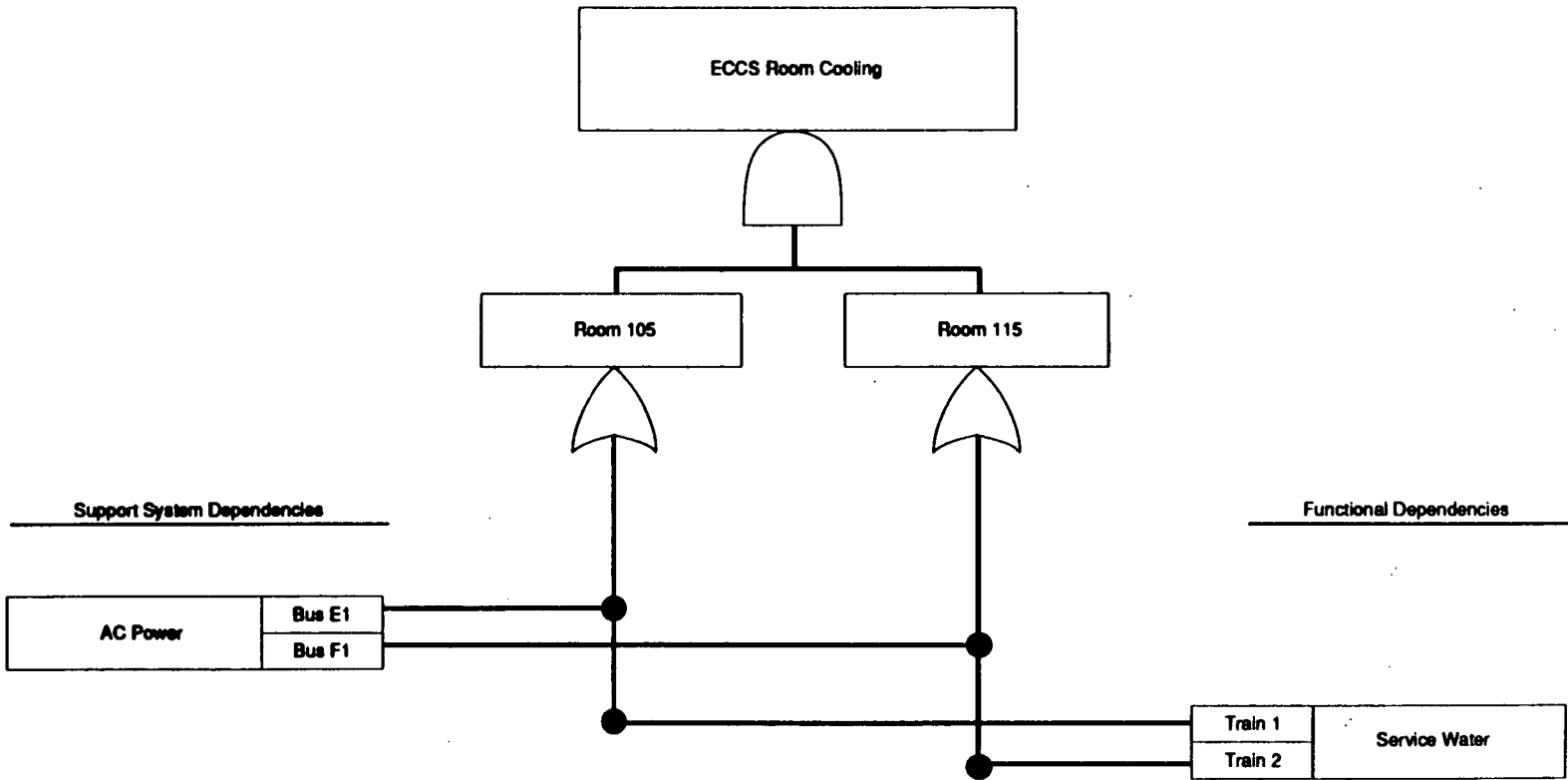


Figure 2-28. ECCS Dependencies

Design and Operation

The ICS is a complete system of control functions capable of automatically controlling the reactor and its associated once-through steam generators over a designated electrical load range. The ICS performs its basic functions by utilizing four independent subsystems: (1) the unit load demand (ULD), (2) the integrated master (IM) control, (3) the steam generator feedwater control, and (4) the reactor control.

The system philosophy is that control of the plant is achieved through feed forward control from the ULD. The ULD produces an electric megawatt demand for control of the reactor, steam generator feedwater, and turbine, while recognizing plant limits. The IM control receives the megawatt demand signal from the ULD and converts this signal into a parallel demand for the reactor control, steam generator feedwater control, and turbine control. The IM control also develops the demand for the turbine bypass system control. The steam generator feedwater control matches feedwater flow to the feedwater demand produced in the IM control. The feedwater demand is applied to the startup feedwater control valves and the main feedwater control valves, while at the same time the feedwater pump speed is adjusted to maintain the necessary flow. The reactor control regulates the control rods in accordance with the reactor demand established in the IM control. The reactor demand signal controls the reactor power in parallel with steam generator feedwater flow while maintaining a constant reactor coolant average temperature from low level limits to 100 percent reactor power.

The basic requirement of the ICS is to match megawatt generation to unit load demand. The ICS does this by coordinating steam flow to the main turbine with the rate of steam generation. During startup and power escalation, and during all modes of manual or automatic control, the system control philosophy is to control the load, the turbine header pressure, the average reactor coolant temperature, and the steam generator water inventory simultaneously. By controlling any three of these four parameters, the fourth is automatically predicted. During startup, when the steam generator levels are held constant, the average coolant temperature is allowed to vary. After an initial load is applied to the turbine, the turbine control maintains a constant turbine inlet steam pressure. Prior to turbine synchronization, the pressure is controlled by the TBVs.

Dependencies

Dependencies associated with the ICS are included in the MFW model and dependency matrix for the MFW system, Figure 2-16.

Role in the Sequence Models

A detailed model was not developed for the ICS. Instead, relatively simple models were developed for those portions of the system required to support operation of equipment needed in the sequences. Thus, the control signals were modeled for the TBVs and the AVVs. The steam generator feedwater control portion was not modeled explicitly; instead, failure of main feedwater after a reactor trip was modeled as a single basic event whose

unavailability was estimated from plant experience, with ICS faults that would cause a loss of feedwater following a trip included.

2.2.15 Electric Power

The ac and dc electric power systems are support systems that are designed to provide power to safety and non-safety related loads. The systems are redundant and must operate during normal and emergency plant conditions. During a loss of offsite power, the system supports essential loads by use of emergency diesel generators (EDGs).

Design and Operation

As shown in Figures 2-29 and 2-30, the electric power system is made up of several subsystems consisting of the 13.8 kvac, 4160 vac, 480 vac, 125/250 vdc, 120 vac, and NNIX/NNIY ac and dc systems.

During normal operation, each of the two 13.8 kvac buses (bus A and bus B) is fed from one of the 13.8 kvac windings of auxiliary transformer 11 (AUX11). During startup and shutdown, each bus is fed from the 13.8 kvac winding of its associated startup transformer. Each bus supplies the following loads: two reactor coolant pumps; two circulating water pumps; one 13.8 kvac - 4160 vac bus-tie transformer; and six 13.8 kvac - 480 vac non-essential substation transformers.

Each 4160 vac bus-tie transformer normally supplies one essential bus (C1 or D1) and one non-essential bus (C2 or D2) and is also used as a reserve power source for the other two buses. Each essential bus supplies the following loads: one service water pump; one HPI pump; one DHR pump; one CCW pump; one makeup pump; and one essential unit substation (4160 v-480 v) transformer. The non-essential buses supply power to non-safety related station auxiliaries.

Two redundant 2600 kW EDGs, one connected to each essential 4160 vac bus, are provided as onsite standby power sources to supply their respective buses upon loss of normal and alternate power sources. Each diesel generator receives a start signal upon sensing an undervoltage condition on its respective 4160 vac bus, on a SFAS level 2 signal, or a manual start signal. Each EDG is equipped with the following support systems: starting air system; fuel oil system; lube oil system; jacket cooling water system; essential 125 vdc control power; and essential 120 vac power for certain auxiliaries and room ventilation.

A third diesel generator, the station blackout diesel generator (SBODG), is provided to supply power to bus D2 in the event of a station blackout. The SBODG can only be synchronized to the grid from the SBODG control panel. The SBODG output breakers on the control room panel can only be used for dead bus transfers. The SBODG auxiliaries are supplied power from bus D3 through a 4160 vac - 480 vac transformer. Separate batteries, independent of the main station batteries, are used in flashing the generator's field.

Each essential 480 vac substation (E1 and F1) is supplied from its corresponding essential 4160 vac bus through redundant transformers, one carrying the load and the other in

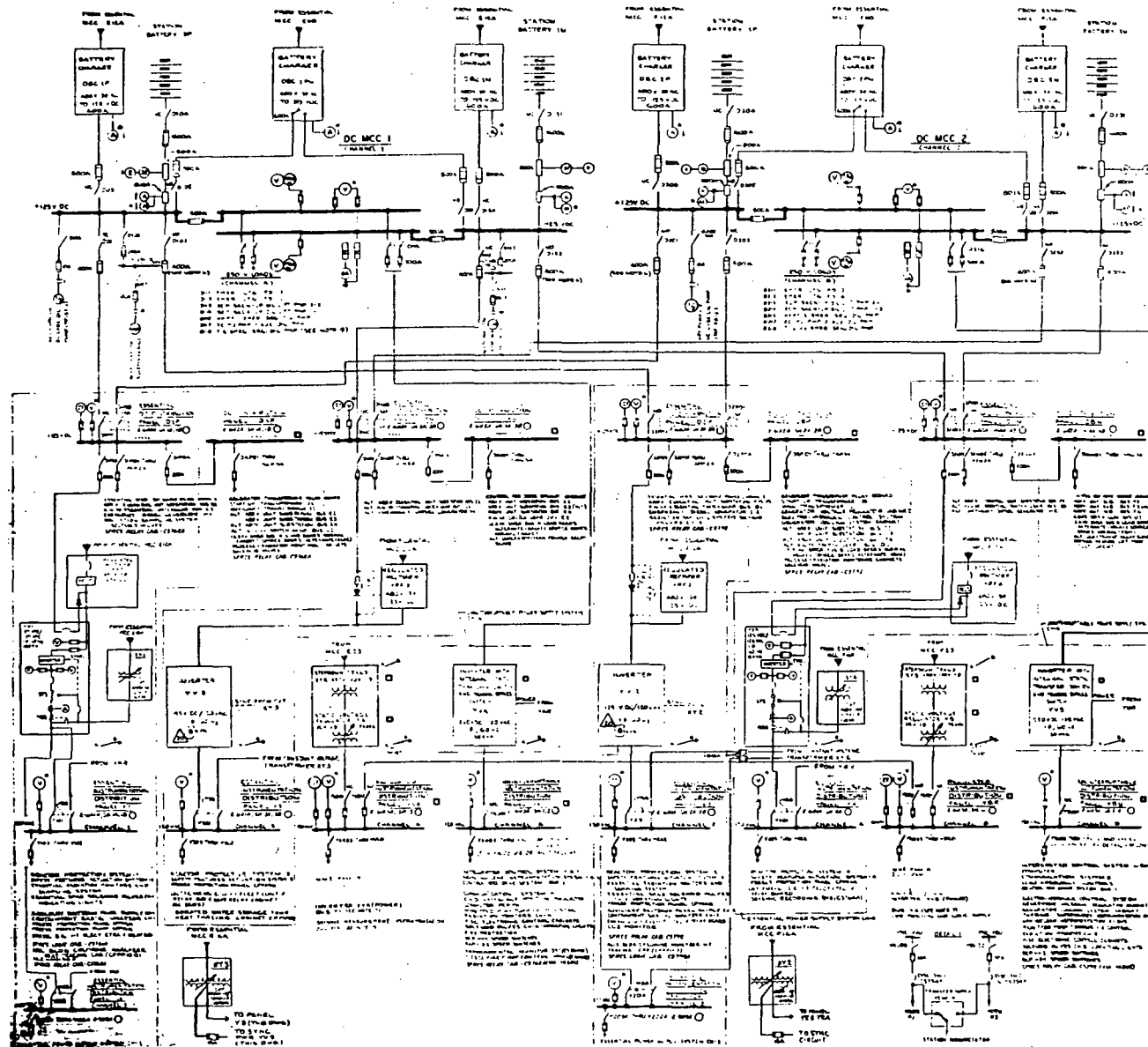
standby (secondary side breaker open). Each non-essential unit substation (E2, E3, F2, F3, EF4, and EF6) is supplied from either bus A or bus B. 480 vac switchgear bus F7 is fed from bus D2. The 480 vac system also consists of two lighting substations (E5 and F5), and four additional distribution centers for outdoor lighting and switchyard supply. The 480 vac system contains approximately 70 motor control centers (MCCs) which are supplied from the unit substations.

The batteries, battery chargers and the 125/250 vdc MCCs are arranged to form two physically separate and independent load groups designated as channels 1 and 2. These channels in turn feed four essential 125 vdc distribution panels designated as channels 1, 2, 3, and 4 (D1P, D1N, D2P, and D2N respectively), and four non-essential 125 vdc distribution panels that are grouped together and designated as channels A and B (DAP and DAN for channel A, and DBP and DBN for channel B). The four essential distribution panels (channels 1-4) supply the following safety related loads: essential SFAS solenoid valves (channels 1-4); RPS (channels 1-4); essential 4160 vac bus control (C1 and D1); essential 480 vac unit substation control (E1 and F1); alternate 120 vac essential inverters (YV1, YV2, YV3 and YV4); and EDG 1-1 and 1-2 normal and alternate control.

Four 125 vdc, 1500 ampere-hour lead-calcium batteries are provided and arranged to form two independent 250/125 vdc MCCs. Each station battery is normally on a "float" charge at approximately 130 vdc from its associated battery charger. The batteries are sized to supply the anticipated dc and instrument ac demand for at least two hours following loss of the battery charger. There are six 125 vdc, 600 amp battery chargers that are arranged into two groups of three. Each group is supplied from one essential 480 vac MCC and constitutes the normal supply for a dc MCC. A battery charger is normally aligned to charge each station battery and provide for steady-state dc loads. Room ventilation is needed to prevent cold temperatures during winter conditions (temperatures less than 40F) from excessively cooling the battery, thereby slowing the chemical reaction and reducing the amp-hour capacity.

There are four 120 vac essential inverters each having its own associated regulated rectifier and distribution panel which together make up an instrumentation channel, designated channels 1, 2, 3, and 4 (Y1/Y1A, Y2/Y2A, Y3, and Y4). Each panel supplies power to one of the four channels in the RPS and SFAS systems. The panels are supplied from essential 480 vac MCCs through regulated rectifiers (YRF1, YRF2, YRF3, and YRF4) and essential inverters (YV1, YV2, YV3, and YV4). A reserve power source to the essential inverters is supplied from the essential dc distribution panels (D1P, D1N, D2P, and D2N). The inverters for channels 1 and 4 are also equipped with a static transfer switch which provides a smooth and nearly continuous transfer to an alternate source in case of inverter failure.

There are two 120 vac uninterruptable distribution panels, YAU (channel A) and YBU (channel B) that supply non-safety related loads such as the integrated control system (ICS) and the electro-hydraulic control (EHC) system. Panel YAU (YBU) is normally powered from the 250 vdc bus of MCC 1 (2) through inverter YVA (YVB). If the dc power supply to the inverter fails or the output of the static inverter fails, the static transfer switch will automatically transfer panel YAU (YBU) to the regulated instrumentation panel YAR (YBR).



REFERENCE DRAWINGS

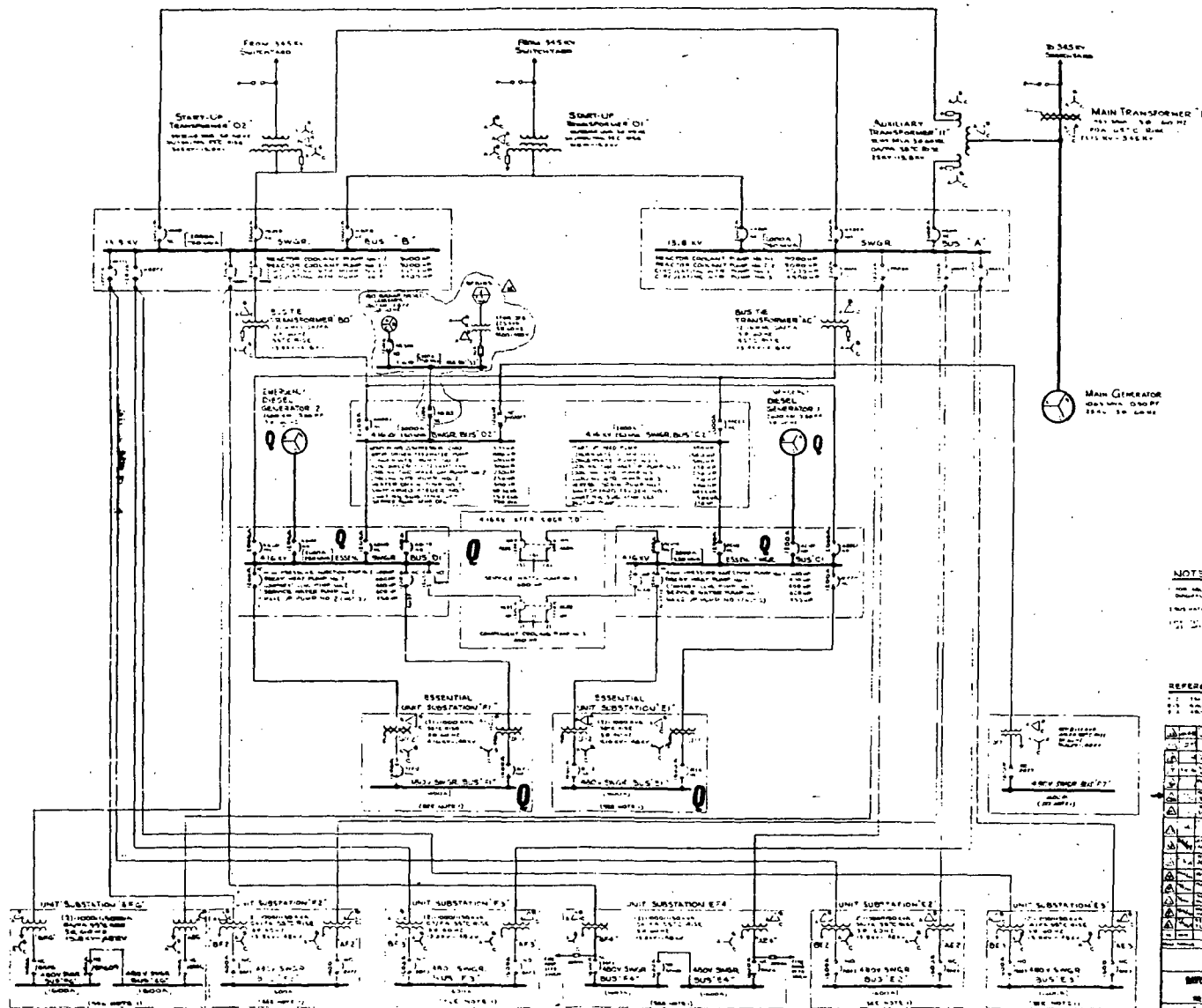
- 1. DRAWING NO. 100-100000-100000-100000
- 2. DRAWING NO. 100-100000-100000-100000
- 3. DRAWING NO. 100-100000-100000-100000
- 4. DRAWING NO. 100-100000-100000-100000
- 5. DRAWING NO. 100-100000-100000-100000
- 6. DRAWING NO. 100-100000-100000-100000
- 7. DRAWING NO. 100-100000-100000-100000
- 8. DRAWING NO. 100-100000-100000-100000
- 9. DRAWING NO. 100-100000-100000-100000
- 10. DRAWING NO. 100-100000-100000-100000
- 11. DRAWING NO. 100-100000-100000-100000
- 12. DRAWING NO. 100-100000-100000-100000
- 13. DRAWING NO. 100-100000-100000-100000
- 14. DRAWING NO. 100-100000-100000-100000
- 15. DRAWING NO. 100-100000-100000-100000
- 16. DRAWING NO. 100-100000-100000-100000
- 17. DRAWING NO. 100-100000-100000-100000
- 18. DRAWING NO. 100-100000-100000-100000
- 19. DRAWING NO. 100-100000-100000-100000
- 20. DRAWING NO. 100-100000-100000-100000

NOTES

- 1. MAIN CONTROL BOARD MOUNTED
- 2. ALL WIRING ON THIS DRAWING IS LISTED IN THE WIRING LIST
- 3. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 4. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 5. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 6. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 7. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 8. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 9. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 10. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 11. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 12. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 13. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 14. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 15. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 16. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 17. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 18. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 19. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST
- 20. ALL WIRING IS TO BE DONE IN ACCORDANCE WITH THE WIRING LIST

NO.	DESCRIPTION	DATE	BY	CHKD.
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Figure 2-30



NOTES

1. THIS DRAWING IS A PART OF THE
DESIGN FOR THE POWER STATION
2. THIS DRAWING IS SUBJECT TO CHANGE
3. THIS DRAWING IS SUBJECT TO APPROVAL BY THE
ENGINEERING DEPARTMENT

REFERENCE DRAWINGS

NO.	DESCRIPTION	DATE
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

RENTAL COMPANY
RENTAL COMPANY
6000-10000 INDUSTRIAL POWER STATION
10000 INDUSTRIAL POWER STATION
10000 INDUSTRIAL POWER STATION
A.C. ELECTRICAL SYSTEM
ONE LINE DIAGRAM
7740 E-1 SH-116

Figure 2-29

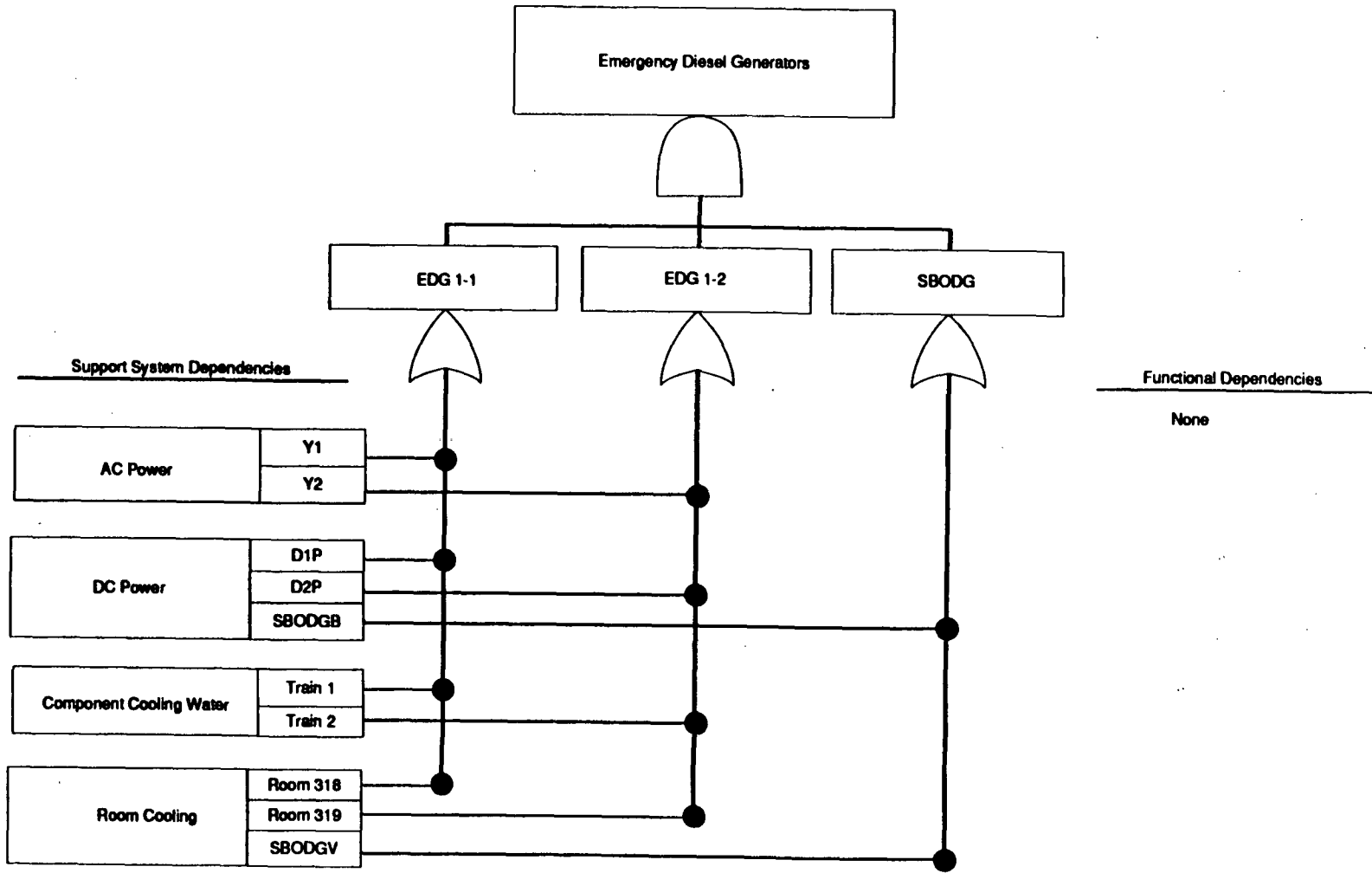


Figure 2-31. Diesel Generator Dependencies

Each of the two 120 vac regulated instrumentation distribution panels YAR and YBR is fed from a non-essential 480 vac MCC through a constant voltage transformer. These panels feed non-safety related instruments and miscellaneous controls. In addition, panel YAR (YBR) provides a manual backup source to either of the safety related instrument panels Y1/Y1A or Y3 (Y2/Y2A or Y4).

The non-nuclear instrumentation (NNI) system measures temperature, pressure, flow, and level in the primary and secondary systems to provide indication and inputs to control systems. The NNI system is made up of eight separate cabinets—cabinets 1-4 being designated X, and cabinets 5-8 being designated Y. Busses YAU and YBU supply 120 vac power to individual field cabinets through an automatic bus transfer (ABT) device. For NNIX (NNIY), the preferred power source is YBU (YAU) and the alternate source is YAU (YBU).

Dependencies

Figure 2-31 outlines the support systems necessary for continued operation of the EDGs and SBODG. Ac and dc control power are required support systems for both EDGs. To prevent overheating, the CCW system supplies cooling water to the EDG cooling jackets. The SBODG is dependent on its own support systems, such as its own room ventilation and dedicated battery for dc control power, which are separate from other plant support systems.

Figure 2-32 shows the support dependencies modeled for dc power, which consists mainly of two sets of AC chargers, three chargers per train, and room ventilation to keep the battery warm during winter conditions.

Role in the Sequence Models

There are numerous top gates within the electric power fault tree which are responsible for supplying electric power to both safety and non-safety related equipment. The system therefore plays a role in virtually every sequence modeled. In particular, the two EDGs directly supply C1 and D1, their own respective safety related buses. Given a loss of offsite power, the SBODG may be required for operation of the MDFP on bus D2, and can supply additional loads if either of the EDGs is unavailable.

2.2.16 Service Water

Service water is a support system designed to supply cooling water to both safety and non-safety related plant systems and equipment. Service water is a redundant safety system and is required for both normal and emergency operations. Service water also provides the ultimate heat sink for decay heat removal from the primary system.

Design and Operation

As shown in Figure 2-33, there are a total of three service water pumps and two independent trains which supply cooling water for various plant loads, such as component cooling water (CCW) and turbine plant cooling water (TPCW). Each service water pump is a

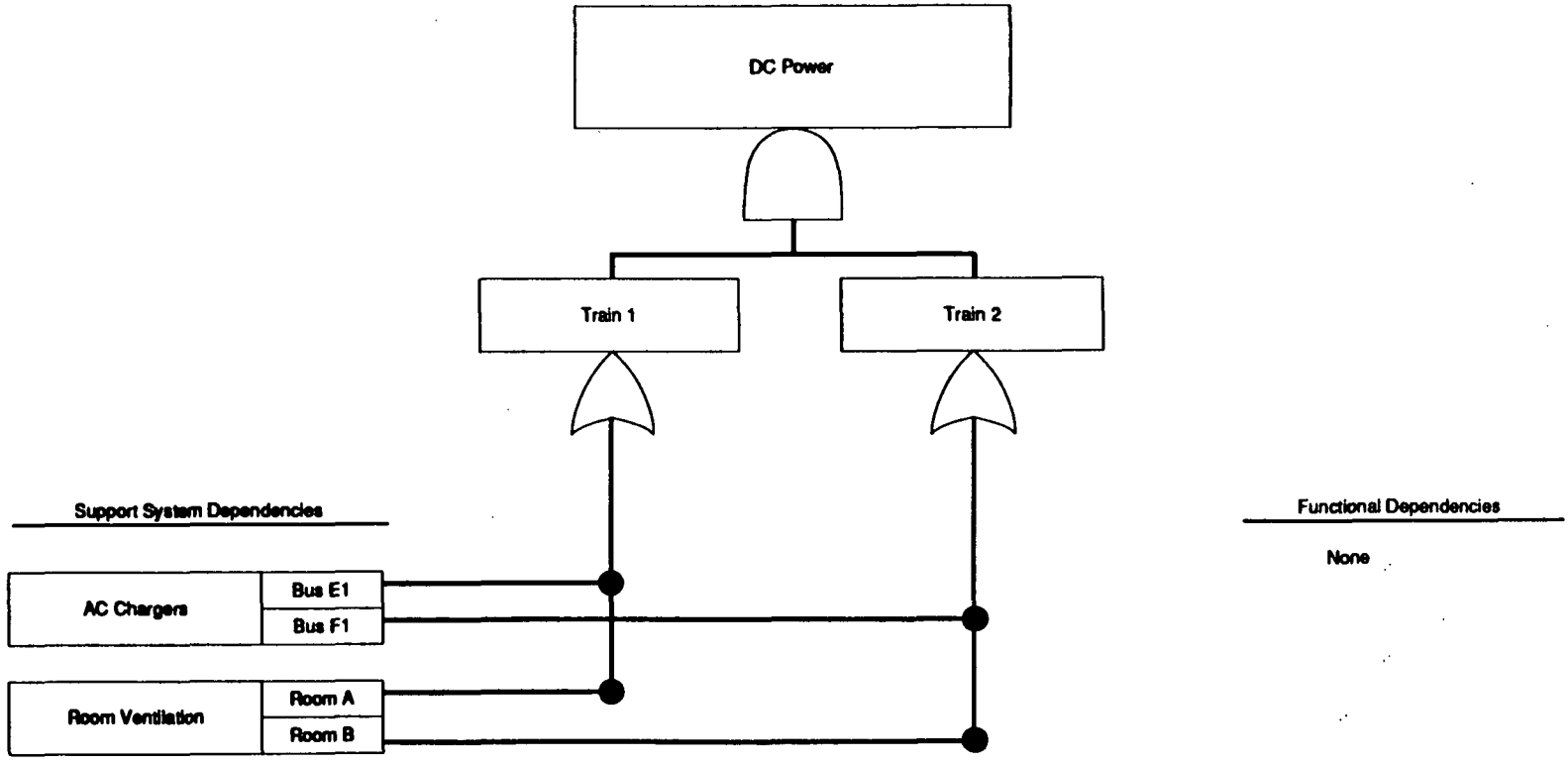


Figure 2-32. DC Power Dependencies

two-stage, solid shaft, vertical turbine, wet pit pump powered by 4160 vac, and rated at 10,250 gpm at 160 feet head. The pumps take their suction from the intake structure. There are normally two pumps operating at all times. Lake water debris is prevented from entering the service water system by a motor-operated strainer at the discharge of each service water pump. These strainers operate when a high service water discharge pressure or high differential pressure across the strainer is detected. The third pump is normally in standby and can be manually aligned to supply flow if needed. There is a fourth pump, the dilution pump, which can also be aligned as a service water pump.

Ventilation is required for the service water pump room and consists of two independent trains, each train consisting of two 50%-capacity fans. The fans are designed to maintain room temperature below 104F. Operation of the fans is normally controlled by automatic temperature switches.

During normal plant operation there are two service water pumps operating, one which supplies the essential or primary loads and the other supplying the nonessential or secondary loads. A third pump is mechanically aligned to serve as a backup to the pump supplying the essential loads.

Following a SFAS level 2 condition, cooling water supplied to nonessential equipment, i.e. TPCW heat loads, will be isolated by automatic closure of valves SW1399 and SW1395. The circulating water system serves as a backup cooling system for these non-essential loads. Isolation of the non-essential loads ensures maximum service water flow and cooling to safety related equipment required during accident conditions. As a result, there are three 100 percent capacity service water pumps that can be made available during emergency operation. In addition, the system is capable of supplying suction to the AFW system when the condensate storage tanks (CSTs) are unavailable.

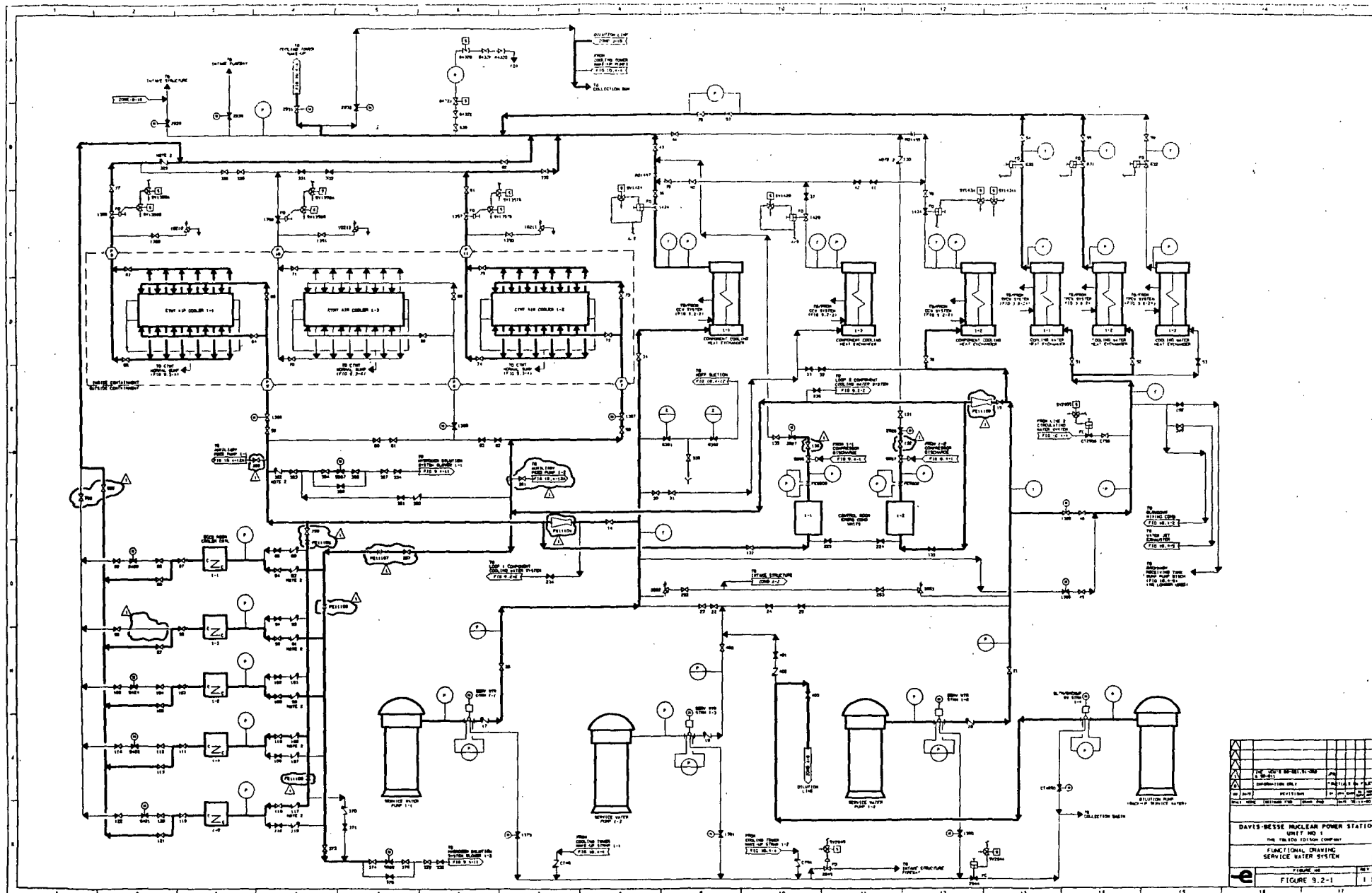
Dependencies

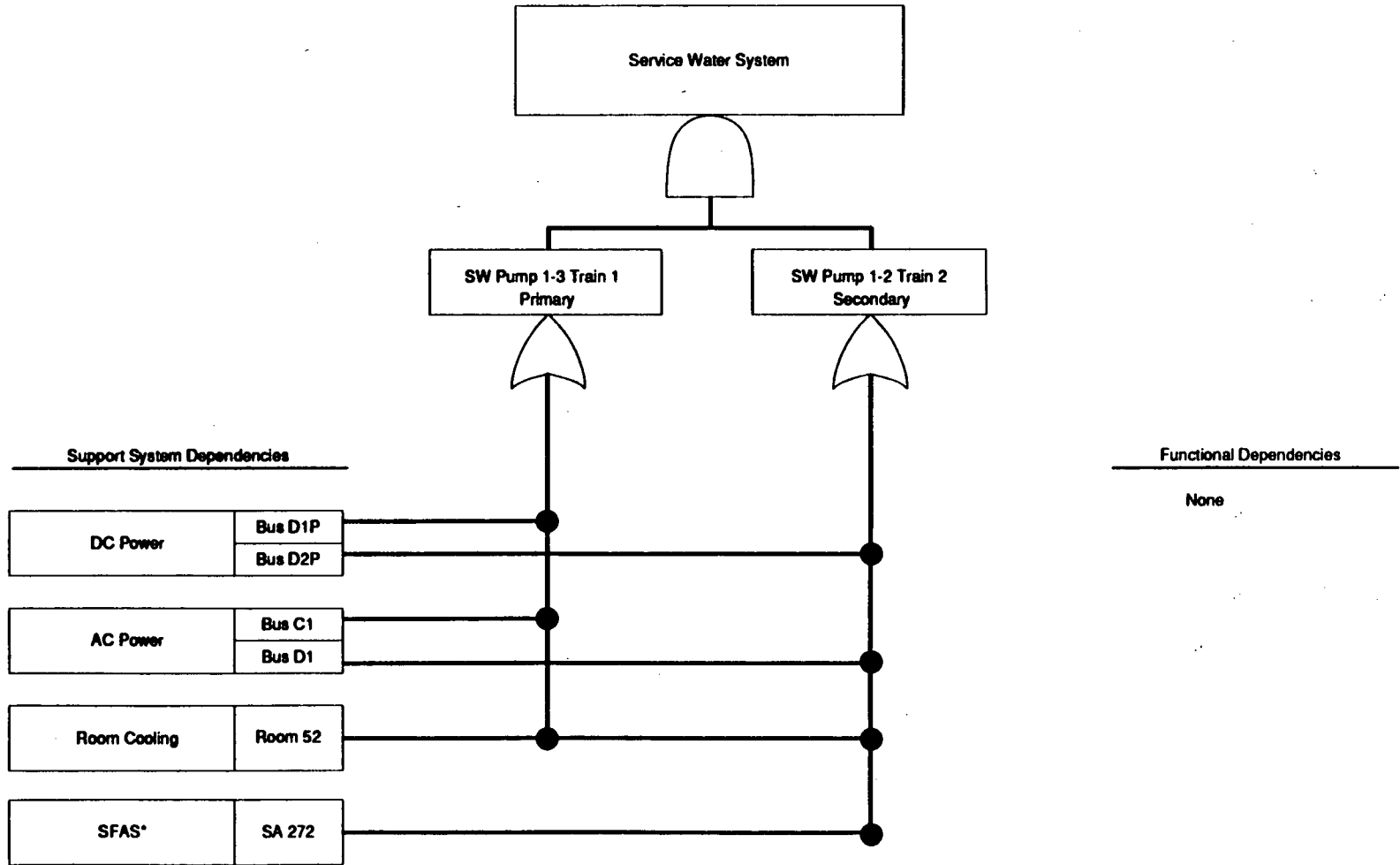
As outlined in Figure 2-34, the service water system requires the function of several auxiliary systems. SFAS actuation signals are necessary for non-essential header isolation to ensure maximum flow to CCW train 2 and therefore cooling of safety related equipment for train 2 during accident conditions. Essential 4160 vac and its associated control power are required for operation of the pumps. Essential 480 vac powers the pump strainers and associated MOVs, room ventilation fans, and the motor-operated valve (SW1395) for SFAS level 2 isolation of TPCW.

Role in the Sequence Models

The service water system fault tree contains many top gates which represent various combinations of component failures that result in an inadequate supply of cooling water to a particular system or component. Cooling water for a number of heat loads is essential for extended operation of front-line safety related equipment.

Service water supplies cooling water to the CCW heat exchangers; flow from CCW is responsible for cooling components in the HPI, DHR, and makeup and purification systems,





* For conditions which necessitate closing valve SW1395.

Figure 2-34. Service Water System Dependencies

as well as the EDGs and RCPs. Service water also directly supplies the ECCS room coolers and CACs. Although a nonessential load, service water indirectly provides cooling for secondary plant components via the TPCW heat exchangers. The system can also serve as an alternate supply of feedwater for the AFW pumps when the normal supply from the CSTs is unavailable.

2.2.17 Component Cooling Water

The component cooling water (CCW) system is designed to supply cooling water to reactor plant auxiliaries and ECCS components during both normal and emergency conditions. As such, the CCW system is considered to be the plant safety related cooling water supply. It also serves as an intermediate barrier between service water and potentially radioactively contaminated systems.

Design and Operation

As shown in Figure 2-35, the CCW system consists of two closed cooling loops, each capable of serving one train of ECCS components and nonessential reactor auxiliary components. Each loop is supplied from one of three 100-percent capacity CCW pumps and its associated heat exchanger. Heat absorbed by the CCW system is transferred to the service water system in the CCW heat exchangers.

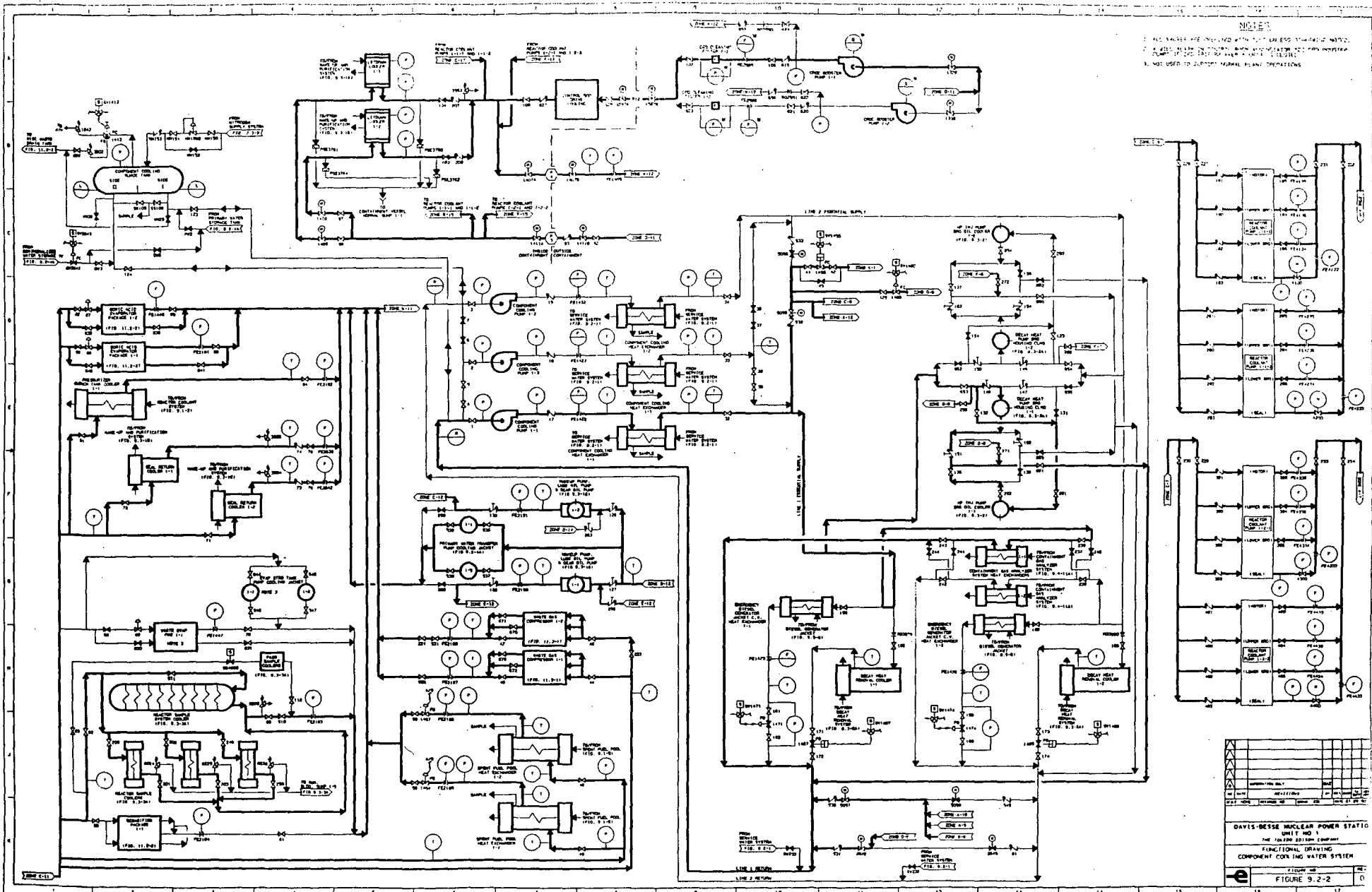
During normal operation, the supply portions of the two essential CCW loops are inactive. One CCW pump and heat exchanger supplies CCW to reactor auxiliaries through three separate nonessential headers. Flow is then returned through a portion of one essential header to the running pump.

The CCW pumps are 400 hp, horizontal centrifugal pumps, rated at 7860 gpm at 150 ft head. Since the CCW system is a closed loop, the pumps take suction from the CCW return line with additional makeup and NPSH provided by a surge tank. There is one pump operating at all times with a second pump in standby which starts upon receipt of an SFAS level 2 signal, startup of its associated emergency diesel generator (EDG), or low flow condition sensed at the discharge of the operating pump. The CCW pumps will trip upon low flow or high CCW temperature conditions provided that a SFAS level 2 condition does not exist.

The CCW surge tank provides the NPSH for the CCW pumps along with providing system inventory control. There is a baffle plate in the middle of the tank to prevent leakage from one CCW train from emptying the entire surge tank and failing both trains. The surge tank provides inventory control by isolating nonessential portions of the CCW system upon actuation of its associated low level switches.

The CCW heat exchangers are a single pass, horizontal shell and tube type, rated for 57 million BTU/hr. Service water flows through the tube side and CCW through the shell side. The CCW outlet temperature is maintained at 95F by a temperature control valve on the service water return from the coolers. Provided no SFAS level 2 signal exists, a CCW

NOTES
 1. ALL VALVES ARE INCLUDED WITH THE END THREADED WELD.
 2. ALL VALVES IN THE LOW PRESSURE SYSTEM ARE FOR PROTECTIVE
 PURPOSES AND ARE NOT TO BE USED FOR OPERATING
 PURPOSES UNLESS OTHERWISE INDICATED.



REVISION	DATE	BY	CHKD

DAVIS-BESSE NUCLEAR POWER STATION
 UNIT NO. 1
 THE YOUNG BROS. COMPANY
 FUNCTIONAL DRAWING
 COMPONENT COOLING WATER SYSTEM
 FIGURE NO. 9-2-2
 SHEET NO. 0

discharge temperature greater than 125F from the heat exchanger will trip its associated pump.

Air-operated isolation valves CC1467 and CC1469 are located in the essential headers downstream from the DHR coolers. These valves are closed during normal power operation, but open on a SFAS level 3 signal to establish CCW flow through the DHR coolers.

Air-operated valves CC1460 and CC1495 provide the direct isolation of the nonessential portions of the CCW system. CC1460 is the nonessential supply isolation valve for the makeup pump gear and lube oil coolers, while CC1495 supplies the auxiliary building nonessential components. These valves both close upon receipt of an SFAS level 3 signal or low surge tank level in order to isolate pipe breaks and to ensure adequate cooling to essential components. Although nonessential flow is isolated to the makeup pumps, CCW cooling is reestablished via the pumps' respective essential supply headers.

During emergency operation, two CCW pumps and heat exchangers are in operation. Each supplies CCW to one train of ECCS equipment through its associated essential header. Flow is returned through separate headers to the CCW pumps. The nonessential headers to the reactor plant auxiliaries are isolated during emergency conditions to ensure maximum flow to the necessary ECCS components.

Dependencies

Figure 2-36 shows the plant systems upon which CCW depends for successful operation. Essential 4160 vac and dc control power are necessary for operation and control of the CCW pumps. Once closed, the CCW pump breakers, like the makeup pump breakers, will remain closed following an interruption of power. CCW system motor-operated valves and room ventilation fans use 480 vac power. Instrumentation and control of the CCW room ventilation system require 120 vac power. SFAS signals are essential in starting the second CCW pump, initiating flow through the DHR coolers, and isolating nonessential CCW loads. Instrument air is required for only the nonessential CCW loads.

Role in the Sequence Models

The CCW system model contains several top gates which represent combinations of component failures that result in a failure of cooling water to various components. CCW supplies cooling water to remove frictional heat generated by the bearings of the makeup, HPI, and DHR pumps. CCW also provides heat removal for continued operation of the EDGs which provide emergency onsite electrical power. Nonessential heat loads include the RCPs for maintaining motor, bearing, and seal integrity, and cooling water for the makeup and purification system letdown coolers. A SFAS level 4 signal actuates isolation of CCW cooling to these nonessential loads.

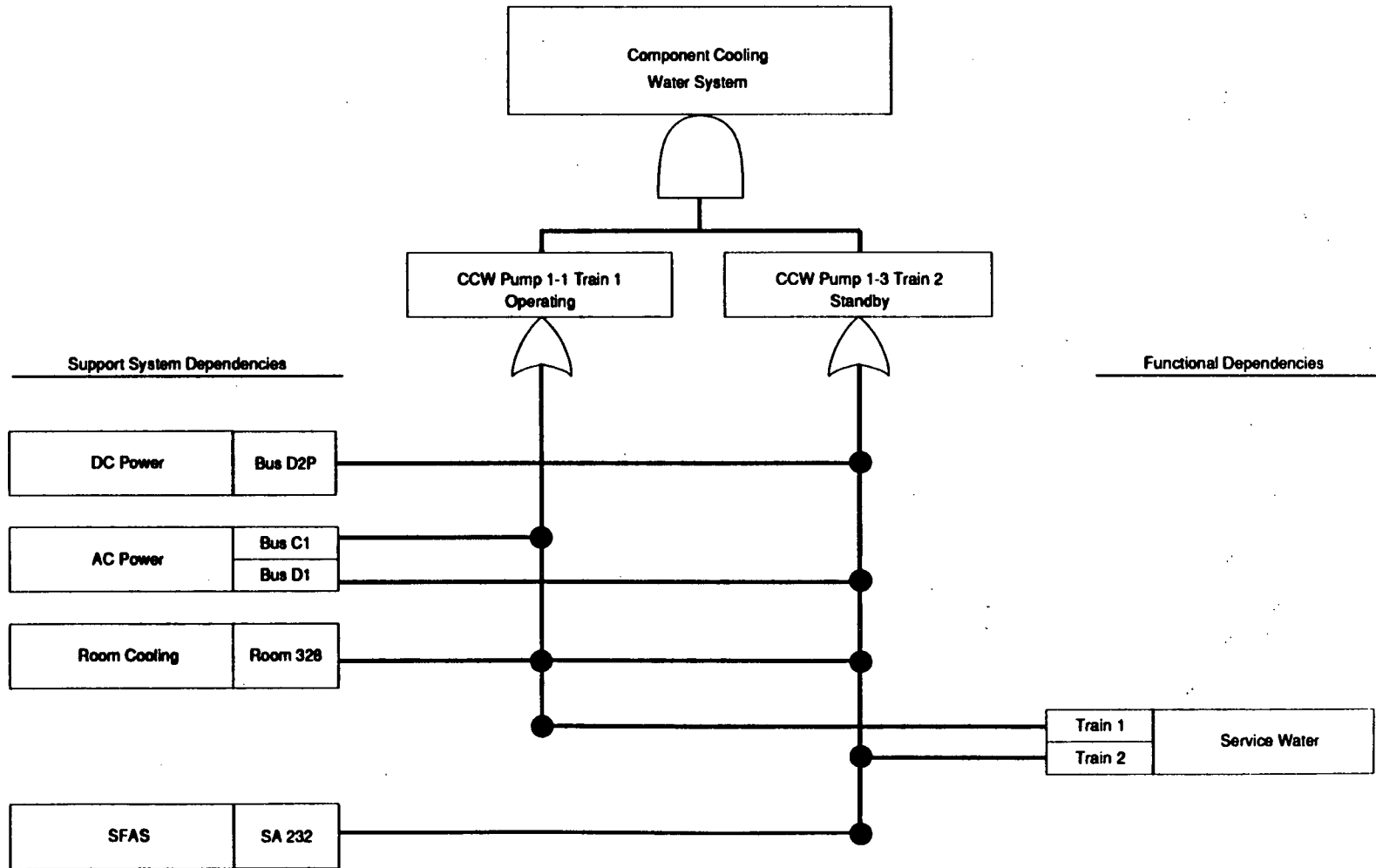


Figure 2-36. Component Cooling Water System Dependencies

2.2.18 Instrument Air

The instrument air (IA) system is a support system designed to provide a continuous supply of 100 psig, oil-free compressed air to air-operated plant components. The IA system provides the force to reposition pneumatically operated valves and pressure for instrument and control signals. Valves operated by IA are required for normal power and shutdown operations.

Design and Operation

A diagram of the IA system is shown in Figure 2-37. The system consists of two station air compressors and an emergency instrument air compressor. Air supplied by these compressors is filtered and dried using pre-filters, dryers, and after-filters. The air is then stored in air receivers which provide a storage volume of clean, dry air for use by air-operated components.

Station air compressor (SAC) 1-1 is a two-stage reciprocating compressor with an intercooler that is cooled by turbine plant cooling water (TPCW). It discharges through a surge tank, aftercooler, and separator before reaching its own receiver.

SAC 1-2 is a three stage, centrifugal compressor equipped with two intercoolers that are also cooled by TPCW. It discharges air through an aftercooler and separator before reaching its air receiver. SAC 1-2 is designed to be continuously run with a modulating bypass system to maintain the compressor fully loaded at the desired pressure. The modulating bypass system senses the compressor discharge pressure and modulates a bypass valve which vents air not required by the system to atmosphere via a muffler. The standby train consists of two pre-filters, an air dryer, and two after-filters. The pre-filter is designed to remove virtually all particulates and liquids and the after-filter is used to remove any desiccant or other fine particles before being sent to the IA header. The air dryer's function is to remove moisture from the air to prevent impingement and erosion of piping surfaces from high speed moisture particles.

During normal plant operation, one of the two SACs (normally SAC 1-2) supplies station and instrument air loads. The other SAC (SAC 1-1) is in standby and automatically starts on low air pressure to provide supplemental air during periods of high demand.

If both SACs are unavailable, the EIAC will start on low EIAC receiver pressure and supply only the instrument air header while the station air header and SAC receivers are automatically isolated.

Dependencies

As outlined in Figure 2-38, the IA system requires the operation of other plant systems in order to successfully perform its function. Nonessential 480 vac for motive power is required for operation of all three compressors. Uninterruptable 120 vac for instrumentation is required for SAC 1-1 and the EIAC. For SAC 1-1, breaker control requires dc power in

starting the compressor. TPCW cooling is required for SACs 1-1 and 1-2, while the EIAC is cooled by its own closed-loop cooling system independent of other support systems.

Role in the Sequence Models

The IA system plays a supporting role in the sequence models as an input to other systems requiring the use of air-operated valves. In particular, IA supplies the two turbine building essential headers which supply air to their respective sets of TBVs. IA also supplies air for operation of the AVVs for each steam generator. The AVVs and TBVs are used for cooling down the RCS in the SGTR sequence events C_I and C_R for the intact and ruptured SGs respectively. For the CCW system, IA maintains valve CC1460 open which serves to supply the normal source of cooling water for the makeup pumps. AOVs for the seal return line from the RCPs and the RCS letdown line are supplied by air from the auxiliary building non-essential header through valve IA605. To maintain heat removal by the TPCW system when service water train 2 is unavailable to the TPCW heat exchangers, circulating water is used as an alternate source of cooling water by operation of an air operated valve (CT2955).

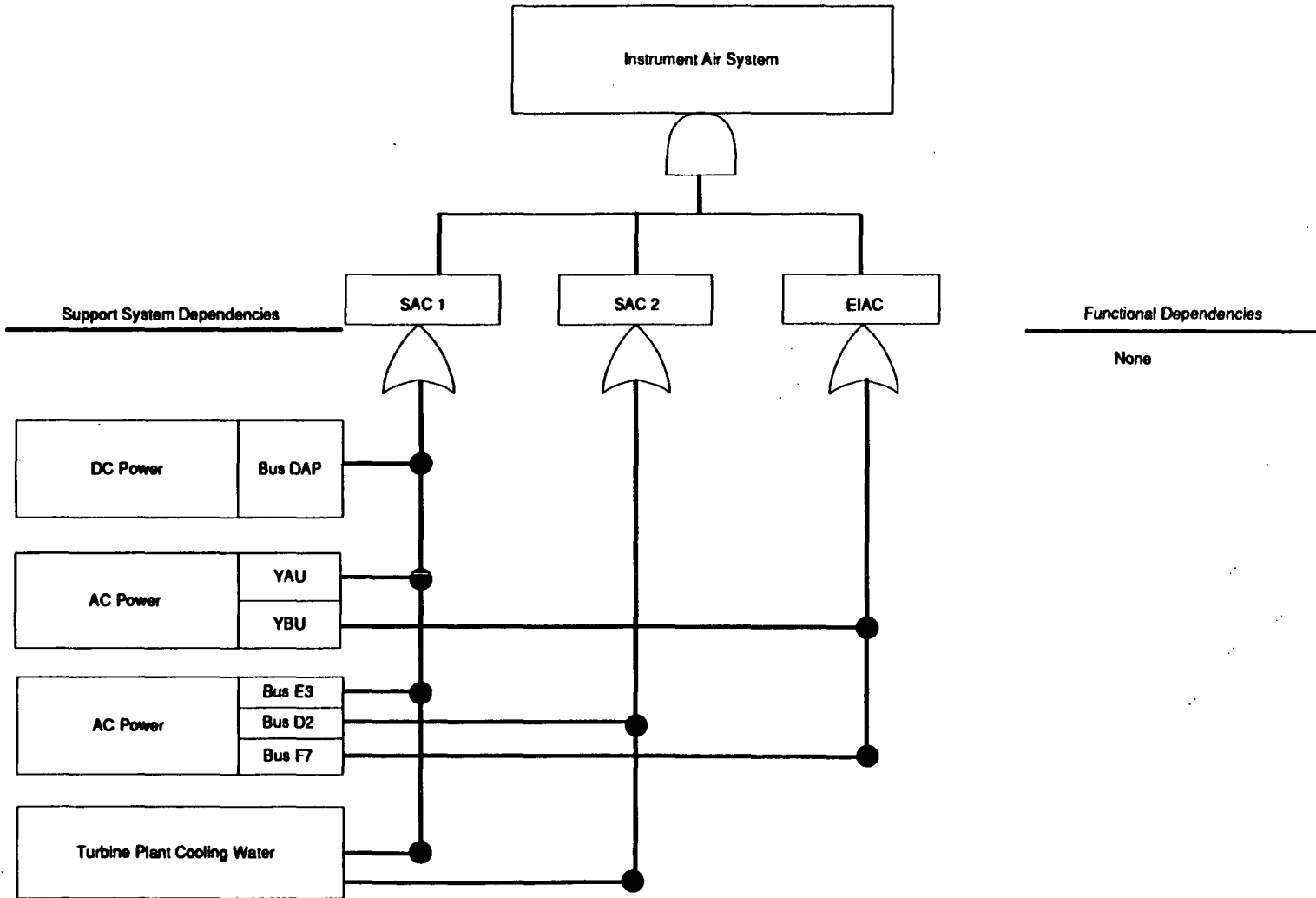


Figure 2-38. Instrument Air System Dependencies

Section 3 SEQUENCE QUANTIFICATION

The sequence quantification entails solving the integrated plant model to identify the combinations of equipment failures that could lead to core damage. This process encompasses the following activities:

- Developing a data base for all initiating event frequencies and component failure rates, including common-cause failures and maintenance unavailabilities;
- Quantifying the different types of human interactions;
- The computer-solution of the integrated model to obtain the cut sets that define the core-damage sequences; and
- Performing the recovery analysis.

The section that follows describes the development of the data base that was used in solving the integrated model. It discusses calculation of the initiating event frequencies, development of the plant-specific and generic data-bases, and the data analysis for the internal flooding evaluation. Subsequent sections describe the human reliability analysis, computer solution of the model, and the recovery analysis.

3.1 DATA ANALYSIS

This section describes the development of the data base used for quantification of the various reliability parameters in the PRA models. It discusses initiating event frequencies, both plant-specific and generic component failure rates, equipment maintenance unavailabilities, and common-cause failure rates.

Davis-Besse began commercial operation in 1977. After little more than one year of operation, the plant was shut down to implement changes required by NUREG-0737 following the Three Mile incident in 1979. Along with the physical changes made to the plant, improvements in plant operating and maintenance practices were implemented. Because of the significance of the changes made and the limited operating experience prior to 1979, the data analysis focused on events occurring following restart from the 1979 outage. In addition, an end date of June 1990 was chosen to support the overall IPE schedule while maintaining as much of the plant operating experience and data as possible. Therefore, the overall data assessment focused on events occurring during the six operating cycles between the July 1979 and June 1990 time period.

3.1.1 Initiating Event Frequencies

A discussion of the initiating events considered in the analysis is included in Section 1 of this report. The purpose of this section is to describe how the initiating event frequencies

were estimated. The following sections discuss calculation of the initiating event frequencies and include information relative to the source of the data used, whether plant-specific or generic. Table 3-1 lists the initiating events and their associated frequencies as they were used in the analysis.

Initiating Events Based on Generic Data

Generic experience was used for calculating initiating event frequencies in cases where plant-specific data was not adequate or available. Generic data was also used to form prior distributions in performing Bayesian updating of the plant-specific data.

The frequencies of all LOCAs were estimated based on generic experience. There have been no LOCAs corresponding to large or medium breaks in the operating history of PWRs. The overall frequency of LOCAs larger than the small category was based on an assessment of no events in 553 reactor-years of operation, using a χ^2 approach as suggested in NUREG/CR-4407 (Ref. 52). This frequency was then split between the two categories, based on the judgment that medium breaks would be on the order of three times as likely as large breaks.

For events such as small LOCAs, steam generator tube ruptures, and feedwater or steamline breaks, generic data was also used. Because these events have occurred within the industry, but not specifically at Davis-Besse, a review of industry events was performed to calculate an appropriate initiating event frequency. Nuclear Power Experience (NPE), a multi-volume subscription service which records operating experience for commercial nuclear power plants, was used in estimating frequencies for these initiators (Ref. 53). Detailed searches were performed for related events and reviewed for applicability to Davis-Besse. Out of the 553 years of plant operating experience, two small break LOCAs, five SGTRs and two feedwater/steamline breaks were identified, and resultant initiating event frequencies were calculated. Copies of the search criteria, descriptions of the actual events considered for these initiators and calculations of the initiating event frequencies are contained in the Davis-Besse project files.

The frequency of a catastrophic rupture of the reactor vessel is expected to be very low, and is not well represented by an assessment of no events in 553 reactor-years of plant operation. Instead, PRAs for other PWRs that estimated the frequency of such an event using a variety of techniques were reviewed. The frequencies suggested by these studies were aggregated in the same manner as that used in developing the generic data for component failure rates, as described in Section 3.1.2.

The loss of offsite power initiating event frequency was calculated by reviewing generic loss of offsite power events and considering specific Davis-Besse experience. Events involving partial or complete losses of offsite power at U.S. nuclear power plants for the period 1975 through 1990 are summarized in NSAC-166 (Ref. 54). Each of these events was examined for applicability to the offsite power distribution system at Davis-Besse. In some cases, the categories to which the events were assigned in NSAC-166 were changed to reflect more directly how they might have affected Davis-Besse. In addition, the events were re-

Table 3-1
Summary of Initiating Event Frequencies

Event	Designator	Mean Annual Frequency	Source
<u>Loss-of-Coolant Accidents</u>			
Large LOCA	A	1.0×10^{-4}	Generic
Medium LOCA	M	3.0×10^{-4}	Generic
Small LOCA	S	3.6×10^{-3}	Generic
Steam generator tube rupture	R	9.0×10^{-3}	Generic
Interfacing-systems LOCA via high pressure injection line	VH	1.8×10^{-6}	PS ¹
Interfacing-systems LOCA via low pressure injection line	VL	2.9×10^{-6}	PS ¹
Interfacing-systems LOCA via failure of isolation in decay heat removal letdown line	VD	3.2×10^{-7}	PS ¹
Interfacing-systems LOCA due to premature opening of decay heat removal letdown line	VS	17×10^{-5}	PS ¹
Reactor vessel rupture	AV	5×10^{-7}	Generic
<u>Transients</u>			
Reactor/turbine trip	T1	6.0	PS ²
Loss of main feedwater	T2	1.7	PS ²
Loss of offsite power	T3	3.5×10^{-2}	PS ³
Spurious safety features actuation	T4	1.3×10^{-2}	Generic
Steam generator 1 unavailable due to break in feedwater or steam line	T5	3.6×10^{-3}	Generic
Loss of makeup to the reactor coolant system	T6	5.8×10^{-2}	PS ¹
Loss of power from bus YAU	T7	0.17	PS ²
Loss of power from bus YBU	T8	0.17	PS ²
Loss of dc power supply for NNI-X	T9	1.8×10^{-2}	PS ²
Loss of primary loop of service water	T10	0.16	PS ¹
Loss of secondary loop of service water	T11	0.16	PS ¹
Total loss of service water	T12	6.5×10^{-4}	PS ¹
Loss of operating train of component cooling water	T13	0.34	PS ¹
Total loss of component cooling water	T14	5.2×10^{-4}	PS ¹

Table 3-1 (continued)
Summary of Initiating Event Frequencies

Event	Designator	Mean Annual Frequency	Source
<u>Transients (continued)</u>			
Loss of power from 4160 vac bus C1	T15	8.6×10^{-3}	PS 1
Loss of power from 4160 vac bus D1	T16	8.6×10^{-3}	PS 1
Loss of dc power from bus D1P	T17	1.1×10^{-2}	PS 1
Loss of dc power from bus D2P	T18	1.1×10^{-2}	PS 1
Loss of instrument air	T19	0.11	PS 3
<u>Internal Floods</u>			
Flood from auxiliary building drainage to ECCS pump room for train 1	FE1	4.1×10^{-3}	PS 2
Flood of ECCS pump rooms due to failure of a line from the BWST	FE2	8.6×10^{-5}	PS 2
Flood of ECCS pump rooms due to drainage from auxiliary building	FE3	1.3×10^{-3}	PS 2
Flood in service water pump room	FS1	7.5×10^{-4}	PS 2
Flood from service water valve room	FS2	3.8×10^{-5}	PS 2
Flood in component cooling water pump and heat exchanger room	FC	3.5×10^{-4}	PS 2

Notes

- 1) Plant specific assessment based on fault-tree model.
- 2) Plant specific data based on operating experience.
- 3) Based on Bayesian updating of generic data with plant-specific evidence.

categorized to be consistent with the modeling requirements for the PRA. First, the events were re-categorized according to whether they were the cause of the plant upsets or the consequence of them. The former were used to estimate the initiating event frequencies (the latter were used in calculating the unavailability of offsite power following a plant trip). The initiating events involving loss of offsite power were further classified as plant-centered, grid-centered or weather-related to permit both proper assessments of their frequencies and appropriate treatment of recovery potential. The detailed assessment of the loss-of-offsite power events along with the calculations performed to support the initiating event frequency (and probability for the loss of offsite power following a plant trip) are contained in the Davis-Besse project files.

The initiating event frequency for the spurious safety features actuation (event T₄) was based on a review of trips that have occurred at Babcock and Wilcox (B&W) PWRs. The B&W Owners Group Plant Performance Committee issued a notebook designed to help track the performance of B&W plants with respect to trip reduction, transient response improvement, and plant performance improvement (Ref. 55). This report describes plant trips that have occurred at B&W plants since 1980. One spurious safety features actuation was identified in over 78 years of commercial operation.

Initiating Events Based on Plant-Specific Data

In cases where sufficient information was available, initiating event frequencies were calculated using plant-specific data. This was the preferred approach and as such it was used in calculating several of the initiating event frequencies. As previously noted, Bayesian updating was performed for a few events because of the limited operating experience at Davis-Besse compared to industry experience.

For initiators such as the reactor/turbine-trip, loss of main feedwater, loss of bus YAU/YBU, and the loss of instrument air, plant-specific data was easily attainable. Plant-specific data was obtained through reviews of various plant records, primarily Transient Assessment Program (TAP) reports and licensee event reports (LERs). In the almost 6 years of operation since 1979, 35 reactor/turbine trips, ten loss of main feedwater events, one loss of bus YAU, and one loss of instrument air have occurred. This data was used in calculating plant-specific initiating event frequencies for these events. Copies of the applicable TAP reports and LERs as they were assessed for the various initiators are contained in the Davis-Besse project files along with calculations of the initiating event frequencies.

An important point to note is the declining number of plant trips following restart from the June 1985 outage. Because the plant has only operated for a few cycles since that time, sufficient data has not yet been collected to warrant deletion of the earlier events. Consequently, all events were retained in calculating initiating event frequencies. If the plant continues with this trend (declining frequency of plant trips), it is expected that the resultant changes in plant-specific initiating event frequencies will improve the overall risk profile for Davis-Besse.

For initiators for which information was not as readily available, fault tree models were developed to calculate plant specific-initiating event frequencies. Fault-tree models were chosen to provide a best estimate of the initiating event frequencies associated with the makeup system, service water system, component cooling water system and the electrical distribution system. Detailed fault-tree models were developed for these initiators, and were then quantified and assessed for potential recovery options. The results were plant-specific initiating event frequencies for the loss of makeup to the reactor coolant system, loss of service water train 1 and 2, loss of all service water, loss of component cooling water train 1, loss of all component cooling water, loss of 4160 v bus D1 and C1 and loss of dc power buses D1P and D2P. Copies of the fault-tree models, data base, and cut sets are contained in the Davis-Besse project files.

Initiating event frequencies associated with the interfacing-systems LOCA analysis were also estimated on a plant-specific basis. Fault-tree models were developed for equipment failures and human interactions that could lead to an interfacing-systems LOCA. Copies of the fault-tree models, data base, and assessments are also included in the Davis-Besse project files.

3.1.2 Generic Data and Analysis

Reliability parameter estimates based on generic data were calculated for all components included in the PRA models. Various generic data sources were reviewed and relevant sources were aggregated into composite estimates for each component type and failure mode. The specific generic data sources used for each component aggregation are identified on the generic data sheets contained in the Davis-Besse project files. Generic data was used in the PRA models for those components for which plant-specific experience was not readily available. The generic data base was also used in Bayesian updating as discussed in Section 3.1.1. Table 3-2 summarizes the generic data base.

3.1.3 Plant-Specific Data and Analysis

In addition to initiating event frequencies, a plant-specific data base was developed for component failure rates and maintenance unavailabilities. Plant-specific component failure rates were calculated for risk significant components, and plant-specific maintenance unavailabilities were calculated for all systems.

Plant-Specific Component Failure Rates

The plant-specific data base was focused on collecting data for the most risk-significant components (e.g., diesel generators; major electrical breakers and busses; batteries and chargers; instrument air components; and pumps). These were chosen because of their importance in previous PRA studies and because of the availability of reliable information that could be extracted from various plant records.

Table 3-2
Summary of Generic Data

Component	Failure Mode	Type Code	Generic Failure Rate	
			Mean	EF
Air-operated valve	Fails to open on demand	AV N	2.2×10^{-3} /dem	2.8
	Fails to close on demand	AV C	2.2×10^{-3} /dem	2.8
	Fails to operate (standby)	AV F	5.9×10^{-6} /dem	14
	Fails to remain open	AV K	2.7×10^{-6} /hr	10
	Internal rupture	AV R	2.7×10^{-6} /hr	10
	External leakage	AV L	1.0×10^{-7} /hr	6.3
Motor-operated valve	Fails to open on demand	MV N	3.5×10^{-3} /dem	2.2
	Fails to close on demand	MV C	3.5×10^{-3} /dem	2.2
	Fails to hold on demand	MV H	2.7×10^{-4} /dem	5.0
	Fails to close while indicating closed	MV X	1.1×10^{-4} /dem	4.2
	Fails to remain open	MV K	3.7×10^{-7} /hr	16
	Internal rupture	MV R	4.3×10^{-8} /hr	2.6
	External leakage	MV L	9.8×10^{-8} /hr	4.2
Solenoid valve	Fails to open on demand	SV N	2.8×10^{-3} /dem	7.5
	Fails to close on demand	SV C	2.8×10^{-3} /dem	7.5
	Fails to remain open	SV K	4.1×10^{-7} /hr	3.0
	Internal rupture	SV R	4.1×10^{-7} /hr	3.0
Manual valve	Fails to open on demand	XV N	2.9×10^{-4} /dem	8.7
	Fails to close on demand	XV C	2.9×10^{-4} /dem	8.7
	Fails to remain open	XV K	8.0×10^{-8} /hr	7.3
	Internal rupture	XV R	4.5×10^{-8} /hr	12
	External leakage	XV L	3.4×10^{-8} /hr	11
Check valve	Fails to open on demand	CV N	1.9×10^{-4} /dem	8.9
	Fails to close on demand	CV C	9.7×10^{-4} /dem	5.2
	Fails to remain open	CV K	4.5×10^{-7} /hr	20
	Internal rupture	CV R	7.6×10^{-8} /hr	6.5
	External leakage	CV L	7.6×10^{-8} /hr	13
Stop-check valve	Fails to open on demand	SC N	1.6×10^{-3} /dem	15
	Fails to close on demand	SC C	1.6×10^{-3} /dem	15
Relief valve	Fails to open on demand	RV N	2.1×10^{-4} /dem	10
	Fails to close on demand	RV C	5.2×10^{-3} /dem	13
	Fails to remain closed	RV R	1.7×10^{-6} /hr	4.2
SG safety relief valve	Fails to open on demand	RX N	3.0×10^{-4} /dem	6.1
	Fails to reseal after steam	RX T	7.5×10^{-3} /dem	4.6

**Table 3-2 (continued)
Summary of Generic Data**

Component	Failure Mode	Type Code	Generic Failure Rate	
			Mean	EF
PZR safety relief valve	Fails to open on demand	RY N	3.0×10^{-4} /dem	6.1
	Fails to reseal after liquid relief	RY Q	1.0×10^{-1} /dem	10
	Fails to reseal after steam relief	RY T	7.5×10^{-3} /dem	4.6
Pilot-operated relief valve	Fails to open on demand	RZ N	6.3×10^{-3} /dem	4.7
	Fails to reseal after liquid relief	RZ Q	1.8×10^{-2} /dem	6.9
	Fails to reseal after steam relief	RZ T	1.8×10^{-2} /dem	6.9
Pressure regulating valve	Fails during operation	PV F	2.7×10^{-6} /hr	3.2
	Fails to remain closed	PV R	1.1×10^{-5} /hr	6.8
Motor-operated damper	Fails to open on demand	MD N	3.5×10^{-3} /dem	6.3
	Fails to close on demand	MD C	3.5×10^{-3} /dem	6.3
	Fails to remain open	MD K	3.0×10^{-7} /hr	10
	Fails to remain closed	MD R	3.0×10^{-7} /hr	10
Backflow damper	Fails to open on demand	MC N	2.2×10^{-3} /dem	2.9
	Fails to close on demand	MC C	2.2×10^{-3} /dem	2.9
	Fails to remain open	MC K	5.1×10^{-6} /hr	9.2
	Fails to remain closed	MC R	5.1×10^{-6} /hr	9.2
Dropout register	Fails to fall	FC F	1.0×10^{-6} /dem	15
Motor-driven pump	Fails to start on demand	MP A	3.1×10^{-3} /dem	3.2
	Fails to run	MP F	2.4×10^{-5} /hr	3.2
	Rupture	MP R	3.2×10^{-8} /hr	5.2
Turbine-driven pump	Fails to start on demand	TP A	2.1×10^{-2} /dem	2.9
	Fails to run	TP F	1.3×10^{-3} /hr	13
Motor-driven strainer	Fails to start on demand	ST A	2.1×10^{-4} /dem	9.0
	Fails to run	ST F	7.9×10^{-6} /hr	5.7
	Plugs during operation	ST P	1.5×10^{-5} /hr	7.6
Motor-driven fan	Fails to start on demand	MF A	3.5×10^{-3} /dem	15
	Fails to run	MF F	9.1×10^{-6} /hr	3.8
Heat exchanger	Tube leak during operation	HX J	2.7×10^{-6} /hr	7.4
	Plugs during operation	HX P	3.4×10^{-6} /hr	8.2
Containment air cooling unit	Fails to start/switch low	CC A	7.4×10^{-3} /dem	5.4
	Fails to run	CC F	2.3×10^{-5} /hr	5.1

Table 3-2 (continued)
Summary of Generic Data

Component	Failure Mode	Type Code	Generic Failure Rate	
			Mean	EF
Room air chiller	Fails to start on demand	AC A	7.7×10^{-3} /dem	4.8
	Fails to continue operating	AC F	4.9×10^{-5} /hr	8.4
Filter	Plugs during operation	FL P	1.2×10^{-5} /hr	6.6
Auxiliary Boiler	Fails to supply steam	BL F	3.6×10^{-4} /hr	4.5
Air compressor	Fails to start on demand	AM A	2.9×10^{-2} /dem	17
	Fails to run	AM F	1.5×10^{-4} /hr	5.1
Air receiver	Fails to supply air	AR F	6.0×10^{-7} /hr	15
Air dryer	Fails during operation	AD F	3.4×10^{-5} /hr	9.2
Air filter	Plugs/fails to deliver flow	AF F	1.8×10^{-6} /hr	9.7
Air header	Fails to maintain pressure	AH F	2.9×10^{-6} /hr	2.2
Diesel generator	Fails to start on demand	DG A	1.8×10^{-2} /dem	5.0
	Fails to run	DG F	2.3×10^{-3} /hr	6.7
Battery	Fails to provide output on demand	BT D	3.2×10^{-3} /dem	23
	Fails to provide output (hourly)	BT F	4.9×10^{-6} /hr	7.1
Battery charger	Fails to maintain output	BC F	1.1×10^{-5} /hr	4.9
Transformer (13.8-4kV)	Fails to maintain power	T1 F	2.1×10^{-6} /hr	6.4
Transformer (480-240V)	Fails to maintain power	T6 F	1.9×10^{-6} /hr	8.8
Electrical bus (13.8kV)	Fails to maintain power	B1 F	5.3×10^{-7} /hr	5.1
Electrical bus (4160V)	Fails to maintain power	B2 F	5.3×10^{-7} /hr	5.1
Electrical bus (480V)	Fails to maintain power	B3 F	3.6×10^{-7} /hr	6.4
Electrical bus (240V)	Fails to maintain power	B5 F	3.2×10^{-7} /hr	7.2
Electrical bus (120V)	Fails to maintain power	B4 F	3.6×10^{-7} /hr	6.4
Electrical bus	Fails to maintain power	BD F	6.1×10^{-7} /hr	5.2
Circuit breaker	Fails to open on demand	CB N	1.2×10^{-3} /dem	4.0
	Fails to close on demand	CB C	1.2×10^{-3} /dem	4.0
	Fails to remain closed	CB R	1.9×10^{-6} /hr	5.7
Circuit breaker	Fails to trip	CD D	8.8×10^{-4} /dem	5.5
Circuit interrupter	Opens spuriously	CI R	6.7×10^{-7} /hr	32

Table 3-2 (continued)
Summary of Generic Data

Component	Failure Mode	Type Code	Generic Failure Rate	
			Mean	EF
Fuse	Fails to remain closed	CF R	6.3×10^{-7} /hr	9.4
Bistable	Fails to trip	BI F	2.2×10^{-5} /dem	42
Contact	Fails to open on demand	CT N	1.8×10^{-4} /dem	34
	Fails to close on demand	CT C	1.8×10^{-4} /dem	22
	Fails to remain open	CT K	7.1×10^{-8} /hr	6.9
	Fails to remain closed	CT R	7.1×10^{-8} /hr	6.9
Relay	Fails to operate on demand	RE D	1.9×10^{-4} /dem	9.0
	Spurious operation to energized state	RE K	8.2×10^{-7} /hr	3.9
	Spurious operation to deenergized state	RE R	2.2×10^{-6} /hr	6.1
E/I converter	Fails to respond	EI D	2.2×10^{-7} /hr	14
E/P converter	Fails to respond	EP D	1.0×10^{-7} /hr	6.8
Inverter	No output	IN F	2.9×10^{-5} /hr	1.1
Regulating rectifier	No output	IR F	1.1×10^{-6} /hr	2.6
Static voltage regulator	No output	IV F	7.1×10^{-6} /hr	2.9
Power supply	No output	PX F	1.4×10^{-6} /hr	1.5
Logic card	Fails during operation	LC F	1.8×10^{-6} /hr	7.3
Logic module	Fails to trip	LM F	1.7×10^{-4} /dem	14
Flow element	Fails high	FE H	3.5×10^{-7} /hr	2.1
	Fails low	FE L	3.0×10^{-7} /hr	2.1
Radiation element	Fails to respond (hourly)	RA D	2.2×10^{-6} /hr	3.0
Signal processor module	Fails to respond	LY D	6.4×10^{-7} /hr	3.3
Temp indicating controller	Fails to respond	TV D	2.1×10^{-6} /hr	2.2
	Fails high	TV H	1.4×10^{-6} /hr	2.2
	Fails low	TV L	1.4×10^{-6} /hr	2.2
Hand switch	Fails to open on demand	SW N	1.7×10^{-5} /dem	15
	Fails to close on demand	SW C	1.7×10^{-5} /dem	15
	Fails to remain open	SW K	8.0×10^{-8} /hr	13
Valve position switch	Fails to close on demand	SZ C	2.5×10^{-4} /dem	5.1
	Fails to remain open	SZ K	4.4×10^{-6} /hr	3.9
	Fails to remain closed	SZ R	4.4×10^{-6} /hr	3.9

Table 3-2 (continued)
Summary of Generic Data

Component	Failure Mode	Type Code	Generic Failure Rate	
			Mean	EF
Static transfer switch	Fails to transfer	IS D	4.9×10^{-3} /dem	31
Speed switch	Fails to open on demand	SX N	2.5×10^{-4} /dem	6.4
Flow switch	Fails to respond	FS D	1.2×10^{-6} /hr	2.0
	Spurious operation	FS L	1.4×10^{-6} /hr	2.7
	Fails to remain closed	SW R	8.0×10^{-8} /hr	13
Level switch	Fails to respond	LS D	1.6×10^{-3} /dem	4.3
	Fails high	LS H	2.3×10^{-6} /hr	8.0
	Fails low	LS L	2.3×10^{-6} /hr	8.0
Pressure switch	Fails to respond	PS D	2.6×10^{-4} /dem	8.1
	Fails to respond (standby)	PS F	3.5×10^{-7} /hr	6.8
	Fails high	PS H	8.5×10^{-7} /hr	4.6
	Fails low	PS L	8.5×10^{-7} /hr	4.6
Temperature switch	Fails to respond	TS D	1.7×10^{-4} /dem	5.6
	Fails high	TS H	3.8×10^{-6} /hr	6.7
	Fails low	TS L	3.8×10^{-6} /hr	6.7
Flow transmitter	Fails to respond	FT D	1.8×10^{-6} /hr	3.6
	Fails high	FT H	2.0×10^{-6} /hr	2.9
	Fails low	FT L	1.8×10^{-6} /hr	3.6
Level transmitter	Fails to respond (hourly)	LT D	2.1×10^{-6} /hr	3.5
	Fails high	LT H	2.0×10^{-6} /hr	3.9
	Fails low	LT L	2.1×10^{-6} /hr	3.7
Pressure transmitter	Fails to respond	PT D	4.9×10^{-7} /hr	5.6
	Fails high	PT H	1.5×10^{-6} /hr	3.3
	Fails low	PT L	1.5×10^{-6} /hr	3.3
Temperature transmitter	Fails to respond	TT D	1.5×10^{-6} /hr	4.4
	Fails high	TT H	1.8×10^{-6} /hr	3.2
	Fails low	TT L	1.8×10^{-6} /hr	3.2
Containment sump	plugged	SM P	2.2×10^{-5} /hr	15
Tank	Rupture	TK G	7.5×10^{-7} /hr	6.3
	Leak	TK J	7.5×10^{-7} /hr	6.3
Piping (D≤6")	Leak or rupture	P1 J	4.7×10^{-9} /hr	5.6
Piping (D>6")	Leak or rupture	P2 J	9.8×10^{-10} /hr	11

The method used in developing the plant-specific data base applies the principles of Bayesian analysis to combine generic data with plant-specific data. This approach was used to supplement the limited amount of data available from Davis-Besse plant records with the significant amount of industry experience. Table 3-3 is a listing of the plant-specific data by component type and failure mode as used in the IPE.

A significant amount of time was expended in collecting, classifying, and analyzing plant-specific data. A computerized listing of all maintenance work orders (MWOs) associated with each risk-significant component was generated. It should be noted that data was collected for all like components; in the case of 4160 v breakers, for example, data was collected for all 4160 v breakers and not only those specifically included in the PRA models. The MWO listings were reviewed for events which indicated potential component failures. For potential failure events, an actual copy of the MWO was obtained. The MWOs were reviewed in detail and retained for further classification only if they involved an actual component failure. In addition to MWO reviews, TAP reports and LERs were also reviewed for component failures. Component failures identified in a TAP report or LER were retained and categorized along with the MWOs. All failure records were finally categorized according to component type and failure mode. The results were the number of failures associated with each component categorized by failure mode. Actual copies of the failure records are contained in the Davis-Besse project files.

Once the failure events were assembled, estimates of equipment exposures (i.e., demands or hours) were made based on a detailed understanding of how each system was operated, maintained, and tested. Exposure was estimated by first considering the function of the component and the conditions under which it would be operating, accounting for maintenance activities and surveillance tests performed on every component in the system. This information, along with the assistance of a licensed operator, allowed for calculations of the equipment exposure rates.

The number of component failures and associated exposure rates were then aggregated to form the basis of the plant-specific data base. This aggregation was done using the Computerized Analysis of Reliability Parameters (CARP) computer code (Ref. 56). Finally, Bayesian analysis was performed using the generic data to form prior distributions, updated with the plant-specific evidence. Copies of the plant-specific data sheets and the Bayesian updating sheets are contained in the plant-specific data files.

Because plant-specific valve data had been collected during previous PRA work at Davis-Besse, this data was used for calculating plant-specific failure rates for valves. It should be noted, however that the valve experience only included the 1979 through June, 1985 time period. Since 1985, substantial changes have been made in the testing and maintenance practices associated with valves. Consequently, if the data were collected for the period beyond 1985, failure rates associated with valves would be expected to improve.

**Table 3-3
Summary of Plant-Specific Data**

Component	Failure Mode	Type Code	Generic Failure Rate		Plant-Specific Evidence		Updated Failure Rate	
			Mean	EF	Failures	Experience	Mean	EF
Air-operated valve	Fails to open on demand	AV N	2.2×10^{-3}	2.8	21	4,280 dem	4.4×10^{-3}	1.4
	Fails to close on demand	AV C	2.2×10^{-3}	2.8	21	4,280 dem	4.4×10^{-3}	1.4
	Fails to remain open	AV K	2.7×10^{-6}	10	0	1.2×10^6 hr	1.3×10^{-7}	10
Motor operated valve	Fails to open on demand	MV N	3.5×10^{-3}	2.2	79	9,800 dem	7.6×10^{-3}	1.2
	Fails to close on demand	MV C	3.5×10^{-3}	2.2	79	9,800 dem	7.6×10^{-3}	1.2
	Fails to remain open	MV K	3.7×10^{-7}	16	3	4.0×10^6 hr	7.3×10^{-7}	2.4
Temperature control valve	Fails to throttle	TC T	2.7×10^{-6}	10	13	3.7×10^5 hr	3.1×10^{-5}	1.6
Check valve	Fails to open on demand	CV N	1.9×10^{-4}	8.9	0	4,130 dem	4.0×10^{-5}	8.9
	Fails to close on demand	CV C	9.7×10^{-4}	5.2	3	4,130 dem	7.6×10^{-4}	2.3
	Fails to remain open	CV K	4.5×10^{-7}	20	0	4.3×10^6 hr	8.4×10^{-9}	20
Stop-check valve	Fails to open on demand	SC N	1.6×10^{-3}	15	2	1,440 dem	1.4×10^{-3}	2.8
	Fails to close on demand	SC C	1.6×10^{-3}	15	3	1,440 dem	2.1×10^{-3}	2.4
	Fails to remain open	SC K	4.5×10^{-7}	20	0	1.9×10^6 hr	1.8×10^{-8}	20
Manual valve	Fails to open on demand	XV N	2.9×10^{-4}	8.7	11	1.0×10^4 dem	1.0×10^{-3}	1.6
	Fails to close on demand	XV C	2.9×10^{-4}	8.7	11	1.0×10^4 dem	1.0×10^{-3}	1.6
	Fails to remain open	XV K	8.0×10^{-8}	7.3	1	1.6×10^7 hr	6.5×10^{-8}	3.5
Pilot-operated relief valve	Fails to open on demand	RZ N	6.3×10^{-3}	4.7	1	175 dem	5.9×10^{-3}	3.1
	Fails to reseal, steam relief	RZ T	1.8×10^{-2}	6.9	2	175 dem	1.2×10^{-2}	2.7
Main steam safety valve	Fails to open on demand	RX N	3.0×10^{-4}	6.1	2	1,870 dem	7.4×10^{-4}	2.6
	Fails to reseal, steam relief	RX T	7.5×10^{-3}	4.6	2	1,870 dem	1.4×10^{-3}	2.5
Atmospheric vent valve	Fails to open on demand	VV N	2.2×10^{-3}	2.8	2	253 dem	3.5×10^{-3}	2.2
	Fails to reseal, steam relief	VV T	2.2×10^{-3}	2.8	5	253 dem	6.1×10^{-3}	1.8

Table 3-3 (continued)
Summary of Plant-Specific Data

Component	Failure Mode	Type Code	Generic Failure Rate		Plant-Specific Evidence		Updated Failure Rate	
			Mean	EF	Failures	Experience	Mean	EF
Main steam isolation valve	Fails to close on demand	IV C	2.2×10^{-3}	2.8	1	159 dem	2.8×10^{-3}	2.4
	Fails to remain open	IV K	2.7×10^{-6}	10	1	1.1×10^5 hr	6.7×10^{-6}	3.7
Turbine bypass valve	Fails to open on demand	BV N	2.2×10^{-3}	2.8	3	727 dem	3.1×10^{-3}	2.0
	Fails to close on demand	BV C	2.2×10^{-3}	2.8	2	727 dem	2.5×10^{-3}	2.2
Reactor coolant pump	Fails to run	MP F	2.4×10^{-5}	3.2	6	2.2×10^5 hr	2.7×10^{-5}	1.8
Makeup pump	Fails to start on demand	MP A	3.1×10^{-3}	3.2	1	288 dem	3.2×10^{-3}	2.6
	Fails to run	MP F	2.4×10^{-5}	3.2	0	5.6×10^4 hr	1.3×10^{-5}	3.2
High pressure injection pump	Fails to start on demand	MP A	3.1×10^{-3}	3.2	2	358 dem	4.1×10^{-3}	2.3
	Fails to run	MP F	2.4×10^{-5}	3.2	0	254 hr	2.4×10^{-5}	3.2
Low pressure injection pump	Fails to start on demand	MP A	3.1×10^{-3}	3.2	3	322 dem	5.6×10^{-3}	2.1
	Fails to run	MP F	2.4×10^{-5}	3.2	1	4.1×10^4 hr	2.5×10^{-5}	2.6
Containment spray pump	Fails to start on demand	MP A	3.1×10^{-3}	3.2	0	240 dem	2.1×10^{-3}	3.2
	Fails to run	MP F	2.4×10^{-5}	3.2	0	182 hr	2.4×10^{-5}	3.2
Service water pump	Fails to start on demand	MP A	3.1×10^{-3}	3.2	4	442 dem	5.9×10^{-3}	2.0
	Fails to run	MP F	2.4×10^{-5}	3.2	2	1.9×10^5 hr	1.4×10^{-5}	2.3
Component cooling water pump	Fails to start on demand	MP A	3.1×10^{-3}	3.2	6	595 dem	6.9×10^{-3}	1.8
	Fails to run	MP F	2.4×10^{-5}	3.2	1	1.4×10^5 hr	1.3×10^{-5}	2.6
Motor driven feedwater pump	Fails to start on demand	MP A	3.1×10^{-3}	3.2	2	72 dem	6.2×10^{-3}	2.3
	Fails to run	MP F	2.4×10^{-5}	3.2	0	597 hr	2.4×10^{-5}	3.2
Motor-driven strainer	Fails to start	ST A	2.1×10^{-4}	9.0	0	52 dem	2.0×10^{-4}	9.0
	Fails to run	ST F	7.9×10^{-6}	5.7	1	1.5×10^5 hr	7.2×10^{-6}	3.3

Table 3-3 (continued)
Summary of Plant-Specific Data

Component	Failure Mode	Type Code	Generic Failure Rate		Plant-Specific Evidence		Updated Failure Rate	
			Mean	EF	Failures	Experience	Mean	EF
Air dryer	Fails during operation	AD F	3.4×10^{-5}	9.2	4	9.6×10^4 hr	4.3×10^{-5}	2.1
Air filter	Plugs/fails to deliver flow	AF F	1.8×10^{-6}	9.7	0	1.9×10^5 hr	6.1×10^{-7}	9.7
Air compressor	Fails to start on demand	AM A	3.5×10^{-4}	17	11	2.1×10^5 dem	5.3×10^{-5}	1.6
	Fails to run	AM F	1.5×10^{-4}	5.1	25	1.1×10^5 hr	2.2×10^{-4}	1.4
Air receiver	Local faults	AR F	6.0×10^{-7}	15	0	2.9×10^5 hr	1.8×10^{-7}	15
Containment air cooling unit	Fails to start/switch low	CC A	7.4×10^{-3}	5.4	1	441 dem	3.0×10^{-3}	3.2
	Fails to run	CC F	2.3×10^{-5}	5.1	0	4.8×10^4 hr	8.0×10^{-6}	5.1
Diesel generator	Fails to start on demand	DG A	1.8×10^{-2}	5.0	6	423 dem	1.4×10^{-2}	1.9
	Fails to run	DG F	2.3×10^{-3}	6.7	7	957 hr	6.6×10^{-3}	1.8
Electrical bus (13.8kV)	Fails to maintain power	B1 F	5.3×10^{-7}	5.1	0	1.9×10^5 hr	4.6×10^{-7}	5.1
Electrical bus (4160V)	Fails to maintain power	B2 F	5.3×10^{-7}	5.1	1	4.8×10^5 hr	9.9×10^{-7}	3.1
Electrical bus (480V)	Fails to maintain power	B3 F	3.6×10^{-7}	6.4	8	9.0×10^6 hr	8.3×10^{-7}	1.7
Battery	Fails to provide output	BT F	4.9×10^{-6}	7.1	0	3.9×10^5 hr	7.1×10^{-7}	7.1
Battery charger	Fails to maintain output	BC F	1.1×10^{-5}	4.9	12	5.8×10^5 hr	2.0×10^{-5}	1.6
Circuit breaker (13.8kV)	Fails to open on demand	C1 N	1.2×10^{-3}	4.0	10	1,300 dem	5.2×10^{-3}	1.6
	Fails to close on demand	C1 C	1.2×10^{-3}	4.0	10	1,300 dem	5.2×10^{-3}	1.6
	Fails to remain closed	C1 R	1.9×10^{-6}	5.7	4	9.6×10^5 hr	3.7×10^{-6}	2.1
Circuit breaker (4160V)	Fails to open on demand	C2 N	1.2×10^{-3}	4.0	0	200 dem	9.4×10^{-4}	4.0
	Fails to close on demand	C2 C	1.2×10^{-3}	4.0	0	200 dem	9.4×10^{-4}	4.0
	Fails to remain closed	C2 R	1.9×10^{-6}	5.7	4	1.4×10^6 hr	2.8×10^{-6}	2.1
Circuit breaker (CD swtchgr)	Fails to open on demand	CD N	1.2×10^{-3}	4.0	5	690 dem	3.9×10^{-3}	1.9
	Fails to close on demand	CD C	1.2×10^{-3}	4.0	5	690 dem	3.9×10^{-3}	1.9

It should also be noted that generic data was used for failures associated with turbine-driven AFW pumps because of the limited operating experience since the numerous modifications made to the AFW system during the June 1985 outage. A substantial amount of the failure data that had been collected prior to June 1985 for the turbine-driven AFW pumps was determined no longer to apply to the current operation and configuration of the AFW system.

Maintenance Unavailabilities

In addition to component failure rates, plant-specific data was also collected for system unavailabilities due to maintenance. Because of changes made in the operating and maintenance practices following the June 1985 outage for all equipment at Davis-Besse, maintenance unavailabilities were based on plant experience for the operating cycles following this outage (cycles 5 and 6). Maintenance data was collected on all systems included in the PRA model. Table 3-4 summarizes the maintenance blocks and provides the calculated estimates of their unavailabilities.

For systems such as DHR where two trains are normally in standby, data was collected for both trains, and identical maintenance blocks were modeled for both. In systems such as service water, however, where two pumps are normally running and a third is in standby available to be lined up as either the primary or secondary pump, maintenance blocks were modeled differently. In this example, data was collected for all three service water pumps. Because two of the pumps are normally operating, and one is in standby, however, all of the maintenance unavailability was assigned to the standby pump.

In calculating the maintenance unavailability for a system, all components in one train were typically included in one maintenance block. For systems such as DHR, however, where different portions of the train are used for different functions and more importantly where portions of the train are used by other systems such as HPI, maintenance unavailabilities were calculated for segments of a train. As an example, suction for recirculation from the containment emergency sump is through valves DH9A and 9B. Failures associated with valves DH9A and 9B would prevent recirculation for not only the DHR pumps but the HPI and containment spray pumps as well. Consequently, a separate maintenance unavailability was calculated for the segment of the DHR train associated with the common recirculation function.

Two methods were employed for calculating maintenance unavailabilities. For systems specifically governed by plant Technical Specifications (a majority of the systems modeled in the PRA), out-of-service equipment is logged in the operator's daily log. To calculate maintenance unavailabilities for these systems, operator logs for cycles 5 and 6 were examined for associated component/system out-of-service entries. Results of this review provided the total number of hours each system was unavailable. The total out-of-service time due to maintenance was then divided by the number of hours that the system was required to be operable during cycles 5 and 6, and adjusted for the number of trains in the system. The results were the plant-specific maintenance unavailabilities for these systems.

Table 3-4
Summary of Maintenance Unavailabilities

Component/System/Train	Maintenance Unavailability
Battery room vent fan A/B	1.1×10^{-3}
Emergency diesel generator 1-1/1-2	5.0×10^{-3}
Station blackout diesel generator	5.0×10^{-3}
Emergency diesel generator room vent fan 1-1/1-2	2.3×10^{-3}
Station blackout diesel generator vent fan	2.3×10^{-3}
Low voltage switchgear room vent fan 428/429	5.6×10^{-3}
Station air compressor 1-1/EIAC	5.2×10^{-2}
Alternate instrument air header	5.6×10^{-2}
High pressure injection train 1/2	6.7×10^{-3}
Low pressure injection train DH1A/DH1B	6.2×10^{-4}
Low pressure injection train DH63/DH64	4.0×10^{-4}
Low pressure injection train DH9A/DH9B	7.5×10^{-5}
Low pressure injection pump 1/2	6.8×10^{-3}
Containment spray	5.8×10^{-3}
ECCS room cooler 1-1/1-2/1-4/1-5	2.3×10^{-3}
Makeup pump 1-1	2.0×10^{-3}
Makeup pump room vent fan	2.2×10^{-3}
Auxiliary feedwater train 1/2	8.0×10^{-3}
Motor driven feedwater pump	8.9×10^{-3}
Standby service water pump	5.2×10^{-2}
Dilution pump	5.3×10^{-2}
Service water pump room vent fans 1/2/3/4	8.6×10^{-4}
Standby component cooling water pump 1-2	6.2×10^{-3}
Component cooling water room vent fan 1/2	8.9×10^{-3}

For the few systems that were not specifically governed by plant Technical Specifications, a different approach had to be employed. For systems like instrument air, a review of the operations tag-out log was performed to calculate a maintenance unavailability. Operational tags are placed on equipment when it is removed from service and logged in the tag-out log. This process proved to be a reliable (although somewhat more tedious) way to estimate maintenance unavailabilities for these systems. The tag-out logs provided the total number of hours components in the system were unavailable due to maintenance activities. The unavailability was then divided by the number of hours that system was required to be operable during cycles 5 and 6, and adjusted for the number of trains in a system. The results were the plant specific maintenance unavailabilities for remaining components/systems.

In the case of the newly installed station blackout diesel generator, plant-specific data was not available. This piece of equipment was recently installed and very limited, if any, operating experience is available. Because it is of similar design and function to the existing emergency diesel generators, and because the proposed maintenance and testing are also similar, maintenance data calculated for the emergency diesel generators was used for the station blackout diesel.

3.1.4 Common-Cause Failure Data

The common-cause data evaluation was based on the procedural guidance outlined in NUREG/CR-4780 (Ref. 57) and the data base of events collected by EPRI (Ref. 58). This data base documents commercial U.S. light water power reactor experience with redundant components that have experienced one or more common-cause events. These industry events were used because multiple equipment failures are rare and none were identified during the plant-specific data analysis.

Each industry event was reviewed for applicability to the components and systems at Davis-Besse. Since the event reports lacked detail, careful consideration of the root causes, coupling mechanisms, and operating conditions were considered. When events did not correspond to similar configurations or conditions at Davis-Besse, or for events that were already explicitly modeled, the events were not directly factored into the calculation on common-cause failure rates, with documentation of the rationale for their exclusion (in accordance with the procedure in NUREG/CR-4780).

The results of this review led to the identification of applicable single and multiple failures necessary to estimate the parameters of the common-cause probability models. The Multiple Greek Letter model was used to calculate the common-cause parameters, accounting for the fact that a common-cause event can fail any number of components within a group. These factors were multiplied by the individual component failure rates to calculate common-cause failure rates for components.

The results of this evaluation are summarized in Table 3-5, which identifies all common-cause events considered in the analysis and the factors used in calculating common-

**Table 3-5
Summary of Common-Cause Data**

Component	Size of CCF Group	Failure Mode	CCF Parameter	Common-Cause Multiplier	Source Note	
Motor-operated valves	2 valves	Fail to open/close on demand	$\beta=0.029$	2 of 2	0.029	1
	2 valves	Fail to throttle	$\beta=0.029$	2 of 2	0.029	1
	4 valves	Fail to open/close on demand	$\beta=0.49$	2 of 4	0.0081	1
			$\gamma=0.50$	3 of 4	0.0042	1
			$\delta=0.49$	4 of 4	0.012	1
Solenoid valves	2 valves	Fail to open/close on demand	$\beta=0.029$	2 of 2	0.029	1
Check valves	2 valves	Fail to open on demand	$\beta=0.042$	2 of 2	0.042	1
	2 valves	Fail to close on demand	$\beta=0.24$	2 of 2	0.24	1
Atmospheric vent valves	2 valves	Fail to open on demand	$\beta=0.10$	2 of 2	0.10	2
Turbine bypass valves	6 valves	Fail to open/close on demand	$\beta=0.10$	2 of 6	0.050	2
			$\gamma=0.50$	3 of 6	0.050	2
			$\delta=0.90$	4-6 of 6	0.045	2
Pressurizer safety valves	2 valves	Fail to open on demand	$\beta=0.05$	2 of 2	0.05	2
Reactor coolant pumps	4 pumps	Fail to run	$\beta=0.10$	4 of 4	0.10	3
Makeup pumps	2 pumps	Fail to start on demand	$\beta=0.033$	2 of 2	0.033	1
	2 pumps	Fail to run	$\beta=0.020$	2 of 2	0.020	1
High pressure injection pumps	2 pumps	Fail to start on demand	$\beta=0.060$	2 of 2	0.060	1
	2 pumps	Fail to run	$\beta=0.020$	2 of 2	0.020	1
Low pressure injection pumps	2 pumps	Fail to start on demand	$\beta=0.10$	2 of 2	0.10	1
	2 pumps	Fail to run	$\beta=0.013$	2 of 2	0.013	1

Table 3-5 (continued)
Summary of Common-Cause Data

Component	Size of CCF Group	Failure Mode	CCF Parameter	Common-Cause Multiplier	Source Note	
Containment spray pumps	2 pumps	Fail to start on demand	$\beta=0.19$	2 of 2	0.19	1
	2 pumps	Fail to run	$\beta=0.050$	2 of 2	0.050	2
Auxiliary feedwater pumps	2 pumps	Fail to start on demand	$\beta=0.057$	2 of 2	0.057	1
	2 pumps	Fail to run	$\beta=0.018$	2 of 2	0.018	1
TPCW pumps	2 pumps	Fail to run	$\beta=0.050$	2 of 2	0.050	2
Component cooling pumps	2 pumps	Fail to start on demand	$\beta=0.10$	2 of 2	0.10	2
	2 pumps	Fail to run	$\beta=0.050$	2 of 2	0.050	1
	3 pumps	Fail to start on demand	$\beta=0.10$	2 of 3	0.050	2
			$\gamma=0.50$	3 of 3	0.050	2
3 pumps	Fail to run	$\beta=0.050$	2 of 3	0.013	2	
		$\gamma=0.50$	3 of 3	0.025	2	
Service water pumps	2 pumps	Fail to start on demand	$\beta=0.099$	2 of 2	0.099	1
	2 pumps	Fail to run	$\beta=0.021$	2 of 2	0.021	1
	3 pumps	Fail to start on demand	$\beta=0.084$	2 of 3	0.017	1
			$\gamma=0.60$	3 of 3	0.051	1
3 pumps	Fail to run	$\beta=0.084$	2 of 3	0.034	1	
		$\gamma=0.19$	3 of 3	0.016	1	
Service-water strainers	2 strainers	Fail to run	$\beta=0.050$	2 of 2	0.050	2
Containment air coolers	2 coolers	Fail to start on demand	$\beta=0.62$	2 of 2	0.62	1
	2 coolers	Fail to run	$\beta=0.15$	2 of 2	0.15	1

Table 3-5 (continued)
Summary of Common-Cause Data

Component	Size of CCF Group	Failure Mode	CCF Parameter	Common-Cause Multiplier	Source Note	
Room cooling unit	2 units	Fail to start on demand	$\beta=0.062$	2 of 2	0.062	1
	4 units	Fail to start on demand	$\beta=0.20$	2 of 4	0.055	1
			$\gamma=0.17$	3 of 4	0.0055	1
			$\delta=0.50$	4 of 4	0.017	1
	2 units	Fail to run	$\beta=0.22$	2 of 2	0.22	1
	4 units	Fail to run	$\beta=0.38$	2 of 4	0.050	1
$\gamma=0.62$			3 of 4	0.017	1	
$\delta=0.79$			4 of 4	0.19	1	
Air compressors	2 compressors	Fail to start on demand	$\beta=0.10$	2 of 2	0.010	2
	3 compressors	Fail to run	$\beta=0.10$	2 of 3	0.050	2
			$\gamma=0.50$	3 of 3	0.050	2
Diesel generators	3 diesels	Fail to start on demand	$\beta=0.0056$	2 of 3	0.0024	1
			$\gamma=0.14$	3 of 3	0.00078	1
	3 diesels	Fail to run	$\beta=0.021$	2 of 3	0.0044	1
			$\gamma=0.57$	3 of 3	0.012	1
Batteries	4 batteries	No output	$\beta=0.042$	2 of 4	0.96	4
			$\gamma=0.043$	3 of 4	0.012	4
			$\delta=1.0$	4 of 4	0.018	4
Battery chargers	4 chargers	No output	$\beta=0.050$	2 of 4	0.013	2
			$\gamma=0.50$	3 of 4	0.025	2
			$\delta=0.90$	4 of 4	0.023	2
13.8kV breakers	2 breakers	Fail to open/close on demand	$\beta=0.11$	2 of 2	0.11	1
4160V breakers	2 breakers	Fail to open/close on demand	$\beta=0.10$	2 of 2	0.10	1

**Table 3-5 (continued)
Summary of Common-Cause Data**

Component	Size of CCF Group	Failure Mode	CCF Parameter	Common-Cause Multiplier	Source Note	
SFAS logic modules	4 modules	Fail to respond	$\beta=0.38$	2 of 4	0.062	5
			$\gamma=0.51$	3 of 4	0.049	5
			$\delta=0.24$	4 of 4	0.046	5
SFAS pressure bistables	4 bistables	Fail to respond	$\beta=0.10$	2 of 4	0.050	2
			$\gamma=0.50$	3 of 4	0.050	2
			$\delta=0.90$	4 of 4	0.045	2
SFAS transmitters	4 transmitters	Fail to respond	$\beta=0.22$	2 of 4	0.050	5
			$\gamma=0.32$	3 of 4	0.019	5
			$\delta=0.20$	4 of 4	0.014	5
SFRCS actuation channels	4 channels	Fail to respond	$\beta=0.33$	2 of 4	0.057	5
			$\gamma=0.48$	3 of 4	0.040	5
			$\delta=0.24$	4 of 4	0.038	5

Notes

- 1) Based on assessment of EPRI data, as discussed.
- 2) Based on generic assessment.
- 3) Based on a simplified beta-factor approach due to the potentially large number of shared common causes of failure for all four pumps.
- 4) Based on data for advanced light water reactors.
- 5) Based on NUREG/CR-3289.

cause failure probabilities. Assessments of the industry events as they applied to Davis-Besse equipment along with the parameter calculations can be found in the project files.

3.1.5 Data Assessment of Frequencies for Internal Floods

The flood study is described fully in a separate report (Ref 30). The purpose of this section is to summarize those calculations. The analysis of the potential for core damage initiated by flooding within plant buildings included a number of screening steps to narrow the focus to areas which had both the potential for flooding and the potential for affecting important plant equipment. Through this screening process six initiating events were determined to require detailed analysis. The initiating events are identified in Table 3-1.

The initiating event frequencies were estimated through development of simple models describing the individual events that could lead to the flood. These simple models included failures of components such as pipe or valve ruptures, and floods induced by human error, such as errors resulting in loss of flow isolation during maintenance. The models also identified particular floods that could occur due to a combination of equipment failures and operations staff errors. Once the failure modes were identified, they were quantified using the component data listed in Section 3.1 and the human reliability methodology described in Section 3.2. In addition, generic industry data regarding flood events was also reviewed. A flood event data base was developed for this task, and this data is provided in Appendix A of the flood hazard study (Ref. 30). The industry data was particularly useful for estimating the overall frequency of maintenance-related floods.

There was one special type of failure rate developed expressly for the flood study. For the flood study it was necessary to consider the timing of flood water accumulation which required an understanding of flow rates associated with component failures. It was therefore necessary to further refine the data for pipe and component ruptures from the data base. Three categories were defined to cover the spectrum of flow rates that might be associated with a loss of integrity: maximum, large, and small. Because data is limited in this regard, it was necessary to quantify these categories of severity through expert elicitation. The result of the elicitation was that 5% of the frequency was assigned to the maximum category, representing essentially complete loss of integrity. The large category was assigned 35% of the frequency. The small category represented a significant circumferential crack, and was assigned 60% of the frequency. The values are very similar to severity factors used in several other studies of plant flooding. These values were used throughout the flood study for the consideration of the severities of equipment failures.

3.2 ASSESSMENT OF HUMAN INTERACTIONS

The assessment of human reliability is one of the most important tasks in a comprehensive PRA. Operating experience has repeatedly demonstrated that human interactions can have a strong influence on the potential for an accident to occur or for one to be avoided. This influence has been reflected in the results of virtually every PRA that has

been performed as well. The importance of this area in PRA is heightened because there are no universally accepted procedures for identifying risk-relevant human events or for quantifying their probabilities of occurrence.

The overall approach taken in the assessment of human interactions in this study is consistent with the SHARP1 framework developed by EPRI (Ref. 59). The SHARP1 framework emphasizes making the human reliability assessment an integral part of the process of developing and quantifying the models that define accident sequences and system failures. It suggests organizing the human reliability assessment into four stages:

- (1) Plant logic model development: including in the development of the event and fault trees the appropriate human actions and, in particular, reflecting explicitly dependencies of systems and equipment on human interactions.
- (2) Quantification: estimating the probabilities of the events included in the logic models.
- (3) Analysis of recovery actions: consideration of actions that could be taken to restore a lost safety function by making repairs or by implementing alternative system configurations during an upset event.
- (4) Internal review: ensuring that the way in which the human interactions are incorporated into the models and quantified is appropriate through review by a multi-disciplinary team.

Section 3.2.1 describes the approaches taken to incorporating the consideration of human interactions into the logic models that define the core-damage sequences. Section 3.2.2 outlines the methods used to quantify the probabilities of different types of human interactions, including the interactions that are part of recovery events. The overall treatment and application of recovery events is described further in Section 3.3. Review of the treatment of human interactions is described in Section 3.2.3.

3.2.1 Integration of Human Interactions Into Plant Models

The consideration of human interactions was an integral element in the process of developing the plant logic models (comprised of the event trees and their supporting logic and the system fault trees). These interactions fall into three general categories (again, consistent with the SHARP1 framework):

- Type A interactions, which take place prior to an initiating event, and which usually leave a component or system in an undesired state that does not manifest itself until an initiating event occurs.
- Type B interactions, which are human actions that contribute to the occurrence of an initiating event.
- Type C interactions, which describe the response of the operating staff to an initiating event or other upset event. Interactions of type C are further categorized as type CP (procedure-driven actions) and type CR (recovery actions not generally governed by procedures).

Efforts during the modeling process were primarily directed at identifying interactions of types A and C. As is usually the case in PRAs, the initiating events for this study were identified and their frequencies estimated without attempting to pinpoint specific causes for the events. Type B interactions are therefore implicitly included in the initiating events, but they are not considered in detail.

One type of post-initiator interaction that requires special consideration is comprised of errors of commission. This refers to cases in which the operators have made a misdiagnosis of the situation, such that they take intentional (but erroneous) actions that exacerbate the accident. At the present time there are no well-developed methods for systematically identifying such actions or for quantifying their probabilities of occurrence. It is generally considered by human reliability analysts that the present use of symptom-based procedures significantly reduces the opportunities for these errors of commission. Throughout the modeling process, the analysts for this study maintained an awareness of the potential for such actions, but none that appeared to merit detailed consideration was identified. A different type of commission error was included in the assessment of both type A and type C interactions. These are execution errors (such as selecting the wrong valve for operation or closing the wrong breaker), rather than cognitive in nature.

Model Integration for Pre-Initiator (Type A) Interactions

Because the nature of type A interactions is to leave equipment unavailable or in a degraded state, events corresponding to this type of interaction were incorporated directly into the system fault trees. The number of credible type A human interactions is much too large to permit detailed modeling of each of them. The modeling effort was therefore actually accomplished in two stages.

In the first stage, each train or other major portion of a system that would be in standby prior to an initiating event was assigned a general pre-initiator human action. For example, a general event was defined to encompass all pre-initiator interactions that could leave one train of the LPI system unavailable. Where a human action could leave multiple trains of a standby system unavailable, a general common-cause event was also identified. An example of such a type A interaction would be the potential to leave both trains of LPI unavailable due to failure to isolate both return lines used for periodic flow testing of the pumps after the tests were completed. A screening value was assigned to each of these general human actions. The screening values permitted those pre-initiator actions that could be important with respect to the frequencies of core-damage sequences to be highlighted during the quantification process. Interactions that were not important to any of the core-damage sequences based on use of the screening values were not modeled or quantified further.

Those interactions that surfaced as potentially important during the sequence quantification process were then evaluated in more detail in the second stage. This entailed breaking down the general events into the specific interactions that could leave portions of the system unavailable. This was done through the following steps:

- (1) All procedures that referred to each relevant component in the portion of the system encompassed by the general human action were identified. Because all components are cross-indexed according to the Davis-Besse procedures that refer to them in a computerized data base (Ref. 60), searching for these procedures was a relatively straightforward process.
- (2) A preliminary review was made to characterize the nature of the references to the components in these procedures. These references were typically to the following types of activities:
 - Change of position (in preparation for and/or following maintenance or testing, or for a different operating configuration);
 - Calibration or testing;
 - Preventive or corrective maintenance; and
 - Monitoring or checking (e.g., verification that a valve was in the correct position).
- (3) The references were organized to define the specific opportunities to leave equipment unavailable, along with the other interactions that could be possible. For example, one opportunity might be the failure to restore the the LPI pump train to operability following major pump maintenance. All of the relevant information would be assembled, including procedures that directed mechanical and electrical isolation of the pump, restoration of the pump train, post-maintenance testing, scheduled periodic walkdowns, etc.

The assembly in the final step provided the specific context for the general human action identified at the outset, including the potential to detect and correct errors prior to the initiating events. These specific contexts served as the basis for the quantification of the type A interactions, as described in Section 3.2.2. By evaluating in more detail each of these opportunities, the important general pre-initiator events were assessed, and the screening values were replaced by the resulting refined probabilities.

Model Integration for Post-Initiator (Type CP) Human Interactions

Consideration of those post-initiator human interactions that are directed by procedures, referred to here as type CP, was a more complex undertaking. Integration of type CP interactions into the modeling process was, however, potentially more important to accurate treatment of the core-damage sequences than was the case for pre-initiator actions.

To delineate system response to particular types of upset events, it can be as important to understand the intended response of the operating crew in using the system as it is to understand the design of the system itself. Thus, in defining the sequence delineation for particular initiating events, it was necessary to review carefully the operating procedures, including the emergency procedure (Ref. 31) and the various abnormal procedures. This review was aimed at identifying any operator-driven considerations that would affect the modeling process, such as the priorities that might come into play when multiple options were available for maintaining core cooling, or the cues that might indicate the need to change operating modes. These procedure reviews were augmented by obtaining input from

operators. This was done by having current and former operators review the sequence logic and system fault trees; through extensive discussions with operators regarding specific scenarios; and, to the extent possible, observing simulator exercises.

At the same time, operator actions whose failures could lead to failures of the safety functions required to maintain core cooling were identified in this process. These interactions typically were of one of the following kinds:

- The failure to change the mode of a system under the appropriate conditions (such as accomplishing the switchover of the safety injection systems to draw suction from the containment sump when the BWST inventory is depleted); or
- The failure to initiate the function of a system that normally requires manual actuation (such as starting the motor-driven feed pump) or to align a backup system.

Type CP interactions in the logic models were included at the highest level consistent with their effects. For example, the failure to initiate makeup/HPI cooling following a total loss of feedwater is included in the supporting logic for the corresponding events in the event trees, rather than being broken down into individual faults associated with each piece of equipment in the system fault trees. This treatment helps to highlight the events, and focuses consideration on cognitive aspects of the response to upset conditions. The methods used to quantify type CP events are described in Section 3.2.2.

Modeling for Non-Proceduralized (Type CR) Human Interactions

Type CR interactions represent the failure to take action to compensate for one or more system failures by means that are not necessarily covered explicitly by procedures. The potential for type CR interactions arises when there is time to make a diagnosis and decide on a course of action, but the actions themselves are not guided explicitly by procedures. In these cases, it is the knowledge base of the operators and, often, of additional support staff such as those in the technical support center (TSC), that is important. Because of these fundamental differences, different approaches are taken in assessing type CP and type CR events. Interactions of type CR were not included directly in the logic models; instead, they were appended to the sequence cut sets as appropriate on a case-by-case basis during the sequence quantification process.

The process of identifying type CR events that should be considered involved a careful review of the minimal cut sets dominating each core-damage sequence. Each of these cut sets was examined first to ensure that the specific context of the scenario it implied was well understood by the analysts. This was especially important for cut sets that included failures of support systems (such as electric power or cooling water). Support system faults could cause both the unavailability of the equipment modeled in the sequence and system logic and, potentially, other equipment that might not have been modeled explicitly, but might be needed to effect a particular recovery option. After developing the appropriate understanding of the context for a cut set, possible measures to use the equipment remaining were considered.

This entailed first an examination of the operating procedures for any general guidance that might apply in such a circumstance, followed by discussions with plant operators to determine the course of action they expected would be most likely to be pursued. Once these options were identified, they were examined more closely to determine whether or not they were feasible, given the time available for decision-making and execution and the impact of other failures in the cut set on the potential for the action to succeed. The potential that a successful recovery or unsuccessful attempt could introduce other sequences of events was also considered. Once these factors were identified, a probability for failure of the recovery action was estimated, as described in Section 3.2.2.

It should be emphasized that relatively few events of type CR were included in the quantification of the core-damage frequencies. Nearly all potentially-important opportunities for recovery are covered well by the emergency or other operating procedures and are hence evaluated as type CP interactions. Only in cases for which there were clear opportunities for success, and especially for those when the time available was relatively long, were type CR interactions considered in detail.

Naming Convention for Human Interactions

As described in Section 2, a naming convention was used to identify uniquely each primary event in the study. All primary event names are made up of eight characters. The use of these characters for the human interactions is summarized below:

First character	Letter designating one of the following: <ul style="list-style-type: none"> • The system to which the interaction applies • The event from the event tree for which the interaction appears in the supporting logic • The letter "Z", for events that do not appear explicitly in the logic, but are appended to the sequence cut sets during the quantification process
Second & third characters	"HA" to denote that the event refers to a human action
Fourth through seventh characters	Defined by the analyst to describe the event itself
Eighth character	"L" for pre-initiator events "E" for post-initiator type CP events "R" for post-initiator type CR events

3.2.2 Quantification of Human Interactions

Methods for quantifying human interactions continue to evolve. The methods that were selected for use in this study are among those that represent the state of the art in actual applications in PRA.

Quantification of Type A Interactions

The overall process for evaluating pre-initiator (type A) human interactions consisted of the following steps:

- (1) As described in Section 3.2.1, general pre-initiator interactions were identified for each standby train of all of the systems modeled in the study.
- (2) Screening values were assigned to these general interactions. A screening value of 0.01 was applied to all interactions that implied failure of a single train, and a screening value of 0.001 was used for common-cause human interactions. A survey of other human reliability analyses suggested the use of screening values ranging from 0.003 to 0.03 for single human interactions. A value of 0.01 was considered to be adequately bounding, and a factor of ten reduction for common-cause interactions is appropriate.
- (3) Based on the use of these screening values, potentially important pre-initiator human interactions were highlighted during the sequence quantification process. All interactions that appeared in cut sets that contributed to the frequency of a sequence (based on their screening values) were considered to be potentially important.
- (4) These potentially important pre-initiators interactions were modeled in terms of the specific types of failures that could come into play, as outlined in Section 3.2.1.
- (5) The failures comprising the more detailed breakdown of the general human interactions were evaluated qualitatively and quantitatively, as described in this section.

Nearly every PRA has used some form of the Technique for Human Error Rate Prediction (THERP, Ref. 61) to assess pre-initiator human interactions, and it is one of the approaches suggested by EPRI (Ref. 59). In this study, a simplified form of THERP developed for the Accident Sequence Evaluation Program (ASEP, Ref. 62) was used. Several plant visits were made to obtain information and to make a determination with respect to the conduct of operations as it might affect the reliability of human interactions. The plant has in recent years experienced a complete revision to all procedures, and they appear generally to be clear and well formulated. It was concluded that the nominal estimates of human error probabilities were appropriate without modification.

Once each pre-initiator human interaction was further defined in terms of the specific failures of interest, the conditions that would affect their probabilities of occurrence were identified. These conditions include the following (Ref. 62, Table 5-2):

- (1) Whether status of the unavailable component would be indicated by a compelling signal in the control room.
- (2) Whether component status would be positively verified by a post-maintenance or post-calibration test.
- (3) Whether there would be a requirement for an independent verification of the status of the component after test or maintenance activities.

- (4) Whether there would be a check of the component status each shift or each day, using a written checklist.

The ASEP methodology provided quantitative estimates corresponding to appropriate combinations of these conditions. Before applying these estimates, however, a second qualitative screening was performed, consistent with the ASEP methodology. This qualitative screening applied the following guidelines:

- It was assumed that failures that would leave equipment in an unavailable state that would be clearly annunciated in the control room would be readily detected and corrected, and
- Failures to reposition valves that would be repositioned by an automatic signal were neglected.

The ASEP methodology does not provide explicit treatment for a case corresponding to the locked-valve procedure at Davis-Besse (Ref. 63). Many of the valves at Davis-Besse that are required to remain in a particular position at all times other than for certain test and maintenance activities are locked to prevent inadvertent realignment. These valves are carefully controlled by a separate procedure, in which the permission of the shift supervisor must first be obtained before their position can be changed, and in which locked valves that are out of their normal positions are tracked through use of a log. The log is reviewed at shift turnover. Signoff by the operator and independent verification, as well as specific signoff by the shift supervisor, are required when the valves are repositioned.

The positions of these valves are also verified prior to plant startup and on a monthly basis (Ref. 64). These verifications entail a positive check of the valve status (i.e., the person performing the verification attempts to move the valve and notes its position), and an independent verification by a separate operator.

The level of control and verification goes beyond that represented by the independent verification as described in the ASEP methodology, but would seem to fall short of the level of verification that would be afforded by a positive test. The recovery factors suggested by the ASEP methodology for these two levels of verification are 0.1 and 0.01, respectively. For locked valves, an intermediate value of 0.03 was therefore applied as a recovery factor for restoration errors. Given that the verification in accordance with the controlling procedure was not successful, the followup (e.g., monthly) verifications were considered as possible means of discovery. Failure to identify a particular mispositioned locked valve was assessed to have a probability of 0.1.

In the ASEP methodology, the factors affecting the likelihood of an unrecovered pre-initiator error are combined to form nine cases. These nine cases, together with three more addressing the special control and verification required for locked valves as outlined above, are summarized in Table 3-6. The conditions associated with each case are identified in Table 3-6, along with the nominal probability of the error. The nominal probability is taken to be the median value of a lognormal distribution; the associated error factor (EF) is also provided.

Table 3-6
Basic Cases for Pre-Initiator Human Interactions*

Case	Compelling Status Ind. in Control Room	Effective Post-Maint. or -Calib. Test	Independent Verification	Status Check Each Shift or Day	Controlled Per Locked-Valve Procedure	Locked-Valve Verif. After Test/Maint.	Basic Probability	EF
I	no	no	no	no	no	no	3×10^{-2}	5
II	no	no	yes	yes	no	no	3×10^{-4}	16
III	no	no	yes	no	no	no	3×10^{-3}	10
IV	no	no	no	yes	no	no	3×10^{-3}	10
V	yes	irrelevant	irrelevant	irrelevant	irrelevant	irrelevant	negligible	—
VI	no	yes	no	no	no	no	3×10^{-4}	10
VIa	no	no	no	no	yes	no	9×10^{-4}	10
VIb	no	no	no	no	yes	yes	9×10^{-5}	10
VII	no	yes	yes	yes	no	no	3×10^{-5}	16
VIIa	no	yes	yes	no	yes	no	3×10^{-5}	16
VIII	no	yes	yes	no	no	no	3×10^{-4}	10
IX	no	yes	no	yes	no	no	3×10^{-5}	16

*Based on Table 5-3 of NUREG/CR-4772.

As described in NUREG/CR-1278 (Ref. 61), the unavailability of a component due to a human interaction can be expressed as follows:

$$U = \frac{pd}{T}$$

where p = the probability of the unrecovered human error, selected from Table 3-6 (and based on the ASEP methodology as outlined above);

d = the average time the error could exist; and

T = the average time between opportunities to make the error.

The average time the error could exist, d , reflects the opportunities to discover the error by test or checking prior to the next time the component would be manipulated. For cases in which the opportunities to uncover the error are uniformly distributed with time (e.g., monthly or quarterly checks), the value of d can be calculated as follows:

$$d = \frac{h(1-c^{T/h})}{1-c}$$

where h = the average length of time between checks, and

c = the probability the error will not be detected at the check.

The ASEP methodology suggests values for c for various types of verification. The time between opportunities for the error (T) was estimated based on plant experience for maintenance practices, and on the periodicity of tests for errors associated with testing. The value of h was also based on the interval between relevant tests or other verification steps.

As an example, suppose that a particular valve is subject to closure for a test that occurs on an 18-month cycle. Restoration of the valve to its normally-open position is verified independently, but would not otherwise be confirmed by an immediate test of the system. If the valve were left closed, it would be detected during quarterly testing of a pump in the system. For this set of circumstances, case III applies, and a basic error probability of 0.003 is recommended. If the quarterly test has a probability of 0.01 of not being performed effectively such that the error is not detected (as suggested by ASEP), the total unavailability due to the error can be calculated as follows:

$$\begin{aligned} U &= \frac{p \cdot h(1-c^{T/h})}{T(1-c)} \\ &= \frac{(0.003)(3 \text{ mos.})(1-0.01^{18/3})}{(18 \text{ mos.})(1-0.01)} \\ &= 5 \times 10^{-4} \end{aligned}$$

Figure 3-1 provides an example of the treatment of an actual pre-initiator human interaction. The example is in the form of the worksheet used for these evaluations. This interaction represents failure to restore one train of the LPI system to operable status following test or maintenance (this is denoted in the logic models as event LHA01TML).

In the worksheet, the interaction to be addressed is first identified according to the name used in the logic models. The guidelines for qualitative screening are then applied to permit focusing on the most important potential errors. In the example, these are identified to be associated with specific valves that are manipulated during various tests. The conditions associated with restoration and verification of the valves are identified, and reference is provided to the specific plant procedures that were reviewed and found to be applicable to the assessment (references to additional procedures that were reviewed but found not to be directly applicable are retained in the project files for the human interaction analysis).

The final portion of the worksheet provides the quantification of the basic error probabilities and the unavailability associated with the interactions, considering subsequent testing that would generally detect the errors. Most of the valves in the example are normally locked in position, and therefore correspond to case VIa of Table 3-6, which is the special case identified previously for those subject to the special locked-valve controls. A simple Boolean equation is provided that outlines the combinations of errors that could lead to the general pre-initiator interaction. For example, unavailability of the LPI train could result if both valves DH66 and DH68 were left open. A level of dependence must be assessed for the two errors associated with these valves, and this is again done based on the ASEP guidance. The error factors are selected based on those provided along with the basic values, which are taken to be median values of a lognormal distribution. The final probability therefore reflects conversion to the corresponding mean value for input to the sequence quantification process.

The pre-initiator human interactions and their probabilities of failure are summarized in Table 3-7. The worksheets for all of the events, along with supporting documentation, are contained in project files at Davis-Besse offices.

Quantification of Type CP Interactions

The post-initiator interactions of type CP that were incorporated into the logic models were each initially assigned a probability of failure of 1.0. This was done, rather than assessing some (lower) screening value, because of the potential for combinations of events to occur in the sequence cut sets. Even a screening value of 0.1 could result in underestimating the combined probability for three or four events occurring together, considering the likelihood that some level of inter-dependence would exist for the events. Detailed estimation of failure probabilities for the post-initiator events was performed only after the sequence quantification was underway, and then only for those events that were found in the sequence cut sets above the cut-off frequencies used.

Quantification of the type CP events that survived this level of screening was performed using a methodology developed relatively recently by EPRI, and described in its

HUMAN INTERACTION WORKSHEET: TYPE A

EVENT INFORMATION

<i>Name</i>	<i>Definition</i>
LHA01TML LHA02TML	Operators fail to restore LPI train 1 (or train 2) to operable status following test or maintenance

DESCRIPTION

Qualitative Screening

This event encompasses failure to restore the LPI train to operable status following various tests, and following maintenance affecting the pump or heat exchanger, including the CCW supplies to both the pump and heat exchanger.

The following air- or motor-operated valves are screened out because they receive confirmatory signals to go to their respective positions on SFAS initiation:

- DH7A(B) Outlet valve from the BWST
- DH2733(2734) Decay heat pump LPI suction valve
- DH14A(B) Decay heat cooler outlet valve
- DH13A(B) Decay heat cooler bypass valve

Valve DH1A(B), decay heat discharge to the RCS, is screened out because its position is clearly annunciated in the control room. Failure to restore it to the correct position following testing would be recognized and corrected.

Breakdown

The valves below are closed for various tests. They are locked-open manual valves, and therefore repositioning them requires control under the locked-valve control procedure. Both valves would also be subject to verification as part of the monthly locked-valve verification, which would also be performed prior to startup. Their positions would also be positively verified during the quarterly pump test.

- DH44(45) Decay heat pump outlet block valve
- DH54(55) Decay heat train recirculation

Valves DH65(66) and 68 are both opened for testing of the decay heat pumps on a quarterly basis. Valve DH65(66) is normally locked closed, and is controlled as described for valves DH44(45) and DH54(55). Valve DH68 is verified closed, but is not controlled as a locked valve. Valves DH65(66) and DH67 are also opened for system leak testing, which is performed at 18-month intervals. The procedures are analogous to those used for the pump testing. Valves DH66, DH67 and DH68 are all located in room 105, but valve DH66 is several feet from the other two. Therefore, they are not in the same visual frame of reference, per the criteria in NUREG/CR-4772. Valve DH65 is in room 115, so it is clearly in a separate reference frame.

Following pump maintenance, valves DH2733 and DH45 could be left closed. Pump maintenance occurred approximately every 14 months (4 events in 42,034 train-hours of operation). No maintenance activities requiring isolation of the CCW supply to the pump bearings, to the decay heat coolers, or of the decay heat coolers themselves were identified in the data base. Each of these is assumed to occur once every 36 months.

Figure 3-1. Example of the Detailed Treatment of a Type A Human Interaction

HUMAN INTERACTION WORKSHEET: TYPE A

sheet 2

Event LHA01TML (continued)

<i>Procedure</i>	<i>Title</i>	<i>Use in the HI Assessment</i>
DB-SP-03131	LPI and CS System Leak Test	Provides requirements and procedures to change positions of locked valves DH44(45), 54(55), 65(66), and 67 during various phases of system leak tests. Tests performed on an 18-month cycle; tests involving closure of valves DH44(45) & 54(55) performed only at cold shutdown.
DB-SP-03133	Forward Flow Test of DH127, 128, 76, and CF30 and Reverse Flow Test of DH125 and 126	Requires closing DH54(55) as part of the test. Tests are performed every cold shutdown, unless one has been performed within the previous 3 mos (average of every seven months).
DB-SP-03136 DB-SP-03137	DH Quarterly Pump and Valve Test (Trains 1 & 2)	Provides requirements to open valves DH65(66) and DH68. Also provides positive test of position of valves DH44(45) and DH54(55).
DB-OP-00008	Operation and Control of Locked Valves	Provides procedure and tracking mechanism for realigning and restoring position of locked valves. Performed each time positions of valves DH44(45), 54(55), 65(66) are changed.
DB-SP-03382	Boron Injection Flowpath Verification	Verifies position of valves DH44(45), 54(55), and 65(66) on a montly basis.
DB-OP-04004	Locked Valve Verification	Verifies position of locked valves DH44(45), 54(55), and 65(66) on a montly basis and prior to leaving cold shutdown.

QUANTIFICATION*Event Probabilities*

Error	Description	ASEP Case	p	EF	h (mos.)	T (mos.)	c	Final Value	Note
a	DH45 left closed after leak test	V1b	9.0E-5	10	1	18	0.1	1.5E-5	1
b	DH55 left closed after leak test	V1b	9.0E-5	10	1	18	0.1	1.5E-5	1
c	DH55 left closed after forward flow test	V1b	9.0E-5	10	1	18	0.1	1.5E-5	1, 2
d	DH66 left open after pump or leak test	V1a	9.0E-4	10	1	3	0.1	8.9E-4	1
e	DH68 left open after pump test	III	3.0E-3	10	3	3		8.0E-3	3

Figure 3-1 (continued). Example of the Detailed Treatment of a Type A Human Interaction

HUMAN INTERACTION WORKSHEET: TYPE A

sheet 3

Event LHA01TML (continued)

QUANTIFICATION (continued)**Event Probabilities**

Error	Description	ASEP Case	p	EF	h (mos.)	T (mos.)	c	Final Value	Note
f	DH68 open given DH66 open	ZD						8.0E-3	
g	DH67 left open after leak test	III	3.0E-3	10	3	18	0.1	1.5E-3	3
h	DH67 open given DH66 open	ZD						1.5E-3	
i	DH45 left closed after pump maintenance	VIIa	3.0E-5	16	1	14	0.1	9.9E-6	1
j	DH45 left closed after cooler maintenance	VIIa	3.0E-5	16	1	36	0.1	3.8E-6	1
j	DH14B left closed after cooler maintenance	VI	3.0E-4	10	3	36	0.01	6.7E-5	3
k	CC165 left closed after cooler maintenance	VIIa	3.0E-5	16	1	36	0.1	3.8E-6	1
l	CC171 left closed after cooler maintenance	VIIa	3.0E-5	16	1	36	0.1	3.8E-6	1
m	CC151 left closed after bearing cooler maintenance	VIIa	3.0E-5	16	1	36	0.1	3.8E-6	1
n	CC148 left closed after bearing cooler maintenance	VIIa	3.0E-5	16	1	36	0.1	3.8E-6	1
LHA01TML = LHA02TML = a + b + c + (d * f) + (d * h) + i + j + k + l + m + n								1.5E-4	

Quantification Notes

1. These errors are subject to recovery during the monthly locked-valve verification and the train's quarterly pump and valve testing.
2. On the average, the forward flow test would be performed every seven months, based on the historical rate at which cold shutdown would occur.
3. These errors are subject to recovery during the train's quarterly pump and valve testing.

Figure 3-1 (continued). Example of the Detailed Treatment of a Type A Human Interaction

Table 3-7
Summary of Pre-Initiator (Type A) Human Interactions

Event Name	Description	Probability
CHA01TML	Core flood tank 1 left isolated after plant startup	negligible
CHA02TML	Core flood tank 2 left isolated after plant startup	negligible
CHA12TML	Both core flood tanks left isolated after plant startup	negligible
EHAEDG1L	Failure to restore cooling water to EDG 1 following maintenance	9.8×10^{-6}
EHAEDG2L	Failure to restore cooling water to EDG 2 following maintenance	9.8×10^{-6}
HHA01TML	Failure to restore HPI train 1 to operable status following test or maintenance	3.7×10^{-4}
HHA02TML	Failure to restore HPI train 2 to operable status following test or maintenance	3.7×10^{-4}
HHA12TML	Failure to restore both HPI trains to operable status following test or maintenance	negligible
IHAAAIRL	Failure to align alternative path through pre- and after-filters following maintenance or system reconfiguration	3.2×10^{-3}
IHAEIACL	Failure to restore emergency instrument air compressor to service following testing or maintenance	1.7×10^{-3}
LHA01TML	Failure to restore LPI train 1 to operable status following a test or maintenance activity	1.8×10^{-3}
LHA02TML	Failure to restore LPI train 2 to operable status following a test or maintenance activity	1.8×10^{-3}
LHA12TML	Failure to restore both LPI trains to operable status following test or maintenance activities	negligible
LHADH79L	Failure to reopen common BWST suction valve (DH79) after maintenance	negligible
MHA01TML	Failure to restore makeup pump 1 following train testing or maintenance	8.6×10^{-4}
QHA0001L	Turbine-driven AFW pump train 1 left unavailable after testing or maintenance	1.1×10^{-4}
QHA0002L	Turbine-driven AFW pump train 2 left unavailable after testing or maintenance	1.1×10^{-4}

Table 3-7 (continued)
Summary of Pre-Initiator (Type A) Human Interactions

Event Name	Description	Probability
QHA0012L	Both turbine-driven AFW pump trains left unavailable after testing or maintenance	4.9×10^{-6}
QHAMDPL	Motor-driven feed pump not reconfigured to AFW lineup following testing, maintenance, or return to power operation	2.0×10^{-3}
SHASW82L	Failure to reopen service water return valve from ECCS room coolers (SW82) after maintenance	3.7×10^{-5}
UHAP017L	Failure to isolate containment integrity leak rate test line (penetration P-17)	negligible
UHAP049L	Failure to isolate refueling canal drain line (penetration P-49)	negligible
WHACCW2L	Standby CCW train left unavailable following test or maintenance	2.6×10^{-4}

report TR-100259 (Ref. 65). The methodology entails considering both the failure to initiate correct response (due to failure in detection, diagnosis, or decision-making), and failure to execute the response correctly. The total probability for a particular human interaction is the sum of the probabilities for these two portions, which are denoted as p_c and p_e , respectively.

The report TR-100259 provides a process for evaluating individual human interactions by breaking down the detection, diagnosis, and decision-making aspects (the p_c portion) into different failure mechanisms, with causes of failure delineated for each. For this reason, EPRI refers to this as a cause-based approach. Eight different potential failure mechanisms are identified in the methodology:

p_{ca}	Availability of information
p_{cb}	Failure of attention
p_{cc}	Misread/miscommunicate data
p_{cd}	Information misleading
p_{ce}	Skip a step in procedure
p_{cf}	Misinterpret instruction
p_{cg}	Misinterpret decision logic
p_{ch}	Deliberate violation

A relatively simple decision tree is provided for each of these mechanisms in the EPRI report (Ref. 65). Each of these decision trees identifies factors that could cause the relevant mechanism to lead to failure to initiate the proper action. It is the task of the human reliability analyst to select branch points in the decision trees that correspond to the aspects of the interaction being analyzed (e.g., the number and quality of cues for the operators, the ease of use of the procedures, etc.). For each outcome in the decision trees, a nominal probability of failure is suggested.

Depending on the failure cause, certain recovery mechanisms may come into play. Table 4-1 in TR-100259 outlines the nature of any recovery that may be credited for each of the eight failure mechanisms relating to the decision-based (p_c) part of the interaction. The potential for recovery is considered as follows:

- Due to self-review by the operator initially responsible for the misdiagnosis or error in decision-making, as additional cues become available or additional procedural steps provide opportunity to reconsider;
- As a result of review by other crew members who would be in a position to recognize the lack of proper response;
- By the shift manager, who serves the role of the shift technical advisor (STA) at Davis-Besse, and whose review might identify errors in response;
- By the technical support center (TSC) when it is staffed and actively involved in reviewing the situation; and
- By oncoming crew members when there is a shift turnover.

For example, if the initial error results from a misinterpretation of the decision logic presented in the procedures (i.e., mechanism p_{cg}), it may be possible that other crew members and/or the shift manager would observe the error and provide input that would lead to taking the proper action.

Thus, after processing each of the decision trees to arrive at estimates for the basic failure mechanisms, the analyst must identify and characterize the appropriate recovery factors. The first element of the type CP interaction (i.e., p_c , the failure to initiate proper response) is then quantified by summing the decision-tree outcomes, as they have been modified by the appropriate recovery factors. This quantification process is relatively straightforward to implement, with the exception that the guidance provided in TR-100259 for characterizing the recovery factors is limited. Clearly, there are often dependencies among the crew members who might have the opportunity to observe errors and contribute to correcting them. It is necessary, therefore, to characterize the crew members involved in the initial actions, and to identify additional personnel and the roles they might play. Table 3-8 identifies the staff at Davis-Besse that would be available to the control room and the time following an upset event at which their contributions might begin to be made. This tabulation is derived from a more general version provided in NUREG/CR-1278 (Ref. 61). A comparison to the staffing levels assumed in NUREG/CR-1278 is also provided in the table.

The normal response to a plant upset is for one of the reactor operators to concentrate on the primary systems and for another to attend to the secondary systems. Two such operators would typically be present in the control room at all times. A third reactor operator may or may not be present to aid with specific tasks. At least one assistant shift supervisor (who is a SRO) is always present in the control room, and it is typically his function to begin following the procedures that are relevant for the symptoms at hand and to direct the actions of the reactor operators. For most of the events in this study, this entails using first the emergency procedure (Ref. 31), supplemented by abnormal or system operating procedures as the need arises. For the failure to initiate proper response (the p_c element of type CP interactions), the initial assessment is therefore assumed to apply to this assistant shift supervisor.

The shift supervisor (also a SRO) has an office at the back of the control room, with a window out onto the control room so that he can monitor operations. A second assistant shift supervisor is also available, either in or nearby the control room; these staff members would be available to respond very quickly as well. The shift supervisor's role would generally be to make an overall appraisal of the situation, taking such actions as to begin considering the need to notify other personnel and to assess whether any action statements under technical specifications were applicable. The second assistant shift supervisor would assist in whatever role was required; this could include taking control for auxiliary panels, such as those dealing with the electrical distribution systems, or organizing and directing equipment operators who would need to accomplish tasks outside the control room.

As indicated above, the role of the STA is filled by the shift manager. The shift manager's office is very close to the control room, allowing for rapid response to an upset

**Table 3-8
Availability of Staff to Respond to Abnormal Events**

Time After Initiating Event	Staffing Available per NUREG/CR-1278	Minimum Staffing at Davis-Besse
0 - 1 min	<ul style="list-style-type: none"> • on-duty reactor operator 	<ul style="list-style-type: none"> • two to three reactor operators • assistant shift supervisor, a senior reactor operator (SRO)
at 1 min	<ul style="list-style-type: none"> • on-duty reactor operator • shift supervisor or other SRO 	<ul style="list-style-type: none"> • two to three reactor operators • assistant shift supervisor • second assistant shift supervisor (SRO) • shift supervisor (SRO)
at 5 min	<ul style="list-style-type: none"> • on-duty reactor operator • assigned SRO • shift supervisor • one or more auxiliary operators 	<ul style="list-style-type: none"> • two to three reactor operators • assistant shift supervisor • second assistant shift supervisor • shift supervisor • shift manager (shift technical advisor, SRO) • two shutdown equipment operators, as needed
at 15 min	<ul style="list-style-type: none"> • on-duty reactor operator • assigned SRO • shift supervisor • shift technical advisor • one or more auxiliary operators 	<ul style="list-style-type: none"> • two to three reactor operators • assistant shift supervisor • second assistant shift supervisor • shift supervisor • shift manager • two shutdown equipment operators, as needed • four equipment operators stationed in plant as needed

event as well. During an upset event, the shift manager monitors the plant conditions and attempts to verify that plant conditions or responses have been recognized and attended to properly by the other members of the control room staff.

Opportunities for recovery are largely a function of the time available for response. Thus, for each type CP interaction a time line was constructed. This time line lays out the activities most immediately relevant for the interaction being assessed. This includes the timing of any failures that lead to the need to take action, the time at which cues to take action (i.e., annunciators or control indications) would be present, and the time by which the interaction must be accomplished to be considered successful. For specific events, this timing was estimated based on observations of simulator exercises, available thermal-hydraulic calculations, simple hand calculations, or estimates from operators. The time required for actual implementation of the action was also estimated, usually based on walkdowns or operator interviews. The time window available for initiating response (T_w) is therefore the time between when the compelling cue to take action is received and when the action must be accomplished, less the time required to implement the action. The time after the initial upset and the time window for initiating action are used to determine the availability of additional personnel to review the response and to provide opportunity for recovery of errors.

In this study, where consideration of recovery via extra crew is considered appropriate, the extra crew members consist of the reactor operator to whom the assistant shift supervisor is giving instructions, and in some cases the other reactor operators (e.g., when failure to take appropriate actions relating to the secondary systems would have distinct effects on the response of the RCS). Where this recovery is credited, a constant value of 0.5 is applied, as suggested by Table 4-1 of EPRI TR-100259. Where Table 4-1 indicates credit for review by the STA, it is assumed that monitoring of the situation by the shift manager and shift supervisor may be considered. The TSC would be staffed within about one hour after an event had been classified as an alert or higher (Ref. 66). This classification is made for a variety of accident types, but would not necessarily be made for a reactor trip. The nature of the event prior to the need for the human interaction must therefore be recognized to determine whether or not recovery via review by the TSC can be credited. For consideration of review during a shift change, it is assumed that the time window must be at least six hours long.

The levels of dependence assumed for the review functions in this study (aside from the constant non-recovery probability of 0.5 used for extra crew members) are summarized in Table 3-9. This table indicates the level of dependence assumed for review by the STA-equivalent function (i.e., the shift manager), by the TSC, and by an oncoming shift, as a function of the relevant time. The qualitative descriptions of the levels of dependence have corresponding quantitative interpretations that are used to estimate the conditional probability of non-recovery. These dependence characterizations are those defined in the model presented in Table 20-17 of NUREG/CR-1278 (Ref. 61). The total probability for a given decision tree is therefore the product of the probability for the basic outcome selected for that

**Table 3-9
Assumed Levels of Dependence for Recovery Factors Applied to
Detection/Diagnosis/Decision-Making Portion of Human Interactions**

Level of Dependence	Applied to Self-Review	Applied to Review by Shift Manager	Applied to Review at Shift Change	Applied to TSC Review
Complete (no credit for recovery)	Time window is very short (i.e., on the order of 10 minutes or less); OR Time window is relatively short (i.e., on the order of 10 to 30 minutes), and the procedure would not provide multiple opportunities for proper diagnosis and decision-making.	Time window is very short (i.e., on the order of 10 minutes or less), such that shift manager would not be able to reach control room and make proper assessment.	Time window is less than about 6 hour.	Time window is less than about 1 hour.
High	Time window is relatively short (i.e., on the order of 10 to 30 minutes), and the procedure would naturally guide the operator through multiple opportunities for proper diagnosis and decision-making.	Time window is relatively short (i.e., on the order of 10 to 30 minutes) and the critical cues would have been received within the first five minutes.	Time window is more than about 6 hour, and recovery based on low dependence assessed for others.	Time window is more than about 1 hour from alert status, and recovery based on low dependence assessed for others.
Moderate	Time window is relatively long (i.e., on the order of an hour or more), and there are multiple opportunities through the procedures and/or additional control indications or alarms to make a proper diagnosis and decision.	Time window is relatively short (i.e., on the order of 10 to 30 minutes) but significant additional cues would have been received after the first five minutes; OR Time window is relatively long (i.e., on the order of an hour or more), and limited additional cues would have been received since the first five minutes.	Not applicable for review at shift change.	Not applicable for TSC review.
Low	Not applicable for self-review.	Time window is relatively long (i.e., on the order of an hour or more), and significant new cues have been received since the first five minutes.	Time window is more than about 6 hour.	Time window is more than about 1 hour after alert declared

tree and whatever non-recovery factors apply. The non-recovery factors are calculated according to the following formulae:

Dependence Level	Non-Recovery Factor
Complete	1.0
High	$\frac{1 + \text{base probability}}{2}$
Moderate	$\frac{1 + 6 * \text{base probability}}{7}$
Low	$\frac{1 + 19 * \text{base probability}}{20}$
Zero	base probability

The second element of a type CP interaction represents failure to implement the action correctly, given that the action is properly initiated. This portion, referred to as p_e , is quantified using an abbreviated version of THERP, in which the specific acts that must be accomplished are identified, and failures to perform them properly (due to errors of omission or commission) are noted. These failures are then quantified using the data in NUREG/CR-1278 (Ref. 61).

In many cases, these execution errors are subject to review and recovery as well. This is particularly true for actions taken in the control room, where additional observers may be able to identify the need for corrective action. As in the case of the initiation errors, a set of guidelines for considering review and recovery by other crew members has been developed. These guidelines are summarized in Table 3-10. The levels of dependence are quantified as in the case of the recovery factors for the p_c portion of the type CP events (i.e., as indicated by the formulae summarized above).

As a further illustration of the application of this methodology, an example is provided in Figure 3-2. This example is a worksheet containing the analysis for failure to actuate the motor-driven feed pump as a backup to the turbine-driven AFW pumps after a total loss of feedwater. As the example illustrates, the worksheet first provides a description of the event and its context relative to the accident scenario(s) to which it applies. The procedures that guide the action, and are the basis for the reliability assessment, are then summarized. In this case, the emergency procedure (Ref. 31) is the primary procedure of interest.

In the second sheet of the worksheet, the time line indicating the relationship of the interaction to other significant aspects of the accident is indicated. The time window is determined based on the total time from the compelling indication to take action to the last time at which it would be successful, less the time required to execute the action. For the example, this time window is estimated to be about 26 minutes, based on a total time of 30 minutes and an execution time of 4 minutes.

Table 3-10
Assumed Levels of Dependence for Recovery Factors Applied to
Execution Portion of Human Interactions

Level of Dependence	Applied to Self-Review	Applied to Review by Extra Crew*	Applied to Review by Shift Manager or Others*
Complete (no credit for recovery)	Time window is very short (i.e., on the order of 10 minutes or less); or Time window is relatively short (i.e., on the order of 10 to 30 minutes), and subsequent steps would not provide opportunity for identifying and correcting previous errors.	No other crew observing (e.g., local manual actions whose effects not directly detectable in control room).	Activities would not be expected to be observed by shift manager or others; or Time window is very short (i.e., on the order of 10 minutes or less).
High	Time window is relatively short (i.e., on the order of 10 to 30 minutes), but subsequent steps would provide opportunity for identifying and correcting previous errors.	Time window is very short (i.e., on the order of 10 minutes or less); or Time window is relatively short (i.e., on the order of 10 to 30 minutes), with limited opportunity for feedback.	Time window is relatively short (i.e., on the order of 10 to 30 minutes), but the activities would be expected to be observed directly or the effects of the error would be clear through other plant response or non-response.
Moderate	Time window is relatively long (i.e., on the order of an hour or more), and there are multiple opportunities for identifying and correcting previous errors through subsequent activities.	Time window is relatively short (i.e., on the order of 10 to 30 minutes), but subsequent steps would provide opportunity for identifying and correcting previous errors.	Time window is relatively long (i.e., on the order of an hour or more), and the activities would be expected to be observed directly or the effects of the slip would be clear through other plant response or non-response.
Low	Not applicable for self-review.	Time window is relatively long (i.e., on the order of an hour or more), and there are multiple opportunities for identifying and correcting previous errors through subsequent activities.	Not applicable for review by shift managers or others.

*Recovery credit given for review by extra crew or by shift manager, et al., but not for both.

HUMAN INTERACTION WORKSHEET: TYPE CPsh. 1
background information**EVENT INFORMATION***Name* *Definition*

BHAMDFPE	Operators fail to actuate motor-driven auxiliary feedwater pump as backup to turbine-driven pumps for transient, small LOCA, or steam generator tube rupture.
----------	---

DESCRIPTION*Context*

Following a loss of main feedwater, the turbine-driven auxiliary feedwater pumps are actuated automatically. If they should fail to start or fail to deliver flow to the steam generators, the motor-driven pump can be started manually and used as a backup. The motor-driven pump is normally aligned to serve as an auxiliary feedwater pump (at power levels above 40%). The starting sequence entails the following:

1. Enabling the flow control valves from the motor-driven pump and closing them fully to provide backpressure to make it easier for the pump to start.
2. Starting the pump at the selector switch.
3. Manually opening the flow control valves to admit flow to the steam generators at a rate sufficient to restore level, but not so great that the motor-driven pump runs out.
4. Placing the flow control valves in the automatic mode to allow them to maintain steam generator level.

The actions and procedures for this event are essentially identical for the three types of initiating events to which it applies. Differences are primarily associated with other elements of the cut sets which require context-specific assessment. This assessment applies to the limiting (with respect to time) case in which both turbine-driven pumps fail to start following an initial loss of main feedwater. In this case, flow from the motor-driven pump must be made available within about 30 min to prevent uncovering the core.

Procedural Guidance

The emergency procedure (DB-OP-02000) provides the primary direction for starting the motor-driven pump. In Section 4.10.4, a step-by-step procedure is given for using the motor-driven pump given that neither turbine-driven AFW pump is delivering flow to a steam generator. Similarly, Section 4.10.5 instructs the operators to start the motor-driven feed pump and align it to the generator not being fed if only one AFW pump has started and is delivering flow to a steam generator.

Figure 3-2. Example of the Treatment of a Type CP Human Interaction

HUMAN INTERACTION WORKSHEET: TYPE CP

BHAMDFPE sh. 3
assessment of pe

QUANTIFICATION (continued)

Execution (pe)

Error	1278 Table (Entry)	Basic Prob.	EE	Stress Mult.	Non-Rec. (Depend.)	Non-Rec. Prob	Final Value	Note
Omit enabling of discharge valves	20-7 (3)	3.0E-3	3	2	(M)*(L)	7.7E-3	5.8E-5	1,2
Select wrong control (HIS 6460/59)	20-12 (4)	5.0E-4	10	2	(M)*(L)	7.2E-3	1.9E-5	1,2
Omit closing of disch valves	-	-	-	-	-	-	0.0E+0	3
Misset rotary control on pump start	20-12 (9)	1.0E-3	3	2	(H)*(L)	2.6E-2	6.5E-5	2,4
Omit establishing flow	20-7 (3)	3.0E-3	3	2	(H)*(L)	2.7E-2	2.0E-4	2,4
Fail to complete establishing flow	20-12 (10)	3.0E-3	3	2	(H)*(M)	7.3E-2	5.5E-4	4,5,6
Probability for pe							8.9E-4	

Notes

1. M = recovery via self review, with (M)oderate dependence assessed due to multiple specific opportunities later in procedure.
2. L = recovery via additional crew/STA-equivalent review, with (L)ow dependence assessed due to time available, multiple opportunities for recovery.
3. If steam generator level is low, discharge valves will open fully when enabled. It is expected that pump would still start with valves fully open, except in cases when steam generator is depressurized.
4. H = recovery via self-review, with (H)igh dependence assessed due to more limited additional cues.
5. Operator is expected to control flow manually to restore steam generator level (while balancing flow to steam generators), then return to automatic control.
6. M = recovery by additional crew, with (M)oderate dependence assessed for observing flow/level problems and correcting error due to relatively short residual time and more limited additional cues.

Quantification Summary

Failure	Probability
Detection, diagnosis, & decision-making	pc 1.5E-3
Execution	pe 8.9E-4
Total event probability	2.4E-3
Assumed error factor	5

Figure 3-2 (continued). Example of the Treatment of a Type CP Human Interaction

HUMAN INTERACTION WORKSHEET: TYPE CP

BHAMDFPE sh. 2
assessment of pc

TIMELINE

<p>T0 Reactor/turbine trip Main feedwater fails SFRCS actuates Turbine-driven auxiliary feedwater pumps fail</p> <p>T1 Flow from motor-driven pump required to maintain decay heat removal via steam generators</p>
<p>Total time from compelling signal: 30 min Time required to accomplish action: 4 min Time window (Tw): 26 min</p>

QUANTIFICATION

Detection, Diagnosis, & Decision-Making (pc)

<u>Tree</u>	<u>Failure Mechanism</u>	<u>Selected Branch</u>	<u>Branch Probability</u>	<u>Non-Rec (Depend.)</u>	<u>Non-Rec. Probability</u>	<u>Probability w/ Recovery</u>	<u>Note</u>
pca	Availability of information	(a)	neg	-	-	neg	
pcb	Failure of attention	(h)	neg	-	-	neg	
pcc	Misread/miscomm. data	(a)	neg	-	-	neg	
pcd	Information misleading	(a)	neg	-	-	neg	
pce	Skip a step in procedure	(h)	0.013	(M)*0.5	7.7E-2	1.0E-3	1, 2
pcf	Misinterpret instruction	(a)	neg	-	-	neg	
pcg	Misinterpret decision logic	(a)	0.016	0.5*(L)	3.3E-2	5.3E-4	2, 3
pch	Deliberate violation	(a)	neg	-	-	neg	
Probability for pc						1.5E-3	

Notes

1. M = recovery via self-review, with (M)oderate dependence assessed based on time, which is at the limit between relatively short and relatively long, and multiple procedural calls for starting MDFP.
2. 0.5 = recovery via additional crew (constant probability of failure of 0.5).
3. L = recovery via shift manager (STA-equivalent), with (L)ow dependence assumed due to time available and multiple cues.

Figure 3-2 (continued). Example of the Treatment of a Type CP Human Interaction

The quantification is presented in two parts. In the first, for the p_c element, the appropriate outcome for each of the eight decision trees is first identified, along with the corresponding probability from TR-100259. Any opportunities for recovery are also identified. These are denoted by the level of dependence assessed to apply. For example, given that the appropriate step in the procedure calling for starting the motor-driven pump is overlooked, moderate dependence is assessed for self-review, since there is ample time for further action and there are multiple procedural calls for starting the pump. Credit is also given for review by additional crew members, with a probability of failure of 0.5 assigned based on Table 4-1 of TR-100259. Note that Table 4-1 indicates that no additional credit should be given for review by the STA, and the time window is too short to consider input from the TSC or an oncoming shift. The non-recovery probability is then calculated as the product of each of the elements of recovery identified. This non-recovery probability is then multiplied by the basic probability of the error to arrive at the contribution for that failure mechanism. Notes are provided to explain the rationale for any recovery actions credited, and to outline any additional considerations that are significant to the assessment.

The second portion of the quantification is for the execution errors (p_e). The various errors of omission or commission that could lead to failure to implement the action correctly are identified, based on the types of errors delineated in NUREG/CR-1278 (Ref. 61). The basic probabilities for the errors are those drawn from the tables in NUREG/CR-1278, and are taken to be median values of a lognormal distribution. A factor to account for stress is also included. In most cases (as in this example), the basic probability is multiplied by a stress factor of two, in accordance with the guidance provided in NUREG/CR-1278. As in the quantification of p_c , potential non-recovery factors are identified (according to the level of dependence assessed to apply, based on the guidance in Table 3-10). The final probability for each error represents the product of the overall non-recovery probability and the basic error probability, converted to a mean value. Notes are provided to explain the recovery treatment and, where appropriate, to describe further the nature of the error.

Finally, the worksheet summarizes the two contributions to the overall probability for the event. An error factor is also provided. This error factor is selected as described later in this report.

As noted earlier in this section, each post-initiator interaction was initially assigned a value of 1.0. This was done to ensure that combinations of human interactions would not be inappropriately assessed as independent, possibly causing them to be lost. This could result if the combined probabilities would produce sequence cut sets below the truncation value used in the quantification process. The use of the screening value of 1.0 resulted in a large number of cut sets containing multiple human interactions. Each set of interactions was examined in the context of the cut sets in which they occurred to obtain a meaningful assessment of their combined probabilities. This was done in each case by laying out a time line for the sequence of events of interest, and by considering qualitatively the factors that implied dependence or independence for the combined events. For cases in which there were more than two events, this entailed considering the level of dependence between the first two events, and then the

conditional level of dependence for successive events, given that the earlier failures had occurred. Once the qualitative levels of dependence were assessed, the corresponding quantitative characterizations summarized above were applied. The qualitative factors taken into account in assessing the level of inter-event dependence included the following:

- Events that refer to the same action were assessed to be completely dependent. For example, in a limited number of cases, separate human interactions could have been used to reflect the failure to initiate different trains of a particular system. This is actually a single event with respect to diagnosis and decision-making.
- Interactions related by time were assessed to have a decreasing level of dependence as the time between them increased:
 - Interactions occurring close in time (i.e., within about 15 minutes) were assessed to be at least moderately dependent (other factors could lead to an assessment of high or complete dependence).
 - Low dependence was assessed for interactions separated by up to about an hour for which no other factors applied.
 - Interactions separated by more than an hour were assessed to be independent, unless factors other than time suggested dependence.
- Interactions which imply actions based on nearly the same cues were assessed using one level of dependence higher than that implied by the nominal time-based delineation described above. For example, two events occurring close in time and based on the similar cues were assessed to be highly dependent.
- In some cases, a scenario might imply a successful action occurring between (in time) two events denoting failures. In these cases, the successful action may decouple the other two interactions (i.e., zero dependence would apply). This would be the case when the interceding event is directly relevant to at least one of the two failures. If the interceding event is completely unrelated, the level of dependence is assessed to be one step lower than that which would otherwise be used.
- For cases in which there are three or more human interactions, the third interaction is generally assessed to be at least moderately dependent on the first two, since each additional interaction may imply that it is more likely the operating crew has made a fundamental misdiagnosis. Subsequent interactions are likewise at least highly dependent on the preceding events. This is applied unless the multiple interactions are widely spaced in time, or later interactions are preceded by a successful action. For example, it is conceivable that two interactions could lead to a total loss of feedwater but that makeup/HPI cooling could be successfully initiated. The failure to establish high pressure recirculation several hours later could be construed to be decoupled from the earlier events.

Clearly, a measure of analyst judgment enters into the selection of the appropriate level of dependence for a particular case. These guidelines help to assure a degree of consistency in the assessments. The review performed both within the project team and by other Davis-Besse personnel helped to improve the consistency obtained.

It should also be noted that lower-bound values were used in place of the calculations, when very low probabilities were assessed for some combinations. These lower bounds were as follows:

- A minimum value of 10^{-4} was used for any single interaction.
- A lower bound of 10^{-5} was used for interactions appearing in combination that were separated by less than about two hours.

As an example of the treatment of a combination of human interactions, the combination of failure to start the motor-driven feed pump (event BHAMDFPE, as in the example provided in Figure 3-2), and the failure to initiate makeup/HPI cooling given total loss of feedwater (event UHAMUHPE) is presented in Figure 3-3. A brief description of the scenario in which the combined events arise is provided, with emphasis on characteristics indicating the level of dependence among the events. A time line describing the temporal relationship of the events is then provided. The combination is then quantified based on the level of dependence assessed. Note that the events are identified according to the time sequence in which they arise, with subsequent events assessed as dependent on earlier ones. In this case, because of the proximity of the two interactions in time and the common elements of the diagnosis required for both, high dependence was assessed. The worksheet automatically prompts the analyst to consider a default minimum value whenever the calculated value is less than 10^{-4} .

As a practical matter, it should be noted that the event names used in the modeling process were retained in the cut sets as "flags" to aid in understanding the sequence of events, with their probabilities set to 1.0. For each cut set in which there were multiple human interactions, a new event representing the event combination was appended to the cut set. These added events all began with the letter "Z", and were numbered consecutively (i.e., ZHAC001E, ZHAC002E, ...). For the cases in which there was only one human interaction in the cut set, the same event name was used, but with the first letter replaced with a "Z". Thus, type CP events beginning with this letter always represent the assessment of a human interaction specific to a particular sequence and cut set. The type CP interactions are summarized in Table 3-11. In addition to the probabilities estimated for each interaction, relevant aspects of the timing for the events are provided in the table. The total time refers to the time from the initiation of the accident to when the interaction would need to be completed. The time window reflects the period from receipt of a compelling indication of the need to take action to the time when action would need to be initiated to be considered successful (as described previously).

Quantification of Type CR Interactions

A limited number of recovery interactions that are not explicitly directed by procedures was assessed in this study. These recovery actions are knowledge-based, rather than procedure- (or rule-) based, and hence cannot be assessed in the same manner as was the case for type CP interactions. Instead, a simplified methodology developed by EPRI was used

HUMAN INTERACTION: TYPE CP COMBINATION

sh. 1
background information

EVENT INFORMATION

Name	Definition
ZHAC008E	Operators fail to provide core cooling by either starting the motor-driven feed pump or initiating makeup/HPI cooling (BHAMDPE * UHAMUHPE)

DESCRIPTION

This event represents the combination of the failure to restore AFW by starting the motor-driven feed pump (event BHAMDPE) and failure to effect makeup/HPI cooling upon loss of all feedwater (event UHAMUHPE). As described for event BHAMDPE, the procedures direct that the motor-driven pump be started in the event of failure of either turbine-driven AFW pump. As in other cases, the operators are instructed to initiate makeup/HPI cooling when feedwater is lost and $T_{hot} > 600^{\circ}F$, irrespective of attempts to restore feedwater.

The timing for initiating makeup/HPI cooling is overlapped by the time during which restoration of feedwater would be successful, with about 20 minutes remaining in which to take action with respect to the motor-driven pump after makeup/HPI cooling would no longer be successful in preventing core damage.

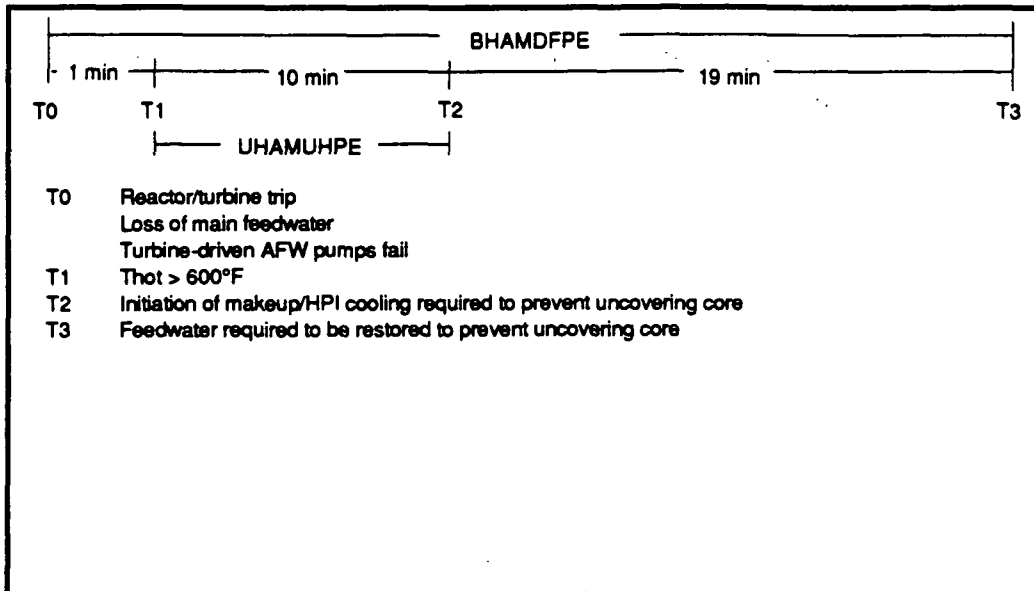
There are different operators involved in the two actions and somewhat different cues, although both are assumed to be guided by the same assistant shift supervisor. A primary aspect of both events is the need to recognize that feedwater was unavailable. Because of the relative proximity in time of the events and common elements of the diagnosis, high dependence is assessed.

Figure 3-3. Example Assessment of Combination of Type CP Human Interactions

HUMAN INTERACTION: TYPE CP COMBINATION

sh. 2
 quantification
 ZHAC008E

TIMELINE



QUANTIFICATION

Event	Failure	HEP	Event HEP	Dep	Dep Prob
BHAMDFPE	Detection, diagnosis, & decision-making	1.5E-3			
	Execution	8.9E-4			
			2.4E-3		2.4E-3
UHAMUHPE	Detection, diagnosis, & decision-making	1.2E-2			
	Execution	4.0E-3			
			1.6E-2	high	5.1E-1
Composite value for event combination					1.2E-3
Assumed error factor					5

Figure 3-3 (continued). Example Assessment of Combination of Type CP Human Interactions

Table 3-11
Summary of Type CP Human Interactions

Event Name	Description	Total Time	Window	Mean Prob.	EF
BHAMDFPE	Failure to actuate motor-driven feed pump as backup to turbine-driven AFW pumps for transient, small LOCA, or steam generator tube rupture.	30 min	26 min	2.4×10^{-3}	5
ZHAMDF2E	Failure to actuate motor-driven feed pump, given delayed loss of feedwater	2 hr	1 hr	5.4×10^{-4}	10
ZHAMDF3E	Failure to actuate motor-driven feed pump before depletion of BWST inventory during makeup/HPI cooling	> 24 hr	> 24 hr	1.0×10^{-4}	10
CHASGDPE	Failure to depressurize steam generators to cool down during steam generator tube rupture	22 hr	14 hr	1.0×10^{-4}	10
DHADHRSE	Failure to initiate shutdown cooling following a steam generator tube rupture	22 hr	12 hr	1.0×10^{-4}	10
EHASBDGE	Failure to align power from station blackout diesel generator to supply motor-driven feed pump given loss of offsite power	26 min	24 min	9.9×10^{-3}	5
HHAMODFE	Failure to balance HPI flow in injection line following medium LOCA involving HPI line break	60 min	55 min	5.4×10^{-3}	5
IHAMSIIVE	Failure to close MSIV to isolate steam generator containing ruptured tube	2 - 22 hr	2 - 22 hr	1.0×10^{-4}	10
KHABORAE	Failure to initiate emergency boration via makeup system following failure of control rods to insert	30 min	20 min	5.1×10^{-3}	5
MHARMVTE	Failure to compensate for loss of room cooling for makeup pumps by opening door to makeup pump room (given loss of offsite power)	30 min	25 min	9.0×10^{-3}	5
ZHARMV2E	Failure to compensate for loss of room cooling for makeup pumps by opening door to makeup pump room (given failure due to other than loss of offsite power)	30 min	5 min	3.2×10^{-2}	5
MHASMUPE	Failure to start standby makeup pump following failure of normally-operating pump	30 min	5 min	4.6×10^{-3}	5

Table 3-11 (continued)
Summary of Type CP Human Interactions

Event Name	Description	Total Time	Window	Mean Prob.	EF
PHADRCSE	Failure to initiate depressurization of RCS following a steam generator tube rupture	14 hr	14 hr	2.1×10^{-4}	10
QHA6459E	Failure to prevent runout of motor-driven feed pump following steam line break and failure of turbine-driven pumps	> 15 min	> 14 min	6.4×10^{-3}	5
QHAOVF1E QHAOVF2E	Failure to take local manual control of AFW turbine speed to prevent overfeeding steam generator following loss of dc power (one division)	2 - 4 hr	12 min	2.8×10^{-2}	5
ZHAOSB1E ZHAOSB2E	Failure to take local manual control of AFW turbine speed to prevent overfeeding steam generators following total loss of dc power	2 - 4 hr	7 min	1.9×10^{-1}	5
QHARCPCE	Failure to trip reactor coolant pumps following total loss of seal cooling	25 min	20 min	4.0×10^{-3}	5
QHARCPRE	Failure to trip reactor coolant pumps following loss of seal return	30 min	29 min	4.9×10^{-3}	5
RHA011CE	Failure to close PORV block valve (RC 11) to terminate LOCA when PORV fails open	> 1 hr	1 hr	3.6×10^{-3}	5
RHA011NE	Failure to open PORV block valve (RC 11) to permit use of PORV for makeup/HPI cooling	16 min	13 min	1.0×10^{-2}	5
UHAMUHCE	Failure to initiate cooldown via makeup/HPI cooling with unaffected steam generator not available for cooldown following a steam generator tube rupture	3 hr	2 hr	3.3×10^{-4}	10
UHAMUHPE UHAMUHSE	Failure to establish makeup/HPI cooling following total loss of feedwater (for transient or small LOCA)	11 min	8 min	1.6×10^{-2}	5
ZHAMUH2E	Failure to establish makeup/HPI cooling following delayed total loss of feedwater	> 2 hr	40 min	1.8×10^{-3}	5
UHAMUISE	Failure to align makeup system for full flow (backup to HPI for small LOCA)	1 hr	59 min	1.0×10^{-3}	10

**Table 3-11 (continued)
Summary of Type CP Human Interactions**

Event Name	Description	Total Time	Window	Mean Prob.	EF
XHACLDNE	Failure to control atmospheric vent valves manually to cool down following a steam generator tube rupture	14 hr	12 hr	1.2×10^{-3}	5
XHAHPRBE	Failure to initiate high pressure recirculation for a small LOCA: heat removal available via steam generators	16 hr	3 hr	5.0×10^{-4}	10
XHAHPRSE	Failure to initiate high pressure recirculation for a small LOCA: heat removal not available via steam generators	4 hr	27 min	3.5×10^{-3}	5
XHAHPRTE	Failure to initiate high pressure recirculation during makeup/HPI cooling (extended loss of feedwater)	26 hr	6 hr	4.8×10^{-4}	10
XHALPRAE	Failure to initiate low pressure recirculation for a large LOCA	44 min	7 min	7.4×10^{-3}	5
XHALPRME	Failure to initiate low pressure recirculation for a medium LOCA	100 min	18 min	4.4×10^{-3}	5
XHASDCSE	Failure to cool down and initiate shutdown cooling via DHR system following a small LOCA	12.5 hr	6.5 hr	3.0×10^{-4}	10
ZHACW01E	Failure to recover component cooling water via use of spare train	85 min	75 min	5.6×10^{-3}	5
ZHAPWMPE	Failure to align power from EDG via bus D2 to supply motor-driven feed pump with station blackout generator unavailable	30 min	24 min	1.7×10^{-2}	5
ZHARSCWE	Failure to start standby component cooling water pump after failure due to spurious protective interlock actuation	85 min	75 min	1.7×10^{-3}	5
ZHASW01E	Failure to recover service water using the backup service water pump (i.e., the dilution pump)	60 min	15 min	4.0×10^{-3}	5
ZHASW02E	Failure to recover service water using the standby service water pump	60 min	15 min	1.8×10^{-3}	5
ZHASW09E	Failure to recover train 2 of service water via pump 3 (previously operating to supply train 1)	60 min	15 min	2.8×10^{-3}	5

to characterize these type CR interactions (Ref. 67). This methodology presents relative likelihoods of failure to accomplish recovery, based on the following attributes:

- The amount of time available for decision-making and action
 - Short (less than about an hour),
 - Intermediate (about one to four hours), and
 - Long (longer than about four hours);
- Whether or not training or some level of procedural guidance is available relative to the specific actions being considered;
- Whether the recovery action is simple (e.g., operating a manual valve) or complex (e.g., multiple steps required to cross-connect two systems); and
- Whether environmental factors, such as the heat, humidity, or radiation levels that might impede recovery efforts, are good or poor.

For various combinations of these factors, a qualitative assessment is made regarding the probability of failure. These qualitative assignments are then associated with a quantitative probability scale. The scale used in this study is the nominal scale from Reference 67. The non-recovery probabilities in this scale are as follows:

Low	0.01	High	0.1
Moderately low	0.03	Very high	0.3
Moderately high	0.05	Maximal	1.0

An example of the treatment of a type CR event is illustrated in Figure 3-4. As with the other worksheets, the first portion is devoted to a description of the event and its context in the sequence to which it applies. The assessment identifies each of the influencing factors identified above, producing an overall qualitative characterization of the likelihood of non-recovery. The corresponding probability is then assigned. The interactions of this type are summarized in Table 3-12.

Uncertainty in Event Estimates

The estimates developed for failure of each of the human interactions reflect use of an approximate methodology, with substantial input based on the judgment of the analysts involved. The narrow objective of the quantification effort relating to human interactions is to provide reasonable estimates that are at least internally consistent (e.g., that a ranking of the interactions by probability would be consistent with a qualitative assessment of the likelihood of successfully accomplishing the interactions). Beyond this narrow objective, the quantification is required for the following reasons:

- To support estimation of the frequencies of the core-damage sequences defined in the model development; and

HUMAN INTERACTION WORKSHEET: TYPE CR EVENT

EVENT INFORMATION

<i>Name</i>	<i>Definition</i>
ZHA1395R	Failure to isolate service water flow to TPCW when SW1395 fails to close automatically

DESCRIPTION

Some events create a demand for the service-water train initially in secondary service (i.e., supplying cooling flow to the TPCW heat exchangers) to cool its respective CCW heat exchanger. This happens when there is a loss of the primary service water train, the operating CCW train, or an SFAS signal. MOV SW1395 receives an automatic signal to close, isolating service water flow to the TPCW heat exchangers to ensure that adequate cooling is available to the CCW heat exchanger. If SW1395 fails to close, the cooling for the CCW heat exchanger will be degraded.

The procedures require verifying that SW1395 closes (upon SFAS, or when header pressure is below 50 psig), but do not provide specific instructions with respect to actions to be taken in the event that it doesn't close. Discussions with operators indicated that they are trained to attempt to close a manual valve to isolate the line, preferably valve SW46. This is the first valve downstream from SW1395. It is readily accessible in the service water valve room. Estimates are that it would take no more than about 10 minutes to dispatch an equipment operator to close the valve and to ensure that it was closed.

If no service water flow were available to the CCW heat exchanger, the heat exchanger would experience rapid heatup after about an hour. The time should be somewhat longer for this case, since some flow is available. Therefore, the time is taken to be intermediate. There is training (as well as limited procedural guidance) for the action, and the action is simple, performed in a good environment.

QUANTIFICATION

Probability Scale

<u>State</u>	<u>Pr(Non-Rec)</u>
Low	0.01
Mod. low	0.03
Mod. high	0.05
High	0.1
Very high	0.3
Maximal	1

Assessment

<u>Influence Factor</u>	<u>Status</u>
Time (short, intermediate, long)	Intermediate
Training/practice (yes, no)	Yes
Complexity (simple, complex)	Simple
Environment (good, poor)	Good
Qualitative non-recovery factor	MLOW
Non-Recovery Probability	0.03
Assumed error factor	5

Figure 3-4. Example Assessment for a Type CR Human Interaction

Table 3-12
Summary of Type CR Human Interactions

Event Name	Description	Total Time Available	Probability
ZHA1395R	Failure to isolate service water flow to TPCW when SW1395 fails to close automatically	intermediate	0.03
ZHA1399R	Failure to restore service water flow to TPCW by opening SW1399	short	0.1
ZHA4KBUR	Failure to attempt recovery of 4 kv bus following bus fault (2 hr available for action)	intermediate	0.05
ZHABWSTR	Failure to initiate makeup flow to BWST in long term following steam generator tube rupture	long	0.05
ZHACW04R	Failure to realign standby and spare CCW pump trains to supply cooling to both load trains	long	0.03
ZHADCBUR	Failure to attempt recovery of dc bus following bus fault (2 hr available for action)	intermediate	0.05
ZHAISODR	Failure to find and isolate interfacing-systems LOCA resulting from hardware failures of DHR letdown valves DH11 and DH12	long	0.1
ZHAISOHR	Failure to find and isolate interfacing-systems LOCA resulting from resulting from reverse flow through HPI check valves	long	0.03
ZHAISOLR	Failure to find and isolate interfacing-systems LOCA resulting from resulting from reverse flow through LPI check valves	long	0.05
ZHAISOSR	Failure to reclose valves DH11 and/or DH12 to isolate break following premature opening while proceeding to cold shutdown	long	0.03
ZHARSCWR	Failure to restart CCW pump after loss due to spurious high-temperature trip	intermediate	0.03
ZHASFA5R	Failure to initiate SFAS level 5 given common-cause failure of BWST level transmitters	intermediate	0.05
ZHASWVTR	Failure to establish an alternative means of ventilation for the service-water pump room when there is partial (but inadequate) room cooling	intermediate	0.05
ZHATDOFR	Failure to restore at least one turbine-driven pump following loss due to overfeeding steam generator	long	0.05

- To serve as a systematic method to yield additional insight into the impact on core-damage frequency of human reliability, and of particular human interactions.

Some measure of uncertainty in these estimates is needed to permit the characterization of uncertainty in the overall results. Because of the nature of the estimates for the human interactions, a rigorous assessment of uncertainty is neither warranted nor possible. The point estimates themselves are taken to be mean values of a lognormal distribution for input to the uncertainty propagation. The general guidelines presented in NUREG/CR-1278 (Ref. 61) were used to assign error factors for each of the events, after the events were quantified. The guidelines as they were used in this assessment are summarized in Table 3-13.

3.2.3 Review Activities for Assessment of Human Interactions

Effective review was a critical element of each step of the study, and this was no exception for the assessment of human interactions. This assessment was subjected to three types of review, in addition to the overall reviews conducted for each aspect of the study.

Each assessment of a human interaction, together with its application in the sequence modeling and/or quantification process, was reviewed by another member of the project team versed in the methods used. The focus of this review was on ensuring that the applications of the methods were consistent from event to event, and that no mechanical errors were made (e.g., arithmetic errors in the basic calculations).

A second stage of review was made by one or more SROs. In addition to obtaining input regarding the conditions that might affect the assessment of particular human interactions, these SROs reviewed the assessments after they were made. They verified that the events properly characterized anticipated plant and staff response in a qualitative sense, and that any assumptions made were appropriate. Although they did not dwell on the details of the calculations, they did comment on the relative assessment of different human interactions. For example, they pointed out cases in which they felt the probabilities of failure assessed for two interactions to be reversed from the order they would expect based on their perspective on the ease of making the diagnoses and implementing the actions. In such cases, the analyses were re-examined to ensure that all of the pertinent factors had been taken into account.

Finally, a PRA expert not directly involved in the modeling process reviewed the human interaction assessment. This analyst's focus was on the methods and the general manner in which they were used, as well as on the specific applications to the events of interest. This reviewer provided further assurance that the treatments were reasonable and consistent, and also pointed out further areas that might not have been adequately considered.

Table 3-13
Uncertainty Parameters for Human Interactions

Type of Event	Probability Range	Assigned Error Factor
Pre-initiator	≤ 0.001	10
	0.001 to 0.01	3
	> 0.01	5
Post-initiator (type CP)	≤ 0.001	10
	> 0.001	5
Post-initiator (type CR)	(all ≥ 0.01)	5

3.2.4 Summary of Human Interaction Assessment

The assessment of human interactions was accomplished using methods that have been developed relatively recently. These methods enabled potential problems in responding to various upset events (e.g., due to omissions in procedures or other deficiencies) to be investigated. The quantitative results obtained are reasonably consistent among different events, and appear to be reasonable when considered in the context of assessments in other PRAs and for other plants. The procedural guidance available generally appears to be very good; explicit guidance is provided through the procedures and related training to permit effective response to the vast majority of events investigated in the IPE.

EPRI has also developed procedures for assessing the diagnosis and decision-making portions of human interactions based on exercises using plant simulators. The simulator for Davis-Besse became operational well after the IPE was undertaken, and training of licensed operators appropriately occupied the simulator during the period in which data might have been collected to support the IPE. Information was obtained from observing training exercises that was valuable as a qualitative input to the human interaction assessment in such areas as the priorities operators would tend to pursue and the timing of event scenarios. It is expected that, in the future, the assessment of human interactions could be revised to reflect more quantitative data from simulator exercises.

3.3 RECOVERY ANALYSIS

In this study, recovery refers to the ability of the operators to restore a failed safety function by reconfiguring a system, using an alternative system in place of the one that failed, or implementing other compensatory measures. Recovery events were not modeled directly in the sequence event trees or system fault trees. They were identified on a case-by-case basis during the process of examining the sequence cut sets in the quantification stage. Where appropriate, events signifying failure to accomplish these recovery actions were appended to individual sequence cut sets to arrive at the most realistic treatment of the scenarios and their frequencies.

Non-recovery events may be comprised of both human interactions and hardware faults, since they typically refer to the use of equipment that was not included in the basic system models. The human interactions that are part of recovery actions may be of either type CP or type CR, depending on the degree to which the actions are explicitly directed by procedures. As described in the preceding section, the reason for this distinction results from the way in which the human interactions are modeled and quantified.

The line between recovery events and other events involving human interactions can sometimes be a fine one. It should be borne in mind that the most important difference is a practical matter of whether or not the affected equipment and associated human interactions are modeled explicitly in the system and sequence logic, or incorporated during the quantification process. In each case in this study, a decision had to be made as to whether to incorporate an option for accomplishing a safety function directly in the logic models or to

treat it as a potential recovery. In making this decision, it was necessary to attempt to strike a balance between the desire to be comprehensive in modeling the plant, and the need to limit the size and complexity of the models so that they could be accommodated in the quantification process. Normal systems and the backups to them most likely to be used in an accident situation were usually included in the models. Further backups, and the use of alternatives, were reserved to be treated as potential recovery options. Thus, recovery needed to be examined only for the most important sequences as determined in the quantification process.

The nature of recovery events can be further clarified through a set of examples. The AFW system at Davis-Besse consists of two turbine-driven pumps that are automatically actuated to supply backup feedwater to the steam generators, and a motor-driven pump that is available for manual actuation if either of the turbine-driven pumps fails. The emergency procedure provides clear and direct instruction with respect to when and how to start the motor-driven pump. The failure modes for the pump itself, along with the human interaction representing failure to start the pump, were included in the fault-tree model for the AFW system, not treated as a recovery option. This human interaction was of type CP.

If no feedwater flow were available, the emergency procedure directs that attempts be made to restore flow by use of the main feedwater system, the AFW pumps, the motor-driven pump, or the startup feed pump. The procedure does not provide explicit direction for regaining flow; additional guidance is provided in the operating procedures for these systems, but they cannot anticipate every possible cause of the loss of flow. Restoring flow from, for instance, the startup feed pump is a potential recovery action. Depending on the situation, there may or may not be some further procedural guidance for establishing flow. In any event, this restoration is a recovery action because it involves considering the use of equipment beyond that explicitly included in the logic models. Both the unavailability of the equipment needed to effect recovery and the human interactions that come into play in using it must be assessed as part of the non-recovery event.

3.3.1 Identification of Recovery Actions

Recovery actions were identified beginning with the initial integration and quantification of the core-damage sequences. Individual sequence-level cut sets were examined to assure that they were logically correct, to establish the context to permit quantification of any human interactions they contained, and to assess the potential for the operators to prevent core damage by taking recovery action. A first attempt was made to identify potential recovery actions by the analysts. In most cases, recovery options were readily identified by continuing to follow the relevant operating procedures down the path represented by the sequence cut sets. Where it was unclear what subsequent steps the operators might be expected to take, one or more SROs were interviewed to determine the most likely course of action. Other actions postulated by the analysts were also confirmed with these SROs. A conscious effort was made to avoid the tendency PRA analysts

sometimes have to postulate all manner of recovery actions, without full regard to their feasibility or to whether or not the operators might be likely to attempt them.

In identifying the recovery actions, several factors were taken into account, aside from those that directly influence the probability of success (e.g., time available, existence and clarity of procedures, quality and availability of control indications, etc.). First, and most importantly, the implications of the sequence cut set had to be clearly understood. For example, if the cut set included an event representing failure of an electrical bus that might be needed to make use of a recovery option, that recovery option was not available. If the cut set contained an event indicating common-cause failure of a set of motor-operated valves, and an equivalent motor-operated valve was required to function for the recovery action to succeed, the conditional unavailability of the valve given the common-cause failure would have to be taken into account.

A second consideration is the availability of personnel to accomplish the actions, especially if they require activities outside the main control room. Implicit or explicit to the scenario is the possibility that certain activities are underway that could deprive the operating staff of control room or equipment operators who could attempt the recovery actions. If sufficient personnel cannot be made available in time to perform the recovery, then it is not possible.

A third aspect that must be taken into account is the possibility that attempted or successful recovery could introduce further potential for undesired events. For example, attempts to start emergency diesel generators that had failed could lead to more rapid depletion of the station batteries, limiting the time available for restoration of offsite power. Similarly, isolation of a flood from the service water system might stop the flood from affecting some equipment, but could lead to a loss of cooling for other equipment. Recovery of a sequence also provides the opportunity for subsequent failures to arise that would have been precluded had the recovery failed. For example, consider the case of a loss of CCW flow that leads to a LOCA due to failure of the seals for the RCPs. In the modeling of such a sequence, high pressure injection would fail due to its dependence on CCW for pump cooling. If an alternative means of cooling the pumps could be devised, failure of injection could be prevented. If this recovery action were successful, it introduces the possibility of other sequences, such as the failure of long-term cooling, which relies on CCW for removal of heat from the decay heat coolers. Because the model implicitly assumed the injection phase would fail for a loss of CCW, the long-term recirculation phase would not have been given the chance to fail. Recovery of the injection phase would, however, make it necessary to consider possible failures in recirculation.

Thus, all of these factors were taken into account in assessing the possibility of recovery actions. Once the recovery action was identified, the equivalent of a small fault tree was constructed to represent its failure. These fault trees include the component failures, maintenance events, and human interactions relevant to the recovery measure, just as if the recovery had been included in the original plant models. Individual events in the non-recovery

tree, including the human interactions, were then assessed to ensure that any dependence on the events in the sequence cut sets was properly characterized.

3.3.2 Quantification of Non-Recovery Events

The quantification of events representing failure to perform recovery actions was generally a straightforward integration of the component-level data and the human interactions. The latter were assessed as described in Section 3.2 (for either type CP or CR interactions). The non-recovery events are, in effect, analogous to the modules used in aggregating failures in the system fault trees.

As an example, consider the failure to restore service water, given the loss of flow from both normally-operating service-water pumps due to common-cause failure of the pumps to run. In this case, recovery may be accomplished by using either the third (standby) service-water pump or the backup service water pump (also referred to at Davis-Besse as the dilution pump). A Boolean equation for this non-recovery event (designated as event ZMMSW02R) is provided in Table 3-14, with a description of each of the failures that make up the event.

The events themselves are also summarized in Table 3-14. In this example, the non-recovery event is made up of both hardware failures and human interactions. Note that there are two human interactions (referring to failure to use the standby service-water pump and failure to use the backup pump), both of which were assessed as type CP interactions due to the explicit procedural guidance associated with them. A third event is used to represent the combination of these interactions, reflecting the dependence between them. It is interesting to note that in this case, as in many others, the probability of non-recovery is dominated by hardware faults: 85% of the overall probability is due to hardware faults alone. Such recovery events tend to be relatively insensitive to the specific nature of the treatment of the human interactions.

In a few cases, generic data for non-recovery of particular types of components or systems was applied directly. This data was taken from a broad review of industry-wide operating experience (Ref. 68). In a small number of additional cases, the non-recovery events reflected the failure to restore a component that was unavailable because it was in maintenance at the start of the accident. In these cases, the non-recovery probability was estimated based on an exponential time-to-repair model, based on the mean repair time suggested by the development of the maintenance unavailabilities.

A separate category of recovery events involved the restoration of offsite power. As industry operating experience was evaluated with respect to the frequency of losses of offsite power, the time required to recover power was also identified for each event for which it was available. The losses of offsite power were categorized according to whether they were plant-centered (e.g., resulted from failure of an auxiliary transformer), grid-centered (involving loss of feed to the switchyard), or weather-related. For each category, the recovery times were assembled and distributions of time to recovery were developed. The three resulting

Table 3-14
Failures Comprising Example Non-Recovery Event

Event	Description	Type	Probability
ZMMSW02R =	(ZHASW02E + SMMSBSWN + SMP01CCF) * SMMSBWP + (SMMSBSWN + SMP01CCF) * ZHASW01E + ZHAC006E		1.1×10^{-2}
ZHASW02E	Failure to recover service water using standby service water pump	human inter. (type CP)	1.7×10^{-3}
SMMSBSWN	Standby service water pump train not available due to independent faults (strainer operation not required)	hardware (module)	5.7×10^{-2}
SMP01CCF	Common-cause failure of standby service water pump to run, given failure of normally-operating pumps to run	hardware (basic event)	1.1×10^{-1}
SMMSBWP	Backup service water (dilution) pump not available to supply service water flow	hardware (module)	5.8×10^{-2}
ZHASW01E	Failure to accomplish recovery of service water via use of the backup service water pump	human inter. (type CP)	3.9×10^{-3}
ZHAC116E	Failure to recover service water when both standby pump and backup pump are options (combination of ZHASW02E and ZHASW01E)	combination of human inter. (both type CP)	8.5×10^{-4}

distributions were then weighted by the relative frequencies of the three types of power loss to form a composite distribution for offsite power recovery.

In assessing the non-recovery probability for each cut set involving loss of offsite power, it was necessary to take into account any time-dependent failures in the cut set. For example, if the cut set included the failure of a diesel generator to run after starting at some point over the nominal 24-hr mission time, the probability of non-recovery of power would depend on when the failure occurred. This was accommodated by breaking down the mission into discrete intervals that permitted the recovery distribution to be combined with the time-dependent failures. Because there are two emergency diesel generators, a separate station blackout diesel generator (with a nominal six-hour supply of fuel, indicating a mission time different from that for the other generators), and two turbine-driven AFW pumps, a large number of different time-dependent recovery cases was identified. Each case was carefully considered to ensure that limiting factors relating to recovery (e.g., the need for dc power to permit closing of bus-tie breakers) were accounted for properly. The non-recovery distribution is illustrated in Figure 3-5.

The non-recovery events used in this assessment (other than those relating to the restoration of offsite power) are summarized in Table 3-15. A nominal breakdown indicating the relative contribution of human interactions and hardware faults is provided for perspective. It should also be noted that only one non-recovery event was applied to any particular cut set, with the exception that recovery of offsite power was treated as independent of other actions (consistent with usual practice in PRA). Dependencies among human interactions associated with non-recovery events were assessed in the same manner as for any other combinations of human interactions.

3.4 QUANTIFICATION OF SEQUENCE FREQUENCIES

Once the integrated model was developed and the reliability data base was assembled, they were used to assess the frequencies of the core-damage sequences. Quantification of these frequencies entailed the following three major steps:

- Computer solution of the integrated event-tree and fault-tree models for each core-damage sequence. These solutions produce a listing of the combinations of events in terms of the initiating events, hardware faults, and human interactions that comprise the core-damage sequences. Each of these combinations of basic events is referred to as a minimal cut set.
- Review and iteration of the computer solution process to obtain final cut sets to eliminate any inconsistencies and excessive conservatisms. Iteration was required because the fault trees represent snapshots of the systems in time, and when they were all integrated, some inconsistencies arose that needed to be addressed directly. Furthermore, as the fault trees were constructed, conservative, simplifying assumptions were sometimes made in areas that were not expected to be important to the results. Some of these conservatisms implied erroneous, large contributors, so that more realistic modeling was required.

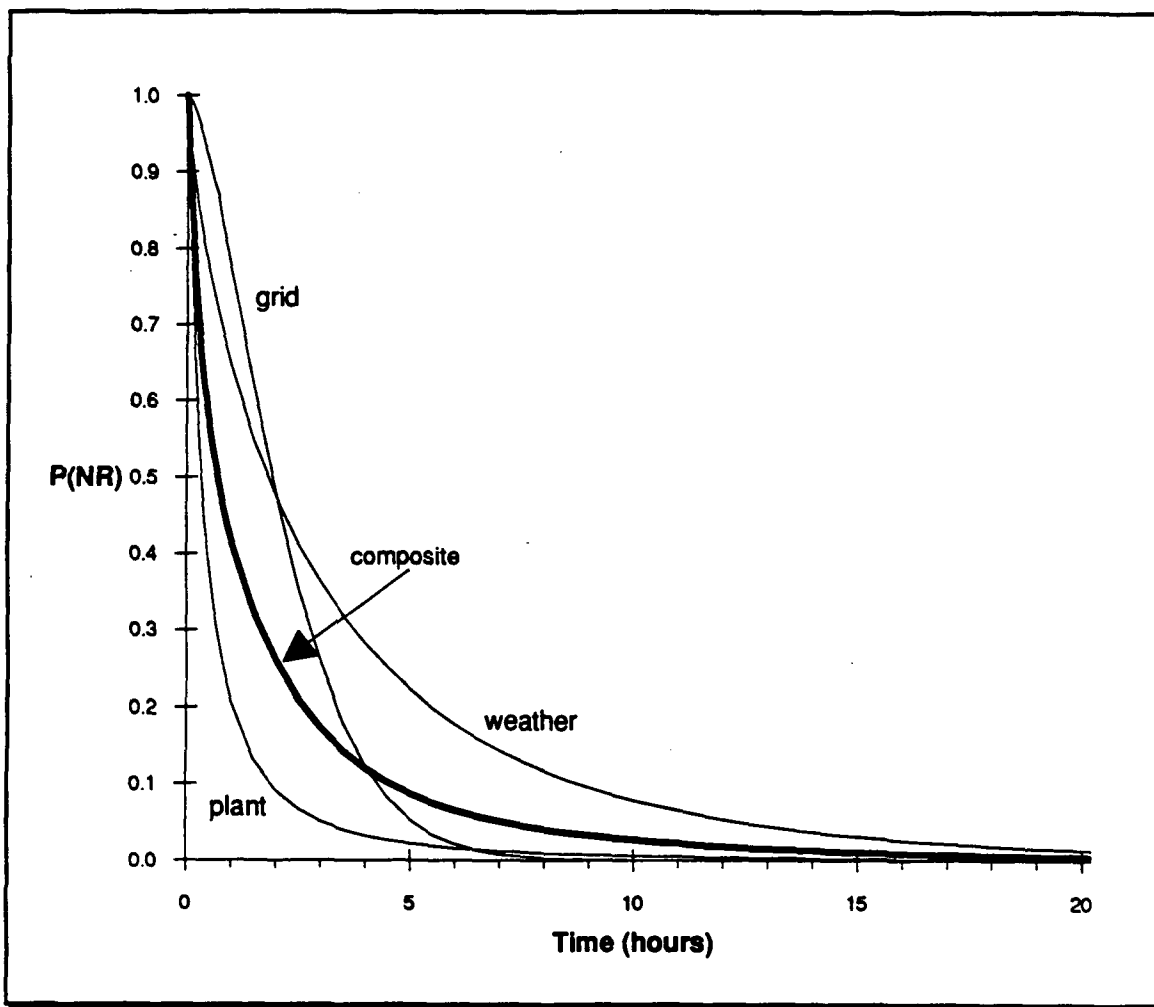


Figure 3-5. Distributions for Non-Recovery of Offsite Power

Table 3-15 (continued)
Summary of Non-Recovery Events

Event Name	Description	Hardware	Human	Prob.
ZMMSW09R	Failure to recover service water flow to train 2 by swapping over pump 3 after loss of CCW train 1 and failure of service water train 2	46%	54%	5.2×10^{-3}
ZMMSW10R	Failure to restore service water flow to TPCW by opening valve SW1399 after loss of normally operating CCW train and switchover to standby train	60%	40%	1.2×10^{-1}
ZMM1395R	Failure to preserve adequate service water flow for CCW when SW1395 fails to close to isolate flow to TPCW	3%	97%	3.1×10^{-2}
ZMMSWPRR	Failure to restore flow to primary service water train via backup or standby pump following failure of the primary service water pump (strainer operation not required)	80%	20%	4.1×10^{-3}
ZMMTDOFR	Failure to recover at least one turbine-driven AFW pump following loss due to overfeeding steam generator (using steam from auxiliary boiler)	57%	43%	1.2×10^{-1}
ZMM4KBUR	Failure to recover power from 4 kV bus after bus fault with at least two hours available	78%	26%	1.9×10^{-1}
ZMMDCBUR	Failure to recover power from dc bus after bus fault with at least two hours available	78%	26%	1.9×10^{-1}
ZMMTDBUR	Failure to recover power from 4 kV bus after bus fault and failure to restore flow from AFW pumps after loss due to overfeeding steam generator (combination of ZMMTDOFR and ZMM4KBUR, with human interactions treated as completely dependent)	16%	84%	5.9×10^{-2}
ZMMMDFPR	Failure to restore motor-driven feed pump from maintenance status, given long time available prior to need for AFW flow	(based on mean time to repair from maintenance data)		1.5×10^{-1}
ZMMMDF2R	Failure to recover motor-driven feed pump after failure to start, given at least two hours to recover pump	(based on generic recovery experience)		2.2×10^{-1}

Table 3-15
Summary of Non-Recovery Events

Event Name	Description	Hardware	Human	Prob.
ZMMCW01R	Failure to recover CCW via spare pump following (independent) failure of the normally operating and spare pumps	73%	27%	2.0×10^{-2}
ZMMCW02R	Failure to recover CCW via spare pump following common-cause failure to run of the normally operating and spare pumps	94%	6%	9.5×10^{-2}
ZMMCW03R	Failure to recover CCW via spare pump following common-cause failure to start of the normally operating and spare pumps	99%	1%	5.1×10^{-1}
ZMMCW04R	Failure to realign standby and spare CCW pumps to supply both trains of CCW loads	41%	59%	5.1×10^{-2}
ZMMSW01R	Failure to establish service water flow from the backup service water pump when normal pumps are unavailable	97%	3%	5.9×10^{-2}
ZMMSW02R	Failure to restore service water from the standby or backup pump given common-cause failure of the normally-operating pumps to run	91%	1%	1.0×10^{-2}
ZMMSW03R	Failure to restore service water from the standby or backup pump given common-cause failure of the service-water strainers to run	96%	4%	3.6×10^{-2}
ZMMSW04R	Failure to restore service water from the standby or backup pump following loss of the primary train, given strainer operation required	92%	8%	1.3×10^{-2}
ZMMSW05R	Failure to recover service water flow to train 2 by using backup pump after loss of CCW train 1 and failure of all normal service water pumps	98%	2%	6.2×10^{-2}
ZMMSW06R	Failure to restore service water from the standby or backup pump given common-cause failure of the normally operating pumps to restart after loss of offsite power (including failure to restore offsite power for backup pump)	99%	1%	1.4×10^{-1}
ZMMSW07R	Failure to restore service water from the backup pump after loss of offsite power and failure of all three normal service water pumps (including failure to restore offsite power)	99%	1%	2.6×10^{-1}
ZMMSW08R	Failure to restore primary service water flow via standby pump following failure of the primary pump (strainer operation not required)	98%	2%	5.8×10^{-2}

- Examination of human interactions and recovery options for each cut set. When the computer solution was performed, the probabilities associated with operator actions following an initiating event were set to 1.0. This was done rather than inputting the best-estimate probabilities so that combinations of human interactions, which may be inter-dependent, were not predicted to have unrealistically low probabilities. It also afforded the opportunity to ensure that the analysis of the human interactions accounted for the specific context of the cut set (e.g., the timing of other failures, the availability of power and control signals, etc.). At the same time, options that the operators might be able to implement to recover from the sequence to prevent core damage, but that were not necessarily included in the models, were identified and evaluated.

In constructing the model used to quantify the core-damage sequences, the first step was to define each of the sequences from the event trees in terms of fault-tree logic. This was done by forming an "AND" gate of all of the failures implied in the sequence. For example, a sequence involving a small LOCA followed by failure of heat removal via the steam generators and failure of safety injection (sequence $SB_S U_S$ from the small LOCA event tree) would be defined as an "AND" gate with the following inputs:

- A basic event representing the LOCA initiator (event S),
- The gate corresponding to the top logic for event B_S (gate BS01), and
- The gate corresponding to the top logic for event U_S given failure of heat removal (gate US11).

The computer file containing the logic for these top events was then integrated with the files containing the logic for all of the individual systems to produce a single master logic file. The integrated fault trees corresponding to each of the core-damage sequences were then solved for their minimal cut sets using the quantification module of the CAFTA PRA workstation (Ref. 69).

Considerations of applicable initiating events, different equipment configurations possible during various SFAS states, and unusual timing considerations were specifically taken into account through the use of basic events signifying flags. These flags could be set as logically true or false, depending on the sequence of interest, thereby acting as switches to include or exclude relevant portions of the logic. For example, in the event of a LOCA, a.n SFAS level 3 actuation (on high containment pressure or low-low RCS pressure) would initiate LPI and isolate the non-essential portions of the CCW system. For these sequences, the appropriate flags were set to true, leading directly to implied unavailability of cooling for the non-essential CCW loads. Similarly, if conditions did not warrant a.n SFAS level 3 actuation, the appropriate flags were set to false, and the CCW system model was not reconfigured.

Many of the core-damage sequences include implied success of some safety functions. For example, in the case of a small LOCA with core damage due to failure of recirculation, successful safety injection is implied. The solution of the integrated model to obtain cut sets would not be practicable if the solution included the complement of the top event representing

failure of injection. Instead, the solution was performed with only the top events that were unsuccessful input. A post-solution step then involved the application of a routine that compared the cut sets for the function or functions whose success was implied to the initial sequence sets. Any cut sets in the sequence solution that were super-sets of those for which success was implied were automatically deleted.

To obtain the sequence cut sets, it was also necessary to use a lower truncation value for the cut set frequencies. For nearly all solutions, a truncation value no higher than 10^{-9} was applied. In the case of the sequence involving a transient with loss of all feedwater and failure of makeup/HPI cooling, there was such a large number of cut sets that it became necessary to use a higher truncation value of 10^{-8} . Even with this truncation limit, the sequence had on the order of 14,000 cut sets that required further review. Tests were performed for important sequences to ensure that non-negligible contributions to the sequence frequencies were not missed due to the application of the truncation limits.

The next step was that of review of the results and iteration. This has two principal objectives: it provides assurance that the results are consistent with the models and data (i.e., there are no errors in the solution process itself), and it allows a final verification that the results reflect the best available understanding of the actual behavior of the plant. The latter objective is a key to the risk analysis; its importance stems from the necessity for making a number of assumptions in order to model the system fault trees.

The final step in the quantification process was the consideration of human interactions in a sequence-specific context. As described in Section 3.2, the post-initiator human interactions were initially assigned values of 1.0 to ensure that important combinations of events were not overlooked. For all of the post-initiator interactions that surfaced in important sequence cut sets, a specific evaluation was made. Opportunities for recovery were also identified during this process. Where appropriate, recovery events were defined conditional on the specific elements of the cut sets, and were added to produce the final cut-set frequencies.

After the initial quantification, which was based on the use of mean values as point estimates for all basic events, an uncertainty analysis was performed. This analysis entailed the propagation of the probability distributions representing data uncertainties for all of the basic events (initiating events, component unavailabilities, and human interactions). The uncertainty analysis involved a Monte Carlo simulation, performed using the UNCERT computer code (Ref. 70). The UNCERT code is a module of the CAFTA workstation.

Despite the numerous and significant sources of uncertainty in PRA results, the qualitative and quantitative results provide very useful information for assessing the strengths and the weaknesses in the plant's capability to respond to abnormal conditions. While it is important to note the uncertainties in the PRA, it is imperative to keep in mind the valuable insights it provides. Insights gained from the PRA can be integrated with other design and deterministic evaluations to make decisions regarding plant modifications and procedure changes as well as operator training enhancements.

Section 4 RESULTS AND SCREENING PROCESS

The preceding sections describe the development of potential core-damage sequences, the modeling of the systems that could play a role in those sequences, and the application of reliability data to permit quantification of the frequencies of the sequences. The results of the quantification process are described in this section. The section focuses first on the estimated frequencies of the core-damage sequences, then addresses the insights from the analyses that might indicate the existence of vulnerabilities for the plant. A discussion of the results relevant to the issue of the overall reliability of the decay heat removal function is then provided as requested by Generic Letter 88-20. Finally, the results and insights are applied to address certain safety issues that have not previously been resolved.

4.1 SUMMARY OF SEQUENCE FREQUENCIES

Table 4-1 summarizes all of the core-damage sequences quantified in this assessment and their annual frequencies. For each sequence, the core-damage bin to which it was assigned is also provided. As the table indicates, the core-damage frequency for Davis-Besse was assessed to be dominated by two sequences, both of which are initiated by transient events. LOCAs and internal floods are smaller contributors. The sequences that are important to the results are described in Section 4.1.1.

A sensitivity study was also performed to identify those sequences whose frequencies would have been above 10^{-6} if the human interactions included in them were postulated to be less reliable than assessed in the study. The results of this sensitivity study are described in Section 4.1.2.

The frequencies of the core-damage bins are summarized in Table 4-2. Included in this tabulation are ranges assessed based on the propagation of data uncertainties.

4.1.1 Summary of Contributing Core-Damage Sequences

As requested by Generic Letter 88-20 (Ref. 71), all sequences with frequencies higher than 10^{-6} per year are described below, as are all sequences that were assessed to have frequencies greater than 10^{-7} per year and that would constitute a bypass of containment. These sequences comprise more than 95% of the core-damage frequency estimated for Davis-Besse, so the additional criterion requiring reporting of all sequences contributing at least 5% to the core-damage frequency is also met. The sequences are discussed below in descending order of frequency.

For each of these sequences, a general description of the types of failures that were found to be most important is provided. The sequence cut sets contain substantially more detail regarding the dominant contributors; they are available in the project files.

**Table 4-1
Summary of Core-Damage Frequencies**

Core-Damage Sequence	Description	Core-Damage Bin	Annual Frequency
<u>Large and Medium LOCAs</u>			
MX _M	Medium LOCA initiating event with failure of low pressure recirculation	MRX	1.6 x 10 ⁻⁶
AX _A	Large LOCA initiating event with failure of low pressure recirculation	ARX	8.7 x 10 ⁻⁷
MU _M	Medium LOCA initiating event with failure of high or low pressure injection	MIX	4.6 x 10 ⁻⁷
AV	Reactor vessel rupture initiating event	ARX	4.6 x 10 ⁻⁷
AU _A	Large LOCA initiating event with failure of low pressure injection	AIX	2.1 x 10 ⁻⁷
Total core-damage frequency for large and medium LOCAs			3.6 x 10 ⁻⁶
<u>Small LOCAs</u>			
SX _S	Small LOCA initiating event with failure of long-term cooling via DHR or recirculation from sump	SRY	1.5 x 10 ⁻⁶
SU _S	Small LOCA initiating event with failure of injection	SIY	5.9 x 10 ⁻⁷
SB _S U _S	Small LOCA initiating event with failure of feedwater and failure of makeup/HPI cooling	SIN	3.8 x 10 ⁻⁸
SB _S X _S	Small LOCA initiating event with failure of feedwater and failure of high pressure recirculation	SRN	< 10 ⁻⁸
Total core-damage frequency for small LOCAs			2.1 x 10 ⁻⁶
<u>Steam Generator Tube Ruptures</u>			
RIP _R	SGTR with failure to isolate ruptured generator, failure to control RCS pressure to reach low pressure	RRY	1.9 x 10 ⁻⁷
RC _U I	SGTR with failure to isolate ruptured steam generator, failure to cool down using unaffected steam generator	RRY	(included above)
RB _U I	SGTR with failure to isolate ruptured steam generator, failure to provide feedwater to unaffected generator	RRY	(included above)
RC _R IP _R	SGTR with failure to cool down via ruptured generator, failure to isolate that generator, and failure to control RCS pressure to reach low pressure conditions	RRY	(included above)
RC _R CU _I	SGTR with failure to cool down using either steam generator and failure to isolate the ruptured generator	RRY	(included above)
RC _R BU _I	SGTR with failure to cool down using the ruptured steam generator, failure to isolate that generator, and failure of feedwater to the unaffected generator	RRY	(included above)

Table 4-1 (continued)
Summary of Core-Damage Frequencies

Core-Damage Sequence	Description	Core-Damage Bin	Annual Frequency
<u>Steam Generator Tube Ruptures (continued)</u>			
RBU _{BR}	SGTR with failure of feedwater to both steam generators, successful makeup/HPI cooling, but failure to restore feedwater to achieve long-term cooling	RRN	1.1 x 10 ⁻⁷
RBU _{BR} I	SGTR with failure of feedwater to both steam generators and failure to isolate the ruptured generator	RRN	(included above)
RC _R BU _{BR}	SGTR with failure to cool down using the ruptured steam generator, failure of feedwater to both steam generators, successful makeup/HPI cooling, but failure to restore feedwater to achieve long-term cooling	RRN	(included above)
RC _R BU _{BR} I	SGTR with failure to cool down using the ruptured steam generator, failure of feedwater to both steam generators and failure to isolate the ruptured generator	RRN	(included above)
RCU _X R	SGTR with failure of cooldown via unaffected steam generator, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation	SRY	1.1 x 10 ⁻⁷
RBUX _R	SGTR with failure of feedwater to unaffected steam generator, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation	SRY	(included above)
RC _R CU _X R	SGTR with failure of cooldown by both steam generators, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation	SRY	(included above)
RC _R BU _X R	SGTR with failure of cooldown by ruptured steam generator, failure of feedwater to unaffected steam generator, successful initiation of cooldown via makeup/HPI cooling, but failure of recirculation	SRY	(included above)
RBU _{BR} U _R	SGTR with failure of feedwater to both steam generators and failure of makeup/HPI cooling	RIN	4.2 x 10 ⁻⁸
RC _R BU _{BR} U _R	SGTR with cooldown via ruptured steam generator not available, failure of feedwater to both steam generators, and failure of makeup/HPI cooling	RIN	(included above)
RU _R I	SGTR with failure of injection and failure to isolate generator containing ruptured tube	RIY	< 10 ⁻⁸
RCU _U R	SGTR with failure of cooldown via unaffected steam generator, failure of injection for cooldown via makeup/HPI cooling	RIY	(included above)
RBU _U R	SGTR with failure of feedwater to unaffected steam generator, failure of injection for cooldown via makeup/HPI cooling	RIY	(included above)

**Table 4-1 (continued)
Summary of Core-Damage Frequencies**

Core-Damage Sequence	Description	Core-Damage Bin	Annual Frequency
<u>Steam Generator Tube Ruptures (continued)</u>			
RCRURI	SGTR with failure of cooldown via ruptured generator, failure to isolate that generator, and failure of injection	RIY	(included above)
RCRCUUR	SGTR with failure of cooldown using either steam generator and failure of injection	RIY	(included above)
RCRBUUR	SGTR with failure of cooldown using ruptured steam generator, failure of feedwater to unaffected steam generator, and failure of injection	RIY	(included above)
Total core-damage frequency for SGTRs			4.6×10^{-7}
<u>Interfacing-Systems LOCAs</u>			
V _D ID	Interfacing-systems LOCA due to hardware failure of DHR suction valves, failure to isolate break	V	9.1×10^{-8}
V _L IL	Interfacing-systems LOCA due to failure in LPI injection line, failure to isolate break	V	1.7×10^{-7}
V _S IS	Interfacing-systems LOCA due to premature opening of DHR suction valves, failure to isolate break	V	5.6×10^{-7}
V _H IH	Interfacing-systems LOCA due to failure in HPI injection line, failure to isolate break	V	6.4×10^{-8}
Total core-damage frequency for interfacing-systems LOCAs			8.8×10^{-7}

Table 4-1 (continued)
Summary of Core-Damage Frequencies

Core-Damage Sequence	Description	Core-Damage Bin	Annual Frequency
Transients			
TB _T U _T	Transient initiating event with total loss of feedwater and failure of makeup/HPI cooling	TIN	3.5 x 10 ⁻⁵
TQU _T	Transient initiating event with RCP seal LOCA and failure of injection	SIY	1.4 x 10 ⁻⁵
TQX _T	Transient with RCP seal LOCA and failure of long-term cooling	SRY	4.3 x 10 ⁻⁶
TB _T QU _T	Transient initiating event with total loss of feedwater, RCP seal LOCA or stuck-open relief valve, and failure of makeup/HPI cooling	SIN	2.9 x 10 ⁻⁶
TB _T LX _T	Transient with extended total loss of feedwater and failure of high pressure recirculation	TRN	3.2 x 10 ⁻⁷
TB _T QX _T	Transient initiating event with total loss of feedwater early, successful makeup/HPI cooling, stuck-open relief valve or RCP seal LOCA, and failure of HPR	SRN	2.9 x 10 ⁻⁷
TK ₁ BP _K	Transient with failure to trip, loss of main feedwater, and excessive RCS pressure	AIX	1.7 x 10 ⁻⁷
TK ₁ BK ₂	Transient with failure to trip, loss of main feedwater, and failure to provide borated makeup	TIY	1.6 x 10 ⁻⁷
TK ₁ BL	Transient with failure to trip and total loss of feedwater	AIX	2.4 x 10 ⁻⁸
TB _T WX _T	Transient with initial loss of feedwater, successful makeup/HPI cooling, stuck-open relief valve when feedwater is restored, and failure of HPR	SRY	< 10 ⁻⁸
TB _T P	Transient initiating event with total loss of feedwater and failure of pressurizer relief valves to open	TIN	< 10 ⁻⁸
Total core-damage frequency for transient initiators			5.7 x 10⁻⁵

**Table 4-1 (continued)
Summary of Core-Damage Frequencies**

Core-Damage Sequence	Description	Core-Damage Bin	Annual Frequency
Internal Floods			
FQU _T	Internal flood with RCP seal LOCA and failure of injection	SIY	1.9 x 10 ⁻⁶
FB _T U _T	Internal flood with total loss of feedwater and failure of makeup/HPI cooling	TIN	3.9 x 10 ⁻⁸
FQX _T	Internal flood with RCP seal LOCA and failure of long-term cooling	SRY	1.2 x 10 ⁻⁸
FQU _T	Internal flood with RCP seal LOCA and failure of injection	SIY	1.9 x 10 ⁻⁶
FB _T U _T	Internal flood with total loss of feedwater and failure of makeup/HPI cooling	TIN	3.9 x 10 ⁻⁸
FQX _T	Internal flood with RCP seal LOCA and failure of long-term cooling	SRY	1.2 x 10 ⁻⁸
FB _T QU _T	Internal flood with total loss of feedwater, RCP seal LOCA or stuck-open relief valve, and failure of makeup/HPI cooling	SIN	< 10 ⁻⁸
FB _T LX _T	Internal flood with extended total loss of feedwater and failure of high pressure recirculation	TRN	< 10 ⁻⁸
FB _T QX _T	Internal flood with total loss of feedwater early, successful makeup/HPI cooling, stuck-open relief valve or RCP seal LOCA, and failure of high pressure recirculation	SRN	< 10 ⁻⁸
FB _T WX _T	Internal flood with total loss of feedwater early, successful makeup/HPI cooling, stuck-open relief valve when feedwater is restored, and failure of high pressure recirculation	SRY	< 10 ⁻⁸
FB _T P	Internal flood with total loss of feedwater and failure of pressurizer relief valves to open	TIN	< 10 ⁻⁸
Total core-damage frequency for internal floods			2.0 x 10 ⁻⁶
Total for all initiating events			6.6 x 10 ⁻⁵

Table 4-2
Summary of Frequencies for Core-Damage Bins

Bin	Description	Nominal Frequency	5th Percentile	Median	Mean	95th Percentile
AIX	Large LOCA, failure of injection	4.0×10^{-7}	2.5×10^{-7}	3.0×10^{-7}	3.2×10^{-7}	4.3×10^{-7}
ARX	Large LOCA, failure of recirculation	8.7×10^{-7}	2.7×10^{-7}	6.4×10^{-7}	9.2×10^{-7}	2.6×10^{-6}
MIX	Medium LOCA, failure of injection	4.6×10^{-7}	3.0×10^{-7}	4.5×10^{-7}	4.7×10^{-7}	7.2×10^{-7}
MRX	Medium LOCA, failure of recirculation	1.6×10^{-6}	4.7×10^{-7}	1.1×10^{-6}	1.6×10^{-6}	4.5×10^{-6}
SIY	Small LOCA, failure of injection, with feedwater	1.7×10^{-5}	6.8×10^{-6}	1.4×10^{-5}	1.7×10^{-5}	3.4×10^{-5}
SRY	Small LOCA, failure of recirculation with feedwater	5.9×10^{-6}	2.0×10^{-6}	4.4×10^{-6}	5.9×10^{-6}	1.5×10^{-5}
SIN	Small LOCA, failure of injection, without feedwater	2.8×10^{-6}	5.7×10^{-7}	1.9×10^{-6}	3.3×10^{-6}	9.7×10^{-6}
SRN	Small LOCA, failure of recirculation w/o feedwater	2.9×10^{-7}	4.2×10^{-8}	1.7×10^{-7}	2.8×10^{-7}	8.5×10^{-7}
RIY	Bypass due to SGTR, failure of injection with feedwater	8.0×10^{-9}	3.1×10^{-9}	8.1×10^{-9}	9.9×10^{-9}	2.2×10^{-8}
RIN	Bypass due to SGTR, failure of injection without feedwater	4.2×10^{-8}	5.0×10^{-9}	2.5×10^{-8}	6.3×10^{-8}	1.9×10^{-7}
RRY	Bypass due to SGTR, failure of recirculation w/ feedwater	1.9×10^{-7}	3.3×10^{-8}	1.2×10^{-7}	1.8×10^{-7}	5.4×10^{-7}
RRN	Bypass due to SGTR, failure of recirculation w/o feedwater	1.1×10^{-7}	2.7×10^{-8}	9.5×10^{-8}	1.9×10^{-7}	5.3×10^{-7}
V	Bypass due to interfacing-systems LOCA	8.8×10^{-7}	2.0×10^{-8}	1.9×10^{-7}	5.2×10^{-7}	2.0×10^{-6}
TIN	Transient without feedwater, failure of injection	3.5×10^{-5}	9.8×10^{-6}	2.8×10^{-5}	4.4×10^{-5}	1.2×10^{-4}
TRN	Transient without feedwater, failure of recirculation	3.2×10^{-7}	7.3×10^{-8}	2.2×10^{-7}	5.1×10^{-7}	1.4×10^{-6}

Sequence TB_TU_T

Sequence TB_TU_T involves a transient initiating event with failure of decay heat removal via the steam generators and failure of makeup/HPI cooling. With an estimated frequency of 3.5×10^{-5} per year, this sequence accounts for about 54% of the total core-damage frequency.

Although this sequence, when defined at a functional level, is responsible for a large fraction of the total core-damage frequency, an examination of the cut sets that make up its frequency indicates that it is not dominated by one or a few initiating events, system faults, or other plant features. Rather, the frequency results from a large number of different features, as discussed below, each contributing a relatively small amount.

In the event of a loss of main feedwater, the two turbine-driven AFW pumps would be actuated automatically. If either or both of these pumps were to fail, emergency procedures call for starting the standby motor-driven feed pump. If no feedwater were available, procedures direct the operators to initiate makeup/HPI cooling to provide decay heat removal when RCS temperature exceeded 600F, irrespective of attempts to regain feedwater. It should be noted that the procedures have been clarified and training modified since the loss-of-feedwater event that occurred June 9, 1985, to provide added assurance that makeup/HPI cooling would be initiated when needed. If no feedwater were available and makeup/HPI cooling were not established, relatively early core damage at high RCS pressure could result.

The overall frequency for sequence TB_TU_T is comprised of a very large number of cut sets that reflect various scenarios that could all lead to a total loss of heat removal following a transient initiator. Among the types of scenarios that were found to contribute are the following:

- Loss of main feedwater (as the direct result of an initiating event or due to system faults following an initiator), followed by failure of the two turbine-driven AFW pumps (independently or due to a common-cause), with failure of the operators to actuate the motor-driven feed pump and to initiate makeup/HPI cooling.
- An extended loss of offsite power with failure of the emergency diesel generators and the station blackout diesel generator, leading to eventual depletion of the batteries and failure of control power for the turbine-driven AFW pumps. If the operators were unable to control the turbine-driven AFW pumps to preserve flow to the steam generators, a total loss of heat removal would result since, without ac power, use of the motor-driven feed pump or establishment of makeup/HPI cooling would not be viable options.
- Loss of a dc power bus, or loss of dc power following another initiating event, leading to loss of control power for one train of the turbine-driven AFW pumps. If the operators were unable to control flow for the affected train, the associated steam generator could be overfilled, possibly leading to carryover of water to both turbines (the steam supplies would usually be cross-connected automatically after system actuation). Depending on which train of dc power was lost, the ability to start the motor-driven feed pump could be affected directly, or the pump could be unavailable. The

loss of one train of dc power would also reduce the number of configurations that would otherwise be available for makeup/HPI cooling.

Sequence TQU_T

Sequence TQU_T reflects the potential for a transient-induced LOCA due to a failure of the RCP seals, followed by failure to provide adequate safety injection. A failure of the RCP seals is postulated to occur if component cooling water (CCW) to the seals' thermal barriers were lost coincident with loss of seal injection from the makeup system, or if seal return flow were lost and the operators did not trip the pumps. In either case, timely operator action to trip the RCPs would prevent serious leakage from the seals. This sequence was estimated to have a frequency of 1.4×10^{-5} per year, accounting for about 21% of the total core-damage frequency.

The CCW and service water systems play a significant role in this sequence. In addition to providing cooling for the RCP seals, CCW is required for operation of both the makeup and injection systems. Thus, an extended loss of CCW would lead to total loss of seal cooling and failure of both injection systems. In addition to faults within the CCW system, loss of service water could lead to heatup of the CCW system and eventual loss of cooling as well. Among the important contributors are the following:

- A plant trip required by total loss of service water, with failure of the operators to trip the RCPs. This, in turn, is dominated by common-cause failure of the three service water pumps (two of which are normally operating) either because they fail to continue operating, or because of loss of ventilation, since all three pumps are located in the same room, and failure to restore service water via a separate backup pump (the dilution pump). During normal operation, the CCW loads on the service water system are relatively low, so that it would take about an hour for loss of service water to lead to loss of CCW. This would allow ample time for recovery, if the third service water pump were not affected by the common cause, or if the separate backup pump were available. Otherwise, without operator action to trip the RCPs, a seal LOCA would result, and the makeup and HPI pumps would not be available to provide injection.
- A plant trip due the total loss of CCW, with failure to trip the RCPs. There are also three CCW pumps, one of which is normally operating, with a second in standby and a third racked out as a spare. The loss of CCW would allow a more limited time for recovery (relative to a total loss of service water) before a seal LOCA could result, although there would still be about an hour to restore cooling before failure of the HPI pumps.
- A plant trip due to the loss of one train of CCW, with failure of the standby train, or failure of service water to supply cooling to the heat exchanger in the standby train. Because of the time required to heat up the standby CCW train, this would be similar to a total loss of service water.
- A plant trip due to loss of one of the operating trains of service water, with failure to provide cooling for the other train of CCW or failure of the other train of CCW.

The other mechanism for inducing a seal LOCA would be for the RCPs to continue to run after seal return had been isolated. The frequency of loss of seal return reflects dependence on several support systems, including instrument air, dc power, and ac power. The contribution to the frequency of core damage for sequences involving loss of seal return is lower than those cited above, however, because there is substantially less dependence between the seal return and the injection systems than is the case for loss of either CCW or service water.

Sequence TQX_T

Sequence TQX_T involves a transient-induced LOCA due to failure of the RCP seals, with failure of long-term cooling after successful injection. The sequence was assessed to have a frequency of approximately 4.3×10^{-6} per year, and contributes about 7% to the total core-damage frequency.

The RCP seal failure in this case results primarily from loss of seal return, since the total loss of seal cooling typically results in conjunction with failure of injection (i.e., sequence TQU_T due to the loss of all CCW). For this scenario, long-term cooling could be accomplished if the operators were able to cool down and establish flow from the DHR system (either in normal shutdown cooling mode or via recirculation from the containment sump), or if they initiated high pressure recirculation before the BWST was depleted. The scenarios that contribute most to the frequency of this sequence include the following:

- Loss of instrument air, which would both cause one of the valves in the portion of the seal return line common to all four RCPs to fail closed, and hamper the ability to cool down the RCS, followed by failure of the operators to initiate high pressure recirculation.
- Loss of dc bus D2P, which would also cause the seal return valve to fail closed, and would cause one train of the systems needed for long-term cooling to be unavailable. In this case, any fault in the opposite train (e.g., of a DHR pump to start) would lead to failure of long-term cooling.
- Loss of seal return by any mode, with failure of the operators to establish some means of long-term cooling, or common-cause failure of the pumps or valves needed for successful long-term cooling.

Sequence TB_TQU_T

Sequence TB_TQU_T involves a transient-induced LOCA due to a failure of the RCP seals or a stuck-open primary relief valve with failure to provide adequate safety injection and failure of decay heat removal via the steam generators. The sequence was estimated to have a frequency of 2.9×10^{-6} per year, and contributes about 4% to the total core-damage frequency.

The LOCA would result primarily from a failure of the RCP seals due to the loss of seal return following the loss of dc bus D2P or instrument air. The loss of bus D2P would also cause one train of the systems needed for long-term cooling to be unavailable and would

lead to a loss of control power to one of the turbine-driven AFW pumps. The following summarizes the important contributors for this sequence:

- Loss of dc bus D2P, which would cause the seal return valve to fail closed, disable one train of the systems needed for long-term cooling (due to the loss of breaker control power), terminate main feedwater and also cause the loss of control power to one train of the turbine-driven AFW pumps. Any fault in the opposite makeup train would lead to failure of makeup/HPI cooling. Similarly, failure of the operators to control feedwater flow in the affected train or failure of the operators to actuate the motor-driven feed pump would result in the loss of all feedwater.
- Loss of instrument air, which would cause one of the valves in the portion of the seal return line common to all four RCPs to fail closed and result in the loss of main feedwater, followed by independent or common-cause failures of both turbine-driven AFW pumps with failure of the operators to actuate the motor-driven feed pump and to initiate makeup/HPI cooling.

Sequence FQU_T

Sequence FQU_T involves an internal flood that results in the loss of all service water or CCW, and in turn causes a LOCA due to failure of the RCP seals, followed by failure to provide adequate safety injection. This sequence is functionally equivalent to sequence TQU_T, but is distinguished by the nature of the initiating event. It has an estimated frequency of 1.9×10^{-6} per year, and contributes about 3% of the total core damage frequency.

Sequence FQU_T is dominated by the internal floods that result in the loss of all CCW or service water. As previously discussed for sequence TQU_T, the CCW system plays a significant role since, in addition to providing cooling for the RCP seals, it is required for operation of the injection systems. In addition to CCW system faults, a loss of service water could lead to heatup of the CCW system and an eventual loss of cooling as well. The floods of interest include the following: a service water or fire-suppression flood in the CCW pump room (room 328); a service water, fire suppression or cooling tower makeup system flood in the service water pump area (room 52); a fire-suppression system flood in the room housing the diesel-driven fire-suppression pump (room 51), adjacent to the service water pump room, or a service water supply or return line rupture or a cooling tower makeup system line rupture in the service water valve room (room 53).

Sequence MX_M

This medium LOCA sequence involves successful high pressure and low pressure injection, but failure of low pressure recirculation. This sequence has an estimated frequency of 1.6×10^{-6} per year, and contributes approximately 3% of the total core-damage frequency.

Sequence MX_M is dominated by failure of the operators to initiate recirculation following a medium LOCA. The combined operation of the injection systems and the containment spray pumps would deplete the BWST in less than about 2 hr, and the operators would have on the order of 20 minutes to initiate recirculation once the BWST lo-lo level was

reached. Switching to recirculation would entail locally closing the breakers for the suction valves from the sump (DH9A and DH9B) and then opening the valves from the control room.

Sequence SX_S

This small LOCA sequence involves failure of long-term cooling via DHR or recirculation from the containment sump after successful injection. With an estimated frequency of 1.5×10^{-6} per year, it contributes about 2% of the total core-damage frequency.

Sequence SX_S is dominated by a small LOCA followed by failure of both DHR or HPI pumps (note that high pressure injection could have been accomplished via the makeup pumps in the event of failure of the HPI pumps, but the makeup pumps would not be used for recirculation from the sump following depletion of the BWST). Common-cause failures of the DHR pumps and failures of ECCS room cooler capability contribute most to the unavailability of long-term cooling. A failure associated with the common ECCS cooler return line (containing manual valve SW82) or common-cause failures of all ECCS room coolers would result in failure of the DHR pumps.

Containment Bypass Sequence V_SI_S

Sequence V_SI_S is postulated to result from a cognitive error that would lead the operators to initiate shutdown cooling via the DHR system during cooldown, but while the RCS pressure was still high. This sequence has an estimated frequency of 5.6×10^{-7} per year, and contributes less than 1% to the total core-damage frequency.

Once plant shutdown has been initiated, the operators would monitor primary system pressure and temperature in order to ensure plant cooldown rates were adhered to. When RCS temperature and pressure were reduced to approximately 280 F and 266 psig, respectively, shutdown cooling would be initiated. It has been postulated (Ref. 72) that the operators might attempt to open the DHR suction valves prematurely (an error of commission that would also require installing jumpers to bypass pressure interlocks), and that high RCS pressure could result in a rupture of the DHR system. If the operators were unable to isolate the break by reclosing one of the DHR suction valves before the BWST inventory was depleted by low pressure injection, core damage could result.

Containment Bypass Bin RRY

Core-damage bin RRY encompasses several sequences that involve a SGTR with failure to establish some stable means of long-term cooling. The sequences include failure to isolate the generator containing the ruptured tube coupled with failure to depressurize the RCS sufficiently to eliminate or minimize leakage through the break; failure to cool down via the intact steam generator; and loss of feedwater to the intact steam generator. Because of the many common aspects of these sequences, the quantification in this case was performed at the level of the core-damage bin, rather than at the sequence level.

If RCS pressure were not controlled to minimize the leakage rate through the broken tube, the BWST inventory would eventually be depleted by injection and lost through the

break, so that the core could be uncovered. Bin RRY was estimated to have a frequency of 1.9×10^{-7} per year, and contributes less than 1% to the total core-damage frequency.

In the sequences comprising core-damage bin RRY, operator action in isolating the generator with the ruptured tube and depressurizing the RCS would be required. Following a SGTR, the operators would be expected to cool down initially using both steam generators. When the RCS was cooled down to about 500F and 1000 psig, the operators would stop steaming the generator containing the ruptured tube before resuming cooldown using the intact generator. Isolating the generator would be potentially important for cases in which the leakage through the tube could not be reduced to a negligible level by reducing RCS pressure. If leakage continued, there could be an eventual loss of inventory due to depletion of the BWST. Failure of the operators to cool down and isolate the steam generator containing the ruptured tube dominates the frequency of this bin.

Containment Bypass Sequence V₁L₁

This sequence represents the failure of the two DHR check valves that are in series and that form the pressure isolation boundary between the RCS and DHR system (valves DH76 and CF30 or DH77 and CF31). This sequence has an estimated frequency of 1.7×10^{-7} per year, and contributes less than 1% of the total core-damage frequency.

The DHR system is comprised of two redundant trains with each injection line supplied by one DHR pump and one core flood tank. If sufficient reverse leakage in a DHR injection line were to occur through both check valves, back leakage of reactor coolant would propagate through the line and cause a failure in the low pressure portion of the DHR system. This would result in an interfacing-systems LOCA. As in sequence V₅I₅, if the operators were unable to isolate the break before the BWST was depleted, core damage could result.

Containment Bypass Bin RRN

Core-damage bin RRN represents a loss of feedwater to both steam generators with subsequent injection via the makeup/HPI system following a SGTR. RCS pressure would remain high, so that leakage through the ruptured generator would continue and would lead to insufficient inventory in the containment sump to support recirculation after the BWST was emptied. As was the case for bin RRY, the sequences comprising bin RRN were quantified in a single solution for convenience. Core-damage bin RRN has an estimated frequency of 1.1×10^{-7} per year, and contributes less than 1% to the total core-damage frequency.

As in the case of sequence TB_TU_T, no single system failures dominate the loss of all feedwater. MFW could be unavailable due to loss of component cooling (via TPCW) after isolation of service water, or lost after the reactor trip. Individual turbine-driven AFW pump faults along with faults of the motor-driven feed pump account for the balance of the loss of feedwater. In addition, passive failures of both steam generator injection valves would have the potential to cause failure of both AFW pumps.

4.1.2 Summary of Core Damage Sequences with HRA Sensitivity

A sensitivity study was performed to identify those sequences whose frequencies would have been above 10^{-6} (10^{-7} for containment bypass sequences) if the human interactions included in them were postulated to be less reliable than was assessed in the original study. Each sequence that was not already identified in Section 4.1.1 was re-evaluated with individual human action rates set to 0.1 and human interaction combinations equivalently adjusted (i.e., the conditional probabilities for some human interactions in combination with others were often already higher than 0.1).

For each sequence whose frequency fell above 10^{-6} (10^{-7} for containment bypass sequences) with the revised human interaction rates, a description of the sequence, the revised frequency, and the human actions found to be important is provided.

SGTR Sequences in Core-Damage Bin SRY

Core-damage bin SRY includes sequences initiated by a SGTR in which the intact steam generator was not available to support the cooldown, but cooldown was initiated via makeup/HPI cooling. For these sequences, the generator containing the ruptured tube was isolated. Core damage would result due to failure of recirculation when the BWST was depleted. The SGTR sequences assigned to bin SRY have a nominal frequency of 1.1×10^{-7} per year, and contribute less than 1% to the total core-damage frequency. If, however, less reliable human interaction rates were assessed, the frequency of their contribution to bin SRY would increase to 1.1×10^{-4} per year.

One of the important operator actions contributing to these sequences is the need to initiate high pressure recirculation before the BWST is depleted. Procedures provide specific instructions to initiate switchover to the containment sump when the BWST level reaches 8 ft. There is an annunciator on lo-lo BWST level at the 8-ft level. Switchover to recirculation is frequently exercised during operator training on the simulator. In addition, operators have on the order of 22 hr before the BWST would reach the 8-ft level for this scenario. Consequently, this human interaction was assessed to have a failure rate of 5.0×10^{-4} in the base-case assessment.

Sequence TB_TLX_T

Sequence TB_TLX_T involves a transient initiating event with an extended loss of decay heat removal via the steam generators and failure of long-term cooling after successful makeup/HPI cooling. Sequence TB_TLX_T was assessed to have an annual frequency of 3.2×10^{-7} . Using less reliable human interaction rates, the frequency would change to 3.6×10^{-5} per year.

The operator action associated with starting the motor-driven feed pump in response to a loss of both main feedwater and auxiliary feedwater was important in this sensitivity study. In the event of a loss of main feedwater, the auxiliary feedwater pumps would be started automatically by the SFRCS. If they should fail to start or fail to deliver flow to the

steam generators, the operators would be directed to start the motor-driven feed pump. The motor-driven pump needs to be started within about 30 minutes to prevent uncovering the core (for the case when all feedwater was lost at the start of the transient; if feedwater were lost at a later time, which is the case for many of the important contributors, much more time would be available in which to start the motor-driven pump). The emergency procedure provides step-by-step directions for starting the pump in response to the loss of either or both AFW pumps. Actuation of the motor-driven feed pump is emphasized in operator training and practiced during simulator drills. Given the detailed procedural guidance and training on the motor-driven feed pump, this action was assessed a failure probability of 2.4×10^{-3} . Other operator actions important in this sensitivity study include the following:

- Locally controlling the AFW pumps in the event control power was lost, to preclude a potential steam generator overfill that could lead to carryover of water to both turbines.
- Initiating high pressure recirculation, following the loss of all feedwater with successful establishment of makeup/HPI cooling.
- Opening the PORV block valve (during operation with it closed) to permit use of the PORV for long-term success of makeup/HPI cooling in the event of a loss of all feedwater.

Because all of these actions are covered by procedures and are an integral part of operator training, human interaction rates were assessed to be less than 0.1 in the base case.

Sequence TB_TQX_T

Sequence TB_TQX_T involves a transient-induced LOCA due to failure of the RCP seals, failure of decay heat removal via the steam generators, and failure of long-term cooling following the success of injection. Sequence TB_TQX_T was assessed to have an annual frequency of 2.9×10^{-7} . With less reliable human interaction rates, the frequency of this sequence would increase to 2.9×10^{-5} per year.

The operator action associated with tripping the RCPs following a loss of seal return was an important contributor in this sensitivity study. The most important causes of loss of seal return in the cut sets was from the loss of instrument air or the loss of dc power. Abnormal procedures provide specific guidance for response to a loss of instrument air or a loss of dc power, including specific instructions to trip the RCPs. The abnormal procedure for the RCPs includes instructions for responding to a loss of seal return flow as well. Based on the multiple procedural guidance, time available for action, and emphasis in operator training, this action was assessed a failure rate of 4.9×10^{-3} . Other operator actions important in this sensitivity study include the following:

- Locally controlling the AFW pumps in the event control power was lost to preclude a potential steam generator overfill, possibly leading to carryover of water to both turbines.
- Starting the motor-driven feed pump in response to a loss of main and auxiliary feedwater.

Because all of these actions are covered by procedures and are an integral part of operator training, human interaction rates were assessed to be less than 0.1 in the base case.

Sequence AX_A

This large LOCA sequence involves failure of long-term core cooling following successful low pressure injection by the DHR system. Sequence AX_T was assessed to have an annual frequency of 8.7×10^{-7} . In the sensitivity study, the frequency increased to 1.0×10^{-5} per year.

In the event of a large LOCA, the BWST would be depleted in approximately 44 minutes. The operators would be instructed to initiate switchover to draw suction from the containment sump when the BWST level reached 8 feet. In addition to monitoring tank and sump level, there is an annunciator on lo-lo BWST level at the 8-ft level. This annunciator would be actuated at the same time that an interlock with the sump valves clears. In addition, there is a separate section within the emergency procedure governing operator response to a large LOCA. These factors were taken into account in assessing a probability of 7.4×10^{-3} of failure for this human action.

Sequence FB_TU_T

Sequence FB_TU_T is similar to sequence TB_TU_T but results from an internal flood rather than a transient initiator. Sequence FB_TU_T also involves a failure of decay heat removal via the steam generators and failure of makeup/HPI cooling. The sequence was assessed to have an annual frequency of 3.9×10^{-8} . With less reliable human interaction rates, the frequency would change to 1.1×10^{-6} per year.

The operator action associated with locally controlling the AFW pumps in the event the flow control valves failed open was important in this sensitivity study. The operator action to start the motor-driven feed pump in response to a loss of both main feedwater and auxiliary feedwater was also important. As previously discussed, because adequate time is available, procedural guidance is provided, and both of these operator actions are an integral part of operator training, human interaction rates were assessed to be less than 0.1 for each of these events in the base case.

Containment Bypass Bin RIY

Core-damage bin RIY represents a SGTR with failure to depressurize the RCS and isolate the ruptured steam generator, along with failure to provide adequate safety injection. RCS inventory would therefore continue to be lost to the atmosphere, and uncovering of the core would eventually result. The sequences comprising bin RIY were assessed to have a combined annual frequency of 9.4×10^{-9} . In the sensitivity study, less reliable human interaction rates associated with depressurizing the RCS or isolating the generator containing the ruptured tube were led to an assessed frequency of 2.0×10^{-6} per year.

The operator actions associated with depressurizing the steam generators so that the RCS could be cooled down to the point at which the steam generator containing the broken

tube could be isolated were important in this sensitivity study. Following a SGTR, the operators would be instructed to commence an orderly shutdown and steam both steam generators using the turbine bypass valves or the atmospheric vent valves. The indication that would uniquely identify the event as a SGTR would be the high radiation alarms. The emergency procedure provides specific guidance for responding to a SGTR. Consequently, relatively high reliability was assessed for the related operator actions for the base case.

Containment Bypass Bin RIN

Core-damage bin RIN includes sequences initiated by a SGTR, followed by failure of all feedwater and failure of makeup/HPI cooling. The bin was assessed to have an annual frequency of 4.2×10^{-8} . With less reliable human interaction rates, the frequency would change to 2.2×10^{-6} per year.

In response to a loss of main and auxiliary feedwater, the operators would be instructed to start the motor-driven feed pump. In the event that heat removal was not available via the steam generators, it would be necessary to establish adequate injection flow from the makeup system to keep the core covered. The emergency procedure directs the operators to initiate makeup/HPI cooling whenever there is a loss of heat removal via the steam generators and hot leg temperature exceeds 600F. The actions that had the most effect in this sensitivity study included failure to start the motor-driven feed pump and failure to establish makeup/HPI cooling.

Conclusions Regarding HRA Sensitivity

Human reliability plays an important role in most of the sequences contributing to the core-damage frequency for Davis-Besse. For a few sequences, the application of best-estimate probabilities for human interactions results in relatively low frequencies that could be substantially higher if the interactions were reassessed to be less reliable. In all cases, however, the individual interactions have been investigated to identify potential problems in their accomplishment, and to reflect in an appropriate manner the procedural guidance, training, and other factors that affect their reliability. Combinations of human interactions that arise for many sequences have also been addressed in a very systematic and careful manner to ensure dependencies are taken into account and that unrealistically low estimates for overall response are not implied. These treatments are considered to be reflective of the state of the art in PRA, and provide the most appropriate set of insights into the risk profile for Davis-Besse.

4.2 SUMMARY OF PLANT VULNERABILITIES

One of the primary objectives of the NRC in initiating the IPE process was to identify weaknesses in the plant designs or operating practices that would constitute vulnerabilities with respect to the potential for core damage or of a serious release. The definition of what constituted a vulnerability was left to each utility (Ref. 73).

In practical terms, a vulnerability is considered to be a plant feature that compels action on the part of the utility to reduce risk, irrespective of regulatory pressures. To qualify as a vulnerability with respect to the potential for core damage, it is necessary for one of the following situations to exist:

- (1) The plant to have an unacceptably high frequency of core damage, with one or a few aspects of the plant design or operating practices assessed to be responsible for that high frequency. An unacceptable frequency for core damage has, by common practice, generally been regarded to be significantly higher than 10^{-4} per year. The few plant features that led to the high assessed frequencies would constitute vulnerabilities.
- (2) A single plant feature (or a very small number of plant features) to be a contributor to core-damage frequency that was substantially higher than all other contributors, even if the overall frequency were deemed to be generally acceptable. These outliers would typically be considered to be vulnerabilities. Note that this might not necessarily be true if the overall core-damage frequency were extremely low.
- (3) The frequency of core damage to be very sensitive to a highly uncertain aspect of plant response. In this case, a vulnerability might exist, although the implications might be that more evaluation to reduce the uncertainty would be a more appropriate response than a change to the plant.

The core-damage frequency for Davis-Besse was estimated to be about 6.6×10^{-5} per year, and is comparable to the frequencies obtained in studies for many other PWRs that do not have serious weaknesses. Although a small number of sequences is responsible for a large fraction of this frequency when the sequences are defined at the very general level of safety functions, examination of these sequences indicates that there are many individual contributors to their frequencies, and no single or small number of features contributes an inordinate fraction of the total core-damage frequency. Furthermore, although there are, as in any PRA, uncertain aspects of the plant models or data that, if assessed differently, could result in higher (or lower) estimates of core-damage frequency, none is considered to be both so uncertain and potentially able to produce such a large contribution to core-damage frequency that it should be considered to be a vulnerability.

This should not be interpreted to imply that no consideration is being given to the results of the IPE with respect to further enhancements that might be desirable with respect to reducing risk or risk uncertainty. Consideration of several enhancements is underway, as described in Part 6 of this submittal. None of these was judged to present a compelling need for change, however, and therefore none was identified as a vulnerability.

4.3 DECAY HEAT REMOVAL EVALUATION

In Generic Letter 88-20, NRC stated that Unresolved Safety Issue (USI) A-45, Shutdown Decay Heat Removal Requirements, would be resolved through the IPE process (Ref. 71). The objectives of USI A-45 were to determine whether the decay heat removal

function at operating plants is adequate and if cost-beneficial improvements could be identified. NRC concluded that a generic resolution (e.g., a dedicated decay heat removal system for all plants) was not cost effective and that resolution could only be achieved on a plant-specific basis. Since the IPE process includes an examination of the decay heat removal functions, NRC subsumed USI A-45 into the IPE.

Appendix 5 of Generic Letter 88-20 summarizes the insights gained from the six limited scope PRAs performed under the USI A-45 project. NUREG-CR 4713 also provides specific insights gained in the shutdown analysis performed for a B&W plant (Ref. 74). In view of these insights, an evaluation of the decay heat removal capability at Davis-Besse was performed to support resolution of USI A-45. This evaluation was based on the IPE results with the objective to identify any potential "vulnerabilities" associated with the decay heat removal systems at Davis-Besse and to identify any cost-beneficial improvements.

The Davis-Besse IPE includes models of the various plant systems that perform the decay heat removal function, including those used for makeup/HPI cooling. All relevant failure modes such as maintenance events, human interactions, common-cause events, and component failure modes are included explicitly in the model. Support systems such as ac and dc power, cooling water systems, room ventilation, etc. which are required to ensure proper system operation are also included. Initiating events which challenge the systems that provide for decay heat removal have been identified and the sequences involving subsequent failures of these systems have been quantified. These results provide the basis for resolving USI A-45. The following paragraphs provide a summary of the decay heat removal functions available for the various types of initiating events.

Loss-of-coolant accidents require the use of high pressure injection or low pressure injection pumps to transfer decay heat from the core to containment. In addition to the two high pressure and two low pressure injection pumps that are part of the ECCS, Davis-Besse has two makeup pumps capable of injecting water from the BWST during high pressure conditions (i.e., for small LOCAs). Each of the two safety injection systems is composed of two independent trains that take suction from the BWST. The ECCS pumps are supplied power and cooling water from independent electrical buses and cooling water trains. During recirculation from the containment sump after a LOCA, decay heat is removed from the core via the DHR system and from containment via the containment air coolers and the containment spray system. The DHR system contains two pumps which take suction from the emergency sump and cool the water through their respective heat exchangers. The coolers transfer heat to the CCW system; it is then transferred to the service water system and, ultimately, to Lake Erie. If recirculation capability were not available, the potential exists to supply additional makeup to the BWST to maintain injection for an extended period of time.

Transients and small LOCAs require use of the main or auxiliary feedwater systems to remove decay heat. The main feedwater system consists of two redundant turbine-driven pumps, associated feedwater heaters and deaerator storage tanks. In the event that MFW is unavailable, SFRCS automatically initiates the AFW system consisting of two redundant, safety-related turbine-driven pumps. In addition, a motor-driven feed pump can be started

manually from the control room to provide auxiliary feedwater in the event that one or both turbine-driven pumps are unavailable. Any one of the three pumps (two turbine-driven and one motor-driven) is capable of supplying 100% of the required flow to the steam generators for decay heat removal. In addition to the two condensate storage tanks that would normally supply suction for auxiliary feedwater, the service water system serves as an automatic backup source of suction to the AFW pumps. The PORV and primary safety/relief valves are available for RCS pressure relief. Main steam safety valves, turbine-bypass valves and atmospheric vent valves provide secondary side pressure relief. In the unlikely event of a loss of all feedwater, procedures direct the operators to initiate makeup/HPI cooling. During the fifth and sixth refueling outages, substantial changes were made to the makeup system to increase the capability and reliability of the makeup/HPI cooling function. Makeup/HPI cooling is possible with one makeup pump taking suction from the discharge of a DHR pump and with the PORV manually opened to serve as a bleed path from the RCS, or with both makeup pumps taking suction from the BWST and the primary safety valves. The addition of a second makeup injection line further enhances the capability of makeup/HPI cooling. In addition to equipment modifications, substantial changes in procedures and operator training have increased understanding of the importance and the effectiveness of this operation.

The PRA summarized in this submittal is primarily concerned with the evaluation of decay heat removal. The results provided in the previous sections discuss specific failures associated with the decay heat removal systems. The contribution to the overall core-damage frequency associated with failure to provide for adequate decay heat removal has been considered with other insights discussed in Section 4.2. Since the decay heat removal function has been considered in an integrated fashion as part of the IPE results, the conclusions relative to the IPE presented in Section 4.2 and in Part 6 encompass all necessary action to resolve USI A-45.

As noted previously, the systems that serve the decay heat removal function at Davis-Besse were not found to be subject to any particular vulnerability to internally initiated severe accident sequences (including internal flooding). Furthermore, the reliability of the feedwater and emergency core cooling systems together with the capability to accomplish makeup/HPI cooling make the Davis-Besse decay heat removal systems sufficiently reliable. In conclusion, Davis-Besse does not exhibit any particular vulnerability to a loss of decay heat removal, and USI A-45 should be considered to be resolved.

4.4 USI AND GSI EVALUATION

As part of the Davis-Besse IPE, unresolved and generic safety issues were screened to identify those issues amenable for resolution using the models, results, and insights gained from the IPE process.

Through the years, numerous nuclear safety issues have been identified by the NRC. Probabilistic risk assessment provides a method for identifying which of these safety issues are of specific concern to Davis-Besse. By considering the implications of each safety issue with

respect to the potential for severe accidents, the PRA can be used to arrive at decisions regarding the need for further corrective action. The IPE process has been used to evaluate the following issues for Davis-Besse:

- USI A-17, Systems Interactions
- Generic Issue (GI)-23, Reactor Coolant Pump Seal Failures
- GI-105, Interfacing Systems LOCA in PWRs
- GI-77, Flooding of Safety Equipment Compartments by Backflow Through Floor Drains
- GI-128, Electrical Power Reliability and Related Issues
- GI-143, Availability of Chilled Water Systems and Room Cooling
- GI-153, Loss of Essential Service Water in LWRs
- GI-65, Probability of Core-Melt Due to Component Cooling Water System Failures

Each of these safety concerns, the evaluation of its relevance to Davis-Besse, and conclusions drawn with respect to the need for further resolution are discussed in the following sections.

4.4.1 USI A-17. Systems Interactions in Nuclear Power Plants

The systems of a nuclear power plant are often complex and inter-dependent networks where failure of one system, structure, or component may have a significant impact on other systems, and therefore, on plant safety. Collectively, these inter-dependencies are referred to as USI A-17. It was determined, however, that the scope of the issue was too broad, and the NRC later focused the effort by defining the specific safety concerns that merited consideration. The effort associated with resolving issue USI A-17 then concentrated on identifying and eliminating adverse systems interactions. The NRC concluded, in Generic Letter 89-18, that USI A-17 could be resolved by taking certain actions (Ref. 75). Licensees are expected to take two actions: (1) to consider insights from the appendix of NUREG-1174 (Ref. 76) in implementing the IPE requirement for an internal flooding assessment, and (2) to continue to review information on events at operating nuclear power plants.

An extensive analysis of internal flooding and water intrusion was performed for Davis-Besse as a part of the IPE. The consideration of flood hazard has been incorporated into the event sequence development, systems analysis, and sequence quantification described in this report. The assessment focused on the auxiliary building, the turbine building, and the service water structure. The scenarios considered flooding and water intrusion from all major sources within the plant; it was determined that no significant threats from internal flooding exist for Davis-Besse, and internal flooding was a relatively small contributor to the overall frequency of core damage (about 3% of the total).

Although the risk of internal flooding was found to be relatively low, a procedure has already been developed to heighten operator awareness and to give general direction for

coping with this type of event to provide added assurance. Any additional actions that might be taken will be based on consideration of the quantitative results and qualitative insights from the flood assessment, consistent with the overall plan for resolving concerns identified as a result of the IPE.

Toledo Edison has an established program for reviewing sources of information on industry experience. This program is controlled by a Nuclear Group Procedure. Inputs to this program include NRC Information Notices, licensee event reports, and INPO's Nuclear Network, as well as others. Each report of an event is evaluated by knowledgeable personnel to determine its applicability to Davis-Besse. Should the information be relevant to the facility, it is distributed to various groups for resolution. If corrective action is necessary to reduce the potential for a similar event at Davis-Besse, the appropriate action is entered into the normal work process of the facility. This program promotes awareness and recognition of systems interactions and assures that realistic, potentially adverse systems interactions are promptly addressed at Davis-Besse.

In addition to the specific evaluations made of internal flooding, the present process of evaluating events at operating nuclear power plants helps to ensure that current information regarding adverse systems interactions is used to improve the ability to cope with such events. Therefore, because USI A-17 is adequately addressed at Davis-Besse, it is considered to be resolved.

4.4.2 GI-23. Reactor Coolant Pump Seal Failures

Generic Issue 23 involves questions of the adequacy of current licensing requirements as they relate to seal integrity for reactor coolant pumps. The issue is concerned with evaluating the risk associated with seal failures which occur randomly during normal power operation, or occur due to failure of support systems during abnormal operations such as a station blackout or loss of various essential cooling water systems. Initial generic work by the NRC indicated that the overall core-damage frequency due to small LOCAs could be dominated by scenarios involving RCP seal failures. Toledo Edison has reviewed and evaluated the design features of the specific RCP seals used at Davis-Besse so that realistic assumptions could be made regarding seal performance for the IPE. The following sections describe the PRA model and its basis.

Davis-Besse has four RCPs, each of which uses a Byron-Jackson Model N-9000 mechanical seal cartridge, which has replaced the original seal design. The N-9000 seal, like its predecessor, uses a multi-stage cartridge. Each of the stages is designed to be capable of sealing against full RCS pressure during off-normal operation, thereby providing triple redundancy. Each cartridge consists of three individual, functionally identical stages which are stacked in series between the RCS and the containment atmosphere. Each of the stages is capable of carrying a pressure drop of at least 2,200 psid, but normally only one-third of this pressure drop (or about 750 psid) is carried across each of the stages.

The N-9000 design has incorporated several improvements relative to the previous pump seals. The new design eliminates the generation of unbalanced loading due to radial shaft displacement. In the old design, unequal hydraulic loading forces could be generated as a result of radial shaft displacement, causing uneven wear of the stationary face sealing nose. Removal of the assembly and secondary seal from the rotating portion of the seal package has eliminated this problem. The balance diameters in the new design have been made equal, thereby eliminating the changes in pump thrust that occur when cavity pressures change. This will result in a reduction of cavity pressure oscillations. Due to an increase in seal face width in the N-9000 design, the seal face unit loading and unit area heat generation rates have been reduced from the old design. The N-9000 design utilizes tungsten carbide as a rotating face ring material. This material offers better fracture resistance and about five times the thermal conductivity of the titanium carbide used in the old design. The stationary face ring material is still resin-impregnated graphite. This combination of face materials has had many years of satisfactory field experience in RCP applications. Additionally, many parts of the seals will now be interchangeable between the three stages. This further reduces the potential for any re-assembly errors that could attribute to seal failures.

A stage consists of a stationary face in a holder assembly and a rotating face in an assembly which is keyed to the RCP shaft. The stationary face holder is spring loaded so the stationary face is pressed toward the rotating face. A thin-film hydrostatic gap of approximately 100 micro-inches is maintained between the stationary and rotating faces by opposing the closing force of the spring and hydraulic forces with the pressure fields generated between the seal faces. A small leakage of fluid through this gap keeps the faces cooled and lubricated as the RCP rotates. Without this lubrication, the faces could overheat and eventually fail potentially causing the seal to become ineffective.

One of the support systems connected to the RCPs is the makeup system. High pressure water (slightly above normal RCS pressure) is injected into the RCP above the thermal barrier which separates the RCS from the seal cartridge. The seal injection flow splits at this point, with some flow passing up through the seal cartridge through controlled bleed-off orifices (CBOs) and the rest flowing downward to enter the RCS. There is a slight leakage between the seal faces in a path parallel to the flow through the CBOs. The seal face path represents a higher flow resistance than the CBO, so the larger flow passes through the CBO path. The flow through the CBO path is recycled to the makeup system via the seal return path. The seal return flow is measured to provide indication of seal problems.

Cooling of the pump seals is also provided by the CCW system. The CCW flow passes through a closed heat exchanger within the RCP. The purpose of this heat exchanger is to cool any hot RCS fluid which might flow up into the seal cartridge. While the seal flow is normally seal injection water from the makeup system, should seal injection flow be lost, hot RCS water would flow up into the seals. In order to maintain an acceptable seal temperature, the RCS water is circulated around the heat exchanger before entering the seal cartridge region. This reduces the RCS fluid temperature to an acceptable level, thus ensuring that the seal integrity is maintained.

In support of the N-9000 development and testing program, a computer model of the seal was developed. A separate, detailed model of the slot configuration of the graphite ring was constructed. This model operates in conjunction with a 3-D finite element model of the seal rings. Computations made included the seal face flow field, pressure distribution, heat dissipation, and topography. This included a complete computation of the flow and pressure fields radially and circumferentially. Areas of cavitation, if they would occur, could be identified. An iterative solution scheme was used which took into account the waviness of the graphite ring, which was solved for by an ANSYS finite element model. The output of parameters from the finite element analysis serves as a starting point for the analysis of the hydropad effect. It is the hydropad effect which is responsible for the forces generated which keep the seal faces apart. The hydropad analysis is computationally intensive, requiring several hundred iterations, together with approximately eight to ten ANSYS runs that are required to arrive at stability for each steady-state condition of the seal. The results of the analysis correspond very closely to the actual performance of the seal as observed in testing. The analysis of the slots conforms to the engineering specification requirement that seal behavior be predictable and that a full liquid lubricating film be maintained under all normal operating circumstances. The models were of sufficient detail that significant insights into the basic operation of the hydropad effect were obtained.

The various support systems for the RCP seals can experience several different failures, either singly or in any combination, which could have an impact on the RCP seal integrity. Specifically, the following failure modes are postulated: loss of seal injection, loss of CCW flow, loss of seal return, and combinations of these failures. These failures could be caused by numerous scenarios, such as inadvertent valve closures, inadvertent safety system actuations, pump failures, or a loss of offsite power. The effects of each of these failure modes on the RCP seal integrity are discussed below.

Loss of Seal Injection

A loss of seal injection flow can occur for many reasons. The net effect of the loss of only seal injection is that the RCS fluid becomes the medium which cools the seals with the heat of the RCS removed by the CCW system. Consequently, as long as this is the only support system failure, the RCPs can continue to run indefinitely without the seal integrity being challenged.

Loss of Seal Return Flow

Should the seal return path become isolated for any reason, the lower two seals would de-stage, causing the full pressure drop of the seal injection or RCS to take place across the last seal face. Each of the stages is designed to withstand the full pressure drop for an indefinite period of time. Should this seal fail, the middle seal would re-stage and continue to provide sealing with minimal leakage. This sequence also applies to the lower stage. Current Davis-Besse procedures direct plant operators to quickly restore the seal return path or to trip the affected RCP(s). If the pump shaft is not rotating, there is no heat generated at the seal

interfaces. Without any heat generation, the seal materials would not experience a significant temperature excursion. Therefore, the seal integrity would not be challenged.

In order to assure that this assessment was correct, the owners of Byron-Jackson RCPs formed a project team to test the N-9000 RCP seal. Babcock & Wilcox (B&W) prepared a report which summarizes the test program and the results of the test (Ref. 77). The test seal cartridge was subjected to a 30-minute run with the seal return path closed and the pump casing side of the seal at full RCS pressure (about 2150 psig). The test was performed after the seal had undergone about 5,000 hours of run time. It is important to note that the test shaft was rotating during this 30-minute test. The test showed no noticeable change in the seal components from conditions found prior to running the loss of seal return test. The third stage leakage during the test was approximately 0.5 gpm.

Due to the three-stage design of the seal cartridge, the seal assembly has built-in redundancy for this particular support system failure. When the seal return path is closed, the CBO orifices cease to work so there is no pressure drop across the first two stages of the seal assembly (i.e., the first two seals "de-stage"). The third stage then carries the full differential pressure drop. If the third stage were to experience gross failure, the second stage should "re-stage" and begin carrying the full pressure drop. This may also occur in the first stage if the second stage were to then have a significant failure.

Based on the design and test experience with the N-9000 seal, it is concluded that closure of the seal return path for a limited period, while the RCP is running, would not cause a significant increase in seal leakage. As stated above, the RCP should be turned off to ensure the seal integrity is not challenged.

Loss of CCW Flow

If CCW flow to the RCP were lost, there is a potential for the seal cartridge to heat up. Normal seal injection flow should keep the seal cool; however, plant operators are directed by procedures to trip the affected RCP if the seal outlet temperature exceeds a specified value. If the seal outlet temperature were to continue to climb, the operators would be further directed to shut off the seal return path to limit the temperature of the seal. Once this was accomplished, the seal temperatures should stabilize, since the RCP would not be rotating (producing no heat at the seal faces), and little flow would be passing up the seal from the seal injection cavity. The seal would therefore be expected to maintain its integrity indefinitely as long as the seal outlet temperature is maintained acceptably low or the appropriate actions are taken to protect the seal.

Multiple Support Systems Failures

Some postulated plant transients, such as a loss of all site ac power (station blackout), can result in the loss of more than one support system. A station blackout would result in a loss of seal injection and a loss of CCW. While the RCPs would also be stopped due to the loss of power, the seals must continue to maintain the RCS pressure boundary integrity. In this situation, the seal would still heat up, even though it was not running, since the hot RCS

water would be flowing up through the seal without being cooled by CCW. Closing the seal return path would limit the flow through the seal which would help to minimize the temperature rise in the seal. The N-9000 seal was specifically tested for these conditions after the normal use testing program was completed (Ref. 78).

The test subjected a static (non-rotating) seal cartridge to 555-575F water over a range of pressures (1700-2250 psig) at the inlet side of the seal. For the first half-hour of the test, the seal return valve was left open in order to preheat the seals, thereby maximizing the severity of the test. In addition, there was no seal injection or seal cooler (CCW) flow throughout the entire eight-hour test. The seal performed essentially as expected throughout the test. There was a marked increase, although still acceptable, in seal leakage after 7.5 hours of testing. This was attributed to a failed third-stage O-ring, which was discovered during a post-test inspection. The specific failure mechanism was later determined to have been precipitated by a manufacturing process defect which has since been corrected. When the O-ring failed, the other two stages of the seal cartridge re-staged and picked up the pressure load immediately. This demonstrated the ability of the first and second stages to serve as backups to the third stage. Other observations from the post-test inspection included extrusion of the O-rings in the two lower seal stages and indication of two-phase flow across the third-stage seal faces. These conditions were anticipated, and their potential occurrence was accounted for in the seal design.

A concern of the NRC in relation to GI-23 was instrumentation of the RCP seals. Davis-Besse has installed the reactor coolant pump monitoring and diagnostic system. This is a computer-based data collection and diagnostic system designed by the B&W. It will generate alarms to alert operators of any critical parameter exceeding prescribed limits. Other parameters are logged and trended for information regarding the seals, the shaft, and general pump performance parameters. The diagnostic system focuses on rotor dynamic vibration and quasi-static parameters related to seal behavior. This system aids the operating staff and diagnostic personnel in detecting early signs of seal degradation.

The Davis-Besse plant employs two means of cooling the reactor coolant pump seals, direct seal injection and seal cavity cooling by means of CCW. Loss of either source of cooling water can produce some temperature changes in the seal cavity, but long-term significant effects on seal performance would not result. These dual systems reduce the probability of total loss of seal cooling. In the event of a station blackout, both sources of seal cooling would be lost. An alternate source of ac power has been installed at the Davis-Besse plant. This new blackout diesel is capable of re-powering the seal support systems, thereby recovering seal cooling.

After examining the information on the testing and design of the Byron-Jackson N-9000 RCP seal, the increased instrumentation to detect seal degradation, and the addition of an alternate source of ac power, it is concluded that the RCP seals will not experience gross failure due to loss of support systems, as long as plant operators take the appropriate actions to stop the affected RCP(s). While the test of the total loss of seal cooling was only run for eight hours, the data did not indicate any developing trends that would denote impending

catastrophic failure. Since the elastomerics in the seals are rated to about 350F before they begin to experience breakdown, and the RCS temperature should be approaching this value after eight hours, further degradation of the seal elastomerics should not occur. Consequently, the seals can be considered to be capable of maintaining their integrity for a sufficient duration to accomplish safe shutdown of the plant under all postulated scenarios. The PRA model incorporates this conclusion by assuming a seal LOCA only if the plant operators fail to trip the affected RCP following a total loss of support systems; as long as the RCPs are tripped in a timely manner, a seal LOCA is not postulated to occur.

The design process and design verification testing program associated with the Byron-Jackson N-9000 RCP seal have provided significant confidence in the seals' capabilities to maintain their integrity under a variety of conditions. The frequency of core damage due to seal LOCA was estimated, based on realistic (and, in a few cases, potentially conservative) assumptions regarding the effects of various losses of seal cooling on the potential for seal failure. Although this was among the important contributors to overall core damage, it was not dominant, and no vulnerabilities were implied. Therefore, this generic issue is considered to be resolved.

4.4.3 GI-105. Interfacing Systems LOCA in PWRs

Generic Issue 105 was issued to address the concern from WASH-1400 (Ref. 79) about the potential for the point of interface between a high pressure system and a low pressure system to become a site for a LOCA. Particular concern was expressed over low pressure systems which penetrate containment, so that the LOCA could bypass any safety features intended to prevent a serious release of radiation, and preclude establishing long-term cooling of the core. The NRC performed a PRA of a generic B&W design, using Davis-Besse as its basis, to determine the magnitude of the risk of this type of event. The results of that work are presented in NUREG/CR-5604 (Ref. 6). Toledo Edison has performed a similar assessment of the event as a part of the IPE, applying insights from the NRC study as appropriate. The scenarios that could lead an interfacing-systems LOCA for Davis-Besse are described in Section 1.2.1. The results of the assessment are summarized in Section 4.1.

The total frequency of core damage due to interfacing-systems LOCAs was estimated to be 8.8×10^{-7} per year. This is not an important contributor to the overall core-damage frequency, although it is important on a relative basis with respect to the potential for early releases (since the containment would be bypassed). The overall frequency of early containment failure, however, was assessed to be quite low. The largest contributor to this frequency was the result of a postulated human error of commission that would entail prematurely opening the DHR suction valves while cooling down the RCS to cold shutdown. The potential for this error was identified during the NRC study. There is substantial question regarding the actual potential for such an error (it would, for example require a conscious decision to violate significant administrative procedures and install a jumper to permit opening one of the suction valves). Nevertheless, the error was retained in the current study for completeness.

The issue of interfacing-systems LOCA at Davis-Besse has been thoroughly evaluated by both NRC and Toledo Edison. The overall risk due to such an event is quite low, and has been further diminished through additional training to increase the awareness of the potential hazards among the operating staff. Therefore, this issue is judged to be resolved.

4.4.4 GI-77. Flooding of Compartments by Backflow Through Floor Drains

Due to events at several nuclear facilities, the NRC initiated GI-77. This issue was concerned with the potential for safety-related equipment to be adversely affected by flood propagation through the floor drain system of a facility. It had been found that flood water from a non-safety related system could propagate into safety-related areas because there were no check valves in some drain systems.

The internal flooding and water intrusion study performed as a part of the IPE (see Section 4.4.1) included consideration of potential flood propagation. The piping systems associated with the floor drains, pipe chases, sump-pump capacities, and other details were specifically included in the evaluation. If the potential for propagation to safety-related areas was identified, the affected rooms were retained for further study. All flooding sources into critical areas, including floor drains, if appropriate, were used in developing initiating event frequencies. Therefore, the concern of GI-77 has been explicitly addressed for the IPE. The details of the review of the propagation pathways are documented in a report that describes the flood hazard assessment (Ref. 30).

Internal flooding was not found to be a dominant contributor to core-damage frequency for Davis-Besse, and the important scenarios relative to flooding did not result from backflow through drains between redundant areas. Therefore, this issue is considered to be resolved.

4.4.5 GI-128. Electrical Power Reliability, and Related Issues

Generic Issue 128 was issued to consolidate several other generic issues related to plant ac and dc distribution systems. Specific issues include the following:

- Loss of 125 volt dc bus (GI-46),
- Limiting conditions for operation (LCOs) for class 1E vital instrumental buses in operating reactors (GI-48),
- Interlocks and LCOs for redundant class 1E tie-breakers (GI-49),
- Instrumentation and control power interactions (GI-76),
- Adequacy of safety-related dc power supplies (USI A-30),and

Each of these issues is concerned with the effects of electrical system failures on the plant due to systems interactions. Specific methods for resolving GI-48 and -49 have been issued by the NRC (Ref. 81). No specific methods of resolving USI A-30 (and related issues) GI-46 and GI-76 have been provided. Toledo Edison has previously closed GI-48 and

GI-49. Various actions, which are discussed below, have been completed to address the other issues.

Actions taken at Davis-Besse to address GI-48 and -49 have been acknowledged by the NRC (Ref. 82). The resolution consisted of demonstrating that adequate LCOs and surveillance requirements exist in the Technical Specifications, as well as procedural controls at the facility, to assure that power supplies to class 1E instrument buses are reliable and do not interfere with the automatic action of the electrical system.

USI A-30, GI-46, and GI-76 all deal with dc bus reliability and system interactions due to failures. Toledo Edison has completed detailed actions to address these issues. A failure modes and effects analysis (FMEA) of the entire dc power system was completed (Ref. 83). The information derived from this analysis was incorporated into plant procedures. Plant operators have been trained on the procedures and have immediate access to the information in the main control room. Consequently, the impact of losing any dc load or bus can quickly be assessed by operators and any compensatory action necessary initiated. This is particularly of value for maintenance activities. In addition, the plant-specific simulator has been used to validate the procedures, which provides a high degree of confidence in their reliability. Plant operators also benefit from participating in accurate electrical system transient simulations. The FMEA identified areas of possible improvement which were incorporated into the plant's routine modification process for potential resolution.

The various aspects of electrical plant reliability were also incorporated into the IPE as initiating events and system failures. Two dc bus failures were modeled as initiating events, as were various ac failures, such as a loss of offsite power and losses of various ac buses. The effects of various system, structure, and component failures, whether induced by electrical failure or other means, has also been included in the models.

Toledo Edison has expended significant effort to analyze the Davis-Besse electrical distribution system. Based on the actions completed, Toledo Edison considers GI-128, which includes USI A-30, GI-46 and GI-76, adequately addressed and therefore resolved.

4.4.6 GI-143. Availability of Chilled Water Systems and Room Coolers

Generic Issue 143 was issued to bring attention to the dependence of safety related systems, structures, and components (SSCs) on adequate heating, ventilation, and air conditioning (HVAC). Industry experience showed an increasing sensitivity to HVAC failures due to increasing compartmentalization to address fire protection concerns and incorporation of temperature sensitive electronics into control devices. The loss of ventilation or room coolers had been found to be a large contributor to core melt probability in some plants.

The PRA models used in the Davis-Besse IPE specifically addressed required support systems, including HVAC for safety related SSCs. The plant's HVAC configuration was explicitly modeled to the level of detail required. Industry failure rates for HVAC equipment were used in order to have the broadest input on equipment reliability. The impact of the

HVAC failures on safety related SSCs were therefore included in the core-damage assessment.

The HVAC system of the main control room was not explicitly modeled in the PRA. As previously discussed in this report, there is sufficient redundancy and procedural direction available to the plant operators to cope with a failure in this system. The design features of the control room equipment include environmental requirements, so that the impact of a control room HVAC failure would be minimal. Consequently, this particular system is considered to be adequately addressed.

Based on the detailed modeling of the plant HVAC systems and the separate evaluation of the main control room ventilation system, Toledo Edison considers GI-143 adequately addressed. Any identified vulnerabilities will be prioritized in the routine plant improvement processes and dispositioned as appropriate. Therefore, Toledo Edison considers GI-143 resolved.

4.4.7 GI-153. Loss of Essential Service Water in LWRs

Generic Issue 153 was identified as a result of continuing NRC concern with the frequent loss of essential service water at nuclear facilities. The causes of the failures were varied and the severity of several events was significant. The NRC determined that for many facilities, a large reduction in public risk could be achieved by evaluating the plant's sensitivity to service water failures with respect to core-damage frequency and taking actions to reduce the effects of identified vulnerabilities.

The Davis-Besse PRA models included a plant specific model of the service water system components deemed required to meet the IPE success criteria. The model also included the necessary support systems required for the proper operation of the service water system. The major system equipment failure rates were developed from plant data, where feasible. Numerous scenarios involving the loss of service water were then quantified to determine the plant's core melt risk.

The results of the PRA have identified the level of plant vulnerability associated with a loss of service water. No serious weaknesses in the system were identified. Based on the work completed for the IPE, Toledo Edison considers GI-153 properly addressed and that the GI is therefore resolved.

4.4.8 GI-65. Probability of Core-Melt Due to Component Cooling Water System Failures

The NRC recognized the high dependence of many systems, particularly safety related systems, on the Component Cooling Water (CCW) system. Additionally, for PWR's, the NRC noted that CCW frequently cools the RCP seals. Generic Issue 65 highlighted the potentially large probability for core-melt scenarios to develop due to CCW failures. The NRC expressed particular concern about SBLOCA's due to RCP seal failures following a loss of CCW. Because of the relationship between CCW system failure and RCP seal failure, the

NRC later integrated Generic Issue 65 into the resolution of Generic Issue 23 (see Generic Issue 23 writeup).

The Davis-Besse PRA models specifically included CCW as an essential support system. The PRA evaluated initiating events involving or leading to a loss of CCW. The evaluation also included the consequences of the CCW system failures. Part 4, Section 4.4.2 of this report discusses in detail the effect of a CCW failure on RCP seal performance. That section addresses both an isolated loss of CCW and a loss of multiple RCP support systems (which could occur during scenarios such as a Station Blackout). That section concluded that there is sufficient redundancy and operator direction to prevent RCP seal failure in the event of a loss of CCW. The PRA also analyzed the effects of CCW failures on safety related equipment required to meet defined success criteria.

The front end PRA analysis would have identified any plant vulnerabilities to CCW failures, as defined in Part 1, Section 4 of this report. The analysis did not reveal any such specific vulnerabilities. Toledo Edison concludes that the PRA adequately addresses Generic Issue 65, based on the analysis and the assessment of CCW failures on RCP seals. Therefore, Toledo Edison considers Generic Issue 65 resolved.



REFERENCES FOR PART 3

1. *Davis-Besse Updated Safety Analysis Report*. Toledo Edison Company, Section 6.3, Rev. 4, July 1986.
2. *Oconee Nuclear Station Unit 3 Probabilistic Risk Assessment*. Duke Power Company, December 1990.
3. Kolb, G. J., et al. *Interim Reliability Evaluation Program: Analysis of the Arkansas Nuclear One-Unit 1 Nuclear Power Plant*. U.S. Nuclear Regulatory Commission Report NUREG/CR-2787, June 1982.
4. *Crystal River-3: Probabilistic Risk Assessment*. Florida Power Corporation (Draft Report), July 1987.
5. Lewis, S. R. "Makeup Requirements for In-Core Instrument Tube LOCA." Informal Calculation, July 1991.
6. Galyean, W. J., and D. I. Gertman. *Assessment of ISLOCA Risk-Methodology and Application to a Babcock and Wilcox Nuclear Power Plant*. U.S. Nuclear Regulatory Commission Report NUREG/CR-5604, April 1992.
7. *B&W Owners Group Probabilistic Evaluation of Pressurized Thermal Shock: Phase 1 Report*. Babcock & Wilcox Company Report BAW-1791, June 1983.
8. Simoner, F. A., et al. *Reactor Pressure Vessel Failure Probability Following Through-Wall Cracks Due to Pressurized Thermal Shock Events*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4483, April 1986.
9. Sugnet, W. R., et al. *Oconee PRA: A Probabilistic Risk Assessment of Oconee Unit 3*. Electric Power Research Institute Report NSAC-60, June 1984.
10. McClymont, A. S. and B. W. Poehlman. *ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients*. Electric Power Research Institute Report NP-2230 (Interim Report), January 1982.
11. *Davis-Besse Updated Safety Analysis Report*. Toledo Edison Company, Section 7.4.1.4, Rev. 2, July 1984.
12. "Loss of RCS Makeup." Davis-Besse Nuclear Power Station Abnormal Procedure DB-OP-02512, Rev. 01, April 6, 1990.
13. *Failure Modes and Effects Analysis of the ICS/NNI Systems at the Davis-Besse Unit 1 Nuclear Power Station*. Science Applications International Corporation, Vol. 1, January 1987.
14. "Loss of Service Water Pumps/Systems." Davis-Besse Nuclear Power Station Abnormal Procedure DB-OP-02511, Rev. 00, April 26, 1990.
15. "Component Cooling Water System Malfunctions." Davis-Besse Nuclear Power Station Abnormal Procedure DB-OP-02523, Rev. 00, April 27, 1990.
16. "Loss of D1P and DAP." Davis-Besse Nuclear Power Station Abnormal Procedure DB-OP-02537, Rev. 00, December 28, 1990.
17. "Loss of D2P and DBP." Davis-Besse Nuclear Power Station Abnormal Procedure DB-OP-02538, Rev. 00, December 28, 1990.
18. "Loss of D1N and DAN." Davis-Besse Nuclear Power Station Abnormal Procedure DB-OP-02539, Rev. 00, December 28, 1990.

19. "Loss of D2N and DBN." Davis-Besse Nuclear Power Station Abnormal Procedure DB-OP-02540, Rev. 00, December 28, 1990.
20. DeMoss, G., et al. *A Risk-Based Review of Instrument Air Systems at Nuclear Power Plants*. U.S. Nuclear Regulatory Commission Report NUREG/CR-5472, January 1990.
21. Cottrell, W. B., et al. *Precursors to Potential Severe Core Damage Accidents: 1980-1981, A Status Report*. U.S. Nuclear Regulatory Commission Report NUREG/CR-3591, Volume 2, February 1984.
22. Minarick, J. W., et al. *Precursors to Potential Severe Core Damage Accidents: 1984, A Status Report*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4674, Volume 4, May 1987.
23. Minarick, J. W., et al. *Precursors to Potential Severe Core Damage Accidents: 1985, A Status Report*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4674, Volume 2, December 1986.
24. Minarick, J. W., et al. *Precursors to Potential Severe Core Damage Accidents: 1986, A Status Report*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4674, Volume 6, May 1988.
25. Minarick, J. W., et al. *Precursors to Potential Severe Core Damage Accidents: 1987, A Status Report*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4674, Volume 8, July 1989.
26. Minarick, J. W., et al. *Precursors to Potential Severe Core Damage Accidents: 1988, A Status Report*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4674, Volume 10, February 1990.
27. Minarick, J. W., et al. *Precursors to Potential Severe Core Damage Accidents: 1989, A Status Report*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4674, Volume 12, August 1990.
28. "Internal Flooding of Power Plant Buildings." Institute of Nuclear Power Operations Significant Operating Experience Report 85-5, December 30, 1985.
29. Su, N. T. "Effect of Internal Flooding of Nuclear Power Plants on Safety Equipment." U.S. Nuclear Regulatory Commission Engineering Evaluation Report AEOD/E90-07, July 23, 1990.
30. Boyd, G. J. and S. R. Lewis. *Identification of Flood Initiating Events for the Davis-Besse Individual Plant Examination*. Safety and Reliability Optimization Services Report SAROS/92-2, May 1992.
31. DeJong, W. E. "RELAP5 Assessment of Response to Large LOCA Without Injection from Core Flood Tanks." Informal calculation, July 1992.
32. Kuhtenia, D. G. "NPSH for Recirculation Without Containment Heat Removal." Informal calculation, October 1991.
33. Lewis, S. R. "Estimated Timing to Empty BWST for Davis-Besse." Informal calculation, August 1991.
34. Domaleski, E. J. "Task 875 - Reactor Trip Success Criteria." Babcock & Wilcox Letter TED-88-252, April 1, 1988.
35. Lewis, S. R. "Estimated Time to Uncover Core for Small LOCA Without Safety Injection." Informal calculation, August 1991.

36. Darby, J. L. "Verify Adequacy of Two Makeup Pumps to Back Up HPI for Small Break LOCAs (0.003 to 0.02 ft²)." Davis-Besse Nuclear Power Station Calculation C-NSA-65.01-009, April 12, 1988.
37. Skidmore, S. A., et al, "RELAP5 Analyses of Make-Up/HPI Cooling for Davis-Besse Unit 1." Babcock & Wilcox Document No. 51-1159699-00.
38. *Davis-Besse Updated Safety Analysis Report*. Toledo Edison Company, Section 9.2.7, Rev. 4, July 1986.
39. "RPS, SFAS, SFRCS Trip, or SG Tube Rupture." Davis-Besse Nuclear Power Station Emergency Procedure DB-OP-02000, June 18, 1990.
40. "Best-Estimate Steam Generator Single Double-Ended Tube Rupture Analysis." Babcock & Wilcox Company Document No. 77-1152840-00, July 1984.
41. Ruger, C. J. and W. J. Luckas, Jr. *Technical Findings Related to Generic Issue 23: Reactor Coolant Pump Seal Failure*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4948, March 1989.
42. Blakely, D. R. and B. G. Malone. "Evaluation of Potential for RCP Seal Failure Due to Loss of Seal Cooling." Davis-Besse memorandum, July 1992.
43. Weimer, J. A. "LOFW F&B Cooling with Modified MU System for TED." Babcock & Wilcox Document 32-1168039-00, April 16, 1987.
44. DeJong, W. E. "PORV Operability Period." Davis-Besse Nuclear Power Station Calculation C-NSA-65.01-007, March 1988.
45. *Analysis of B&W NSS Response to ATWS Events*. Babcock & Wilcox Company Report BAW-1610, January 1980.
46. "Plant Specific ATWS Analysis for a Loss of Main Feedwater." Babcock & Wilcox Document No. 32-1173570-00, February 26, 1989.
47. *Analysis of Anticipated Transients Without Trip*. Babcock & Wilcox Company Report BAW-10016, September 1972.
48. "ATWS Stress Analysis for Davis-Besse." Babcock & Wilcox Document 12-1174341-00, February 9, 1989.
49. Personal communication, C. Gallier, B&W Nuclear Services Co., to D. G. Kuhtenia, September 17, 1991.
50. Personal communication, F. Szanyi, Davis-Besse Performance Engineering, to D. G. Kuhtenia, September 22, 1991.
51. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. American Nuclear Society, Institute of Electrical and Electronics Engineers, and U.S. Nuclear Regulatory Commission Report NUREG/CR-2300, January 1983.
52. Wright, R. E., et al. *Pipe Break Frequency Estimation for Nuclear Power Plants*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4407, May 1987.
53. "Nuclear Power Experience." Database of Industry Events and Experience, Published by Stoller Power, Inc.
54. Wyckoff, H. *Losses of Off-Site Power at U.S. Nuclear Power Plants Through 1990*. Electric Power Research Institute Report NSAC-166, April 1991.
55. *Plant Performance Committee Trip Reduction Report*. Babcock & Wilcox Owners Group, 1991.

56. *Computerized Aggregation of Reliability Parameters (CARP)*. Science Applications International Corporation, July 1987.
57. Mosleh, A., et al. *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4780 (EPRI NP-5613), January 1988.
58. Fleming, K. N., et al. *A Database of Common Cause Events for Risk and Reliability Evaluations*. Electric Power Research Institute TR-100382, June 1992.
59. Wakefield, D. J., et al. *SHARPI—A Revised Systematic Human Action Reliability Procedure*. Electric Power Research Institute Report NP-7183-SL (Interim Report), December 1990.
60. Davis-Besse Maintenance Management System (DBMMS).
61. Swain, A. D. and H. E. Guttmann. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. U.S. Nuclear Regulatory Commission Report NUREG/CR-1278, August 1983.
62. Swain, A. D. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4772, February 1987.
63. "Operation and Control of Locked Valves." Davis-Besse Nuclear Power Station Operating Procedure DB-OP-00008.
64. "Locked Valve Verification." Davis-Besse Nuclear Power Station Operating Procedure DB-OP-04004.
65. Parry, G. W., et al. *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment*. Electric Power Research Institute Report TR-100259 (Draft), November 1991.
66. Davis-Besse Nuclear Power Station Emergency Plan.
67. Moieni, P., et al. *Modeling of Recovery Actions in PRAs*. Report APG #15 (NUS-5272) for Electric Power Research Institute (Draft), April 1991.
68. *Faulted Systems Recovery Experience*. Electric Power Research Institute Report NSAC-161, May 1992.
69. "CAFTA Users Manual." Science Applications International Corporation, November 30, 1990.
70. "UNCERT User's Manual." Science Applications International Corporation, April 1991.
71. Crutchfield, D. M. "Individual Plant Examination for Severe Accident Vulnerabilities." U.S. Nuclear Regulatory Commission Generic Letter 88-20, November 23, 1988.
72. Galyean, W. J. and D. I. Gertman. *Assessment of ISLOCA Risk—Methodology and Application to a Babcock and Wilcox Nuclear Power Plant*. U.S. Nuclear Regulatory Commission Report NUREG/CR-5604, April 1992.
73. Barrett, R., et al. *Individual Plant Examination: Submittal Guidance*. U.S. Nuclear Regulatory Commission Report NUREG-1335, August 1989.
74. Cramond, W. R. *Shutdown Decay Heat Removal Analysis of a Babcock and Wilcox Pressurized Water Reactor*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4713, March 1987.

75. "Resolution of Unresolved Safety Issue A-17, Systems Interactions in Nuclear Power Plants." U.S. Nuclear Regulatory Commission Generic Letter No. 89-18, September 6, 1989.
76. Thatcher, D. *Evaluation of Systems Interactions in Nuclear Power Plants*. U.S. Nuclear Regulatory Commission Report NUREG-1174, May 1989.
77. Morris, D. J., et al. *B&W Design Review Report for the Byron Jackson N-9000 Seal*. Babcock & Wilcox Company Report BAW-1990, August 1988.
78. Morris, D. J., et al. "N-9000 Seal Appendix R Evaluation." Summary Calculation by Babcock & Wilcox Company, June 24, 1988.
79. *Reactor Safety Study: Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. U.S. Nuclear Regulatory Commission Report WASH-1400 (NUREG 75/014), October 1975.
80. *Qualification Testing of Protection System Instrumentation*. Babcock & Wilcox Company Topical Report BAW-10003A, Rev. 4, January 1976.
81. "Resolution of Generic Issues 48, LCO's for Class 1E Vital Instrument Busses, and 49, Interlocks and LCO's for Class 1E Tie Breakers, Pursuant to 10 CFR 50.54(f)." U.S. Nuclear Regulatory Commission, July 18, 1991.
82. Response to Generic Letter 91-11, "Resolution of Generic Issues 48, LCO's for Class 1E Vital Instrument Busses, and 49, Interlocks and LCO's for Class 1E Tie Breakers, Pursuant to 10 CFR 50.54(f)" for the Davis-Besse Nuclear Station, Unit No. 1. U.S. Nuclear Regulatory Commission, August 17, 1992.
83. Station 125 vdc Distribution System Failure Analysis Manual, Drawing E-2013 series.

Part 4
BACK-END ANALYSIS

Contents

<u>Section</u>	<u>Page</u>
List of Tables	vi
List of Illustrations	vii
1 PLANT DATA AND PLANT DESCRIPTION	1
1.1 Site Location.....	1
1.2 Site Characteristics.....	1
1.3 Plant Description.....	1
1.4 Plant Systems.....	2
2 PLANT MODELS AND METHODS FOR PHYSICAL PROCESSES	55
2.1 Severe-Accident Response Using MAAP	55
2.2 Investigation of Specific Issues.....	66
2.2.1 Ex-Vessel Corium Coolability	66
2.2.2 Submerged Vessel Corium Cooling.....	68
2.2.3 Creep Rupture	69
2.2.4 Flammable Gas Generation and Combustion	73
2.2.5 Containment Performance Improvement Program	76
3 BINS AND PLANT-DAMAGE STATES	77
3.1 Attributes of Plant-Damage States.....	77
3.2 Definition of Core-Damage Bins.....	81
3.3 Bridge Trees	84
3.3.1 Top Events in the Bridge Trees.....	84
3.3.2 Description of Bridge Trees	86
3.4 Summary of Plant-Damage States	97
4 CONTAINMENT FAILURE CHARACTERIZATION	109
4.1 Capacity of the Containment Vessel	109
4.1.1 Assessment of Containment Vessel Strength	110
4.1.2 Development of a Distribution for Pressure Capacity.....	110
4.2 Other Potential Failure Mechanisms	111
4.3 Overall Containment Failure Characterization.....	117
5 CONTAINMENT EVENT TREE	119
5.1 Development of the Containment Event Tree	119
5.2 Top Events in the CET.....	126
5.2.1 Event A: Arrest of Core Damage In-Vessel.....	127

Contents (continued)

<u>Section</u>	<u>Page</u>
5	CONTAINMENT EVENT TREE (continued)
5.2.2	Event R: Submerged-Vessel Cooling of Core Debris..... 133
5.2.3	Event V: Containment Bypass Is Prevented 134
5.2.4	Events B ₁ and B ₂ : Containment Isolation..... 139
5.2.5	Event E: Early Containment Failure Prevented..... 141
5.2.6	Event C: Ex-Vessel Cooling of Core Debris..... 162
5.2.7	Event D: No Failure of Containment Side Wall 167
5.2.8	Event L: Late Failure of Containment Prevented 169
5.2.9	Event F: No Late Revaporization Release 173
5.2.10	Event S: Scrubbing of Fission Products..... 177
5.2.11	Common Supporting Logic for Top Events 178
6	ACCIDENT PROGRESSION AND QUANTIFICATION FOR THE CONTAINMENT EVENT TREE 199
6.1	Containment Response for Representative Accidents..... 199
6.1.1	Large LOCAs 199
6.1.2	Medium LOCAs 200
6.1.3	Small LOCAs 208
6.1.4	Transients 212
6.1.5	Steam Generator Tube Ruptures..... 220
6.2	Quantification of the CET 224
6.3	Frequencies for CET Outcomes 227
6.3.1	Containment Bypass 230
6.3.2	Early Containment Failure 233
6.3.3	Side Wall Failure 235
6.3.4	Late Containment Failure..... 235
6.3.5	Basemat Melthrough 237
6.3.6	Prevention of Vessel Failure 240
6.3.7	Summary of CET Results 240

Contents (continued)

<u>Section</u>	<u>Page</u>
7 RADIONUCLIDE RELEASE CHARACTERIZATION	243
7.1 Estimation of Release Fractions	243
7.2 Definition of Release Categories	245
7.2.1 Release Category 1	245
7.2.2 Release Category 2	247
7.2.3 Release Category 3	247
7.2.4 Release Category 4	249
7.2.5 Release Category 5	249
7.2.6 Release Category 6	251
7.2.7 Release Category 7	251
7.2.8 Release Category 8	253
7.2.9 Release Category 9	253
7.3 Estimated Release Frequencies	253
REFERENCES FOR PART 4	261

List of Tables

<u>Table</u>		<u>Page</u>
1-1	Reactor Core and Vessel Data	16
1-2	Primary System Data	20
1-3	High Pressure Injection System	25
1-4	Decay Heat Removal System	25
1-5	Core Flood Tanks	26
1-6	Containment Structure	36
1-7	Interior Structural Heat Sinks	36
1-8	Containment Spray System	39
1-9	Containment Air Cooling System (Emergency Operation)	39
1-10	Component Cooling Water System	49
1-11	Service Water System	53
1-12	Makeup System	53
2-1	Model Benchmarks Used in the IDCOR Program	56
3-1	Summary of Core-Damage Bins	83
3-2	Containment Systems States from Bridge Trees	99
5-1	Probability Scale for CET Basic Events	128
5-2	RCS Pressure Ranges of Interest Prior to Vessel Breach	181
6-1	Conditional Probabilities of Containment Failure Modes	228
7-1	Release Category 1	246
7-2	Release Category 2	248
7-3	Release Category 3	248
7-4	Release Category 4	250
7-5	Release Category 5	250
7-6	Release Category 6	252
7-7	Release Category 7	252
7-8	Release Category 8	254
7-9	Release Category 9	254
7-10	Frequencies and Conditional Probabilities of Release Categories	257

List of Illustrations

<u>Figure</u>	<u>Page</u>
1-1 Station General Arrangement - Section "A-A"	3
1-2 Station General Arrangement - Section "B-B"	5
1-3 Station General Arrangement - Section "C-C"	7
1-4 Station General Arrangement - Elevation 545'	9
1-5 RCS and Supporting Structures - Elevation.....	11
1-6 Functional Drawing - RCS	13
1-7 Reactor Vessel and Internals General Arrangement	15
1-8 Incore Penetration Locations.....	18
1-9 Incore Instrumentation Penetrations	19
1-10 Emergency Core Cooling System Flow Diagram	23
1-11 Key Penetration Locations	27
1-12 Containment Internal Structures	29
1-13 Containment Internal Structures Sheet 1	31
1-14 Containment Internal Structures Sheet 2	33
1-15 Functional Drawing - Containment Spray System.....	37
1-16 Functional Drawing - Main Steam Reheat System	41
1-17 Functional Drawing - Main Feedwater System	43
1-18 Once-Through Steam Generator Cross Sectional Diagram	46
1-19 Functional Drawing - Auxiliary Feedwater System	47
1-20 Functional Drawing - Makeup and Purification System.....	51
2-1 Application of PWR Primary System Nodalization to a B&W Design.....	61
2-2 Davis-Besse Containment Nodalization	63
2-3 Modeling of Inter-Compartment Flows for Davis-Besse.....	64
2-4 Creep Rupture for Hot Legs.....	70
2-5 Creep Rupture for Steam Generator Tubes.....	71
2-6 Creep Rupture for Surge Line	72
2-7 Nominal Flammability Limits for Hydrogen	75
3-1 Bridge Tree for Core-Damage Bin AIX.....	88
3-2 Bridge Tree for Core-Damage Bins ARX and MRX.....	89
3-3 Bridge Tree for Core-Damage Bin MIX.....	90
3-4 Bridge Tree for Core-Damage Bins SIY, SIN, and Tin.....	92
3-5 Bridge Tree for Core-Damage Bins SRY, SRN, and TRN.....	94

List of Illustrations (continued)

<u>Figure</u>	<u>Page</u>
3-6 Bridge Tree for Core-Damage Bin TIY.....	95
3-7 Bridge Tree for Core-Damage Bins RIY and RIN.....	96
3-8 Bridge Tree for Core-Damage Bins RRY and RRN	97
4-1 Probability of Containment Failure Due to Internal Pressure.....	112
4-2 Seal Life as a Function of Time at Temperature	116
5-1 Generic B&W Containment Event Tree	120
5-2 Davis-Besse Containment Event Tree	121
5-3 Logic for Failure of CET Event A—Core Damage Not Arrested In-Vessel	130
5-4 Logic for Failure of CET Event R—Submerged-Vessel Cooling of Core Debris Fails.....	135
5-5 Logic for Failure of CET Event V—Containment Bypass	136
5-6 Logic for Failure of CET Event E—Early Containment Failure	142
5-7 Cumulative Probability Distributions for In-Vessel Generation of Hydrogen.....	152
5-8 Cumulative Probability Distribution for Pressure Rise at Vessel Breach Due to Pressurized Melt Ejection	160
5-9 Logic for Failure of CET Event C—Core Debris Fails to be Cooled Ex- Vessel.....	163
5-10 Logic for Failure of CET Event D—Containment Side Wall Failure from Ablation by Core Debris	168
5-11 Logic for Failure of CET Event L—Late Containment Failure	170
5-12 Logic for Failure of CET Event F—Late Revaporization Release from RCS	175
5-13 Logic for Failure of CET Event S—Fission Products Not Scrubbed Prior to Release.....	179
5-14 Common CET Supporting Logic for Low RCS Pressure Prior to Vessel Breach.....	182
5-15 Common CET Supporting Logic for Intermediate RCS Pressure Prior to Vessel Breach.....	190
5-16 Common CET Supporting Logic for Moderately High RCS Pressure Prior to Vessel Breach.....	191
5-17 Common CET Supporting Logic for Very High RCS Pressure Prior to Vessel Breach.....	193
5-18 Common CET Supporting Logic for Debris Dispersal to Lower Elevation	195
6-1 Large LOCA Response (1 of 3)	201
6-2 Large LOCA Response (2 of 3)	202
6-3 Large LOCA Response (3 of 3)	203

List of Illustrations (continued)

<u>Figure</u>	<u>Page</u>
6-4 Medium LOCA Response (1 of 3).....	205
6-5 Medium LOCA Response (2 of 3).....	206
6-6 Medium LOCA Response (3 of 3).....	207
6-7 Small LOCA Response (1 of 4).....	209
6-8 Small LOCA Response (2 of 4).....	210
6-9 Small LOCA Response (3 of 4).....	211
6-10 Small LOCA Response (4 of 4).....	213
6-11 Transient Response (1 of 5)	215
6-12 Transient Response (2 of 5)	216
6-13 Transient Response (3 of 5)	217
6-14 Transient Response (4 of 5)	218
6-15 Transient Response (5 of 5)	219
6-16 Steam Generator Tube Rupture Response (1 of 5)	221
6-17 Steam Generator Tube Rupture Response (2 of 5)	222
6-18 Steam Generator Tube Rupture Response (3 of 5)	223
6-19 Steam Generator Tube Rupture Response (4 of 5)	225
6-20 Steam Generator Tube Rupture Response (5 of 5)	226
6-21 Overall Summary of Conditional Probabilities for Containment Failure Modes	231
6-22 Contributions of Plant-Damage States to Frequency of Containment Bypass	232
6-23 Contributions of Plant-Damage States to Frequency of Early Containment Failure	234
6-24 Contributions of Plant-Damage States to Frequency of Side Wall Failure of Containment	236
6-25 Contributions of Plant-Damage States to Frequency of Late Containment Failure	238
6-26 Contributions of Plant-Damage States to Frequency of Basemat Melthrough	239
7-1 Overall Conditional Probabilities for Release Categories Given Core Damage	255

Section 1

PLANT DATA AND PLANT DESCRIPTION

This section provides an overview of the plant design, with emphasis on the relevance of plant features to the assessment of containment response. Further detail regarding the operation of plant systems and their roles with respect to the potential for core-damage sequences can be found in Section 2.1 of Part 3.

1.1 SITE LOCATION

The Davis-Besse Nuclear Power Station is located on the southwestern shore of Lake Erie in Ottawa County, Ohio. The land area surrounding the site is generally agricultural with no major industry in the vicinity. The site is approximately six miles northeast of Oak Harbor, Ohio which is the closest town.

The station structures are located approximately in the center of the site, 3000 feet from the shoreline, which provides a minimum exclusion distance of 2400 feet from any point on the site boundary. The low population zone has been established as an area within a radius of two miles from the center of the containment structures.

1.2 SITE CHARACTERISTICS

The topography of the site and vicinity is flat with marsh areas bordering Lake Erie with the upland areas rising from ten to fifteen feet above the lake low water datum level. The site itself varies in elevation from marsh bottom to approximately six feet above lake level. The site areas surrounding the station structures have been built up from six to fourteen feet above the existing grade to an elevation of 584 feet above sea level, or 15.4 feet above Lake Erie Low Water Datum of 568.6 feet IGLD (International Great Lakes Datum). This provides flood protection from the maximum credible water level condition of Lake Erie. The three sides of the station area with exposure to the lake are provided with a dike to elevation 591 IGLD to protect the facility from wave effects during the maximum credible water level condition. The site is underlain by dolomitic limestone, fourteen to twenty-two feet below the original site grade.

1.3 PLANT DESCRIPTION

The Davis-Besse Nuclear Power Station has a PWR nuclear steam supply system furnished by The Babcock & Wilcox Company. The Bechtel Corporation and its affiliate, The Bechtel Company, provided to Toledo Edison architect-engineering services for the station design. Figures 1-1 through 1-4 show the general arrangement of the major components of the Davis-Besse Nuclear Power Station.

The reactor coolant system (RCS) consists of the reactor vessel, two vertical once-through steam generators, four shaft-sealed, vertical suction, horizontal discharge, single-stage centrifugal coolant circulating pumps, an electrically heated pressurizer, and interconnecting piping. See Figure 1-5 for the general arrangement of the reactor coolant system and Figure 1-6 for a functional flow diagram of the system. The system is arranged as two heat transport loops, each with two circulating pumps and one steam generator. The RCS is designed to contain and circulate reactor coolant at pressures and flows necessary to transfer the heat generated in the reactor core to the secondary fluid in the steam generators. In addition to serving as a heat transport medium, the coolant also serves as a neutron moderator and reflector, and as a solvent for the soluble boron utilized in chemical shim reactivity control. Lithium hydroxide is added to the RCS for pH control, and hydrazine is added for oxygen control.

The reactor and the nuclear steam supply system are contained within the reactor building, a prestressed, reinforced concrete cylinder and dome with a free standing steel liner.

1.4 PLANT SYSTEMS

This section is intended to provide an overview of the major plant systems. The focus of this section is on the system designs. As indicated previously, additional detail relating to the roles of the systems in the front-end analysis can be found in Section 2.1 of Part 3.

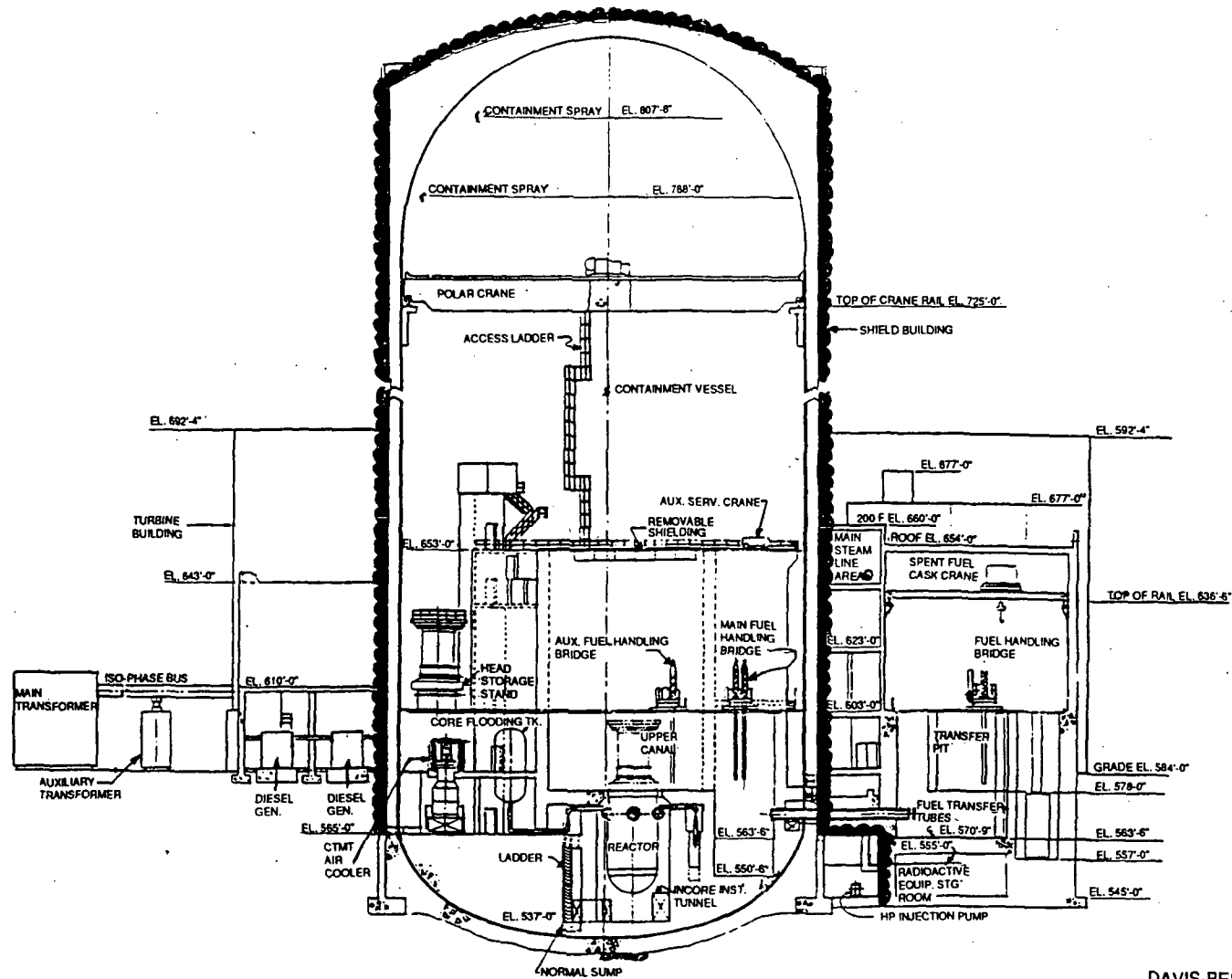
Reactor and Reactor Coolant System

The Davis-Besse Nuclear Station has a Babcock & Wilcox 177FA (fuel assembly) reactor and a raised loop RCS. The raised loop is unique in that all other B&W 177 plants are lower loop. The raised loop design provides enhanced natural circulation capabilities during conditions in which all four reactor coolant pumps are inoperative. See Figure 1-5 for the general arrangement of the RCS.

Each of the 177 fuel assemblies in the reactor core contains 208 fuel rods made of uranium dioxide pellets enclosed in zircaloy tubes with welded end plugs. The tubes are constrained and supported in the fuel assemblies by spacer grid assemblies and the upper and lower end fitting assemblies.

The core is contained within the reactor vessel, which consists of a cylindrical shell, a spherically dished bottom head, and a "O-ring" fitted ring flange to which a removable reactor closure head is bolted. The core support assembly rests on a ledge on the inside of the vessel flanges. It is held in place by the closure head which is secured in place by bolts. See Figure 1-7 for the general arrangement of the reactor vessel and internals, and Table 1-1 for specific core and vessel data.

Within the region above the core, the reactor coolant flow splits into two outlet hot leg nozzles. Referring to Figures 1-5 and 1-7, the flow is carried along the hot leg piping to the upper plenums of the two once-through steam generators (one generator in each loop).



SECTION "A"- "A"

Figure 1-1

DAVIS-BESSE NUCLEAR POWER STATION
GENERAL ARRANGEMENT
SECTION "A"- "A"

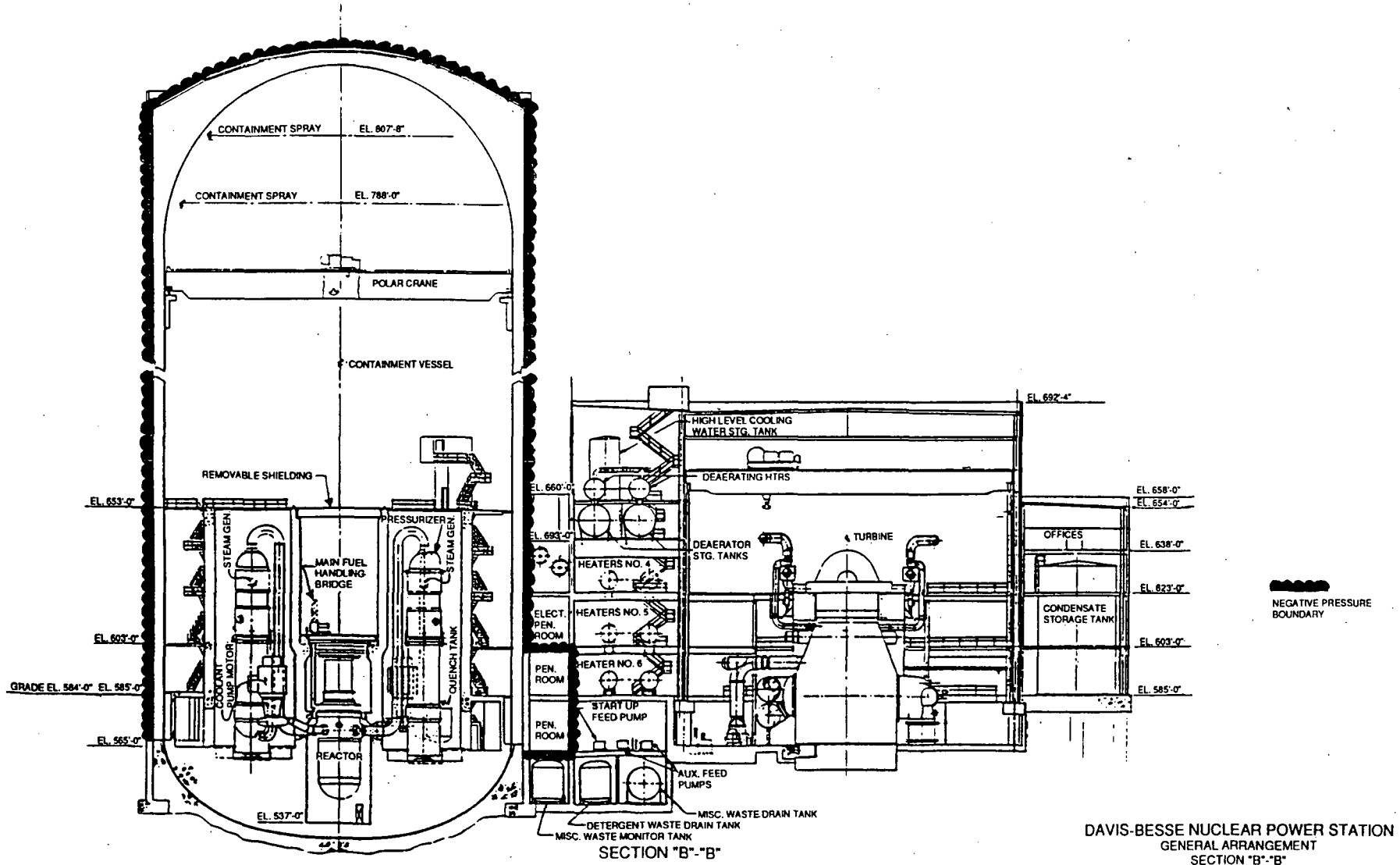
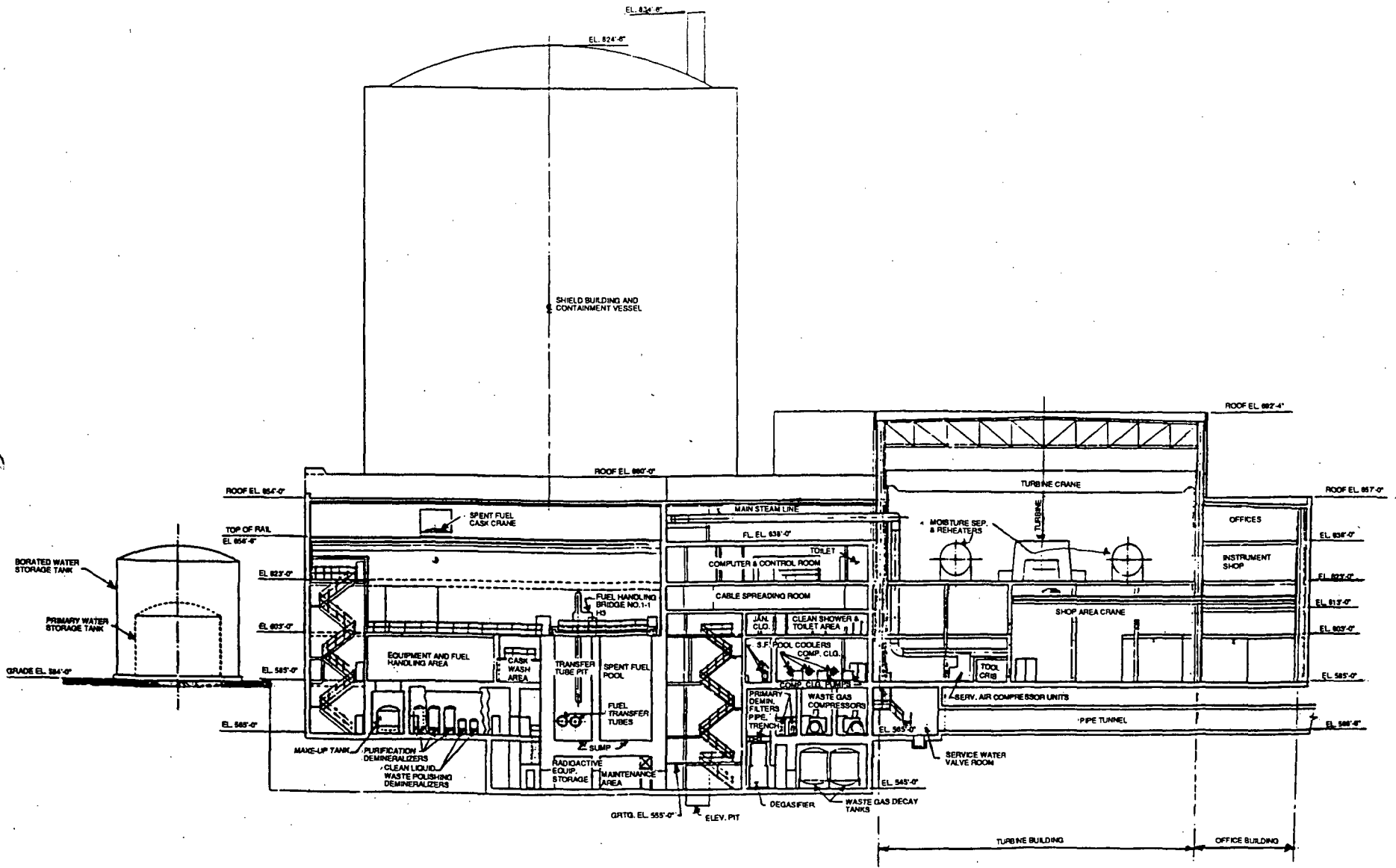


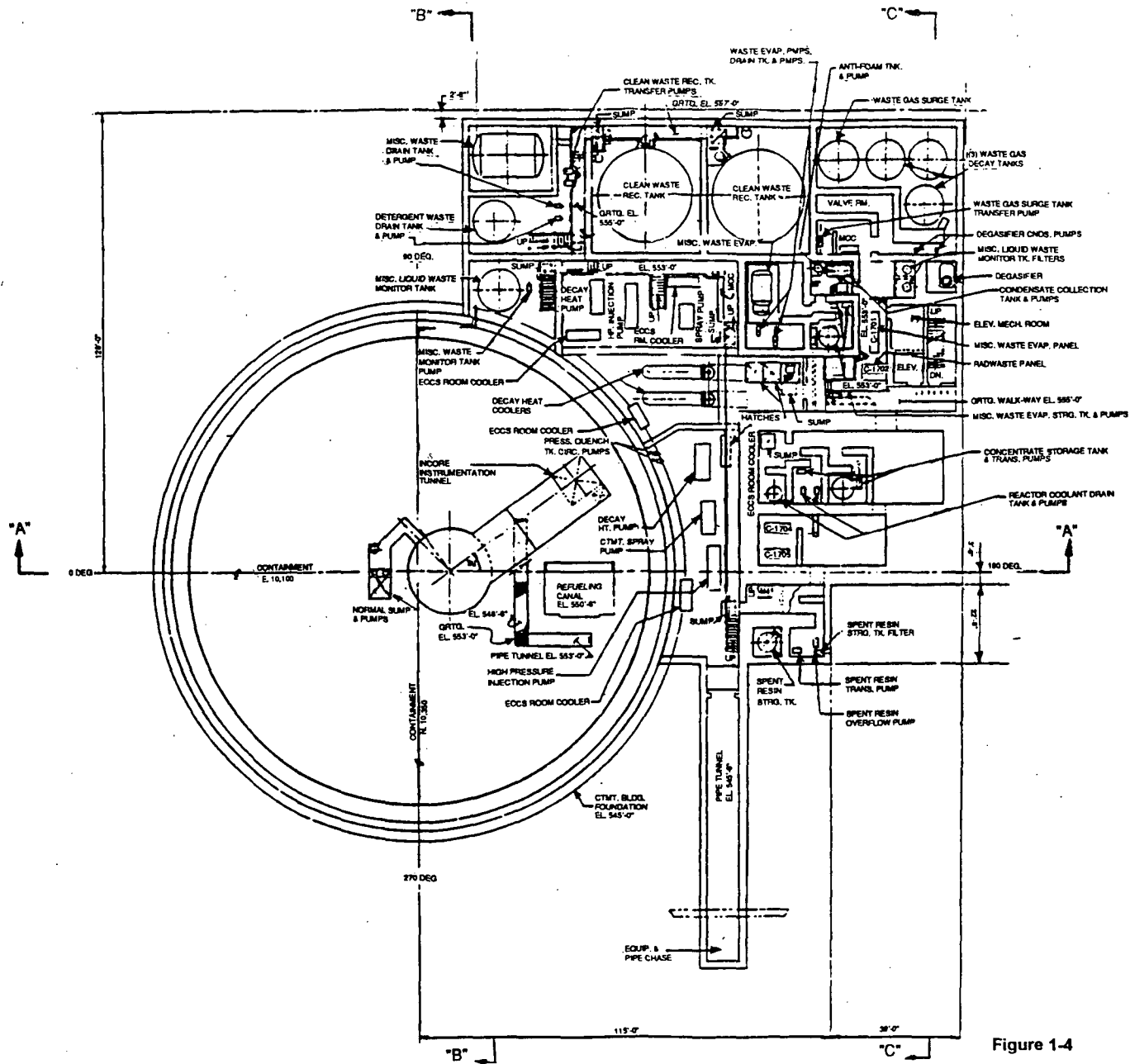
Figure 1-2



DAVIS-BESSE NUCLEAR POWER STATION
GENERAL ARRANGEMENT
SECTION "C"-"C"

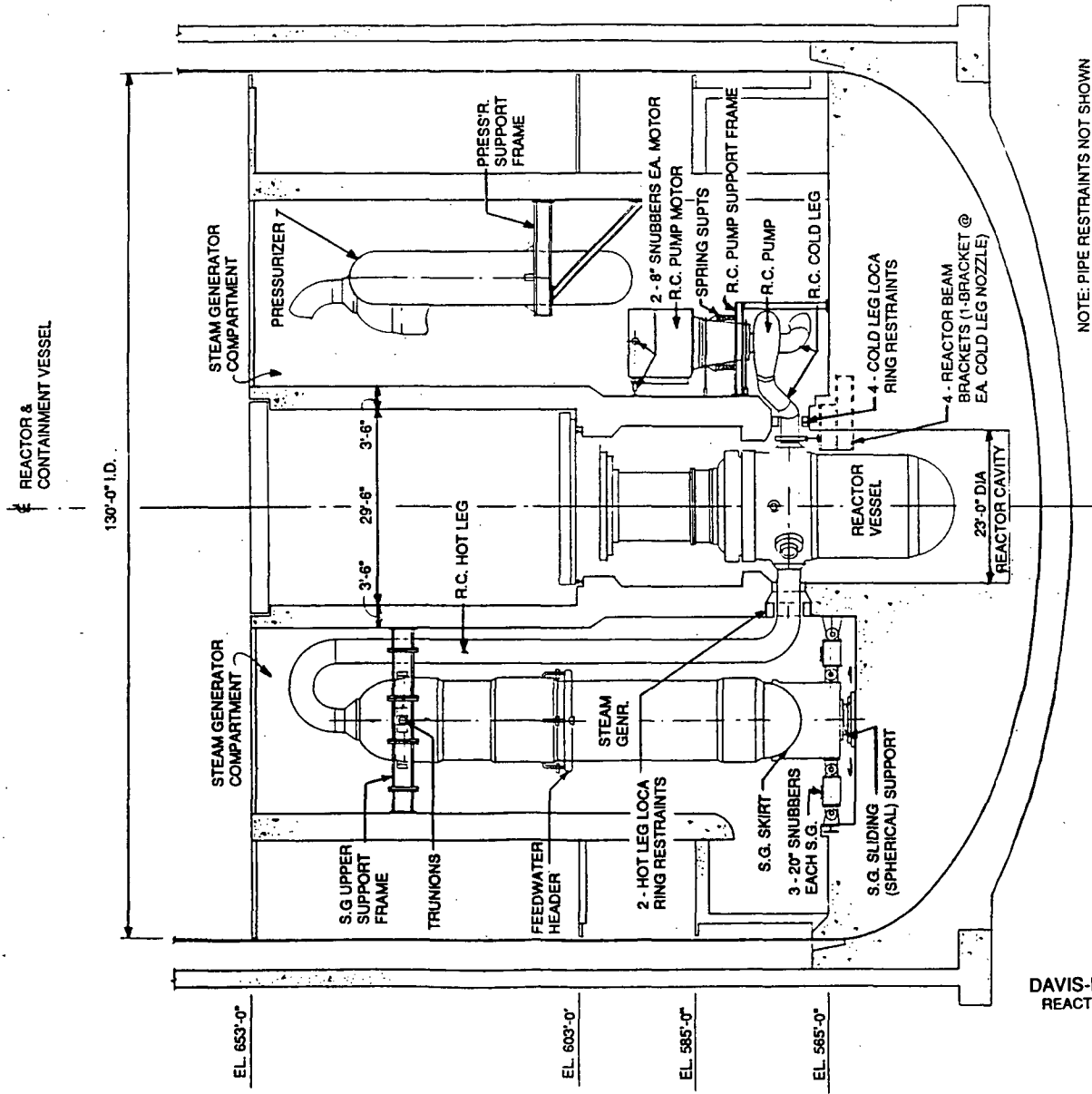
SECTION "C"-"C"

Figure 1-3



DAVIS-BESSE NUCLEAR POWER STATION
 GENERAL ARRANGEMENT PLAN
 AT ELEVATION 545'

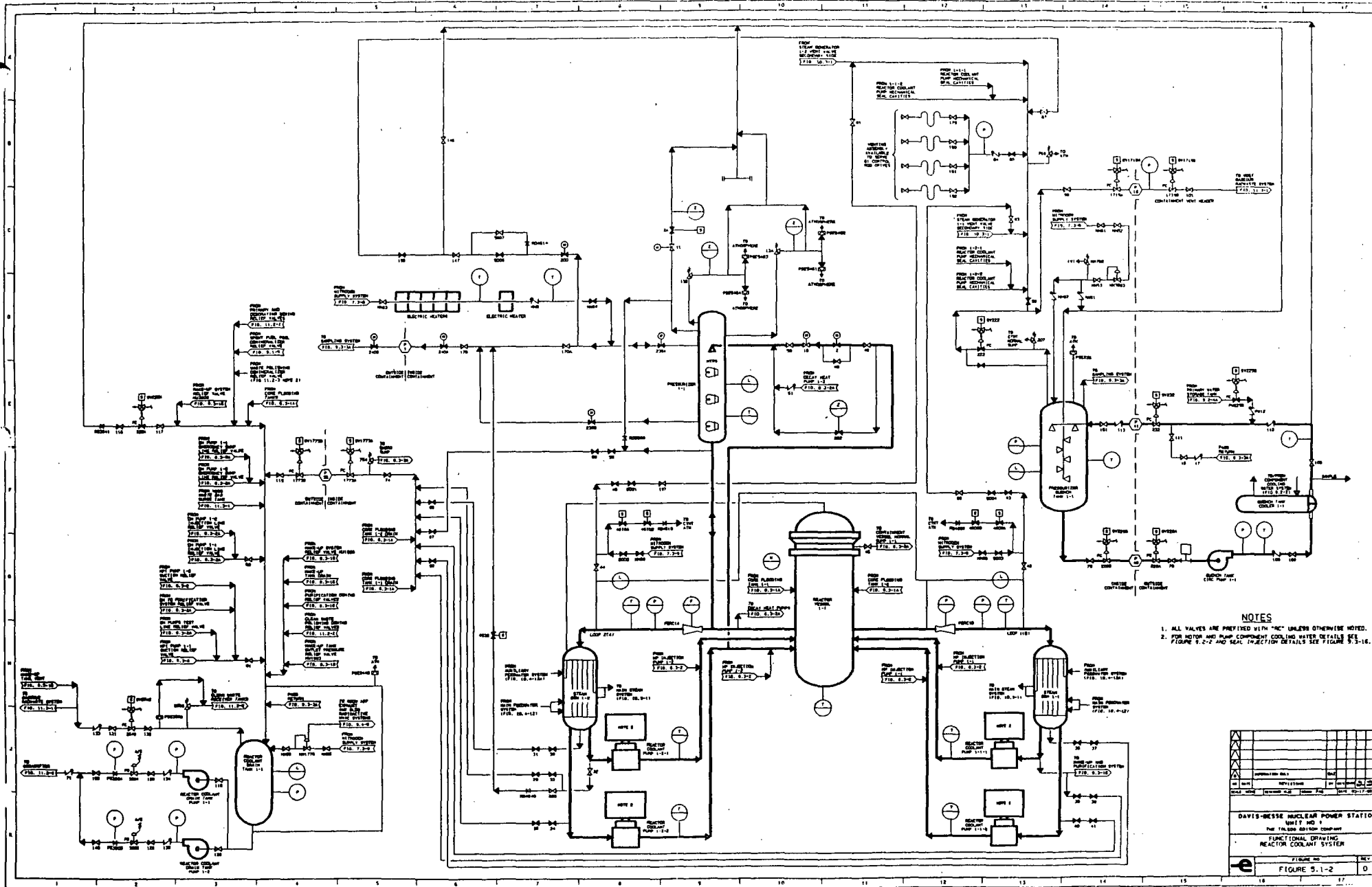
Figure 1-4



NOTE: PIPE RESTRAINTS NOT SHOWN

DAVIS-BESSE NUCLEAR POWER STATION
 REACTOR COOLANT SYSTEM AND SUPPORTING
 STRUCTURES - ELEVATION

Figure 1-5



NOTES

1. ALL VALVES ARE PREFIXED WITH "RC" UNLESS OTHERWISE NOTED.
2. FOR MOTOR AND PUMP COMPONENT COOLING WATER DETAILS SEE FIGURE 9.2-2 AND SEAL INJECTION DETAILS SEE FIGURE 9.3-16.

DAVIS-BESSE NUCLEAR POWER STATION UNIT 1 AND 2 THE TOLSON ADVISON COMPANY FUNCTIONAL DRAWING REACTOR COOLANT SYSTEM	
FIGURE NO. 2 SHEET NO. 1-2	REV. D

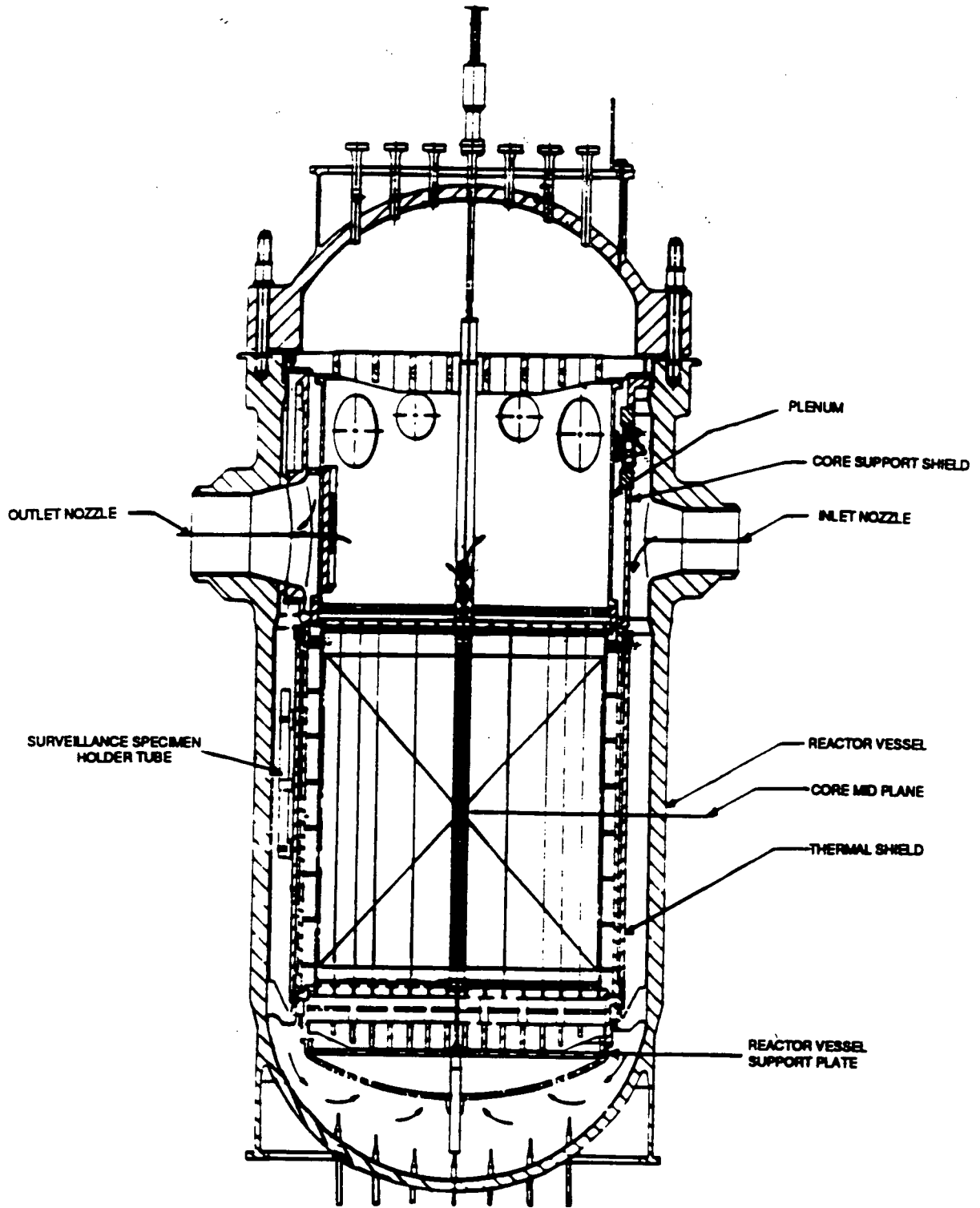


Figure 1-7. Reactor Vessel and Internals: General Arrangement

**Table 1-1
Reactor Core and Vessel Data**

Parameter	Value
Core full power	2772 MWt
Mass of UO ₂ in core	207,290 lbm
Fuel enrichment	3.23%
Mass of Zr in core	51,650 lbm
Mass of Zr in cladding, surrounding the fuel	45,000 lbm
Mass of control rod absorber material	5,003 lbm
Composition of control rods	Ag/In/Cd (80/15/5)
Mass of steel in vessel & core structures	
plenum assembly and core-support shield assembly	156,500 lbm
core-support plates	48,000 lbm
reactor vessel (not including upper head closure assembly)	664,000 lbm
thermal shield & core barrel assembly upper head	163,300 lbm
Physical dimensions	
vessel diameter	14.2 ft
minimum vessel thickness	0.427 ft
active fuel length	11.93 ft
fuel assembly size	15 x 15 fuel rod configuration

The RCS flow makes a single pass downward through the tube side of the steam generator in a counter-flow direction to the upward secondary side boiling flow. There are two exit nozzles in the lower plenum of each steam generator. The flow from each exit nozzle enters a short section of piping and then passes into the suction of a shaft-sealed coolant circulating pump. From the discharge of the pump, piping then carries the flow from each of the coolant pumps to four inlet nozzles symmetrically placed around the reactor vessel perimeter. The inlet and outlet nozzles are located above the top of the core so as to maintain a flooded core following a loss-of-coolant accident (LOCA). The flow of the four cold legs is turned downward and is recombined in the vessel downcomer, which is an annulus formed between the thermal shield surrounding the core and the inside wall of the reactor vessel. The flow is turned upward in the lower plenum of the vessel, passes through the flow distributor plate and the reactor core, and finally closes the path above the core assembly. An additional flow path from the upper vessel to the downcomer, which bypasses the steam generators, can exist through the reactor vessel vent valves during a sufficiently large cold leg LOCA or during certain phases of natural circulation in the RCS.

There are two smaller inlet nozzles located between the main inlet nozzles on the perimeter of the reactor vessel which provide injection points for the emergency core cooling system (ECCS) as well as inlets for decay heat cooling flow.

As Figure 1-8 shows, the bottom head of the vessel is penetrated by instrumentation nozzles which provide for passage of the incore temperature and neutron flux instrumentation. The details of these incore instrumentation penetrations are shown in Figure 1-9. The vessel closure head is penetrated by flanged nozzles to which the control rod drive mechanisms are attached. One of these flanged nozzles, not connected to a control rod drive mechanism, is attached to a 2.5-inch pipe which provides a flow connection to the upper plenum of one of the steam generators. This path, which is unique in Babcock & Wilcox designed reactor coolant systems, is designed to allow the transport of condensable and non-condensable gasses out of the upper vessel head in the event of a bubble formation within the upper head of the vessel.

During normal operation, the RCS pressure is controlled by electric heaters in the lower portion of the pressurizer and by condensation of steam in the vapor space caused by the injection of cold leg reactor coolant through a pressurizer spray nozzle located in the top vapor space of the pressurizer. The pressurizer provides a compressible vapor space surge volume to accommodate fluctuations in reactor coolant volume and pressure. The pressurizer is equipped with a pilot-operated relief valve (PORV) and two safety relief valves which protect the RCS against overpressure. The PORV can also be operated manually from the control room to reduce RCS pressure. Flow from the PORV is routed to a quench tank while flow from the safety relief valves is discharged into the containment atmosphere. Refer to Table 1-2 for specific primary system data.

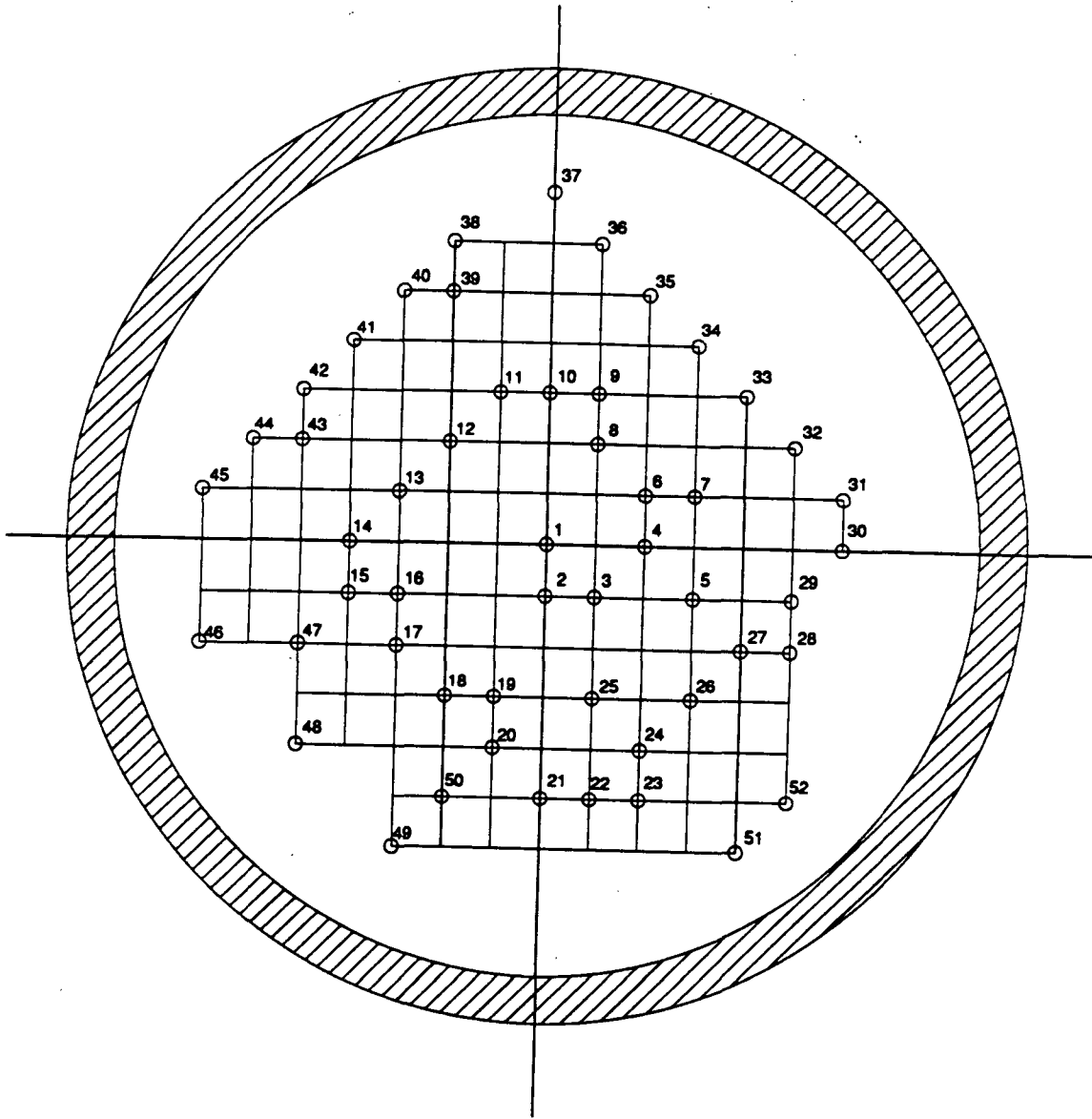


Figure 1-8. Incore Penetration Locations

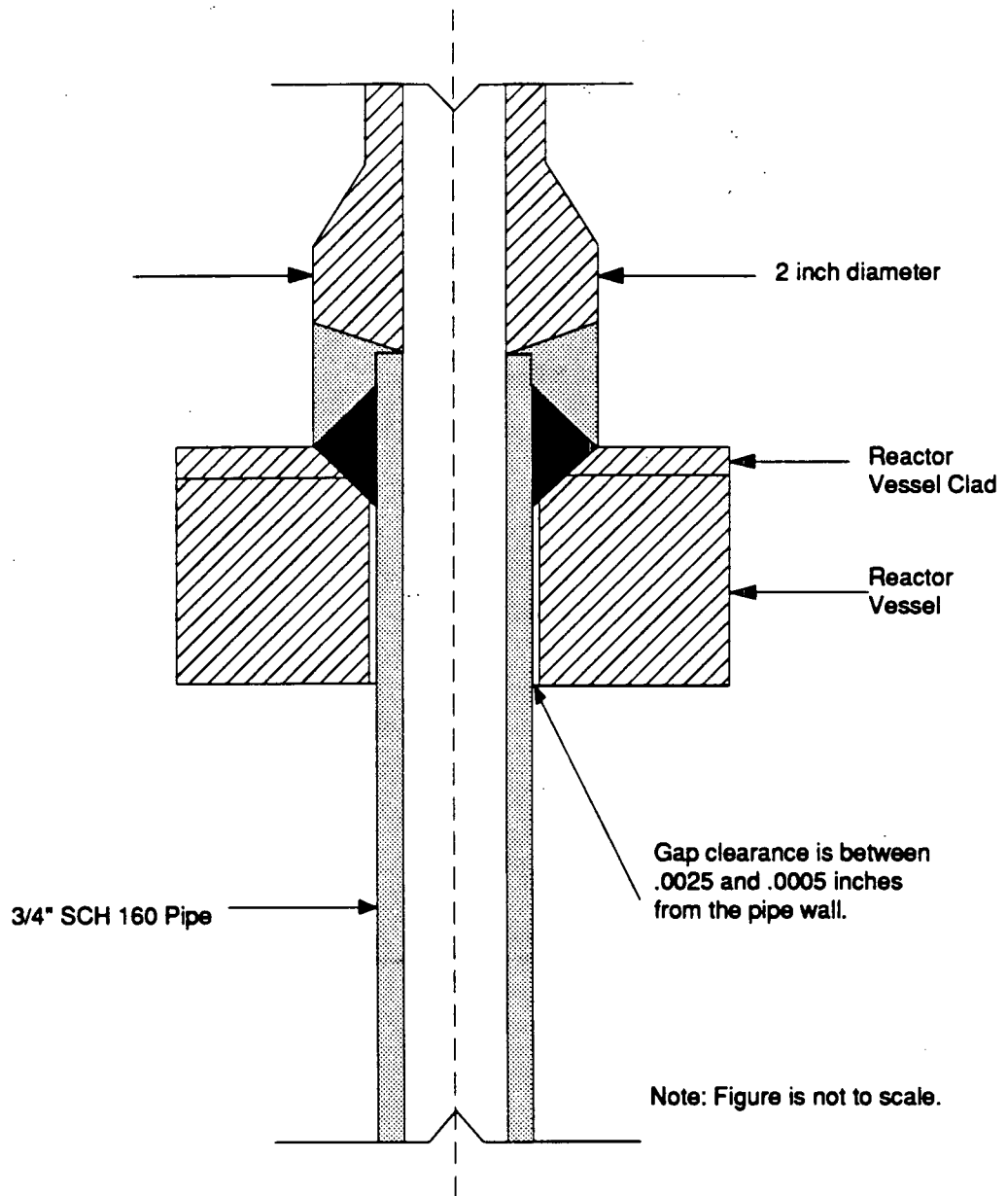


Figure 1-9. Incore Instrumentation Locations

**Table 1-2
Primary System Data**

Parameter	Value
Total water inventory (normal full power)	83,500 gal
Pressurizer water inventory (normal full power)	6460 gal
Pressurizer steam inventory (normal full power)	638 cubic ft
Steam generators	
type	vertical, once-through
number	2
Total primary flow rate (normal full power)	76 mpph/loop
PORV capacity	223,470 lbm/hr @ 2450 psig
Primary safety valve capacity	375,985 lbm/hr steam @ 2575 psig
Safety valve settings	2 at 2500 psig
System temperature (normal full power)	Tave = 582 F
System pressure (normal full power)	2155 psig
Pressurizer temperature (normal full power)	647 F

Protective and Control Systems

The reactor protection system (RPS) monitors parameters related to safe operation of the RCS and will initiate a gravity insertion of all control rods when a transient condition causes one or more of the predetermined setpoints to be exceeded.

The safety features actuation system (SFAS) monitors system variables to detect a loss of RCS boundary integrity. Upon detection of a limiting condition, it initiates operation of the high pressure injection (HPI), low pressure injection (LPI), containment vessel cooling and isolation, containment vessel spray, and emergency ventilation systems as dictated by plant conditions. It also starts the two emergency diesel generators.

The steam feedwater rupture control system (SFRCS) is designed to detect conditions under which the steam or feedwater system loses integrity. The faulted steam generator is then isolated.

The anticipatory reactor trip system (ARTS) is designed to detect the failure of certain plant components (such as the main turbine) and then provides an early "anticipatory" trip signal to the reactor.

Normal plant control of the reactor coolant system is accomplished by the integrated control system (ICS). The ICS is an electronic analog control system with the principal job of matching the reactor thermal power and the energy removal capability of the steam generator feedwater flow to the electrical generation demand. It does this while keeping certain key plant variables such as RCS average temperature and secondary pressure within acceptable limits. The principal plant variables under its direction are normally reactor control rod position, feedwater turbine speed, feedwater valve position and control valve delta pressure, and turbine control valve position. Operators may override the individual control functions by placing the particular control module in manual or "hand".

Emergency Core Cooling Systems

As Figure 1-10 shows, the emergency core cooling system is composed of the HPI system, the decay heat removal (DHR) system, and the core flood system. The following is a description of each.

The HPI system injects borated water into the core at high RCS pressure when a LOCA has occurred. Specifically, it is designed to prevent uncovering of the core in the case of a small RCS piping leak of less than 0.5 ft² equivalent break size. In the event that a pipe break is large enough to exceed the makeup system capacity and small enough to maintain pressure above the LPI initiation setpoint, the HPI pump can be aligned to take suction from the DHR pump which has the effect of increasing the head and flow capabilities of the HPI. The HPI pumps in a stand-alone configuration cannot develop sufficient head to pump significant flow against full RCS pressure. See Table 1-3 for specific high pressure injection information.

During normal conditions, the DHR system removes fission product decay heat and sensible heat from the RCS during the latter stages of cooldown. In the event of a LOCA, the DHR system injects borated water into the reactor vessel for long-term emergency core cooling in the LPI mode. The DHR system also provides auxiliary spray to the pressurizer for complete depressurization when main spray is not available, maintains a low RCS temperature during refueling operations, and provides a means of filling and partial draining of the refueling canal. Either path of DHR is sufficient to supply long term emergency core cooling for the entire spectrum of rupture sizes in the RCS. See Table 1-4 for specific DHR system information.

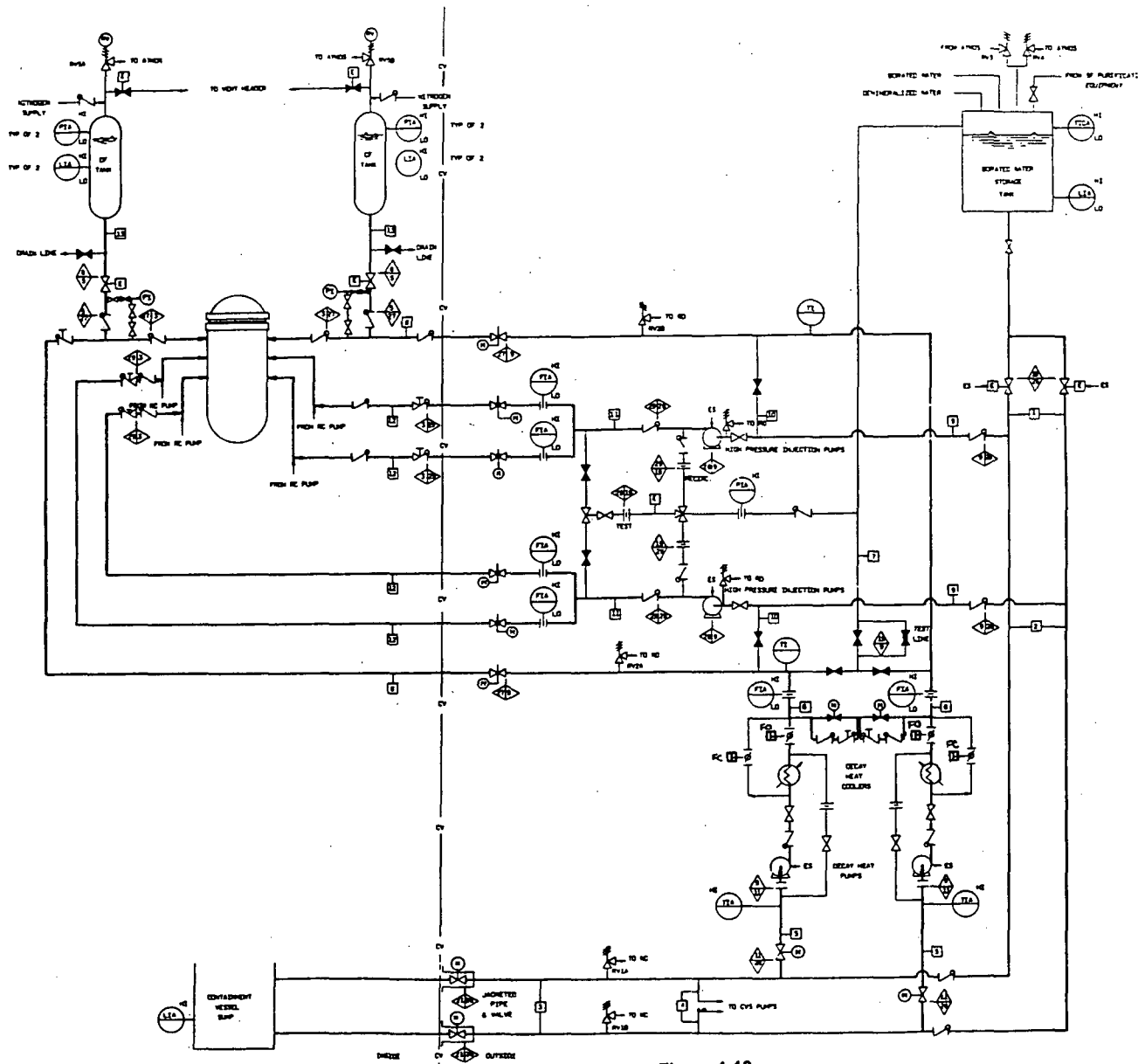
The core flood system is a passive engineered safety feature which stores borated water in two nitrogen-pressurized tanks to be automatically injected into the reactor vessel following a loss of RCS pressure. The core flood tanks contain a sufficient volume of borated water to perform a refill of the core following a design-basis accident. The core flood system, which is located within the reactor building, is composed of two pressurized flooding tanks, each directly connected to a reactor vessel nozzle. The system provides automatic, passive core flooding by an initiation of the flow of borated water when RCS pressure decreases below the core flood tank pressure. Specific information can be found in Table 1-5.

Containment Safety Features

The containment for the station consists of three basic structures: a steel containment vessel, a reinforced concrete shield building, and the internal structures. Figure 1-11 illustrates the overall size and the key penetration locations of the Davis-Besse containment building. Additional features of the containment building may be seen in previous Figure 1-5. Figures 1-12 through 1-14 show various views of the reactor pit and incore instrumentation tunnel.

The containment vessel is a cylindrical steel pressure vessel with hemispherical dome and ellipsoidal bottom. It is completely enclosed by a reinforced concrete shield building having a cylindrical shape with a shallow dome roof. An annular space is provided between the wall of the containment vessel and shield building, and clearance is also provided between the containment vessel and dome of the shield building. The containment vessel and shield building are supported on a concrete foundation founded on a firm rock structure. With the exception of the concrete under the containment vessel there are no structural ties between the containment vessel and the shield building above the foundation slab. Above this there is unlimited freedom of differential movement between the containment vessel and the shield building.

The containment internal structures are comprised of the reactor cavity, the primary shield wall, the secondary shield wall, the refueling pool, the operating floors, miscellaneous equipment supports, stairs, and service missile shields. The primary coolant system, including the reactor, steam generators, pressurizer, and reactor coolant pumps, is supported by these structures. Internal walls and floors are constructed of reinforced concrete. Structures are supported by the massive concrete fill within the containment vessel bottom head. The



- ▲ 2500 PSIG - 200P
- ▲ 2500 PSIG - 200P
- ▲ 700 PSIG - 200P
- ▲ 400 PSIG - 200P
- ▲ 300 PSIG - 200P
- ▲ 75 PSIG - 200P
- ▲ 6000 GROSS PRESS - 200P
- ▲ 75 PSIG - 200P
- ▲ 2500 PSIG - 200P
- ▲ 2000 PSIG - 200P
- ▲ 2000 PSIG - 200P

DAVIS-BESSE NUCLEAR POWER STATION
 EMERGENCY CORE COOLING
 SYSTEM FLOW DIAGRAM
 FIGURE 6.3-6

Figure 1-10

**Table 1-3
High Pressure Injection System**

Parameter	Value
Total flow rate per train	335 gpm @ 1400 psig
Number of pumps	2
Shut-off head	1625 psig
Actuation setpoint	1616 psig
Source of suction	
emergency injection (automatic operation)	BWST
piggy-back or recirculation operation	DHR pump discharge

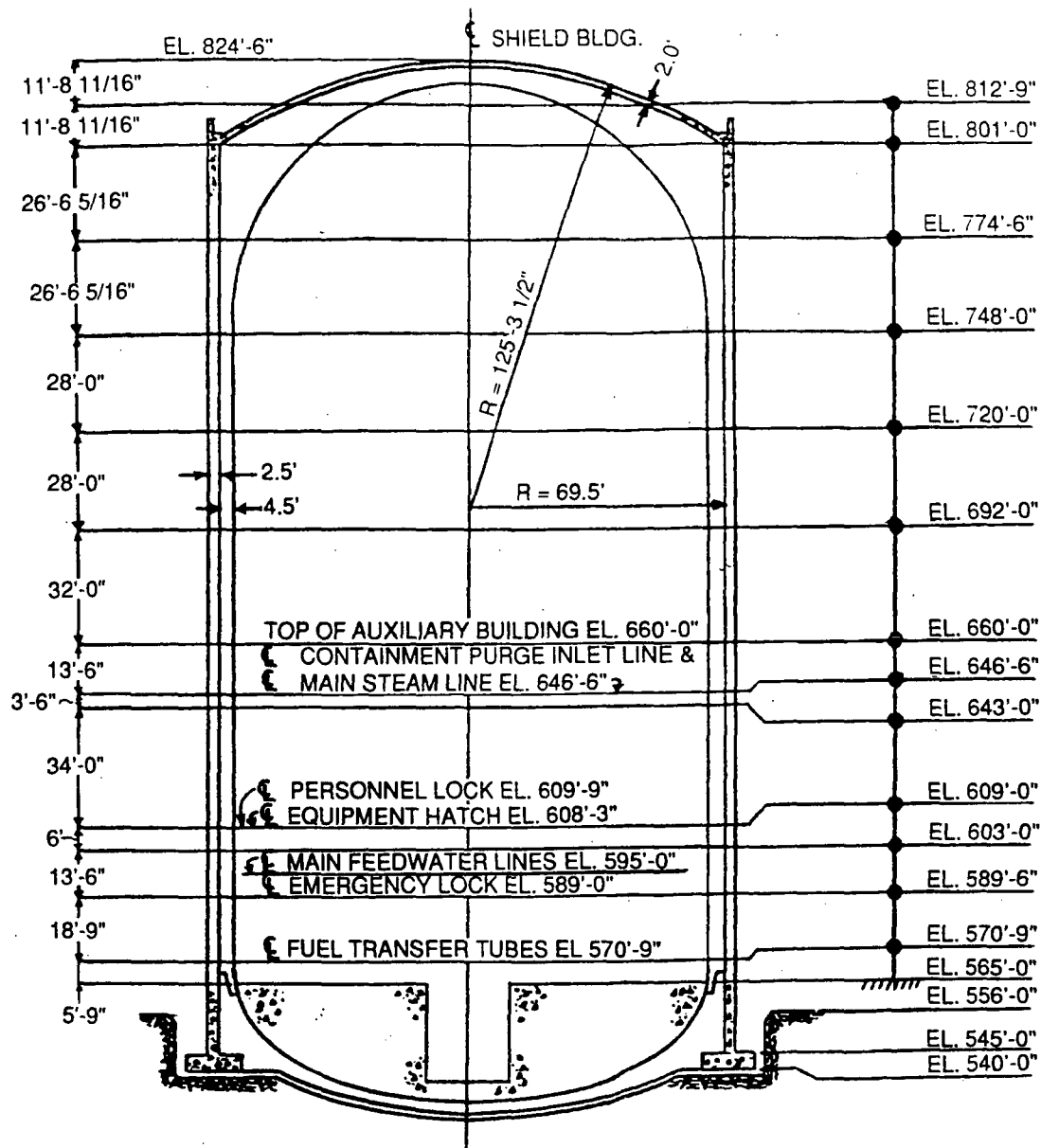
**Table 1-4
Decay Heat Removal System**

Parameter	Value
Total flow rate per train	2250 gpm @ 120 psig ¹
Number of pumps	2
Shut-off head	200 psig
Actuation setpoint	416 psig
Source of suction	
normal shutdown cooling	RCS hot leg drop line
emergency injection	BWST
recirculation operation	containment emergency sump
Heat load	
normal (DHR operation)	30 E6 btu/hr (rated heat transfer ²)
emergency	105 E6 btu/hr (rated heat transfer ³)

1. With suction from the borated water storage tank (BWST).
2. Cooling water inlet temperature of 95 F, primary inlet temperature of 140 F.
3. Cooling water inlet temperature of 119 F, primary inlet temperature of 250 F.

**Table 1-5
Core Flood Tanks**

Parameter	Value
Number of core flood tanks	2
Total mass of water	64,182 lbm (1040 cubic ft)
Normal temperature	120 F
Normal pressure	600 psig
Type of overpressure gas	nitrogen



DAVIS-BESSE NUCLEAR POWER STATION
KEY PENETRATION LOCATIONS

Figure 1-11

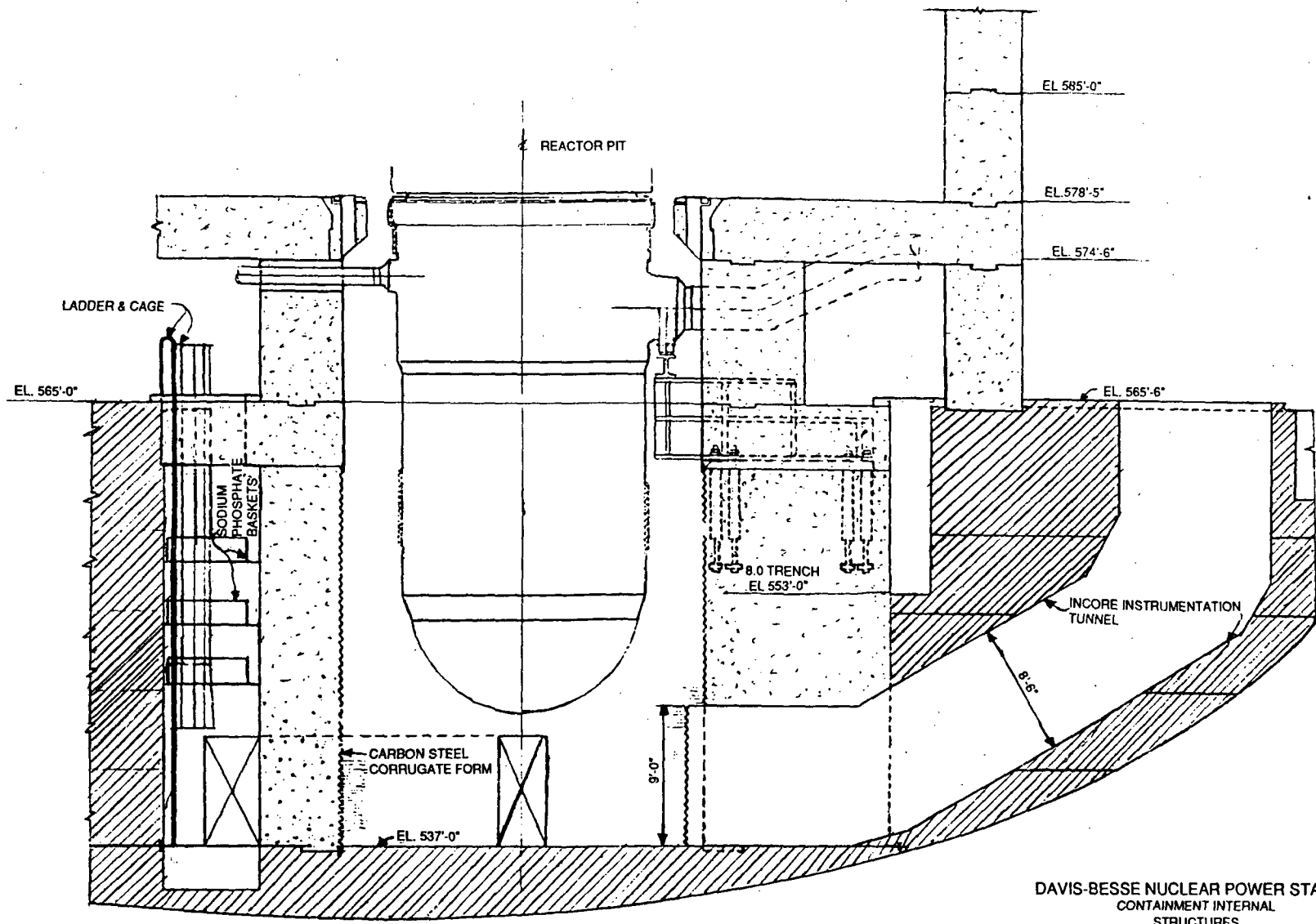


Figure 1-12

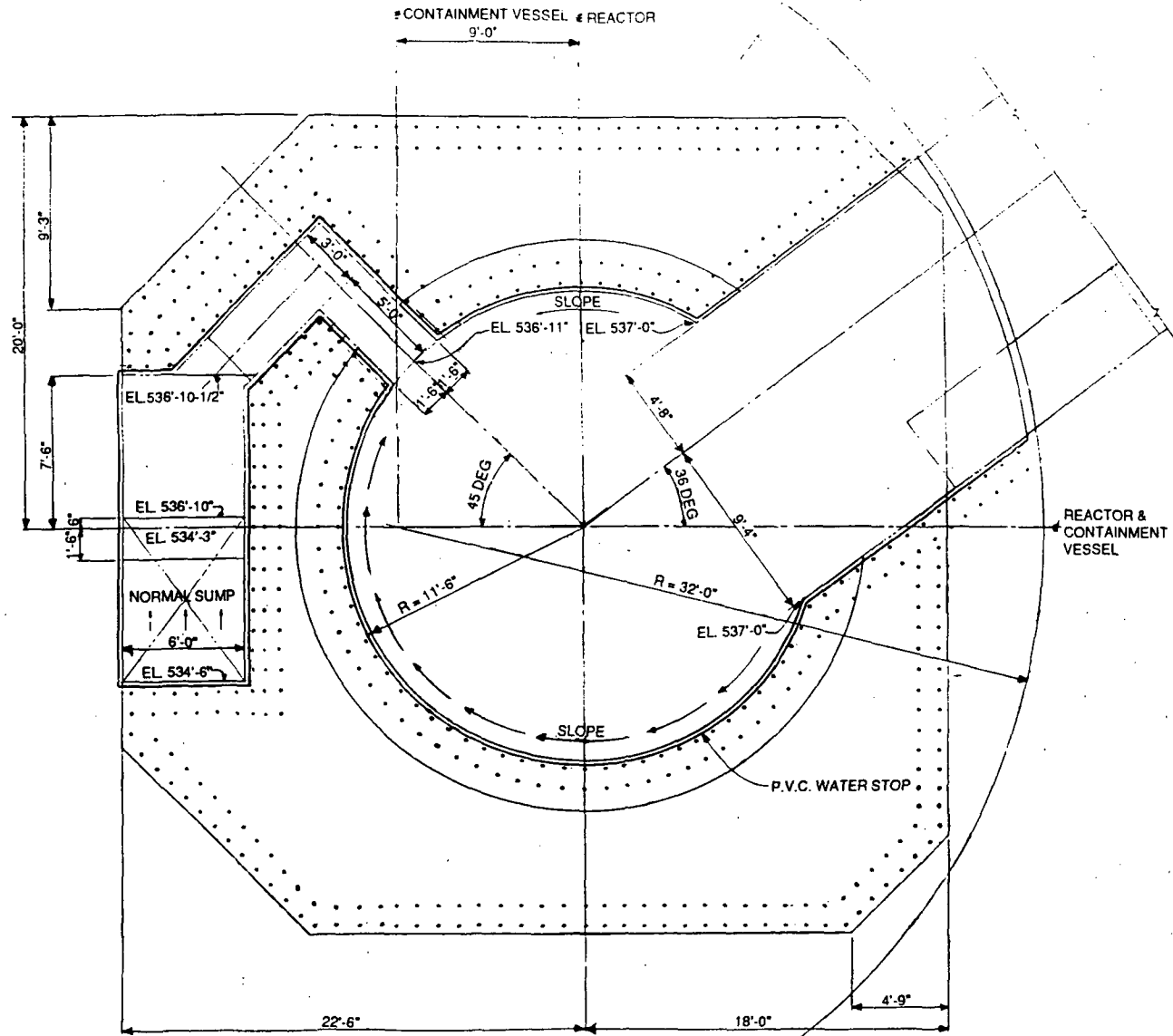


Figure 1-13

DAVIS-BESSE NUCLEAR POWER STATION
CONTAINMENT - INTERNAL
STRUCTURES, SHEET 1

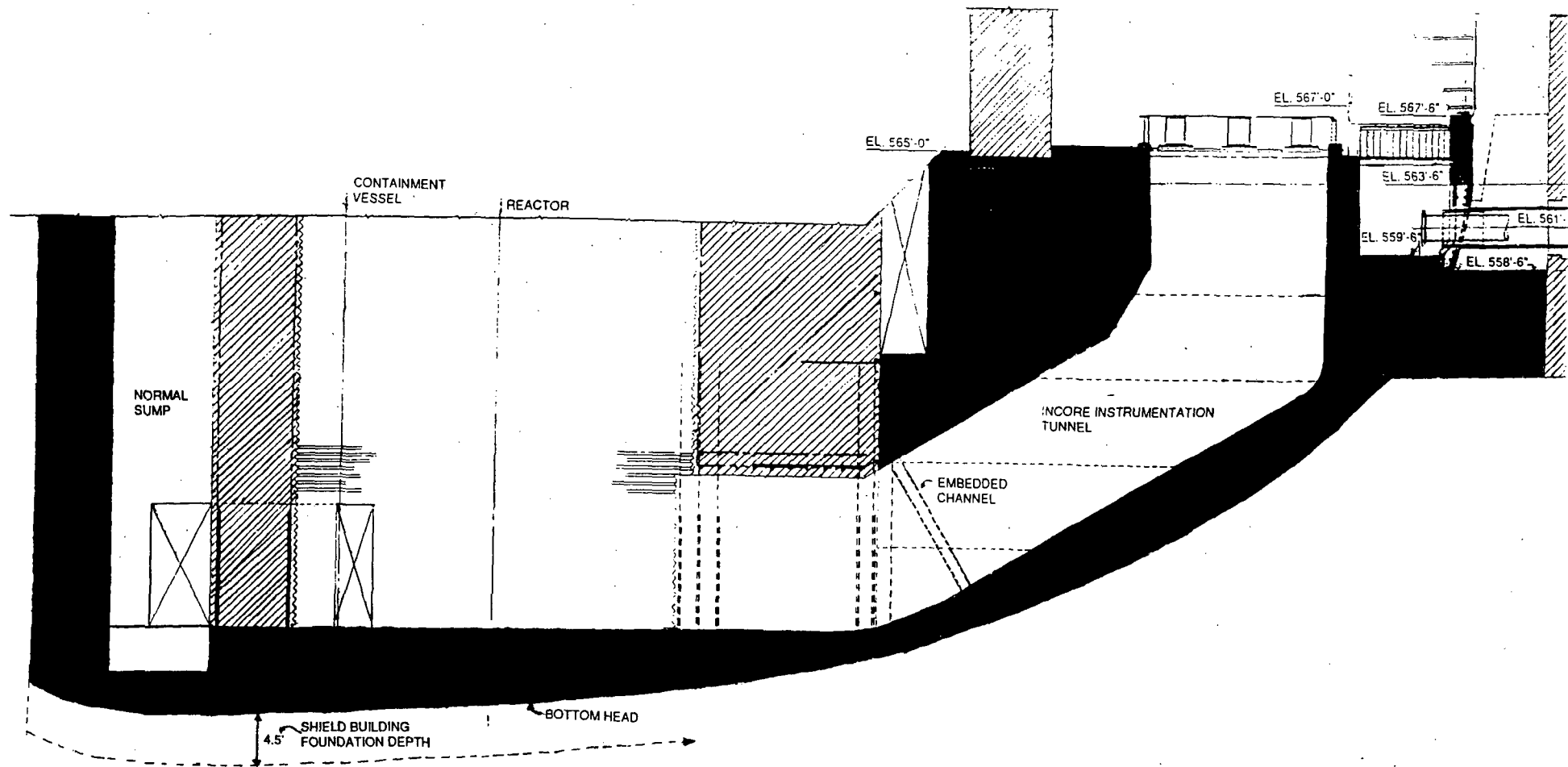


Figure 1-14

internal structures are isolated from the containment vessel by steel grating panels with sliding supports; this construction allows free differential movement between the internal structures and the vessel.

The containment vessel has an inside diameter of 130 feet and a net free volume of 2.834 million cubic feet. The cylindrical shell and bottom head thickness, exclusive of reinforced areas, is 1.5 inches with a dome thickness of 13/16 inches. A 180-ton polar crane is supported from the cylindrical vessel shell by a 14' - 6 1/2" deep by 5' - 11" wide circular crane girder. Access to the containment is provided by an equipment hatch, a personnel air lock and an emergency air lock. Electrical and mechanical penetrations are provided for services to the containment.

The containment system is designed to provide protection for the public from the consequences of any break in the reactor coolant piping up to and including a double-ended break of the largest reactor coolant pipe. The design internal pressure is 36 psig with a coincident design temperature of 264 F. See Tables 1-6 and 1-7 for additional containment data. Section 4 contains details of the overall containment material and failure characteristics. The containment safety features include the containment spray system, the containment air cooling system, and the containment isolation system.

There are two independent containment building sprays, each designed for 50% of the heat load imposed by a RCS hot leg LOCA (see Figure 1-15 and Table 1-8). The containment building spray is designed for emergency use only, and it serves no function during normal operation. Heat removal is accomplished by directing borated water, initially from the borated water storage tank (BWST), and when that tank is empty, from the containment vessel emergency sump, into the containment atmosphere through two separate spray headers located in the ceiling of the containment dome. Steam within the containment atmosphere is condensed, and the non-condensable gases are cooled by the spray, thereby reducing containment pressure. The spray and condensate collect in the containment vessel normal sump, dissolving sodium phosphate stored there in baskets. Upon emptying of the BWST, the containment building spray suction is switched to the vessel emergency sump. Note that the containment spray system does not have a separate, dedicated heat exchanger.

The containment air cooling system consists of three independent containment air cooling units, each with a 50% heat load removal capability. These air cooling units are used for both normal and emergency cooling. The system is automatically shifted to emergency operation upon receipt of a SFAS signal resulting from a high containment pressure or a low RCS pressure. Additional information on the containment air coolers is given in Table 1-9.

The containment vessel isolation systems close all containment penetrations not required for operation of the engineered safety features systems. Leakage through all penetrations not serving accident-consequence limiting systems is minimized by a double barrier so that single failures or malfunctions will not result in loss of isolation. Isolation occurs on a SFAS high containment radiation signal. Upon loss of actuating power, the

**Table 1-6
Containment Structure**

Parameter	Value
Containment type	Large dry, free standing steel
Type & chemical composition of concrete in basemat	"Limestone/limestone" dolomitic
Weight fraction of concrete free and bound water	Free - 0.042; Bound - 0.014
Free volume	2.834E6 ft ³
Design pressure	36 psig, max. pressure 40 psig
Normal pressure at full power	0 psig
Normal temperature at full power	< 120 F
Reactor cavity floor area	~ 568 ft ²
Containment liner thickness	N/A
Wall thickness	
Cylindrical portion	1.5 inches
Dome portion	13/16 inches
Basemat thickness	5.7 ft (minimum)

**Table 1-7
Interior Structural Heat Sinks¹**

Parameter	Value
Area of inner containment vessel surface	103,330 ft ²
Area of other steel structures	192,500 ft ²
Area of exposed concrete (excluding floor areas)	60,760 ft ²

1. All values approximate.

**Table 1-8
Containment Spray System**

Parameter	Value
Number of injection pumps	2
Total design flow rate per train (containment at 35 psig)	
BWST full	1660 gpm
BWST empty	1500 gpm
Containment setpoint for spray initiation	24 psig
Initial volume of water available from BWST	522,500 gal
Setpoint for switch to containment sump	8 ft (manual operator action)
Spray additives (passive addition via baskets in reactor cavity/normal sump region of containment)	Na ₃ PO ₄ (trisodium phosphate)

**Table 1-9
Containment Air Cooling System (Emergency Operation)**

Parameter	Value
Heat removal capacity per train	70.75E6 btu/hr
Number of fans	3 (2 + 1 standby)
Flow rate per fan	60,000 cfm
Primary inlet temperature	85 F (max. service water temperature)

isolation valves are designed to maintain their position or take the position that provides the greater safety (e.g., pneumatically operated valves fail closed).

The shield building is a reinforced concrete structure of right cylinder configuration with a shallow roof. An annular space is provided between the steel containment vessel and the interior face of the concrete shield building of approximately 4.5 feet which permitted construction operations and allows periodic inspection of the steel containment vessel. The volume contained within this annulus is approximately 678,700 cubic feet. The building has a height of 279.5 feet, as measured from the top of the foundation ring to the top of the dome. The thicknesses of the wall and the dome are approximately 2.5 feet and 2 feet, respectively.

Steam and Power Conversion Systems

The main steam system (see Figure 1-16) directs superheated steam, produced in the once-through steam generators (OTSGs), to the turbine-generators. Main steam is also supplied to the turbine gland seal system, auxiliary steam, and the main and auxiliary feedwater pump turbines. Pressure relief for the main steam system is provided by the turbine bypass valves (TBVs), atmospheric vent valves (AVVs), and main steam safety valves. When the turbine is tripped, the turbine bypass valves modulate to remove decay heat by relieving steam flow to the condenser, or to the atmosphere through the AVVs if the condenser is not available. The main steam safety valves provide a code safety function and will also normally momentarily lift during a load rejection.

The main turbine is an 1800 rpm tandem-compound unit with fourflow, low pressure stages. Superheated steam from the steam lines is supplied to four main turbine stop valves, then to the four control valves, before entering the center span of the high-pressure turbine casing. Extraction steam is taken from specified stages of the high and low pressure sections to be used for feedwater preheating and eventual collection in the condenser.

The main feedwater system, shown in Figure 1-17, receives condensate flow from the high and low pressure condensers. This condensate is first delivered to the deaerator tanks and heaters where non-condensable gases are removed. Ammonia is added for pH control, and hydrazine is used to minimize oxygen concentration. Morpholine is also added to the feedwater system. Booster pumps take suction from the deaerators and provide the source of water for the two main steam-driven feedwater pumps. Both the booster pump and main feedwater pump are driven by a steam turbine via a common shaft. The steam-driven turbines are controlled by the ICS. The ICS also controls the amount of feedwater flow to the steam generators so as to balance the heat generation and heat removal capabilities of the reactor and steam generators. Extraction steam from the low and high pressure turbine extraction stages is used to preheat the feedwater.

There are two other smaller pumps which can be used for startup operations. The motor driven feed pump, which is normally used, can take suction from the deaerator storage tanks, the condensate storage tanks, or the service water header. The startup feed pump would only be used if no other sources of feedwater were available.

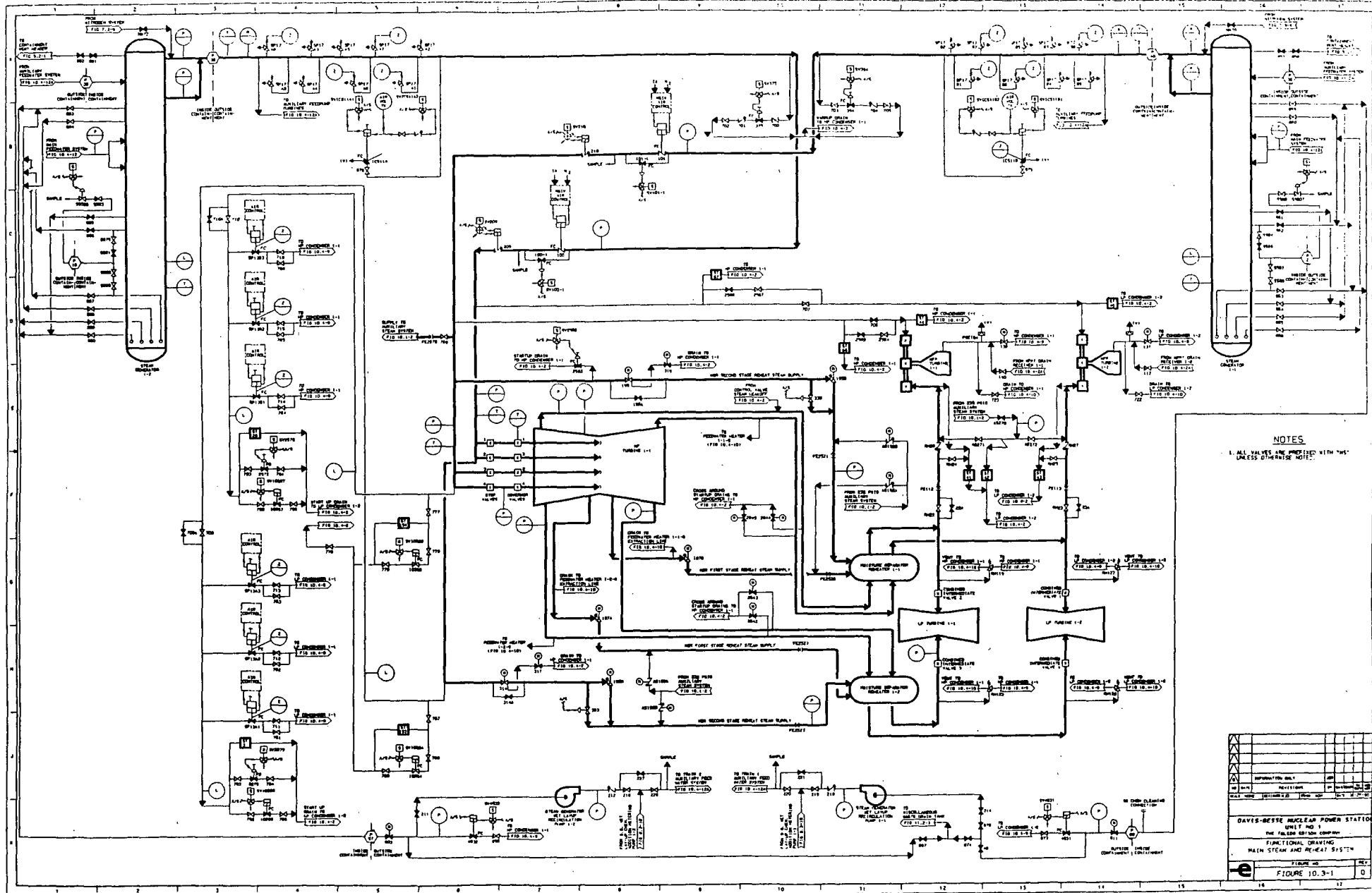
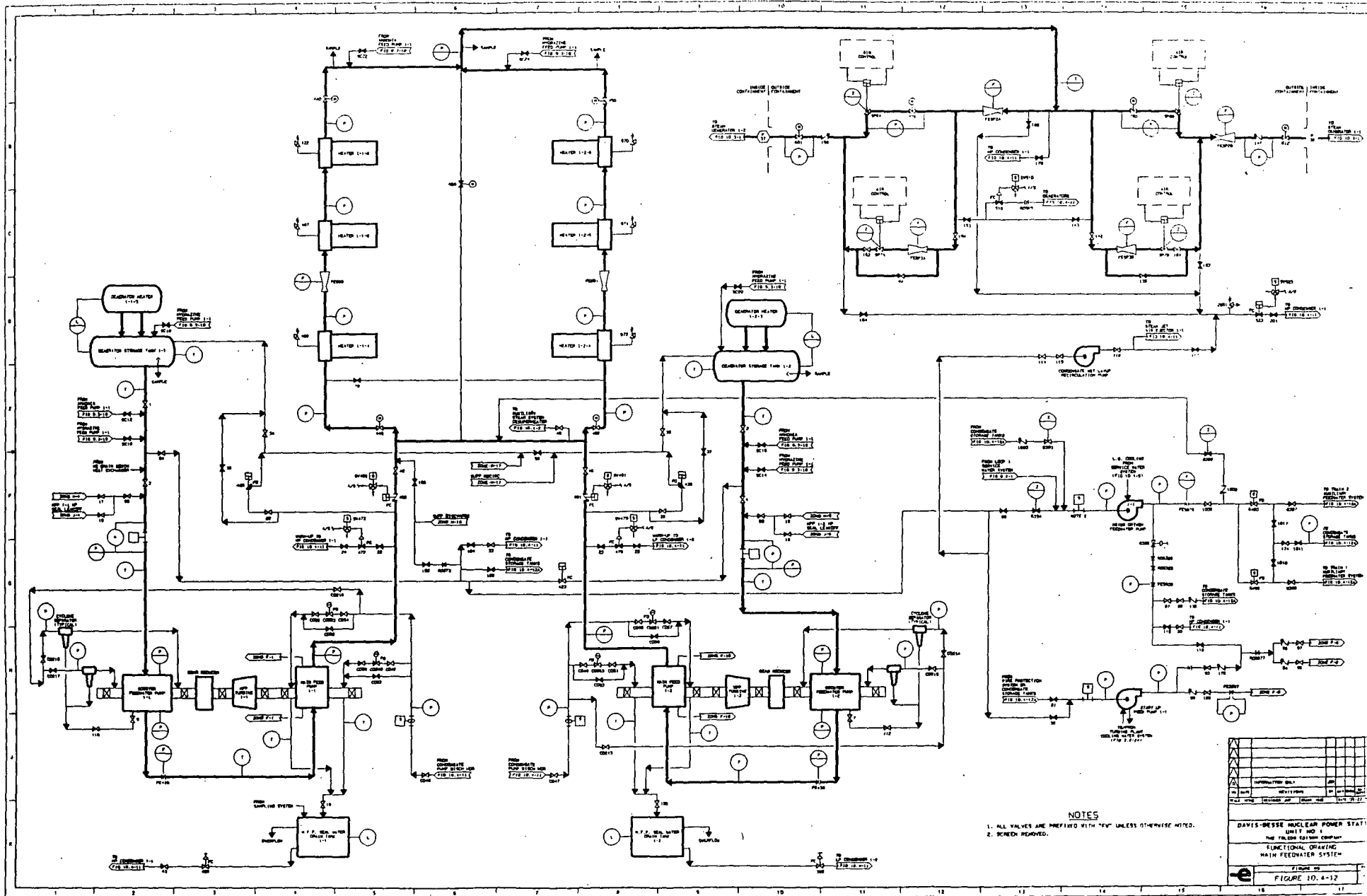


FIGURE 1-16



NOTES
 1. ALL VALVES ARE PREFIXED WITH "V" UNLESS OTHERWISE NOTED.
 2. SCREENS REMOVED.

DAVIS-BESSE NUCLEAR POWER STATION
 UNIT NO. 1
 FUNCTIONAL DRAWING
 MAIN FEEDWATER SYSTEM
 FIGURE NO. 10.4-12
 FIGURE 10.4-12

FIGURE 10-17

The subcooled feedwater initially enters the steam generator downcomer region through a manifold supplying radially spaced ports which enter the steam generator and end in spray heads at the top of the steam generator downcomer. A functional drawing of the OTSG is shown in Figure 1-18. In the downcomer, the still subcooled feedwater is heated to saturation by aspirated steam drawn from the shell side of the steam generator mixing with the sprayed feedwater. The net flow, at near saturated conditions, then enters the steam generator tube region and turns in direction to flow upward (in a reverse direction to the reactor coolant flow), removing heat from the primary system along the tube nest. The feedwater is boiled, and the resulting saturated steam is superheated in the upper portion of the tube nest. The superheated steam turns cross flow to the tube nest near the top of the generator into a downward flowing annulus region, and then exits by two nozzles into the main steam lines.

Auxiliary Systems

In the absence of main feedwater flow to either of the OTSGs, the auxiliary feedwater (AFW) system would provide flow to the steam generators for the removal of reactor decay heat and system sensible heat. In the case of a loss of all four reactor coolant pumps, the high injection point of the AFW will promote sufficient natural circulation of the RCS. A functional drawing of the AFW system is shown in Figure 1-19. The AFW system consists of two steam turbine-driven feedwater pumps and related piping, valves, controls and instrumentation. The AFW pumps can take suction from either the condensate storage tanks, the service water system, or the fire protection system. Each pump is capable of discharging the auxiliary feedwater to its respective steam generator or, in the case of a sensed failed steam generator, to the opposite steam generator. During normal plant operation, the AFW system performs no function. It is a standby system to be used in the event of a loss of the main feedwater system.

There are two emergency diesel generators (EDGs), which provide an onsite standby power source for essential electrical loads. Each EDG is independent of the other. Upon loss of the normal and reserve power sources to the 4160 v essential buses C1 and D1, the associated EDG will start and supply its respective bus. The EDG is designed to start and operate with the 125 vdc station batteries as the only power source. In addition, there is a station blackout diesel generator independent of both of the EDGs which can be started by the control room operators.

The circulating water system removes the latent heat of condensation from the turbine exhaust steam in the condenser and transfers this heat to the atmosphere via a natural draft cooling tower. Makeup water for the cooling tower is taken from Lake Erie. The circulating water system also provides back-up for the service water supply to the turbine plant cooling water heat exchangers.

The component cooling water (CCW) system removes heat from the reactor auxiliary systems and the ECCS during normal plant operation, plant cooldown, and design-basis accident conditions. Additional data can be found for this system in Table 1-10.

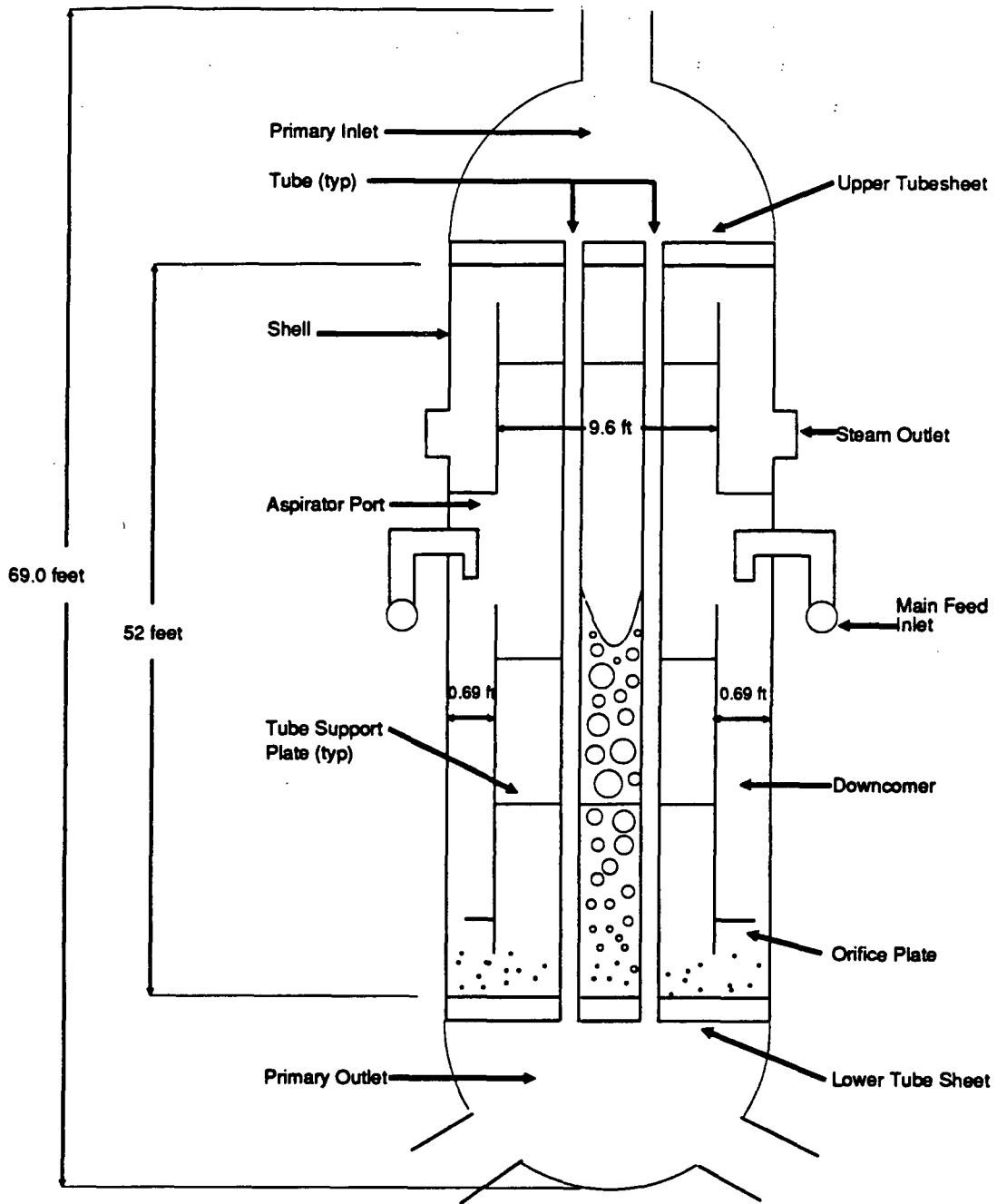
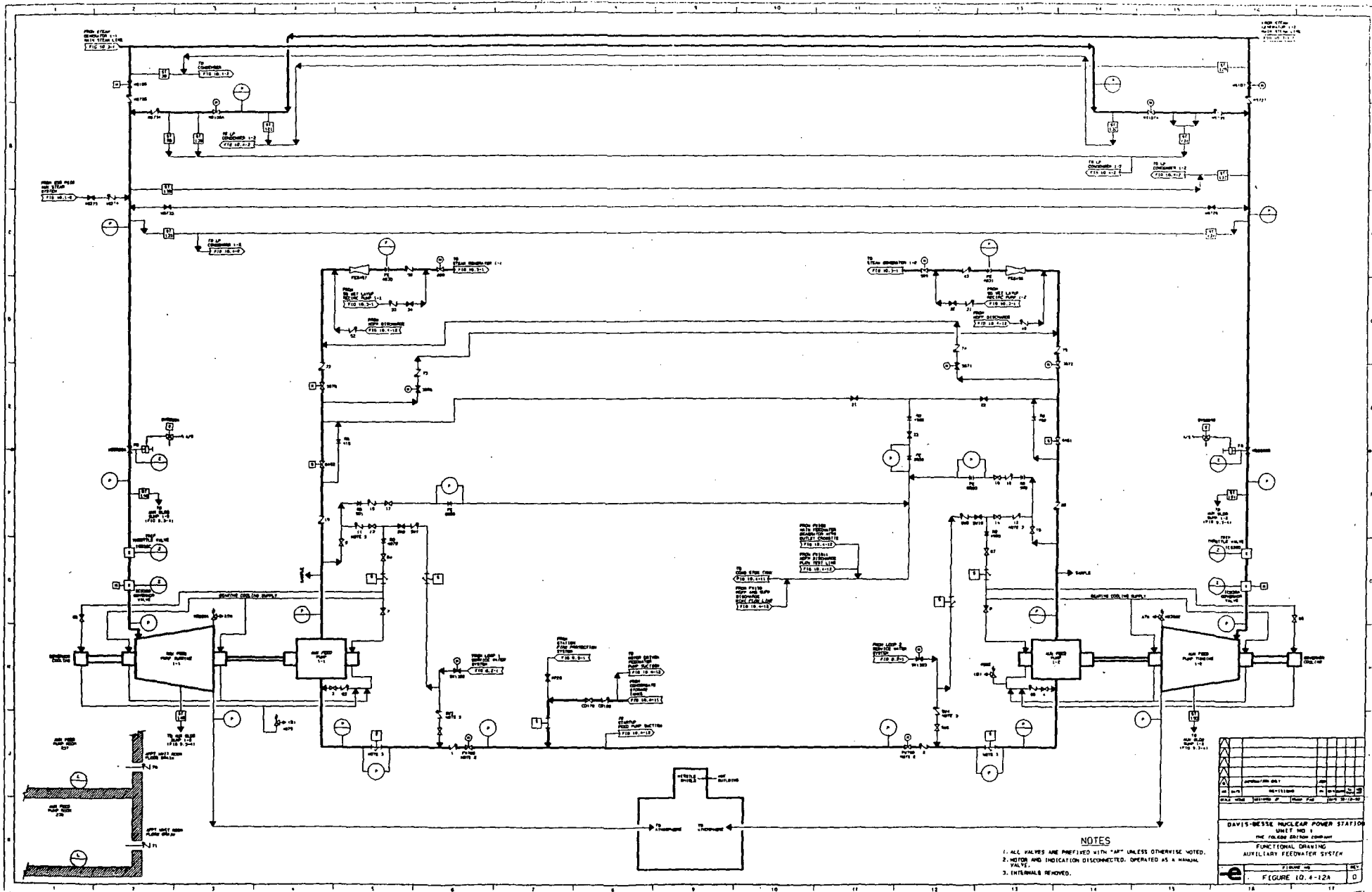


Figure 1-18. Once-Through Steam Generator Cross-Sectional Diagram



NOTES

1. ALL VALVES ARE PREFIRED WITH "AM" UNLESS OTHERWISE NOTED.
2. MOTOR AND INDICATION DISCONNECTED. OPERATED AS A MANUAL VALVE.
3. INTERNALS REMOVED.

NO.	DESCRIPTION	DATE	BY	CHECKED

DAVIS-BESSE NUCLEAR POWER STATION
 SHEET NO. 1
 THE OHIO STATE COMPANY
 FUNCTIONAL DRAWING
 AUXILIARY FEEDWATER SYSTEM
 FIGURE NO. 10.4-12A
 D

Table 1-10
Component Cooling Water System

Parameter	Value
Total flow rate per train	7860 gpm @ 150 ft
Number of pumps	3 (2 + 1 in standby)
Heat load per train	
normal	57.E6 btu/hr
emergency	114.E6 btu/hr

The service water system takes suction from the Lake Erie intake structure and supplies lake water to the various components in the system for heat removal. During normal operation, cooling water is supplied to the CCW heat exchangers, the containment air coolers, and the turbine plant cooling water heat exchangers. During an emergency, the service water system provides a redundant path to the engineered safety features. Only one path, with one of three service water pumps, is necessary to provide adequate cooling to one train of emergency equipment. In addition, there is a fourth service water pump (the dilution pump). Two service water trains are needed if both emergency equipment trains are in service. Normally, two service water pumps are running with a third pump mechanically lined up but electrically deenergized. During emergency operation, under non-safety actuation, service water provides a backup source of water to the AFW system or to the motor-driven feed pump through manually positioned valves. See Table 1-11 for additional information on the service water system.

The makeup and purification system is operated during all phases of the nuclear steam supply system operation. A functional drawing of the makeup and purification system is shown in Figure 1-20. During normal operations, one makeup pump continuously supplies flow to the seals of the reactor coolant pumps and to a makeup line which is connected to the reactor inlet through a high pressure injection line. The makeup flow is regulated based on signals from the liquid level controller of the pressurizer. Letdown from the RCS is processed to remove impurities and returned via the makeup system. The makeup system can also provide makeup to the RCS to help replenish inventory lost due to a small break in the RCS pressure boundary, although no credit for its operation is taken to mitigate design basis accidents. However, in the event that all steam generator cooling is lost, core cooling can be accomplished by a feed-and-bleed process. The makeup pumps are the only pumps at the plant that can pump against the normal RCS pressure and relieve cooling flow through the PORV. In the piggyback mode (the makeup pump in series with the low pressure injection pump), the makeup system can relieve cooling flow through the primary code safety valves. See Table 1-12 for additional information on the makeup system.

**Table 1-11
Service Water System**

Parameter	Value
Total flow rate per train	10,250 gpm @ 160 ft
Number of pumps	4 (2 + 1 in standby + 1 backup)
Heat load per train	
normal	~ 82.E6 btu/hr
emergency	~ 190.E6 btu/hr
Source of suction	Intake structure (Lake Erie water)

**Table 1-12
Makeup System**

Parameter	Value
Total flow rate per train	196 gpm @ 2000 psig ¹
Number of pumps	2
Shutoff head	2725 psig
Source of suction	
normal	makeup tank
emergency	BWST

1. Makeup pump taking suction from BWST, with recirculation valve and valve MU32 (bypass) closed.

Section 2

PLANT MODELS AND METHODS FOR PHYSICAL PROCESSES

To characterize the containment response to a core-damage sequence, a primary analytical tool was selected, with supplemental input provided by review of technical literature, in-house calculations, and other technical input. The Electric Power Research Institute (EPRI)-maintained Modular Accident Analysis Program (MAAP) version 3.0B revision 18 (Ref. 1) was selected as the primary analytical code for back-end analyses, which were run in-house on SUN workstations. To help assure proper code utilization, Davis-Besse personnel actively participated in the MAAP Users Group, including presentation of technical papers and hosting of a users group meeting.

2.1 SEVERE-ACCIDENT RESPONSE USING MAAP

MAAP was originally developed as part of the Industry Degraded Core (IDCOR) Program to address the phenomenology of accident scenarios that could lead to a damaged core, primary system failure, and containment failure in light water reactors. The code is designed to provide realistic assessments of severe-accident phenomena, including fission product release, transport, and deposition. Table 2-1 provides a summary of a portion of the experimental basis for many of the code analytical models.

The MAAP 3.0B model of the RCS is divided into fifteen nodes, as shown in Figure 2-1. This figure and Table 2-1 were taken from a draft version of the user's manual (Ref. 1). Nodes exist for the following components of the RCS (note that instead of having "loop 1/loop 2" or "loop A/loop B," MAAP nomenclature denotes "broken loop/unbroken loop"):

- (1) Core
- (2) Downcomer
- (3) Upper plenum
- (4) Reactor dome
- (5) Broken loop cold leg
- (6) Broken loop intermediate leg
- (7) Broken loop cold leg tubes (steam generator tubes)
- (8) Broken loop hot leg tubes
- (9) Broken loop hot leg
- (10) Unbroken loop cold leg
- (11) Unbroken loop intermediate leg
- (12) Unbroken loop cold leg tubes (steam generator tubes)
- (13) Unbroken loop hot leg tubes
- (14) Unbroken loop hot leg
- (15) Pressurizer

Table 2-1
Model Benchmarks Used in the IDCOR Program

Physical Process	Experiment/Code	Type of Comparison						Documentation			
		Separ.-Effects Experiments		Integral Experiments		Experience (TMI-2)	Detailed Analysis	Open Literature	IDCOR Reports	MAAP Manual	EPRI Reports
		Small Scale	Large Scale	Out-of-Reactor	In-Reactor						
Core heatup	PBF-SFD Tests			x					x		
	LOFT PF-2			x							x
	TMI-2					x		x	x		x
	BWR Heatup Code						x	x	x	x	
	PWR Heatup Code						x	x	x	x	
Clad oxidation	Numerous Exps.	x							x		
	LOFT PF-2				x						x
	TMI-2					x			x		x
	BWR Heatup Code						x	x	x	x	
	PWR Heatup Code						x	x	x	x	
Fission-product releases	ORNL Experiments	x						x	x	x	
	SASCHA Exps.	x						x	x	x	
	PBF-SFD Tests				x				x		
	LOFT FP-2				x						x
	TMI-2					x			x	x	
Aerosol transport and deposition	ABCOVE Tests		x						x	x	
	ORNL (NSPP) Tests		x						x		
	AI Tests		x						x	x	
	MARVIKEN Tests			x					x		

Table 2-1 (continued)
Model Benchmarks Used in the IDCOR Program

Physical Process	Experiment/Code	Type of Comparison						Documentation			
		Separ.-Effects Experiments		Integral Experiments		Experience (TMI-2)	Detailed Analysis	Open Literature	IDCOR Reports	MAAP Manual	EPRI Reports
		Small Scale	Large Scale	Out-of-Reactor	In-Reactor						
Aerosol transport and deposition (continued)	JAERI (Japan) Tests	x							x	x	
	CEA (France) Tests		x						x		
	CSE Tests		x						x	x	
	EPRI Tests	x							x		
	DEMONA Tests			x					x		
	LACE Tests			x					x		
	Gillespie and Langstroth	x							x		
Hydrogen combustion	Complete	Westinghouse Data		x				x	x	x	
		Thermodynamic Analyses					x	x	x	x	
		TMI-2					x		x		
	Incomplete	Whiteshell Tests		x					x	x	x
		EPRI Tests		x					x	x	
		EPRI FMC Model						x		x	x
		SNL VGES Tests		x						x	
		EPRI Nevada Tests		x						x	

Table 2-1 (continued)
Model Benchmarks Used in the IDCOR Program

Physical Process	Experiment/Code	Type of Comparison						Documentation			
		Separ.-Effects Experiments		Integral Experiments		Experience (TMI-2)	Detailed Analysis	Open Literature	IDCOR Reports	MAAP Manual	EPRI Reports
		Small Scale	Large Scale	Out-of-Reactor	In-Reactor						
Debris fragmentation	Sandia FITS Tests	x						x	x		
	ISPRA Tests	x						x	x		
	Higgins Exps.	x						x	x		
	ALCOA Tests	x						x	x		
	Burton, et al.	x						x	x		
	LNG Experiments		x					x	x		
Debris dispersal	ANL Experiments			x					x		
	Sandia Exps.			x							
Debris coolability	1st SNL Steel-Concrete Exps.			x							
	UK Experiments	x						x	x	x	
	KfK Experiments	x						x	x	x	
	EPRI Experiments	x						x	x	x	
	ANL Particle Bed Experiments	x						x	x	x	
	ANL NTP Tests	x									
	ANL CMTI Tests	x									
	ANL SHOTDROP Tests	x									
	SNL SWISS Exps.				x						

Table 2-1 (continued)
Model Benchmarks Used in the IDCOR Program

Physical Process	Experiment/Code	Type of Comparison						Documentation			
		Separ.-Effects Experiments		Integral Experiments		Experience (TMI-2)	Detailed Analysis	Open Literature	IDCOR Reports	MAAP Manual	EPRI Reports
		Small Scale	Large Scale	Out-of-Reactor	In-Reactor						
Debris coolability (continued)	TMI-2					x					
	USBM Burro Exps.		x								
	Purdue Exps.	x									
	Lave Quenching		x								
Core-concrete attack	1st SNL Steel-Concrete Exp.			x							
	WECNSL Analysis						x	x	x	x	
	SNL SWISS Exps.	x		x							
	SNL TURC Exps.	x		x							
Reflective insulation	EPRI Experiments	x									
Wall ablation	Closed Form Solution						x				
Fan cooler	Westinghouse Experiments	x									
Revaporization	Preliminary ANL Results	x									

Table 2-1 (continued)
Model Benchmarks Used in the IDCOR Program

Physical Process	Experiment/Code	Type of Comparison						Documentation			
		Separ.-Effects Experiments		Integral Experiments		Experience (TMI-2)	Detailed Analysis	Open Literature	IDCOR Reports	MAAP Manual	EPRI Reports
		Small Scale	Large Scale	Out-of-Reactor	In-Reactor						
Primary system T/H	DBA Analysis					x	x	x	x		
	RELAP5 SBO Analysis					x	x				
	Davis-Besse LOFA Browns Ferry					x		x			
Primary system natural circulation	Westinghouse Experiments			x					x	x	
	SIAM Code						x				
Containment natural circulation	HEDL		x								
	Mixing Exps. FAI Brine-Water Experiments	x									x
Containment strain	Canadian Exps.		x							x	x
	SNL Experiments		x							x	x
	SNL Analyses						x			x	x

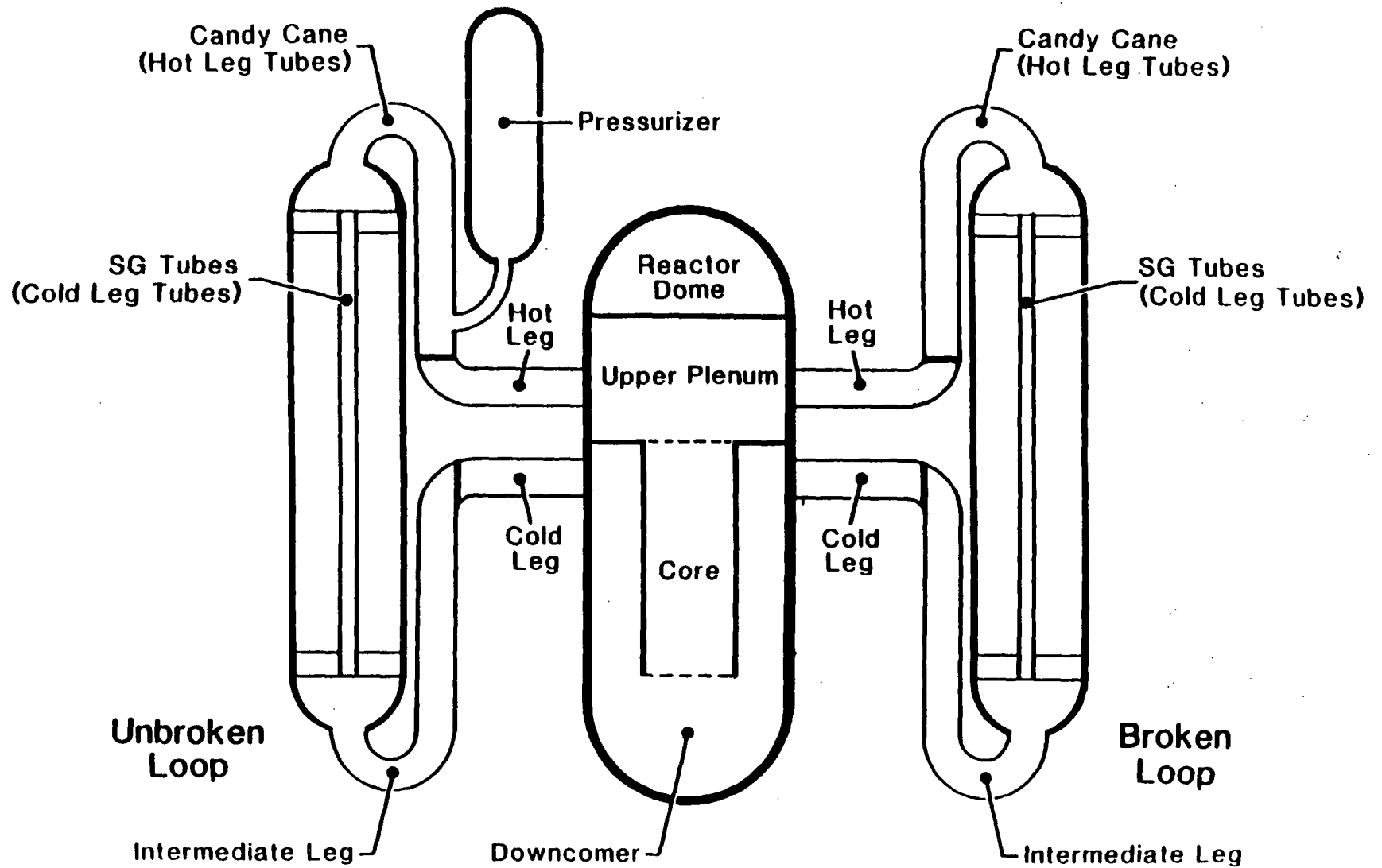


Figure 2-1. Application of PWR Primary System Nodalization to a B&W Design

The core node is further divided into four radial and seventeen axial nodes to allow for more detailed fuel/cladding/coolant interaction models.

For the IPE the primary system model was entirely plant-specific, with system details derived from reactor vessel drawings, plant drawings, system descriptions, and other plant-specific code input deck calculation files (e.g., for RETRAN).

The entire emergency core cooling system (ECCS) was also modeled. Specific system flow curves were used for the high pressure injection, low pressure injection, and containment spray systems. Injection by the makeup system was also assumed where applicable. Various ECCS pump configurations such as "piggyback" operation were modeled when applicable. Proper code utilization of input system flow curves was verified via test cases. Other components important to accident progressions were also modeled, such as pressurizer code safety valves, the pressurizer pilot-operated relief valve (PORV), steam generator main steam safety valves, and steam generator atmospheric vent valves.

Of particular interest was the use of revision 18 of MAAP 3.0B. It had been noted in EPRI-sponsored MAAP thermal-hydraulic qualification studies that "... MAAP's ability to model Babcock and Wilcox PWRs was less mature than its capabilities vis-a-vis other U.S. plants" (Ref. 2). In response, and in-part at the request of Toledo Edison, several changes were made to code thermal-hydraulic models, and incorporated into revision 18. Of particular interest was the modeling of reactor vessel vent valves during small break LOCA sequences. As a result of these changes, documentation for revision 18 noted that "B&W users in particular will notice greater fidelity for transients that involve voiding of the primary system because modeling of natural circulation through the candy canes has been improved" (Ref. 3).

The application of MAAP 3.0B containment nodalization to Davis-Besse is shown in Figure 2-2. The overall containment nodalization was as follows: the upper compartment included all the volume above the containment "D-rings;" the lower compartment included the volume contained within the D-rings, including the refueling canal; the annular compartment included the annular volume between the D-rings and the containment wall; and the cavity compartment included the volume of the reactor cavity/normal sump/incore tunnel region. The lower and annular compartments have the same upper and lower elevations and have large mixing areas, such that they respond essentially as one compartment to accident sequences. Extensive walkdowns were performed to ensure that all important structures and components were properly considered in the model.

The integrated manner in which MAAP accounts for mass and energy flows between the primary system and containment, as well as between the various containment compartments, is shown in Figure 2-3.

There are several plant-specific containment details affecting the MAAP model which merit specific mention. Containment floor drains (including the refueling canal drains) all lead to the containment normal sump, connected and adjacent to the reactor cavity. As such, water which is released to the various levels of containment (e.g. RCS leak flow, safety relief valve/PORV flow, containment spray, containment air cooler condensate, etc.) is drained to

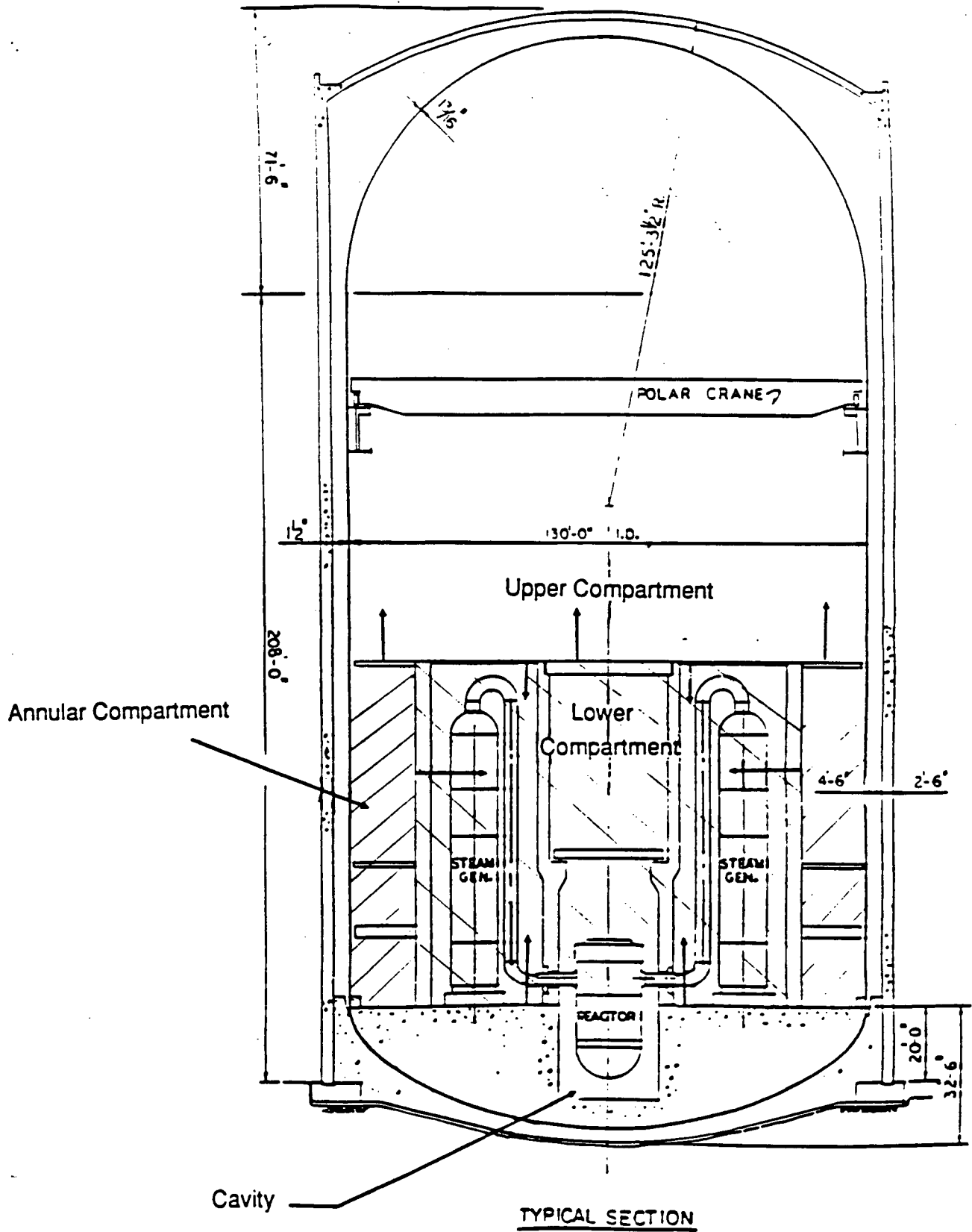


Figure 2-2. Davis-Besse Containment Nodalization

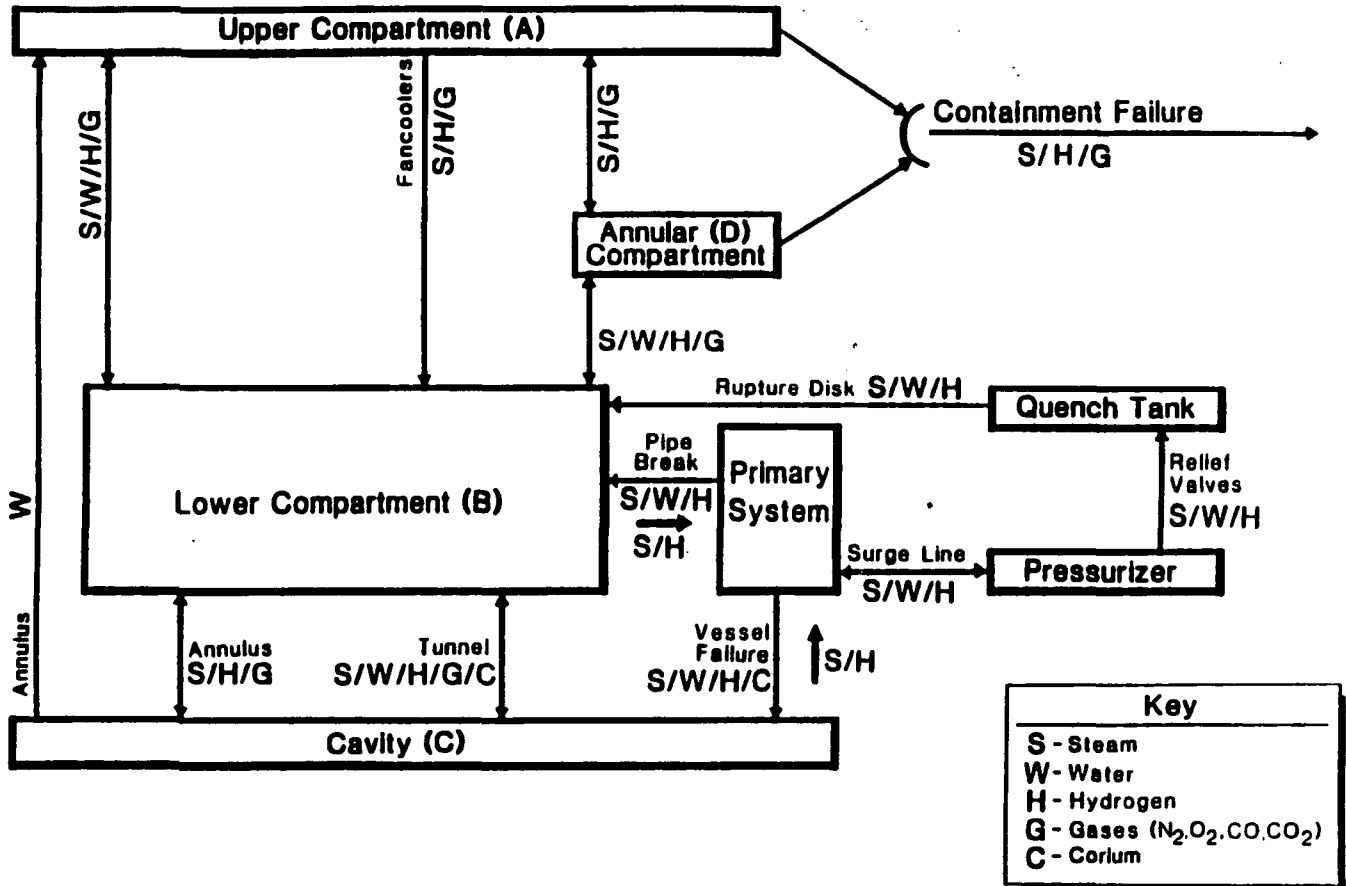


Figure 2-3. Modeling of Inter-Compartment Flows for Davis-Besse

the normal sump/reactor cavity region. The containment emergency sump is located at an elevation which requires approximately 150,000 gallons of water to be contained within the bottom of containment prior to water flowing into the sump. At the elevation corresponding to the annular/lower compartment floor (i.e. the "basement" floor), there is a 1.5 ft wide by 2.5 ft high concrete curb along the containment vessel wall.

Guidance for specific code physical input parameters was taken from the MAAP Users Guide (Ref. 4), which is controlled by the code maintenance consultant, Fauske & Associates, Inc. In general, realistic, nominal values were used for plant parameters as opposed to minimal licensing-basis values. Where possible, 100% reactor power plant data for RCS and containment parameters (e.g. temperatures, flows, etc.) were used for code initialization.

Along with physical details, several operational specifics were also incorporated into the MAAP analytical model. MIPS (Ref. 5), an input/output processor code for MAAP, was utilized to facilitate modeling of automatic safeguards and certain operator actions not included in the default MAAP actuation logic. Equipment operations modeled included the auxiliary feedwater steam generator level high setpoint (~ 120 inches) after safety features actuation, revised containment spray flow when suction is from the containment emergency sump (due to automatic action of containment spray discharge throttling valves), and reactor trip based on direct RCS pressure (vs. default pressurizer pressure). Operator actions modeled included emergency procedure "Specific Rules" and inadequate core cooling (ICC) actions. The four specific rules are located in a special section of the main station emergency procedure and apply to all portions of the procedure. Specific rules are highly emphasized during operator training and extensively practiced and used as an evaluation criterion during simulator exercises. Actions modeled included tripping RCPs and raising steam generator levels on loss of subcooling margin, throttling injection based on excessive subcooling margin and pressurizer level, and switching ECCS pump suction to the emergency sump based on BWST level. ICC actions modeled included depressurization of the steam generators, restart of RCPs, and RCS depressurization based on the degree of superheat in the core region.

Implicit to using MAAP or other similar codes is the need to perform phenomenological uncertainty studies to ascertain the possible range of containment response to a given sequence. Guidance for relevant sensitivity studies was primarily derived from the document "Recommended Sensitivity Analyses for an Individual Plant Examination Using MAAP 3.0B" (Ref. 6). Additional guidance was provided via an onsite review by the EPRI MAAP Project Manager (Ref. 7), and review of the containment event tree. All the recommended sensitivities were evaluated for applicability to the IPE, with the following general categories specifically evaluated:

- Hydrogen production: blockage/no blockage model, time of vessel failure following core melt, double-sided cladding oxidation, eutectic heat of fusion, and time of emergency sump recirculation initiation.
- Natural circulation models: "Westinghouse-type" vs. "B&W-type" internal vessel flow patterns.

- Recovery of damaged core: effects of operator action, variation of injection flow rates.
- Fission product revaporization: cesium compound vapor pressure, secondary side cooling.
- Debris dispersal and distribution: reactor cavity gas flow bypass area.
- Special prompt containment failure modes: degree of corium fragmentation and interaction.
- Coolability of debris in containment: nucleate boiling critical heat flux multiplier, corium spread areas in reactor cavity and lower containment.
- Induced (creep rupture) LOCAs: blockage/no blockage model, simulated RCP starts.
- Hydrogen and carbon monoxide ignition and burning: autoignition and jet burning temperature criteria, offset ignition hydrogen mole fraction, location and timing of assumed burn initiation.

2.2 INVESTIGATION OF SPECIFIC ISSUES

There are several technical issues which depend on plant-specific geometries, materials, etc. for evaluation. These were addressed through the sensitivity studies outlined above, reviews of technical literature, and separate calculations, as described in the following sections.

2.2.1 Ex-Vessel Corium Coolability

An obviously important issue is whether or not corium released from the reactor vessel is in a coolable geometry. Nominal spread areas were estimated for both the cavity/normal sump region underneath the reactor vessel and the area in the lower containment where corium could relocate to in a high pressure reactor vessel failure sequence.

The spread area under the reactor vessel is approximately 568 square feet. At a nominal corium density of 500 lbm/cubic foot and assuming the entire corium mass is in the cavity, an evenly distributed average depth of 10.1 inches is calculated.

The estimated spread area in the lower containment area where corium would be most likely to relocate given a sufficiently high RCS pressure at the time of reactor vessel failure is about 1272 square feet. At nominal corium density and accounting for the entire mass, an evenly distributed depth of 6.2 inches is calculated.

Regarding coolability, Generic Letter 88-20 Supplement 1, Appendix 1 part 4 states the following:

“The staff recommends that assessments be based on available cavity (spread) area and an assumed maximum coolable depth of 25 cm. For depths in excess of 25 cm, both the coolable and noncoolable outcomes should be considered.”

Therefore, if all debris were retained in the reactor cavity, the depth would be essentially at the 10-inch (25 cm) criterion. If the corium were dispersed to the lower region of containment, the larger spread area would result in a depth well below this criterion. While it would be expected that the debris would be coolable in either case, there is additional confidence that a coolable geometry would form in the lower level. Note that, in the containment event tree (CET), the possibility that the debris would not be coolable in either location is explicitly considered.

As noted previously, the Davis-Besse containment arrangement is such that all levels drain to the reactor cavity/normal sump region (including via normal floor drains and the refueling canal). As such, it is always the case that corium which remains in the reactor cavity will be covered with whatever amount of liquid is present in containment. There are also two separate areas which require further consideration: the normal containment sump and the containment emergency sump.

As shown in Figure 1-14, the normal containment sump area is located adjacent and connected (via a 3 ft wide by 7 ft high access tunnel) to the reactor cavity. An essentially common floor area is formed between these areas, with the cavity floor preferentially sloped toward the sump. The normal sump is approximately 2.6 feet deep, and, as the lowest spot in containment, has the "thinnest" underlying concrete basemat. At this location the depth of concrete between the bottom of the normal sump and base of the containment shield building foundation is about 5.7 feet.

To evaluate the possibility of concrete ablating to a depth greater than the minimum concrete depth in the normal sump, MAAP calculations were performed for a large break LOCA for which two conservatisms were imposed on coolability. First, a conservative equivalent corium-concrete interaction area was defined to enable MAAP to calculate corium cooling in the normal sump. Second, a reduction by a factor of 5.0 was applied to the overlying water boiloff maximum heat transfer rate, limiting the rate to a level similar to simple conduction.

The resultant bounding analysis indicated significant ablation, but that well over a foot of concrete still remained beneath the normal sump region. As such, ablative failure of the containment basemat below the normal sump was not considered to represent a special failure mode requiring treatment separate from that for general treatment of cavity corium cooling phenomenology.

As also shown in Figure 1-14, the containment emergency sump opening is located on the lower (i.e., 565') elevation of containment, adjacent to the incore tunnel opening. The emergency sump is also adjacent to the containment vessel wall, and a 1.5 ft. wide by 2.5 ft. high concrete curb is located along the elev. 565'/containment vessel wall interface. For sequences where corium relocated to the lower containment, this location was evaluated for the possibility of corium directly interacting with the containment vessel. At this location, there are two principal areas of consideration: ablative effects of corium which relocates to

inside the emergency sump, and ablation by relocated corium of the concrete curb along the containment wall.

For both cases, the corium remained quenched while overlying water was present. When dryout occurred in the emergency sump, the metal guard pipe and/or recirculation flow line would likely be ablated through. The emergency sump penetration assembly, however, is entirely encased in the shield building concrete foundation such that failure of the guard pipe would not result in a direct leakage path to the environment. The auxiliary building side, or far end of the penetration assembly, is also a fully capable containment pressure boundary such that ablation of the guard pipe/process pipe interface inside containment does not result in a leakage path to the environment. Additionally, direct radiative heat transfer to the far end of the penetration assembly is negligible due to the minimal view factor. As such, there is little nominal potential for a breach of containment boundary due to ablation in the containment emergency sump.

If dryout of relocated corium occurred in the lower containment, the potential exists for ablation to commence and eventually ablate to a depth sufficient to directly impact the containment wall. With a width of 1.5 ft., ablation along the lower containment concrete curb is of the greatest interest. For the estimated spread area of corium in the lower containment, dryout of corium does not result in the immediate initiation of ablation. The spread area, resultant corium depth, and lower containment geometry are such that convective and radiative heat transfer allows the corium to stay below the melting temperature of the containment limestone/limestone concrete. Note that of the three types of concrete found in containments (basaltic, limestone/common sand, and limestone/limestone), limestone/limestone has the highest melting temperature. As such, there is little nominal potential for a breach of containment boundary due to ablation along the lower containment concrete curb.

The above corium coolability discussion is for nominal conditions. To account for phenomenological uncertainty, several sensitivities were performed on corium relocation parameters and factored into the appropriate containment event tree probability distributions (refer to Section 5.2.6).

2.2.2 Submerged Vessel Corium Cooling

An issue affecting whether or not the reactor vessel is actually breached after significant fuel melting is submerged vessel cooling. For sequences where reactor cavity water levels are sufficiently high to result in a substantial portion of the vessel being surrounded by water, the possibility exists for the resultant boiling on the outer surface of the vessel to prevent critical depths of vessel ablation.

The Davis-Besse reactor cavity geometry is such that just over 39,000 gallons of water are sufficient to begin wetting the outside of the vessel. For comparison, the RCS initially has roughly 83,000 gallons at nominal power conditions. With the BWST injected, the resultant level is just below the bottom of the reactor vessel inlet and outlet nozzles. As such, for any sequence with significant injection, submerged vessel cooling is a potential consideration.

Evaluation was first performed by developing a simple model of a corium/steel/water geometry to gain an understanding of whether or not cooling was possible. Results indicated that, in fact, significant cooling was possible for a simple corium/steel/water submerged geometry. For example, the maximum steel temperature was less than 2000 F after one hour, with one half of the original vessel thickness remaining less than 1400 F (important for creep rupture considerations).

Two serious difficulties, however, were identified during the analysis process. The first was analytical treatment of the incore guide tubes. As Figure 1-9 shows, the incore penetration/reactor vessel geometry represents a complex materials and heat transfer problem. The second problem was associated with the handling of radiative heat transfer from corium which would now be resident in the bottom of the vessel for an extended period of time. Given the remaining high corium temperatures, significant heat transfer would occur to reactor internals which could lead to vessel failure modes not previously considered.

Together, these difficulties, combined with a current lack of benchmarks for the evaluations, led to the conclusion that further analysis was not justified at the current time. It should be noted that industry models are currently under development (e.g. MAAP 4.0, etc.) which will eventually enable a more confident evaluation of the effectiveness of submerged vessel cooling. This will be of particular use in future severe accident management guidance. The treatment of this issue for Davis-Besse is discussed in Section 5.2.2.

2.2.3 Creep Rupture

With a sufficient pressure loading across RCS pressure boundary piping coupled with elevated temperatures for a sufficient duration, significant strain can occur such that rupture results. Utilizing a Larsen-Miller parameter approach, plant-specific curves similar to those presented in NUREG-1265 (Ref. 8) can be developed that relate time to rupture vs. metal temperature for various differential pressures. As the Larsen-Miller parameter approach is based on material and stress considerations, plant-specific materials and dimensions must be utilized and applied to specific pressure boundary components. Based on available material creep data and nominal component dimensions, Figures 2-4 through 2-6 show creep rupture behavior for the hot legs, steam generator tubes, and pressurizer surge line, respectively.

The Davis-Besse hot legs are stainless clad carbon steel, the steam generator tubes Inconel 600 and the pressurizer surge line stainless steel. Comparison of the resultant curves indicates that for a given temperature and differential pressure, the hot legs are more likely to undergo a creep rupture than the other components. This is of particular importance given natural convective circulation flows in the raised-loop configuration of the plant. For the sequences analyzed, the horizontal portion of the hot leg immediately downstream from the reactor vessel outlet nozzle was generally raised to higher temperatures at earlier sequence times than the other components. As such, the hot legs were generally the most likely portion of the RCS to sustain a creep rupture for high pressure/high temperature sequences.

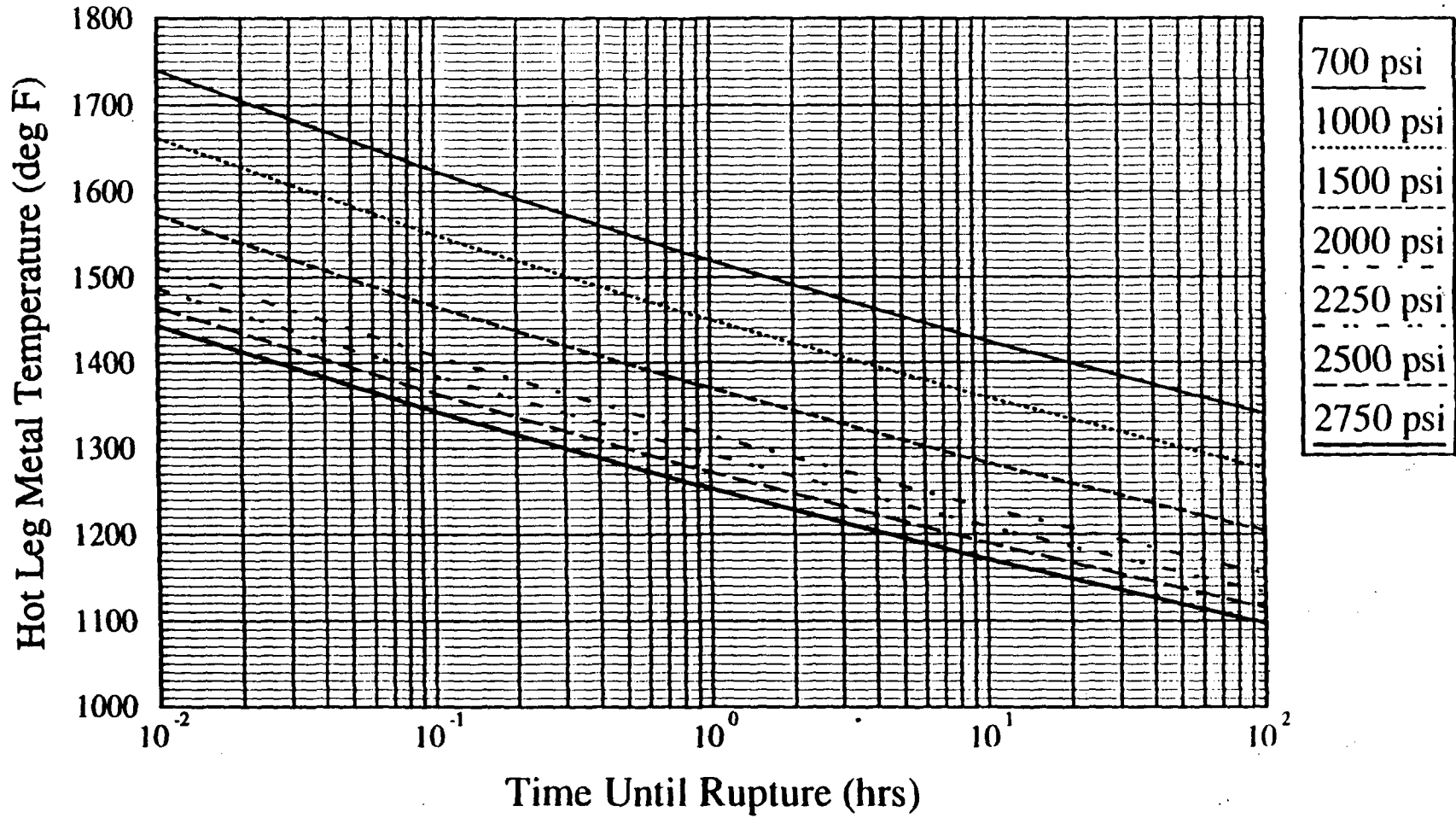


Figure 2-4. Creep Rupture for Hot Legs

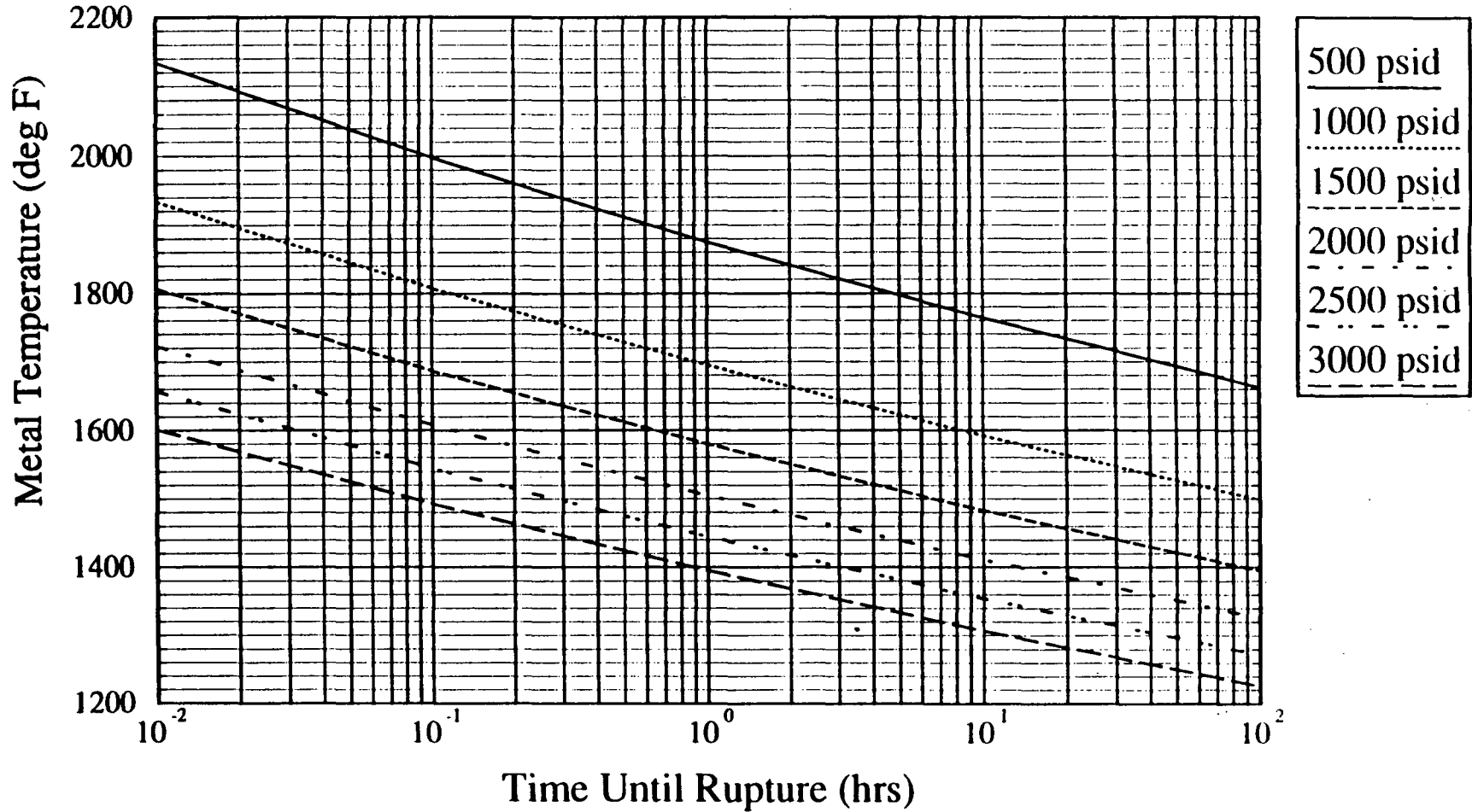


Figure 2-5. Creep Rupture for Steam Generator Tubes

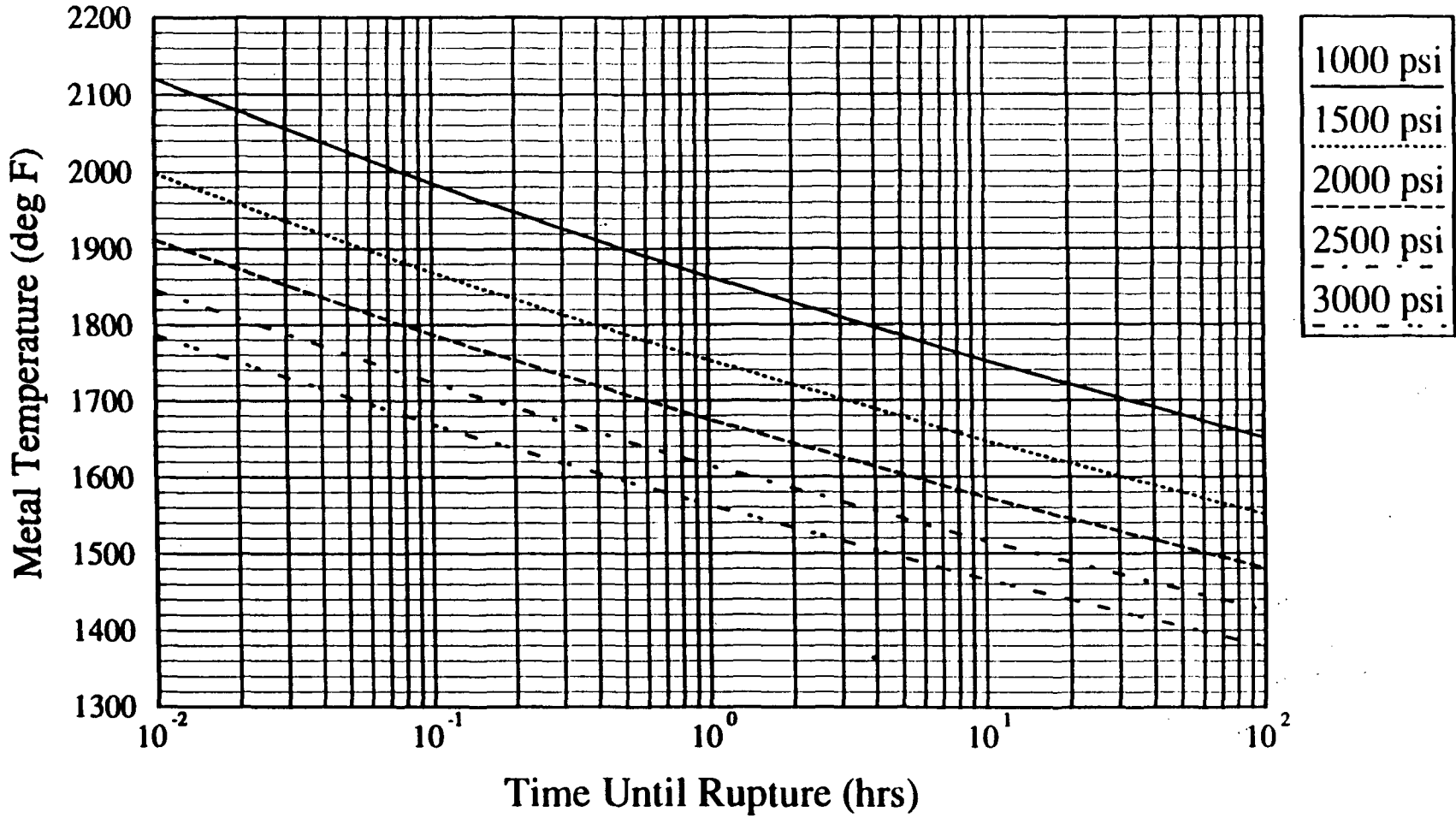


Figure 2-6. Creep Rupture for Surge Line

An additional consideration, however, was the relative heatup times of thick-walled components such as the RCS hot legs as compared to the thin-walled steam generator tubes. Estimations based on thick plate approximations indicated a heatup lag in thick-walled hot legs of approximately 30 to 45 minutes.

For sequences which involve forced circulation with a very high system void coefficient such as RCP restarts during core ICC conditions, MAAP has limited RCS flow modeling capabilities (RCP start is modeled by artificially "clearing the pump bowls"). Therefore, to evaluate creep rupture potential for these cases, the circulating gas temperature was assumed to be equivalent to the reactor vessel upper plenum gas temperature. The above considerations were explicitly taken into account in the CET (refer to Section 5.2.3).

2.2.4 Flammable Gas Generation and Combustion

The potential combustion of gases within containment is of importance during all portions of analyzed sequences. Both the amount of gas available for combustion and the extent (or completeness) of possible burns are important.

Generation

For all analyzed sequences, MAAP provided estimates of hydrogen generated, both in-vessel and ex-vessel. For all base cases analyzed, the "no blockage model" was utilized, allowing for oxidation and gas flow through degraded core regions (and hence hydrogen production) for an extended period until the region is essentially plugged solid with core debris. Sensitivity studies (as noted previously in Section 2.1) were also conducted to better understand code hydrogen generation values.

Other references were also reviewed regarding hydrogen generation. As part of the NUREG-1150 expert elicitation process, probability distributions of hydrogen generation were estimated (Ref. 9). Base-case MAAP results were generally close to the 50%-tile aggregate expert estimations, normally in the 30% - 40% clad oxidation range. As an upper bound, the value of 75% clad oxidation referred to in 10 CFR 50.44 (Ref. 10) was utilized. It is worthwhile to note the maximum generated in the base-case MAAP runs was for a medium LOCA where ICC operator actions resulted in a collapsed core configuration and resultant significant increase in clad oxidation (to approximately 57%).

While increased zirconium oxidation can occur in-flight for corium ejected at high pressure, overall ex-core combustible gas generation is closely associated with corium coolability (which is addressed in Section 2.2.1). If core-concrete interaction occurs, gases liberated from the concrete can interact with molten corium to form other gases, such as carbon monoxide and additional hydrogen. For instance the reaction $Zr + 2CO_2 \rightarrow ZrO_2 + 2CO$ (Ref. 11) is of interest given the containment concrete. The limestone/limestone concrete at Davis-Besse is approximately 38% CO_2 upon decomposition, which is then available to react and form carbon monoxide. Additional hydrogen can also be formed from the reaction of iron (e.g., basemat rebar) and steam.

Combustion

Prior to potential corium-concrete interactions (and attendant CO production), hydrogen burns are of principal interest. For a hydrogen burn to occur, a minimum concentration threshold, or "lower limit of flammability" must be reached. Although burning can occur at concentrations moderately above this lower limit, the resultant combustion is relatively incomplete, without widespread flame propagation (global burning). If hydrogen concentrations increase sufficiently, global burns can occur, consuming most available hydrogen in the containment. Hydrogen concentrations necessary to achieve a lower limit of flammability are about 4%, and for global propagation are about 8% to 9%. Partial propagation can occur at about 6% hydrogen (Ref. 12).

Along with necessary hydrogen concentrations, the possibility of inerting (especially due to steam) has a distinct effect on combustion. Figure 2-7 (Ref. 13) indicates that increasing concentrations of steam, particularly above 25%, act to increase the lower limit of flammability. Eventually, at steam concentrations just above 50%, total inerting exists such that no hydrogen burns would occur, regardless of the hydrogen concentration present.

The total free volume of the Davis-Besse containment is 2.834 million cubic feet. If 55% of all zirconium in the core was oxidized and containment was at atmospheric pressure and 95 F, a hydrogen concentration of about 8.8% would exist, which is in the range where global burns could be sustained. The overall rise in pressure in accident sequences, however, is almost entirely due to added steam mass in the contained volume (e.g., the rise in pressure from heatup of existing air from 120 F to 300 F is only about 3 psi). This mass addition has the dual effect of adding inertment and reducing the volumetric fraction of hydrogen. As an example, one of the medium LOCA sequences analyzed (Ref. 14) had the same 55% clad oxidation level, no containment spray actuation, but both trains of containment air cooler functioning. Containment conditions at a sequence time of 48 hours were total pressure of 23 psia, temperature of 180 F, steam fraction of 29%, and a resultant hydrogen fraction of 6.5% which is below the necessary fraction to support a global burn.

While MAAP calculates burn pressures for a given predicted hydrogen concentration, the effect of burning imposed higher hydrogen concentrations for the CET quantification was accomplished via separate calculations. Based on a review of literature (References 15, 12, etc.) a simplified computer program was created to estimate burn pressure rises for complete combustion (effects of steam in the containment atmosphere included), with the following reduction factors applied based on overall hydrogen concentrations:

<u>Containment Hydrogen Concentration</u>	<u>Pressure Rise Reduction Factor*</u>
< 4%	N/A—no combustion
4% - 6%	0.5
6% - 8%	0.66
> 8%	1.0—complete combustion assumed

* Applied to sequences with or without containment air coolers functional.

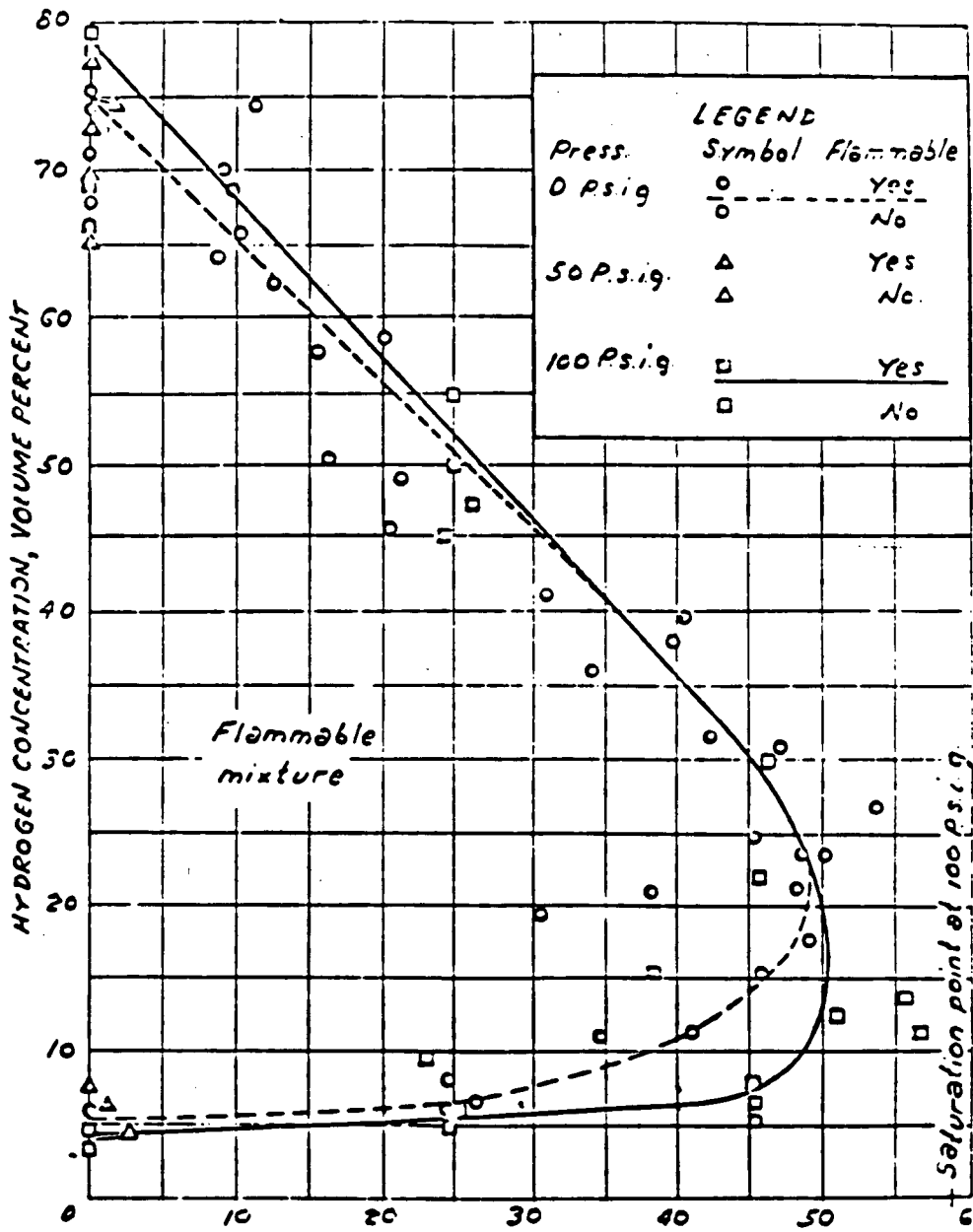


Figure 2-7. Nominal Flammability Limits for Hydrogen

2.2.5 Containment Performance Improvement Program

Generic Letter 88-20 Supplement 3 contains information regarding completion and insights of the NRC Containment Performance Improvement Program (CPIP). For PWR dry containments, the supplement states the following:

“Depending on the degree of compartmentalization and the release point of the hydrogen from the vessel, local detonable mixtures of hydrogen could be formed during a severe accident and important equipment, if any is nearby, could be damaged following a detonation. Licensees with dry containments are expected to evaluate containment and equipment vulnerabilities to localized hydrogen combustion and the need for improvements (including accident-management procedures) as part of the IPE.”

The supplement also states that “...NUREG/CR-5275 provides a discussion of one method that has been used to evaluate the potential for local hydrogen detonations.”

NUREG/CR-5275 (Ref. 16) provides a discussion of a method that has been used to evaluate the potential for a local hydrogen detonation within geometries typically found in a nuclear power plant containment. This method was used in NUREG/CR-4803 (Ref. 17) to investigate the possibility of a local detonation in the containment of the Bellefonte Nuclear Power Plant. The report concluded that there was a low potential for a hydrogen detonation in the Bellefonte containment except for one volume, and only then in a few cases.

In general, the Davis-Besse containment appears to be even more open than the Bellefonte containment. There are, however, two portions of the Davis-Besse containment which offer a geometry which may be conducive to hydrogen detonation (e.g., deflagration-to-detonation transition phenomena). The first is the incore tunnel which extends from the reactor vessel cavity to the room containing the containment emergency sump. While geometrically favorable, this tunnel will be steam inerted or flooded for virtually all cases in which significant amounts of hydrogen could be collected in this tunnel. This compartment is therefore considered unlikely to develop a hydrogen detonation. Note that Bellefonte is also a raised loop B&W NSSS, and has a ventilation tunnel adjacent to its reactor cavity which is generally similar in geometry to the Davis-Besse incore tunnel.

A second possible area which offers a potential favorable geometry is the region which contains the opening of the incore tunnel and the emergency sump, and exits into the open building. In this case, there appears to be no reasonable mechanism to locally elevate the hydrogen concentration within this region to a point that detonation could be possible.

The remainder of containment is open with large pathways between compartments. This tends to allow circulation and mixing of hydrogen and is not conducive to the creation of locally detonable concentrations.

It is therefore concluded that none of the Davis-Besse containment compartments would be classified as conducive to the creation of locally detonable hydrogen concentrations.

Section 3

BINS AND PLANT-DAMAGE STATES

At several stages in this assessment, elements of the accident sequences have been grouped according to similarities in characteristics. For example, many of the initiating events defined in Part 3 actually represent groups of different specific initiators that all have similar effects on the systems required to respond to them. Component failures that have similar effects on the availability of a portion of a system have been grouped into modules in the system fault trees. This grouping process is used primarily to make the overall analysis process more efficient and tractable by limiting the number of discrete events and scenarios that must be considered, while retaining the degree of discrimination required to understand differences in potential accident sequences.

Of particular importance are the groupings of accident sequences formed before they are evaluated in the containment event tree. These groupings, referred to as plant-damage states, permit the consideration of characteristics of the accident sequences that can have an impact on the likelihood and severity of different releases from containment. Thus, in addition to consolidating scenarios with similar characteristics, they provide a mechanism for coordinating the front-end and back-end analyses.

The plant-damage states reflect binning of accident sequences at two major levels. First, the accident sequences up to the onset of core damage are grouped into core-damage bins according to similarities in their impact on subsequent containment response. These bins help to ensure that the core-damage sequences are developed in sufficient detail to permit them to be tracked properly in the containment event tree. The second level encompasses the status of the containment systems (the containment air coolers, containment spray, etc.). The status of these systems defines in large measure the capability of the containment to prevent a serious release as a result of the core-damage accidents. The core-damage bins together with the states for the containment systems comprise the plant-damage states. The development of these damage states is described in the sections that follow.

A final grouping of accident sequences has been made based on the outcomes from the containment event tree. In this case, accidents that could produce similar releases of fission products are grouped into release categories. If an assessment were to be made of the offsite consequences of an accident, these release categories would constitute the principal inputs. The release categories are described in Section 7.

3.1 ATTRIBUTES OF PLANT-DAMAGE STATES

The conditions in the RCS and, to some extent, the conditions in containment prior to vessel breach, form the basis for the core-damage bins. The remaining considerations relating to the containment conditions and the status of the containment safety features complete the definitions of the plant-damage states. The types of parameters considered to be of most importance include those discussed below.

Timing of Core Damage

The rate of melting of the core and the energy loads in containment depend to some extent on the level of decay heat at the onset of core damage. During the initial period following the start of the accident, there will be a relatively large heat load that will decrease rapidly. After a few hours, the rate at which decay heat decreases slows substantially. Therefore, only relatively large differences in timing are important with respect to the effects on containment (e.g., whether core damage starts within one or two hours after the initiation of an accident or core cooling succeeds for several hours).

A finer discrimination of accident timing is of interest in the event that a full assessment is to be made of offsite consequences. In that case, the time between the starting of core melt and the release from containment can have a significant impact on the ability to evacuate the areas near the plant. This, in turn, can affect the potential for early health effects.

Since this assessment does not directly address offsite consequences, this finer level of discrimination is not necessary. It is sufficient to identify whether core cooling is lost near the time of the shutdown, or at a period at least several hours later.

Rate of Leakage from the RCS

The rate of leakage from the RCS clearly has an impact on the timing of core damage. Beyond that, it affects such considerations as the timing of release of hydrogen produced during core degradation, the potential for holdup of fission products in the RCS, and the blowdown loads on containment. The leakage rates considered in this study range from those associated with a large LOCA, in which the inventory of the RCS would be lost in a short time and there would be little holdup of gases in the RCS, to those caused by cycling of pressurizer relief valves with no continuous breach in the RCS and no steam generator cooling. Consistent with the treatment in most PRAs for PWRs, the following categories of leakage were defined:

- Large LOCA, which would entail rapid blowdown of the RCS inventory, and subsequent discharge at a rate dictated by the decay heat load and/or the amount of water being injected.
- Medium LOCA, which would involve substantial leakage over a much longer period of time.
- Small LOCA, with a relatively small but continuous rate of leakage.
- Cycling relief valves, with leakage driven by decay heat but no breach in the reactor coolant system.

RCS Pressure Prior to Vessel Breach

The pressure at the time of vessel breach is among the most important attributes of the core-damage sequences with respect to subsequent containment response. The loading on containment at the time of vessel breach can be strongly affected by RCS pressure (e.g., due to the potential for direct containment heating). Pressure also affects the possibility that there

will be a creep rupture in some other portion of the RCS prior to vessel breach as a consequence of the high temperatures that develop during core degradation. Pressure prior to vessel breach is closely tied to the rate of RCS leakage rate, especially for larger breaks. For small LOCAs and for transients, the availability of feedwater and the possibility that the operators may take steps to depressurize the reactor (e.g., by opening the PORV) can also have a significant impact on the RCS pressure.

Calculations of accident response for Davis-Besse and a review of treatments for other PWRs indicate that pressure ranges of interest could be adequately characterized as follows:

- High (greater than about 2000 psig). At this level, the blowdown forces are likely to produce wide dispersal of the core debris, possibly sufficient to cause direct containment heating. The potential might also exist for creep rupture to affect the integrity of the RCS pressure boundary due to the pressure differential available.
- Moderately high (about 1000 to 2000 psig). Moderate pressure could also provide a driving force for significant dispersion of molten core debris, but would be substantially less likely to provide the pressure differential necessary to induce a failure elsewhere in the RCS.
- Intermediate (200 to 1000 psig). In this pressure range, there would be substantially lower potential for high-pressure melt ejection, and consequently for dispersal of debris beyond the reactor cavity. The pressure would still be considered to be high enough to suppress an in-vessel steam explosion.
- Low (less than about 200 psig). If the reactor vessel were at low pressure immediately before it was breached, it is unlikely that substantial amounts of debris could be dispersed beyond the reactor cavity.

Heat Removal Via the Steam Generators

For at least some types of accidents, the availability of heat removal via the steam generators can be important to the outcome of an accident. The availability of heat removal can affect RCS pressure and the timing of core damage. Perhaps more significantly, a continuing supply of feedwater to the steam generators can provide cool surfaces to which some fission products may adhere, so that the fraction released to the containment (and ultimately available for release to the environment) can be reduced. Thus, whether cooling is available to at least one of the steam generators is one of the conditions to be considered.

Presence of Water in Reactor Cavity

The amount of water present in the reactor cavity and in the lower level of containment (i.e., the basement) is very important to determining containment response. Deep flooding of the reactor cavity offers some potential that the core debris could be cooled sufficiently after slumping that the reactor vessel bottom head might not be breached. If sufficient water is present following vessel breach, it is probable that the core debris would be quenched and cooled sufficiently to prevent significant core-concrete interactions. Overlying

water can also provide an effective means to scrub some fission products released from the debris after exiting the reactor vessel.

Because of the geometry of the reactor cavity and the lower compartment at Davis-Besse, if only the contents of the RCS (with or without the volume of the core flood tanks) were to be lost to containment, the cavity would be flooded to a depth of a few feet. If the BWST contents were to be injected, the cavity would be deeply flooded (up to about the level of the hot-leg nozzles). The flooding would extend up to a few feet in the lower compartment. Only in the event of a sequence entailing containment bypass would the cavity be dry. Therefore, three conditions require consideration with respect to the amount of water in the reactor cavity:

- Deeply flooded cavity (BWST contents injected),
- Partially flooded cavity (BWST contents not injected), and
- Dry cavity (bypass sequence).

Status of Containment Pressure Boundary

Breaches in the containment pressure boundary other than those due to the loadings produced by the accident can be assigned to two categories: pre-existing leakage, such as failure of a penetration to be properly isolated, and containment bypass, in which leakage directly from the RCS to a point outside containment contributes to the occurrence of core damage. Clearly, it is necessary to track both of these possibilities for their effects on releases from containment.

Status of Containment Heat Removal

For many sequences, the ability to provide for removal of decay heat from containment is critical to preventing overpressurization of the containment. The status of containment heat removal is also important with respect to determining the base pressure in containment prior to the occurrence of phenomena such as hydrogen burns or direct containment heating that could cause an incremental rise in pressure. Finally, the status of heat removal could play a role in determining the degree to which hydrogen burns might be prevented due to steam inerting of the containment atmosphere.

Two means of providing removal of decay heat from containment are considered: the function of the containment air coolers (CACs), and operation of low pressure recirculation of water from the containment sump. The containment spray system is not considered with respect to containment heat removal, at least in the long term. At Davis-Besse, the spray system would act to suppress steam pressure while it was injecting cool water from the BWST. When the BWST inventory was depleted, the spray system would draw directly from the containment sump, and would therefore recirculate warm or hot water.

Status of Fission-Product Spray Removal

Although the spray system is of limited benefit with respect to removing decay heat from containment, it may serve as an effective mechanism for removing fission products from the containment atmosphere before they can be released to the environment. Operation of the spray system would also ensure that the contents of the BWST were injected into containment, so that the reactor cavity and lower compartment were flooded. Therefore, the status of the spray system in both the injection and recirculation phases is relevant to most of the core-damage accidents.

3.2 DEFINITION OF CORE-DAMAGE BINS

The general attributes of interest for the plant-damage states were identified in the preceding section. Some of these attributes relate to the nature of the core-damage sequences, and were used to define the core-damage bins. As they are used in this study, the core-damage bins are each defined by three attributes. A three-letter designator is used to identify each of the bins, with each letter signifying one of the three attributes. The attributes and the criteria for their application are described below.

Type of Initiating Event

The first attribute defines the type of initiating event. This determines in large measure the leakage rate from the RCS and the RCS pressure at the time of vessel breach. The type of initiating event can also represent whether there is a bypass of containment. The types used and their designators are as follows:

- A Large LOCA
- M Medium LOCA
- S Small LOCA (including LOCAs resulting from stuck-open relief valves or RCP seal LOCAs following a transient initiating event)
- R Steam generator tube rupture, with bypass of containment due to leakage through the broken tube
- V Interfacing-systems LOCA, with a large bypass path via another connection to the RCS
- T Transient (i.e., no LOCA, but possibly cycling pressurizer relief valves)

Timing of Failure of Core Cooling

As noted in the previous section, a coarse representation of the accident timing is also required. Losses of core cooling are assigned to one of two categories:

- I Loss of core cooling early (e.g., at the start of the injection phase)
- R Loss of core cooling late (e.g., at the start of the recirculation phase)

The accident type, coupled with the phase of the accident in which core cooling is lost, provide an adequate definition of the timing of the accident. By using these time phases, some information regarding whether or not the contents of the BWST have been injected can also be tracked. In all but the cases of the bypass sequences (accident types R or V), failure at the time of recirculation would imply that the BWST contents had been injected. Failure in injection would be less definitive, since the contents could be injected by the spray system or by an injection system that would not have been capable of providing core cooling (e.g., injection by the DHR system after vessel failure for a small LOCA or transient in which RCS pressure remained high during core degradation).

Availability of Steam Generator Cooling

The final attribute refers to the availability of feedwater in at least one of the steam generators. The presence of feedwater can provide cool surfaces that would lead to plateout of some fission products. For all but the large and medium LOCAs, the accident timing and RCS pressure would be further defined by whether feedwater was available. For example, in the case of a small LOCA with failure of injection, the availability of feedwater could cause vessel breach to be delayed by several hours beyond the time when it would fail if there were no feedwater. The status of steam generator cooling is defined by the following:

- Y Feedwater is available to at least one steam generator
- N Feedwater is not available to either generator
- X The availability of feedwater is largely irrelevant to the course of the accident (e.g., for a large or medium LOCA)

Summary of Core-Damage Bins

The attributes outlined above are combined to define the core-damage bins used for Davis-Besse. They are summarized in Table 3-1. Note that an exception was made to the convention of using three-letter designators for the bins in the case of the interfacing-systems LOCA. Since other attributes are generally not of interest for this case, it is identified simply as core-damage bin V.

It should be noted that there are other attributes that could have been included in the definition of the core-damage bins. Perhaps most important among these would have been further definition of the RCS pressure associated with the sequence. While all three of the attributes that were used have a bearing on RCS pressure at the time of core degradation, it would also be important to understand whether or not the operators had taken steps to depressurize the RCS (e.g., by opening the PORV). This and other attributes were relegated to the bridge trees described in the next section. In the judgment of the analysts, this was desirable from the standpoint of avoiding further complexity in the definition of the core-damage sequences. Those events that were included specifically to aid in characterizing the core-damage bins (e.g., the inclusion of a branch point for steam generator cooling for some

**Table 3-1
Summary of Core-Damage Bins**

Designator	Description
AIX	Large LOCA leakage rate, failure of injection (availability of feedwater is not relevant)
ARX	Large LOCA leakage rate, failure of recirculation
MIX	Medium LOCA leakage rate, failure of injection
MRX	Medium LOCA leakage rate, failure of recirculation
SIY	Small LOCA leakage rate, failure of injection, with feedwater available
SIN	Small LOCA leakage rate, failure of injection, with feedwater not available
SRY	Small LOCA leakage rate, failure of recirculation, with feedwater available
SRN	Small LOCA leakage rate, failure of recirculation, with feedwater not available
RIY	Bypass due to steam generator tube rupture, with failure of injection but availability of feedwater
RIN	Bypass due to steam generator tube rupture, with failure of injection and failure of all feedwater
RRY	Bypass due to steam generator tube rupture, with successful injection but failure of long-term cooling, with feedwater available
RRN	Bypass due to steam generator tube rupture, with successful injection but failure of long-term cooling, with feedwater not available
V	Bypass due to interfacing-systems LOCA
TIN	Transient (i.e., no LOCA) with failure of feedwater and failure of injection
TRN	Transient with failure of feedwater and failure of recirculation
TIY	Transient with failure of injection, but feedwater available

scenarios) fit well with the overall definition of the sequences, and were judged not to introduce unnecessary complications in the definition or quantification of the sequences.

3.3 BRIDGE TREES

The second major element that defines the plant-damage states is the status of the containment systems. The status of these systems, together with other attributes of the plant-damage states that were defined in Section 3.1 but that were not represented in the core-damage bins, is identified through the construction of a set of event trees. These event trees essentially provide a mechanism for apportioning the core-damage bins among the various plant-damage states. Because these event trees provide the link between the sequences from the event trees developed to delineate core damage and the containment event tree, they are referred to as bridge trees. The focus of the bridge trees is on the availability of the containment systems (containment isolation, heat removal, and spray operation). In combination with the core-damage bins, they also permit the plant-damage states to identify whether the contents of the BWST have been injected into containment, whether the RCS has been depressurized after the onset of core damage (for high-pressure sequences), and whether the potential exists for core cooling to have been restored after this depressurization.

For convenience, a series of bridge trees was developed, rather than using a single tree to connect all of the core-damage bins to the containment event tree. Each bridge tree accommodates one or more of the core-damage bins. These bridge trees are described in the following sections.

3.3.1 Top Events in the Bridge Trees

The top events used in the bridge trees are outlined in this section. Some bridge trees do not use all of the events, and in some cases the definitions of the top events are different for particular bridge trees. These aspects are described in Section 3.3.2.

Event B: Containment Isolation

The first event in all of the bridge trees except those used for bypass scenarios represents the status of containment isolation. This event has three branches. The top branch indicates that the containment is isolated, the middle branch is used for cases in which there is a small isolation failure (designated outcome B₁), and the bottom branch represents a large isolation failure (outcome B₂). The unavailability of containment isolation was assessed to be dominated by failure to isolate either of two types of lines:

- The line from the normal containment sump. This line is normally open, and isolation would be provided by two motor-operated valves, one inside containment and the other outside. The line penetrating containment is 4 inches in diameter, but it is fed by two 1-1/2-inch lines, so that the leakage path is effectively smaller than 4 inches. It leads to the miscellaneous waste drain tank, so that releases would tend to be well scrubbed. Therefore, it is

considered as a potential small isolation failure and corresponds to outcome B₁ in the bridge trees.

- The lines containing the containment vacuum breakers. There are eight of these lines, each containing a normally-open motor-operated valve and a vacuum breaker. The motor-operated valves should receive a signal to close during accident conditions, and pressurization of containment should cause the vacuum breakers to close. These lines are 8 inches in diameter, so that failure of any of them would constitute a large leak, outcome B₂ in the bridge trees.

Event H₁: Containment Heat Removal Via CACs

The primary means of providing heat removal from containment is by use of the containment air coolers. Event H₁ therefore represents the success or failure of the CACs.

Event G₁: Containment Spray Operates in Injection

Event G₁ represents the availability of the containment spray system to operate in the injection mode (i.e., taking suction from the BWST and injecting into containment). Operation in this mode provides early suppression of steam in the containment atmosphere, ensures that the contents of the BWST are available to flood the reactor cavity, and has the potential to provide for removal of fission products from the containment atmosphere. If the spray system is not available in the injection mode, it is assumed to be unavailable for recirculation from the containment sump as well. Note that the possibility of making the system operable by restoring electric power is addressed separately in the containment event tree.

Event G₂: Containment Spray Operates in Recirculation

In the event that the containment spray system is available to operate in the injection mode, its availability during the recirculation phase is addressed by event G₂. While long-term operation of the containment spray system would not have a significant, directly positive impact on containment pressure, it could continue to serve as a means for fission-product removal from the containment atmosphere.

Event P: Depressurization of RCS

The emergency procedure calls for use of the PORV and other means to depressurize the RCS in the event that conditions of inadequate core cooling were reached. The primary reason that instructions for depressurizing the RCS are included is to enable the contents of the core flood tanks to be injected. In some cases, this would restore core cooling temporarily, providing additional time to establish some other, more permanent mode of core cooling. With respect to the core-damage sequences considered in this study, it is both this aspect (i.e., the ability to restore core cooling, possibly arresting core damage that has already begun), and the apparent benefits of lowering RCS pressure with respect to reducing the effects on containment that may result from accidents that progress at high pressure that are of interest. Event P is used to account for the fraction of the sequences in which

depressurization using the PORV may be available. The actual role of the PORV in depressurization is examined in the context of the containment event tree, based on whether or not it is available, as determined by the plant-damage states.

Event Y: Availability of Injection After Depressurization of RCS

Event Y is used to permit consideration of two potentially important aspects of the plant-damage states. The first is the possibility that core damage may occur under conditions during which systems that are operable may not be capable of injecting. For example, it may be that core degradation may proceed at high pressure, but that following the depressurization that accompanies the failure of the reactor vessel, the DHR system, in the LPI mode, may be able to inject the contents of the BWST into the vessel. This would permit the core debris to be covered, and possibly cooled in the long term.

The second possibility is similar, and relates to the potential that the depressurization of the RCS, such as by use of the PORV, may lead to conditions in which core damage may be arrested before the vessel is breached. Once again, for example, depressurization of the RCS for a small LOCA may lead to conditions in which LPI can permit the core to be covered and to terminate core damage that may have started.

The specific makeup of event Y depends on the core-damage bin, as described in the following section. It generally encompasses consideration of the HPI and DHR systems.

Event H₂: Containment Heat Removal Via Low Pressure Recirculation

As noted earlier in this section, it is possible for the DHR system to provide containment cooling by recirculating water from the emergency sump. Thus, for cases in which containment cooling is not available via the CACs, the availability of this mode of heat removal is considered. In this case, the containment spray system and DHR system, operating in the recirculation mode, would work together to provide containment cooling, since there are no heat exchangers in the recirculation path for the spray system.

3.3.2 Description of Bridge Trees

The structure of the bridge trees and the application of the top events identified in the previous section are described in this section. A total of eight bridge trees were constructed to accommodate the core-damage bins.

No bridge tree was constructed for core-damage bin V, corresponding to a large bypass of containment, since none of the containment safety features would apply. The only event in the containment event tree that is relevant relates to the potential that the release would be scrubbed by overlying water. This is handled within the supporting logic for the containment event tree, and does not require further discrimination of the plant-damage state.

Bridge Tree for Bin AIX

The bridge tree constructed to accommodate core-damage bin AIX is shown in Figure 3-1. This bin is for large LOCAs with failure of injection by the DHR system. The first four top events are as described in Section 3.3.1. Since the RCS is depressurized by the initiating break, it is not necessary to consider operator intervention to use the PORV. In addition, the failure of the DHR system in the injection mode is assumed to preclude its use to remove decay heat from containment in the recirculation mode. Therefore, the event tree does not include events P and H₂. Event Y reflects the possibility of injection of the BWST contents by the HPI system. Although that system would not be able to provide sufficient makeup to prevent uncovering of the core, it could help to ensure that the reactor cavity and lower compartment were deeply flooded. Note that branch points are included for event Y only for cases in which the containment spray system fails in the injection phase, since the spray system would serve to inject the BWST contents much more rapidly than would the HPI system.

For cases in which there is a large leak from containment (outcome B₂ for event B), note that the remaining tree structure is simplified. With a large leak, it is assumed that the containment will not be pressurized by the generation of steam or long-term production of non-condensable gases. Therefore, branch points are not included for the top events relating to containment heat removal. This is true in all of the remaining bridge trees as well.

Bridge Tree for Bins ARX and MRX

Bins ARX and MRX are similar in that both refer to substantial LOCAs with failure of the DHR system in the recirculation mode. The bridge tree used for these two bins is shown in Figure 3-2. The structure of the tree is very similar to that described for bin AIX. The notable exception is that top event Y is omitted, since by definition the sequences involve successful injection of the BWST contents into containment. Because both bins also entail failure of the DHR system in the low pressure recirculation mode, restoration of core cooling in the context of event Y is also precluded.

Bridge Tree for Bin MIX

A separate bridge tree was constructed to link medium LOCA bin MIX to the containment event tree, as illustrated in Figure 3-3. The first four events are identical to those described for the previous two bridge trees. Event Y is different from that used for large LOCA bin AIX, and the tree includes event H₂.

For medium LOCAs, the success criteria in the front-end analyses require that both HPI and LPI must function to prevent core damage. Thus, it is possible that one or the other of these systems could succeed in injecting the contents of the BWST but for at least some uncovering of the core to occur. Moreover, if the LPI system functions, it is possible that core damage will be arrested before the vessel is breached. Event Y therefore encompasses aspects both of BWST injection (for consideration relative to containment response) and of possible termination of core damage. For cases in the event tree in which the containment

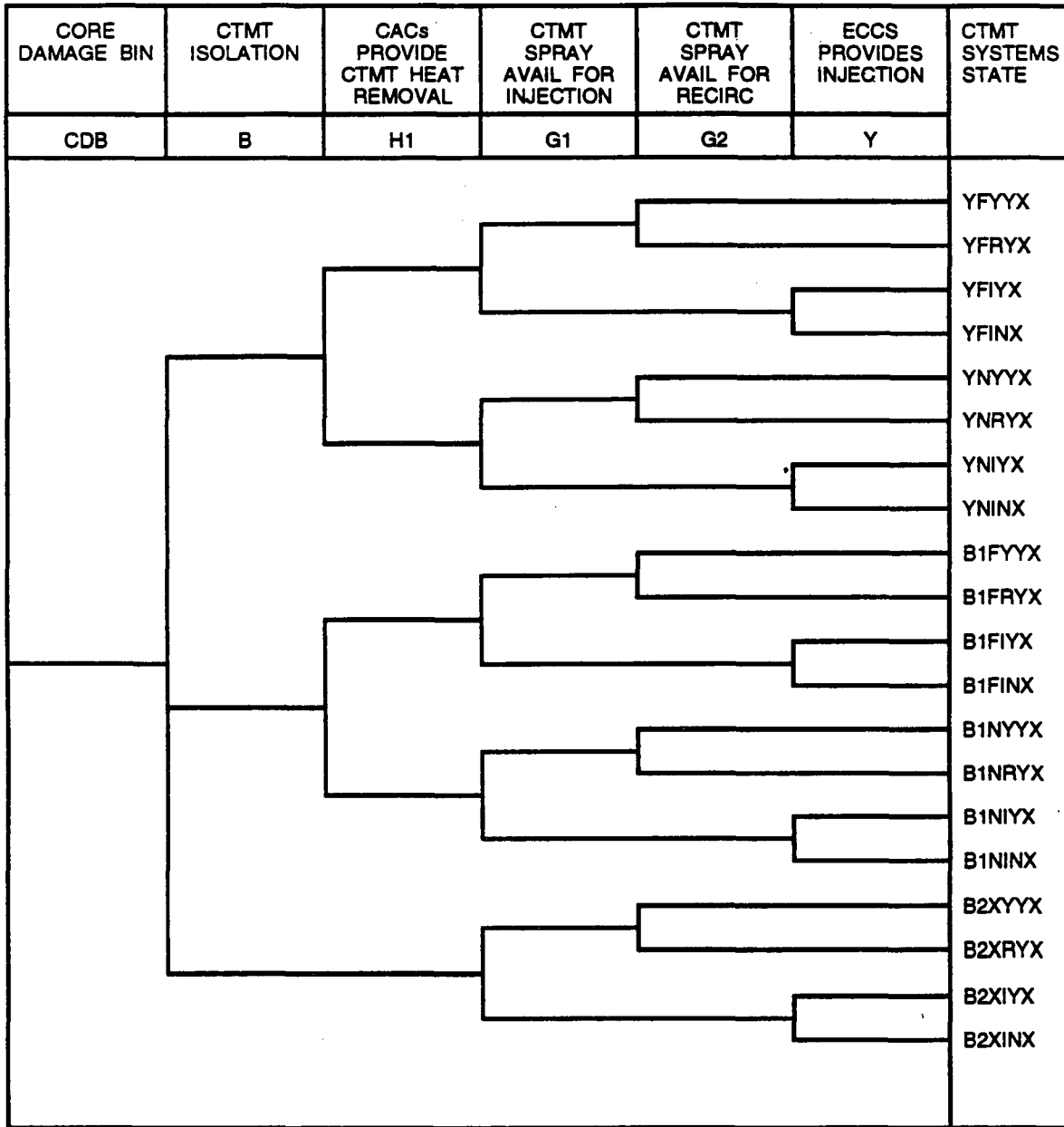


Figure 3-1. Bridge Tree for Core-Damage Bin AIX

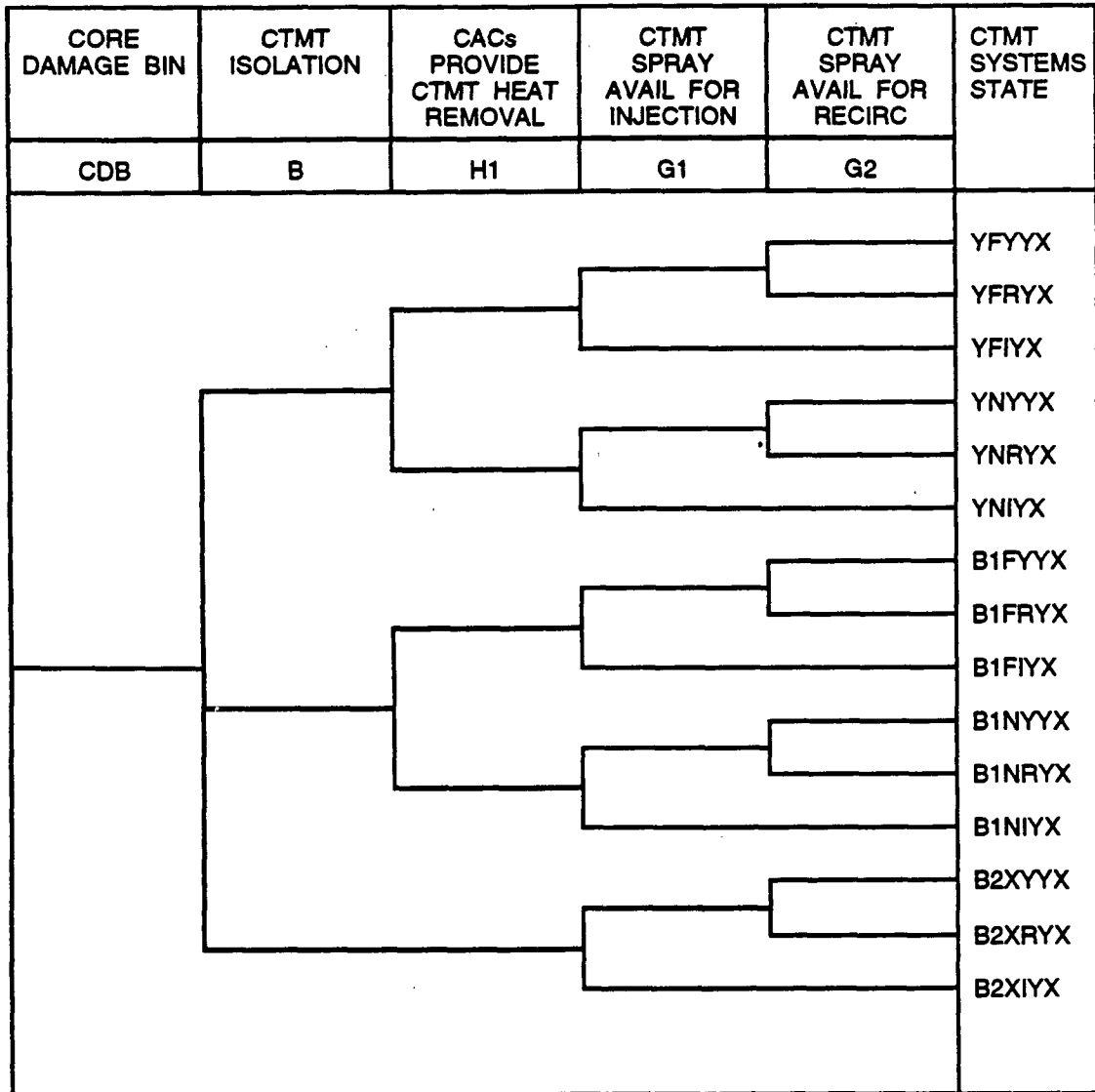


Figure 3-2. Bridge Tree for Core-Damage Bins ARX and MRX

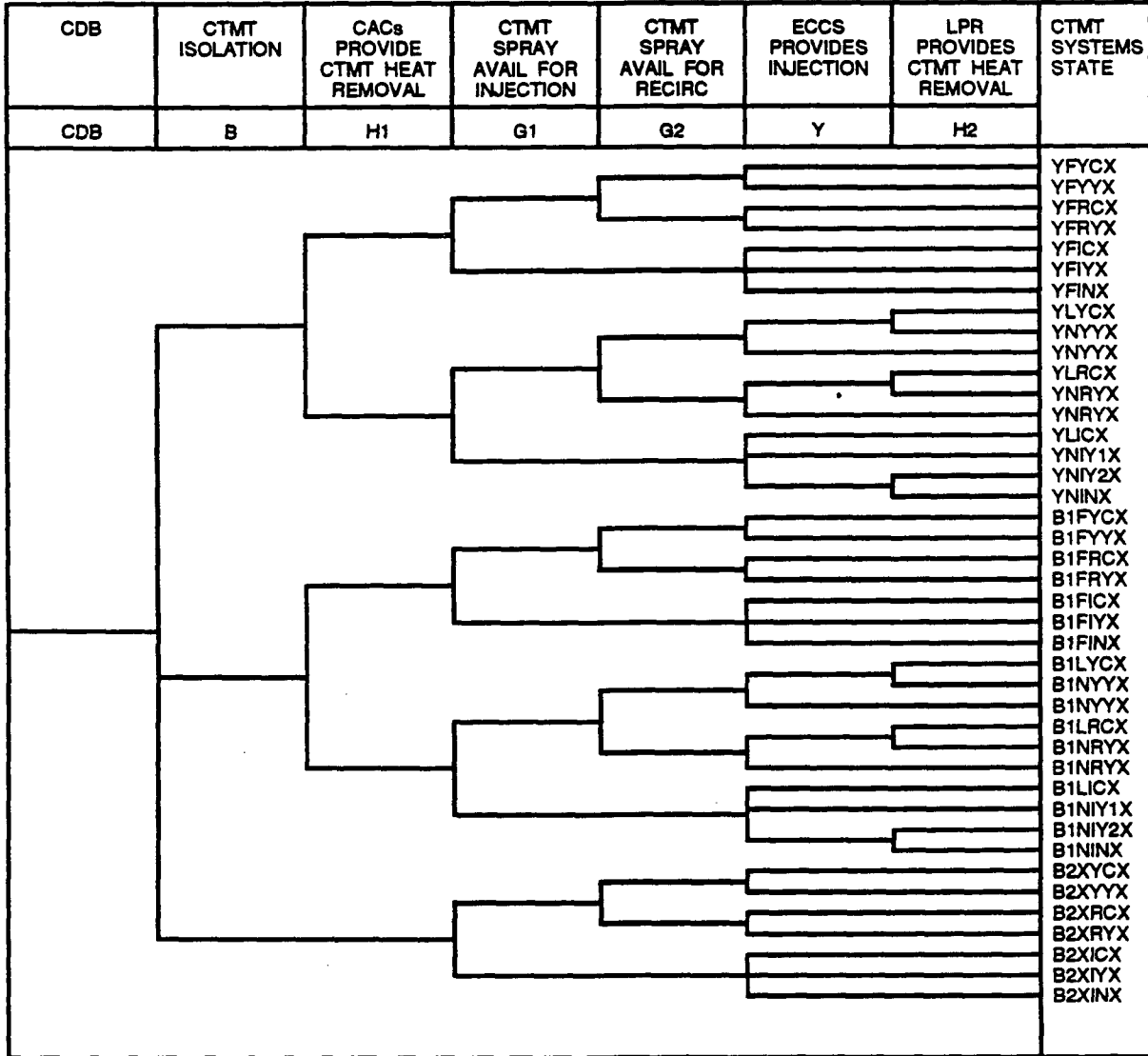


Figure 3-3. Bridge Tree for Core-Damage Bin MIX

spray system succeeds in injecting the BWST inventory, event Y addresses only the success or failure of LPI. Success of LPI in these cases implies that core cooling may be available following some core damage that results from the failure of HPI. Failure of LPI for these cases indicates that core damage will not be arrested by injection, but is irrelevant with respect to ensuring flooding of the reactor cavity and lower compartment.

For cases in which injection by the containment spray system fails, three branches are indicated for event Y. In the first, LPI succeeds, so that the BWST contents are injected, and core damage may be arrested. For the second branch, LPI fails but HPI succeeds. Melting of the core cannot be prevented (HPI will fail when the BWST inventory is depleted), but the BWST contents will be injected. In the third branch, neither system is available, and the contents of the BWST would not be injected into containment.

Because it is possible that the DHR system may be available, event H₂ is included to reflect the potential for containment heat removal to be provided by low pressure recirculation. Success or failure of event H₂ is considered only for scenarios in which heat removal via the CACs fails but injection by LPI succeeds. In these cases, as noted above, containment heat removal (and possibly prevention of vessel breach) may be assured by long-term operation of low pressure recirculation.

Bridge Tree for Bins SIY, SIN, and TIN

Core-damage bins SIY and SIN involve small LOCAs with failure of injection, and bin TIN refers to a transient with total loss of feedwater and failure of makeup/HPI cooling (i.e., failure of injection as well). The bridge tree for these bins is provided as Figure 3-4. These bins are all similar with respect to the consideration of events in the bridge trees. Once again the events relating to containment isolation, heat removal via the CACs, and operation of the containment spray system are identical to their treatment in the preceding bridge trees. In this case, event P is considered as well, as are events Y and H₂.

Event P refers to availability of the PORV to support depressurization of the RCS. If the PORV can be opened when inadequate core cooling conditions are reached, RCS pressure can be reduced substantially before vessel breach. Opening of the PORV also introduces the possibility that core damage may be arrested by the provision of injection from the DHR system. This is considered in event Y. Branch points for event Y are included if there is success for event P, indicating the possibility of recovering core cooling, or if there is a failure of injection by the containment spray system, since the DHR system might inject the BWST contents after the RCS was depressurized (even if the depressurization came about because of the eventual failure of the reactor vessel).

Bridge Tree for Bins SRY, SRN, and TRN

Core-damage bins SRY and SRN are small LOCAs with failure of recirculation cooling (with and without availability of cooling in the steam generators). Transients with total loss of feedwater, success of makeup/HPI cooling, but failure of recirculation for long-

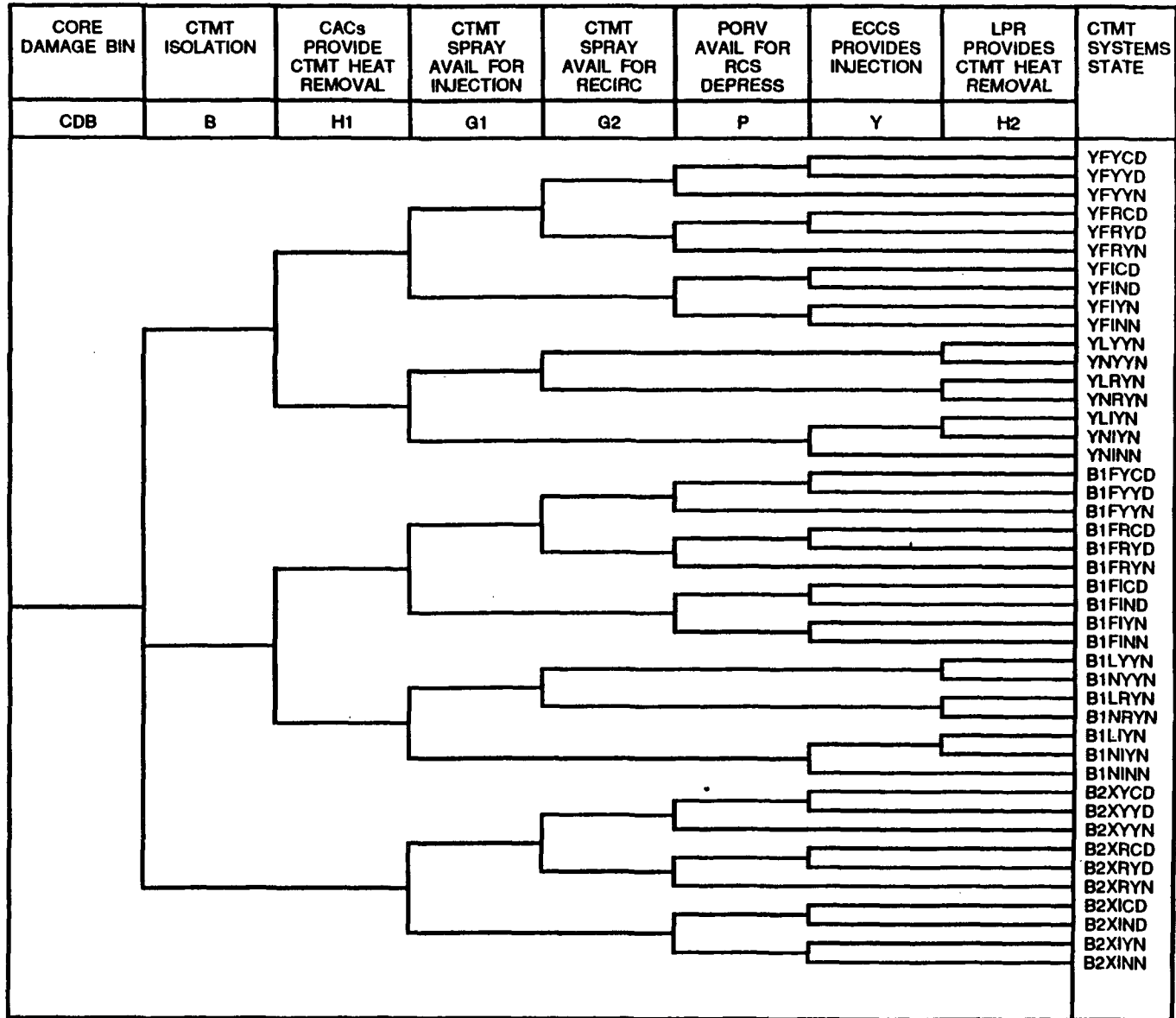


Figure 3-4. Bridge Tree for Core-Damage Bins SIY, SIN, and TIN

term cooling are assigned to bin TRN. The bridge tree used for these bins is shown in Figure 3-5. It is very similar to the tree used for bins SIY, SIN, and TIN; the primary difference is that questions relating to the injection of water by the DHR system are relevant only with respect to consideration of the possibility of arresting core damage in-vessel, since by definition the bins imply that the BWST contents have been injected into containment.

Bridge Tree for Bin TIY

Bin TIY is used uniquely for a sequence involving failure of the reactor to trip, with failure to achieve shutdown. RCS pressure would remain high for an extended period of time, causing inventory to be lost from the RCS despite the availability of feedwater to at least one of the steam generators. The power level and RCS pressure remain relatively high until there is sufficient voiding in the RCS to cause the reactor to shut down. At that point, there may be insufficient water in the RCS to support heat removal via the steam generators.

The bridge tree for bin TIY is shown in Figure 3-6. In this case, it is assumed that pressure will remain too high for the PORV to be effective as a means to depressurize the RCS. Therefore, neither event P nor the availability of injection via the DHR system (event Y) is addressed. Only the availabilities of containment isolation, the CACs, and the containment spray system are reflected in the bridge tree.

Bridge Tree for Bins RIY and RIN

Bins RIY and RIN represent SGTRs in which insufficient makeup and/or early heat removal are available to keep the core covered. The bridge tree used to develop the plant-damage states for these two bins is shown in Figure 3-7. In this case, containment isolation is irrelevant, since the tube rupture constitutes a bypass sequence. Events H₁, G₁, and G₂ define the status for the CACs and containment spray system, as for the previous trees. They are considered because of their potential impact on more severe containment failure modes (e.g., rupture due to the pressure loading from direct containment heating), and for possible reduction in releases after the reactor vessel fails.

The ability to depressurize the RCS using the PORV is evaluated in event P. As for other bridge trees, if the RCS can be depressurized, it may be possible for the DHR system to restore core cooling and to prevent breaching the reactor vessel. Likewise, event Y refers to the availability of injection via the DHR system, as in the case of bins SIY and SIN.

Bridge Trees for Bins RRY and RRN

Bins RRY and RRN refer to SGTRs with successful injection, but failure of long-term cooling. It is assumed for these bins that the reactor cavity would be dry, with the BWST inventory lost through the ruptured tube. As in the previous case, it is assumed that containment isolation is not relevant. The only question is whether the PORV is opened to depressurize the RCS, because of the possible effects relative to the potential for more severe failures of containment (e.g., as a consequence of direct containment heating). The event tree, shown in Figure 3-8, therefore has only one top event.

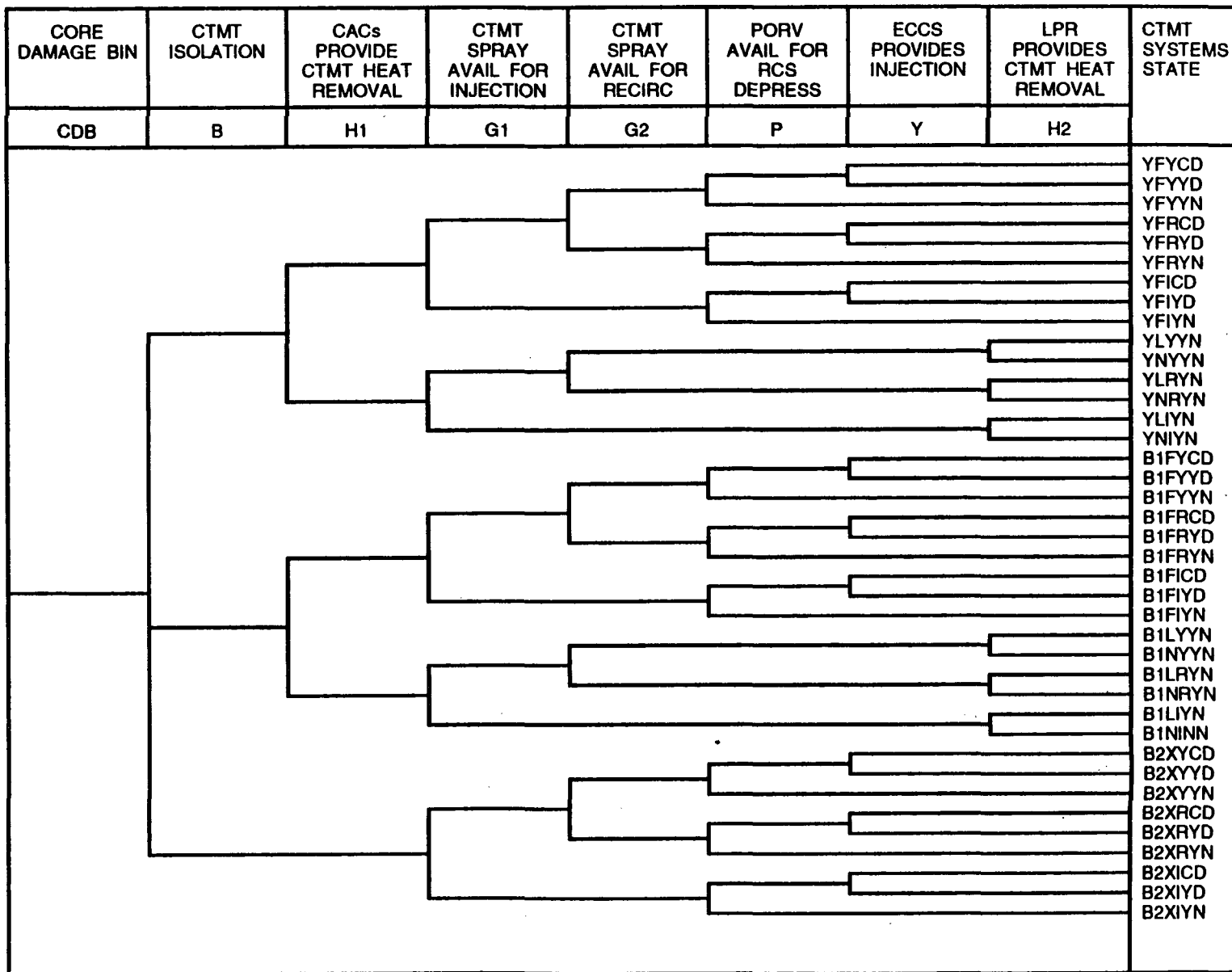


Figure 3-5. Bridge Tree for Core-Damage Bins SRY, SRN, and TRN

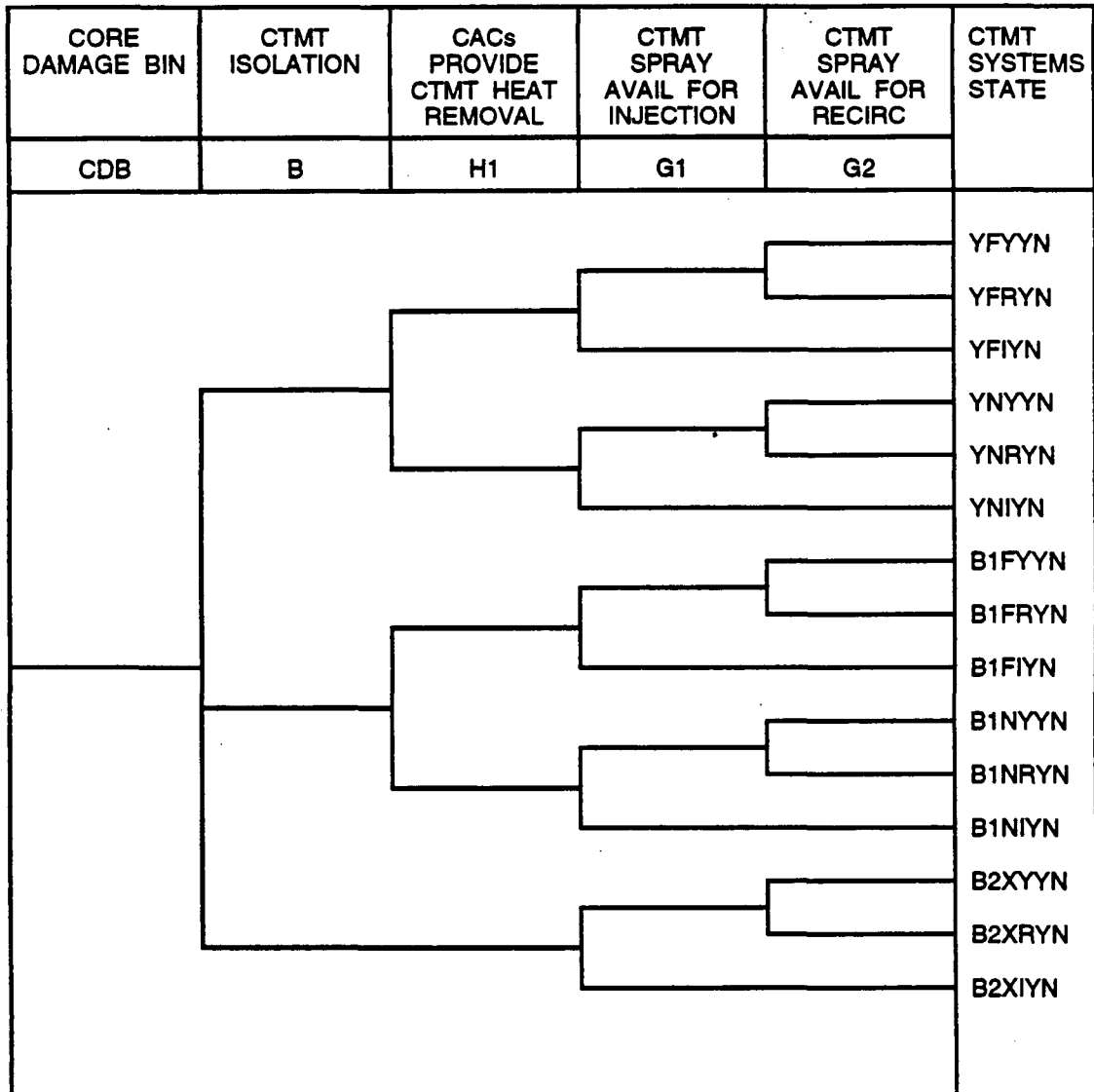


Figure 3-6. Bridge Tree for Core-Damage Bin TIY

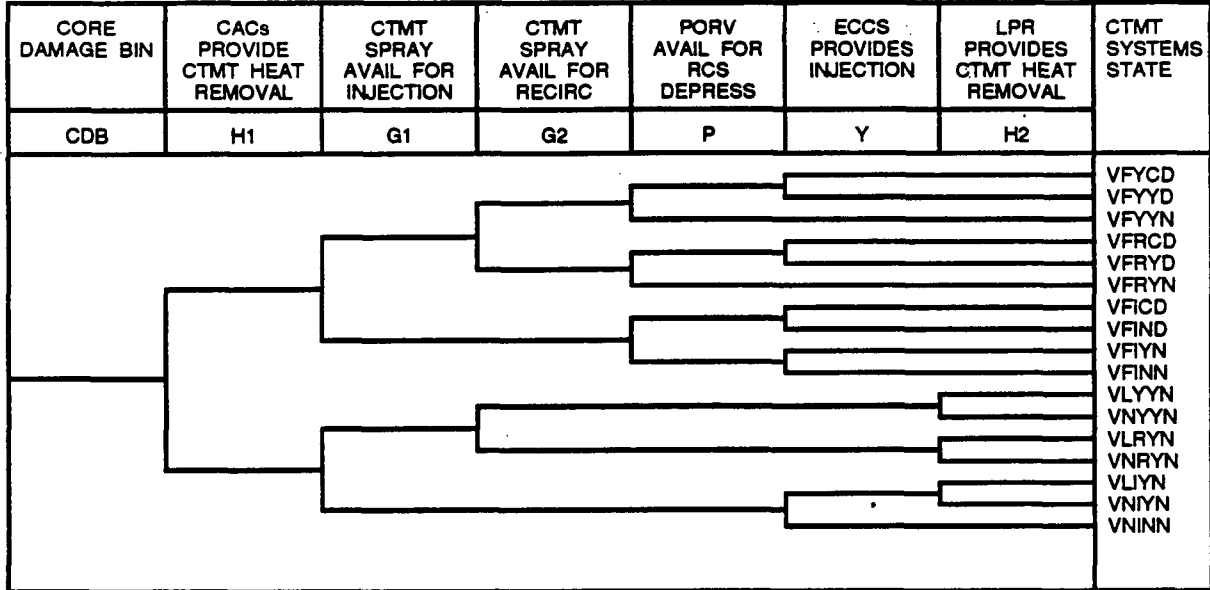


Figure 3-7. Bridge Tree for Core-Damage Bins RIY and RIN

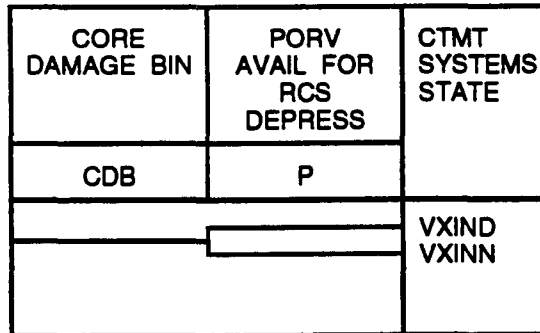


Figure 3-8. Bridge Tree for Core-Damage Bins RRY and RRN

3.4 SUMMARY OF PLANT-DAMAGE STATES

The plant-damage states are comprised of the core-damage bins described in Section 3.2 and the containment systems states corresponding to the end points in the bridge trees outlined in Section 3.3. By combining these two elements, a very large number of possible plant-damage states could exist. The number of states is actually much more limited, since some combinations produce negligible frequencies. Typically, only a very few of the end states from the bridge trees are applicable for any particular core-damage bin.

The containment systems states are designated in the bridge trees by five elements. The five elements are defined below:

(1) Status of containment isolation

- Y Containment is isolated
- B1 Small containment isolation failure
- B2 Large containment isolation failure
- V Containment bypass

(2) Status of containment heat removal

- F Heat removal provided by the CACs
- L Heat removal available via low pressure recirculation
- N Heat removal not available
- X Heat removal not relevant (e.g., for a bypass sequence)

(3) Status of containment spray

- Y Containment spray available in injection and recirculation phases
- R Containment spray available in injection but fails in recirculation
- I Containment spray fails in injection (not available for recirculation)

(4) Availability of BWST injection to reactor vessel or containment

- C BWST contents injected, with potential to restore core cooling
- Y BWST contents injected, but injection not able to restore core cooling (i.e., recirculation failure led to core damage, BWST injected by containment spray, or injection after failure of the reactor vessel)
- N BWST contents not injected, recovery of core cooling in-vessel not available

(5) Availability of PORV for RCS depressurization

- Y PORV available
- N PORV not available
- X PORV availability not relevant

These five elements make up the containment system states that are the end points for the bridge trees. For reference purposes, all of the end states from the bridge trees are defined in Table 3-2.

**Table 3-2
Containment Systems States from Bridge Trees**

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
YFYXX	isolated	available via CACs	available in both injection and recirculation	not available for core cooling, not needed for BWST injection	not relevant
YFRYX	isolated	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not relevant
YFIYX	isolated	available via CACs	not available in injection	available to inject BWST inventory but not for core cooling	not relevant
YFINX	isolated	available via CACs	not available in injection	not available; BWST not injected	not relevant
YNYYX	isolated	not available	available in both injection and recirculation	not available for core cooling, not needed for BWST injection	not relevant
YNRYX	isolated	not available	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not relevant
YNIYX	isolated	not available	not available in injection	available to inject BWST inventory but not for core cooling	not relevant
YNINX	isolated	not available	not available in injection	not available; BWST not injected	not relevant
YFYCX	isolated	available via CACs	available in both injection and recirculation	available for potential recovery of core cooling	not relevant
YFRCX	isolated	available via CACs	available in injection but not in recirculation	available for potential recovery of core cooling	not relevant

**Table 3-2 (continued)
Containment Systems States from Bridge Trees**

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
YFRYX	isolated	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not relevant
YFICX	isolated	available via CACs	not available in injection	available for potential recovery of core cooling and to inject BWST	not relevant
YLYCX	isolated	available via low pressure recirculation	available in both injection and recirculation	available for potential recovery of core cooling	not relevant
YLRCX	isolated	available via low pressure recirculation	available in injection but not in recirculation	available for potential recovery of core cooling	not relevant
YLICX	isolated	available via low pressure recirculation	not available in injection	available for potential recovery of core cooling and to inject BWST	not relevant
YNIY1X	isolated	not available	not available in injection	DHR available to inject BWST, but not for core cooling	not relevant
YNIY2X	isolated	not available	not available in injection	HPI available to inject BWST, but not for core cooling	not relevant
YFYCD	isolated	available via CACs	available in injection and recirculation	available for potential recovery of core cooling	available
YFYD	isolated	available via CACs	available in injection and recirculation	not available for core cooling, not needed for BWST injection	available
YFYYN	isolated	available via CACs	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available

Table 3-2 (continued)
Containment Systems States from Bridge Trees

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
YFRCD	isolated	available via CACs	available in injection but not in recirculation	available for potential recovery of core cooling	available
YFRYD	isolated	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	available
YFRYN	isolated	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
YFICD	isolated	available via CACs	not available in injection	available for potential recovery of core cooling and to inject BWST	available
YFIND	isolated	available via CACs	not available in injection	not available; BWST not injected	available
YFIYN	isolated	available via CACs	not available in injection	available to inject BWST but not for recovery of core cooling	not available
YFINN	isolated	available via CACs	not available in injection	not available; BWST not injected	not available
YLYYN	isolated	available via low pressure recirculation	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
YNYYN	isolated	not available	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
YLRYN	isolated	available via low pressure recirculation	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available

Table 3-2 (continued)
Containment Systems States from Bridge Trees

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
YNRYN	isolated	not available	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
YLIYN	isolated	available via low pressure recirculation	not available in injection	available to inject BWST but not for recovery of core cooling	not available
YNIYN	isolated	not available	not available in injection	available to inject BWST but not for recovery of core cooling	not available
YNINN	isolated	not available	not available in injection	not available; BWST not injected	not available
B1FYYX	small isolation failure	available via CACs	available in both injection and recirculation	not available for core cooling, not needed for BWST injection	not relevant
B1FRYX	small isolation failure	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not relevant
B1FIYX	small isolation failure	available via CACs	not available in injection	available to inject BWST inventory but not for core cooling	not relevant
B1FINX	small isolation failure	available via CACs	not available in injection	not available; BWST not injected	not relevant
B1NYYX	small isolation failure	not available	available in both injection and recirculation	not available for core cooling, not needed for BWST injection	not relevant
B1NRYX	small isolation failure	not available	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not relevant

Table 3-2 (continued)
Containment Systems States from Bridge Trees

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
B1NIYX	small isolation failure	not available	not available in injection	available to inject BWST inventory but not for core cooling	not relevant
B1NINX	small isolation failure	not available	not available in injection	not available; BWST not injected	not relevant
B1FYCX	small isolation failure	available via CACs	available in both injection and recirculation	available for potential recovery of core cooling	not relevant
B1FRCX	small isolation failure	available via CACs	available in injection but not in recirculation	available for potential recovery of core cooling	not relevant
B1FRYX	small isolation failure	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not relevant
B1FICX	small isolation failure	available via CACs	not available in injection	available for potential recovery of core cooling and to inject BWST	not relevant
B1LYCX	small isolation failure	available via low pressure recirculation	available in both injection and recirculation	available for potential recovery of core cooling	not relevant
B1LRXC	small isolation failure	available via low pressure recirculation	available in injection but not in recirculation	available for potential recovery of core cooling	not relevant
B1LICX	small isolation failure	available via low pressure recirculation	not available in injection	available for potential recovery of core cooling and to inject BWST	not relevant
B1NIY1X	small isolation failure	not available	not available in injection	DHR available to inject BWST, but not for core cooling	not relevant

Table 3-2 (continued)
Containment Systems States from Bridge Trees

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
B1NIY2X	small isolation failure	not available	not available in injection	HPI available to inject BWST, but not for core cooling	not relevant
B1FYCD	small isolation failure	available via CACs	available in injection and recirculation	available for potential recovery of core cooling	available
B1FYVD	small isolation failure	available via CACs	available in injection and recirculation	not available for core cooling, not needed for BWST injection	available
B1FYVN	small isolation failure	available via CACs	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
B1FRCD	small isolation failure	available via CACs	available in injection but not in recirculation	available for potential recovery of core cooling	available
B1FRVD	small isolation failure	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	available
B1FRVN	small isolation failure	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
B1FICD	small isolation failure	available via CACs	not available in injection	available for potential recovery of core cooling and to inject BWST	available
B1FIND	small isolation failure	available via CACs	not available in injection	not available; BWST not injected	available
B1FIYN	small isolation failure	available via CACs	not available in injection	available to inject BWST but not for recovery of core cooling	not available
B1FINN	small isolation failure	available via CACs	not available in injection	not available; BWST not injected	not available

Table 3-2 (continued)
Containment Systems States from Bridge Trees

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
B1LYYN	small isolation failure	available via low pressure recirculation	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
B1NYYN	small isolation failure	not available	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
B1LRYN	small isolation failure	available via low pressure recirculation	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
B1NRYN	small isolation failure	not available	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
B1LIYN	small isolation failure	available via low pressure recirculation	not available in injection	available to inject BWST but not for recovery of core cooling	not available
B1NIYN	small isolation failure	not available	not available in injection	available to inject BWST but not for recovery of core cooling	not available
B1NINN	small isolation failure	not available	not available in injection	not available; BWST not injected	not available
B2XYYX	large isolation failure	not relevant	available in both injection and recirculation	not available for core cooling, not needed for BWST injection	not relevant
B2XRYX	large isolation failure	not relevant	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not relevant
B2XIYX	large isolation failure	not relevant	not available in injection	available to inject BWST inventory but not for core cooling	not relevant
B2XINX	large isolation failure	not relevant	not available in injection	not available; BWST not injected	not relevant

Table 3-2 (continued)
Containment Systems States from Bridge Trees

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
B2XYCX	large isolation failure	not relevant	available in injection and recirculation	available for potential recovery of core cooling	not relevant
B2XRCX	large isolation failure	not relevant	available in injection but not in recirculation	available for potential recovery of core cooling	not relevant
B2XICX	large isolation failure	not relevant	not available in injection	available for potential recovery of core cooling and to inject BWST	not relevant
B2XYCD	large isolation failure	not relevant	available in injection and recirculation	available for core cooling; not needed for BWST injection	available
B2XYXD	large isolation failure	not relevant	available in injection and recirculation	not available for core cooling, not needed for BWST injection	available
B2XYYN	large isolation failure	not relevant	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
B2XRCD	large isolation failure	not relevant	available in injection but not in recirculation	available for core cooling, not needed for BWST injection	available
B2XRYD	large isolation failure	not relevant	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	available
B2XRYN	large isolation failure	not relevant	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
B2XICD	large isolation failure	not relevant	not available in injection	available for potential recovery of core cooling and to inject BWST	available

**Table 3-2 (continued)
Containment Systems States from Bridge Trees**

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
B2XIND	large isolation failure	not relevant	not available in injection	not available; BWST not injected	available
B2XIYN	large isolation failure	not relevant	not available in injection	available to inject BWST but not for recovery of core cooling	not available
B2XINN	large isolation failure	not relevant	not available in injection	not available; BWST not injected	not available
VFYCD	bypass (SGTR)	available via CACs	available in injection and recirculation	available for core cooling, not needed for BWST injection	available
VFYD	bypass (SGTR)	available via CACs	available in injection and recirculation	not available for core cooling, not needed for BWST injection	available
VFYYN	bypass (SGTR)	available via CACs	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
VFRCD	bypass (SGTR)	available via CACs	available in injection but not in recirculation	available for core cooling, not needed for BWST injection	available
VFRYD	bypass (SGTR)	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	available
VFRYN	bypass (SGTR)	available via CACs	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
VFICD	bypass (SGTR)	available via CACs	not available in injection	available for potential recovery of core clg and to inject BWST	available
VFIND	bypass (SGTR)	available via CACs	not available in injection	not available; BWST not injected	available

Table 3-2 (continued)
Containment Systems States from Bridge Trees

Bridge Tree Designator	Containment Isolation	Containment Heat Removal	Containment Spray	ECCS Injection	Depressurization via PORV
VFIYN	bypass (SGTR)	available via CACs	not available in injection	available to inject BWST but not for recovery of core cooling	not available
VFINN	bypass (SGTR)	available via CACs	not available in injection	not available; BWST not injected	not available
VLYYN	bypass (SGTR)	available via low pressure recirculation	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
VNYYN	bypass (SGTR)	not available	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
VLRYN	bypass (SGTR)	available via low pressure recirculation	available in injection but not in recirculation	not available for core cooling, not needed for BWST injection	not available
VNRYN	bypass (SGTR)	not available	available in injection and recirculation	not available for core cooling, not needed for BWST injection	not available
VLIYN	bypass (SGTR)	available via low pressure recirculation	not available in injection	available to inject BWST but not for recovery of core cooling	not available
VNIYN	bypass (SGTR)	not available	not available in injection	not available for core cooling, not needed for BWST injection	not available
VNINN	bypass (SGTR)	not available	not available in injection	not available; BWST not injected	not available
VXIND	bypass (SGTR)	not relevant	not available in injection	not available; BWST not injected	available
VXINN	bypass (SGTR)	not relevant	not available in injection	not available; BWST not injected	not available

Section 4

CONTAINMENT FAILURE CHARACTERIZATION

Some of the severe accidents addressed in this study can result in significant internal loadings on the containment vessel. Several different types of loadings and corresponding containment failure modes are reflected in the containment event tree used to delineate response to severe core-damage accidents. These include penetrations that fail to be isolated, missiles that could be generated and that could breach containment, dynamic loads due to detonations and steam explosions, accidents that bypass the containment altogether, and direct attack on the vessel by core debris. For all of those types of threats to containment integrity, the focus in the analysis is on the potential for occurrence of the associated phenomena; if they occur, it is generally assumed that there would be a release from containment.

For many accidents, the primary threat to containment stems from static or quasi-static internal pressure loadings. For these accidents, a meaningful assessment of the capacity of the containment to retain its integrity is needed. This section describes the evaluation of the pressure-retention capacity of the containment vessel and the assessment of the failure mode(s) that could result from accidents that could exceed that capacity.

In the discussion that follows, the evaluation of containment capacity involved two primary areas of investigation:

- (1) The strength of the containment vessel itself, and
- (2) The potential for failure at discontinuities in the vessel, such as at penetrations, or of the penetrations themselves.

4.1 CAPACITY OF THE CONTAINMENT VESSEL

The evaluation of the pressure capacity for the containment vessel was based on an assessment performed for St. Lucie (Ref. 18), and is documented in detail in a separate calculation (Ref. 19). Both Davis-Besse and St. Lucie use large, dry containments that are free-standing steel cylinders with hemispherical top heads and ellipsoidal bottom heads. Both vessels were built by the Chicago Bridge and Iron Company (CBI).

Consistent with the approach used for St. Lucie, the analysis of pressure capacity was accomplished by first developing an estimate of the minimum yield pressure for the containment vessel. This minimum yield pressure was based on the shell membrane capacities for the cylindrical and hemispherical components of the vessel. The minimum yield pressure for the limiting component was then used to develop a distribution of failure pressure for the containment.

In addition to evaluating the basic pressure capacity of the containment, the potential for lower pressure capacity as a result of sustained high temperatures was also evaluated.

4.1.1 Assessment of Containment Vessel Strength

Based on the approach used in NUREG/CR-2442 (Ref. 18), the containment capacity was estimated using the Mises-Hencky "Distortion Energy" failure theory in two dimensions. This theory was applied to the cylindrical and hemispherical shell membranes that constitute the primary components of the containment vessel. The shell membrane capacities for the vessel were estimated from the following equations:

$$P_{\text{cyl}} = \frac{K\sigma t}{R} \text{ and } P_{\text{head}} = \frac{2\sigma t}{R}$$

where σ = minimum yield stress

t = membrane thickness

R = containment radius

$$K = 2/\sqrt{3}$$

Using the equations above and the yield stress values found in the ASME codes for SA-299 steel, the minimum yield pressures were calculated to be 88.8 psig for the cylindrical vessel wall and 87.5 psig for the hemispherical head (Ref. 19). Although the two results differ by only 1.3 psi, the hemispherical head would be more likely to reach its limiting pressure first, and was thus used as the basis for the failure mechanism and location (i.e., large shell membrane failure located high in the containment vessel). These results are based on minimum yield stress values at room temperature ($\sim 70^\circ\text{F}$, Ref. 20).

For accidents that could lead to pressurization of the containment over a long period of time, the containment vessel could be at a temperature substantially higher than ambient. A review indicated that the yield strength of stainless steel tends to decrease in a linear fashion over the range of temperatures that could be of interest for accidents at Davis-Besse (Ref. 21). Values of yield stress for the containment vessel were readily available for both temperature conditions (Ref. 20). It was concluded that a more appropriate characterization of containment capacity for long-term overpressurization scenarios would be obtained based on the strength at the higher temperature. Because the change in strength is small over relatively small temperature differences, it was also judged that this single curve could be applied for all cases involving extended heatup of the containment atmosphere. The minimum yield pressure for the containment head corresponding to a temperature of 264°F was calculated to be 78.2 psig, based on the equation above.

4.1.2 Development of a Distribution for Pressure Capacity

After determining the limiting mechanism for the containment vessel's pressure capacity, the minimum yield pressures were converted to median pressure capacities with a lognormal distribution, consistent with the approach used in NUREG-2442. Following this relatively simple procedure, the yield stress was multiplied by 1.1 and 0.11 to obtain the mean

yield stress and its associated standard deviation, respectively. Since pressure is proportional to the yield stress, the raw mean failure pressure was calculated to be 96.3 psig at room temperature. This raw mean failure pressure was further modified by multiplying by a resistance modeling error value of 0.99 (Ref. 18). The resulting mean failure pressure is 95.3 psig. With further consideration of the material and modeling uncertainties, an overall coefficient of variation (COV) was calculated to be 0.16 (Ref. 22). With the mean failure pressure and COV, a lognormal probability density function and corresponding cumulative distribution function (CDF) were generated.

Using the same approach, the minimum yield stress for pressurization coincident with elevated temperatures was used to obtain a mean failure pressure of 85.2 psig. The CDF of failure pressure for both temperature conditions is shown in Figure 4-1. This curve represents the failure probability for the hemispherical head. The probability distribution for the cylindrical portion was not added to this distribution since the material properties are the same, resulting in a close correlation between the two curves. The bounding curve is therefore represented by that of the hemispherical head alone.

The nature of the containment failure cannot be predicted with certainty. For reinforced concrete containments, there is evidence that the failure may be relatively benign, at least for a relatively slow pressurization (e.g., a leak may develop initially, and this leak may arrest further pressure increases, precluding a more severe failure). For steel containments, it is expected that the failure may be of a more catastrophic nature, based on experimentation and analytical work. Therefore, for Davis-Besse it was assumed that a shell membrane failure of the containment vessel would result in a large breach of containment. For purposes of calculating containment response and source terms, this breach was assumed to be equivalent to 1 ft².

4.2 OTHER POTENTIAL FAILURE MECHANISMS

In addition to the potential for overpressurization of the containment vessel itself, it is necessary to consider the possibility that penetrations or other discontinuities in the vessel might have lower capacities. A review of other potential failure modes determined that the containment capacity was adequately characterized based on the strength of the containment vessel itself. The potential for these other failure modes is described in this section.

Piping Penetrations

The analysis of piping penetrations drew upon an evaluation performed for the Sequoyah containment, which is also a free-standing cylindrical steel vessel (Ref. 23). The limiting pressure at the interface between the containment vessel and penetrating pipe (P_{OI}) was estimated based on the penetrating pipe diameter (d), the pipe wall thickness (t), containment vessel diameter (D), and the vessel wall thickness (T), using the following equation:

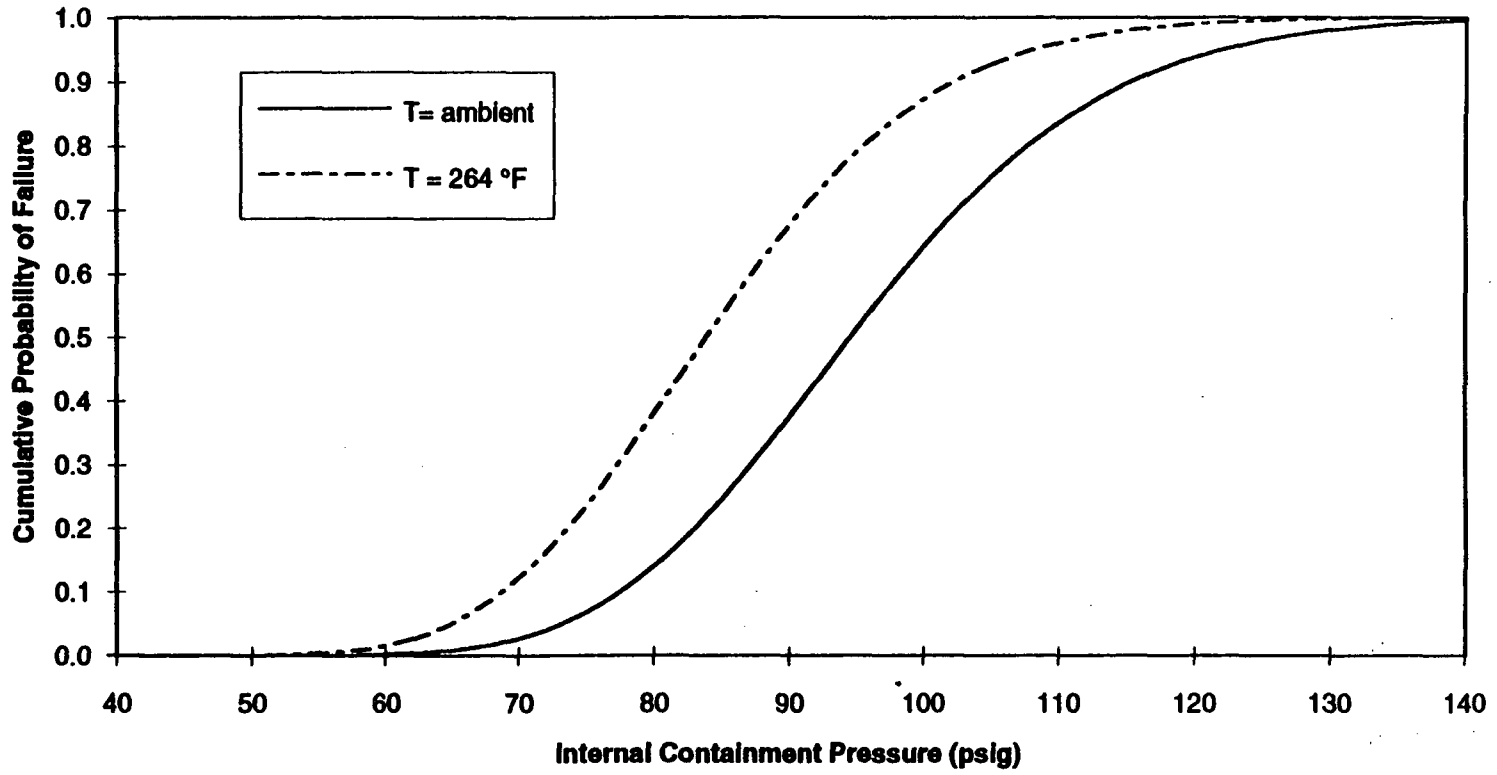


Figure 4-1. Probability of Containment Failure Due to Internal Pressure

$$P_{ot} = \frac{[162(t/T) + 228(t/T)(d/D) + 210]K + 155}{[108K + [228(d/D) + 228]K + 155]} * P_{co}$$

$$\text{where } K = d/D * \sqrt{D/T}$$

$$P_{co} = 2\sigma(T/D)$$

$$\sigma = \text{minimum yield stress}$$

Each of the piping penetrations was evaluated using this equation (Ref. 19). The results indicated that the penetrations each had a limiting pressure of approximately 150 psig or higher, showing they were less limiting than the membrane shell.

Equipment Hatch and Emergency Escape Lock

The equipment hatch and emergency escape lock present relatively large discontinuities in the containment vessel. Each was evaluated to determine its respective limiting failure mechanisms. For the equipment hatch, a conservative buckling failure pressure of 179 psig was estimated (Ref. 19). Therefore, it would be much less limiting than the limiting pressure associated with shell membrane failure for the hemispherical head.

Based largely on an analysis performed by CBI, there was also found to be a significant margin against failure for the emergency escape lock (Ref. 24). The CBI analysis was performed for a test pressure of 75 psig. The stresses from that analysis were scaled to the yield pressure for the hemispherical head in order to confirm this margin.

Personnel Lock

A review was made of the stress levels associated with the components of the personnel lock. It was determined that the primary horizontal stiffener was calculated to have the smallest difference between the allowable value per the ASME code and the calculated stress at the design pressure of 36 psig (Ref. 25). Therefore, it was assumed that the stiffener would be the weakest component of the personnel lock. The primary horizontal stiffener was calculated to yield at 87.1 psi (Ref. 19), but this pressure produces a maximum deflection of only about 0.1 inch. It would be expected this would produce only a small leak through the inner door of the personnel air lock and would thus do little to mitigate any further pressure increase that might lead to failure of the hemispherical head. Even if a leak were to develop through this door, it would not be a direct release from containment owing to the presence of the outer door within the lock. Thus, it was reasonable to assume that the hemispherical head would still be the limiting factor with respect to containment overpressurization.

Electrical Penetration Assemblies

In previous assessments of the sealing capability of electrical penetrations, it has been found that the most likely leak path in the electrical inserts is between the electrodes and weldment assembly, which contains a filler material. Electrical penetrations similar to those used at Davis-Besse have been tested to 100 psig without leakage (Ref. 26). In addition, there is a nitrogen gas purge placed on the electrical penetration assemblies and associated

modules. Conax, the manufacturer of Davis-Besse's electrical penetrations, has stated that continuous pressurization of the purge gas in excess of 70 psig (up to 100 psig) will not affect seal functioning capability (Ref. 27). Based on this evidence, the electrical penetrations for Davis-Besse's containment vessel were judged to have a pressure capacity greater than that for the vessel's hemispherical head.

Bellowed Penetration Assemblies

Some of the mechanical penetrations are sealed by a two-ply bellows assembly. This was considered to be the weak link for such penetrations as the main steam and main feedwater piping. Excessive pressures inside the containment vessel would tend to balloon the convolutions, but this would not affect the pressure-retaining capability of the bellows itself. The Tube Turns Corporation, which was the bellows supplier for the Sequoyah plant, reviewed all of the bellows assemblies, concluding that the minimum rupture pressure for the bellows was 256 psig (Ref. 26). Based on this evidence, and the fact that Davis-Besse utilizes the same type of bellows assembly (Ref. 20), it was determined that this penetrating seal mechanism would not be more pressure-limiting than the containment vessel itself.

Recirculation Line Guard Pipe Enclosure Assembly

In the case of a severe accident where molten corium was postulated to collect in the emergency containment sump, it was assumed that the annular space between the recirculation line and guard pipe would become exposed to containment pressure due to failure of the welded isolation plate. Based on the analysis of the guard pipe and bellows assembly surrounding the recirculation valves DH9A/B (Ref. 19), it was determined that the pressure-limiting component was the bellows assembly, at a rupture pressure of approximately 250 psig at ambient conditions. In comparison, this value proves to be larger than the raw mean failure pressure of 96.3 psig for the containment vessel reported in Section 4.1.2.

Additionally, the manufacturer of the bellows assembly was contacted regarding design information. It was stated that the bellows' design pressure is 108 psig, and also that the short-term hydrostatic test pressure is 170 psig (Ref. 28). The manufacturer also stated that the actual failure pressure would be approximately four times the design pressure. As such, it was determined that this component, as well as the entire guard pipe enclosure assembly, would have a greater capacity than the containment vessel itself.

Containment Vessel Wall Embedment

The containment vessel at the basemat juncture is embedded in concrete with a sand-filled zone approximately 5 feet in depth surrounding the vessel's outer periphery (Ref. 25). The stresses on the vessel have been calculated based on an internal pressure of 36 psig and a temperature gradient corresponding to the design-basis accident (Ref. 25). The results indicate high surface metal stresses in the sand-filled region on the order of 30,000 psi, but the shell membrane stresses within the wall itself are on the order of 9,000 psi, approximately 10,000 psi less than the maximum membrane stress in the unconstrained cylindrical wall above

the embedment. Because the vessel is made of a ductile material (SA-299 steel), the vessel wall in the region of high surface stress would undergo plastic deformation and thus tend to relax or relieve the bending stress without the membrane shell undergoing rupture. Therefore, this portion of the containment vessel is not considered more limiting than the vessel's hemispherical head.

Thermal Effects

The elevated temperatures during some postulated severe accidents indicated the need to investigate the durability of non-metal sealing materials, such as gaskets and O-rings. The gasket material used for the emergency, equipment, and personnel hatches is a spliced length of silicon rubber, 3/4" wide by 1/2" thick. Figure 4-2 provides information on the seal life of various basic elastomer compounds as a function of temperature versus exposure time (Ref. 29). The asymptotic value, where exposure time required to produce failure approaches infinity, for silicon rubber is approximately 450 F. This value is about 100 F greater than the maximum temperatures to which these materials might be exposed for significant periods of time during an accident. It was therefore concluded that this material would not significantly degrade during a severe accident.

The subject of electrical penetrations at elevated temperatures has been addressed by IDCOR Technical Report 10.1, which states that electrical penetrations will not be challenged by conditions which grossly exceed the conditions for which they have been tested. This report states that containment electrical penetration assemblies were satisfactorily tested at 325 F for 15 minutes and at 281 F for several hours at 125 psig without failing (Ref. 26). Even though the post-accident containment atmospheric temperature may be higher than the tested conditions, heat losses through the containment would mitigate the temperature effects at the penetration assembly. For power cables at elevated temperatures, tests of power cables installed at the Sequoyah nuclear power plant showed no inability to pass current at the rated voltage when subjected to a temperature of 700 F for 45 minutes. Also, due to the design of the penetration assembly, a failure of the sealing material or wire on the containment side at a higher pressure would tend to push the material together, tending to have a sealing effect (Ref. 26). Based on this, the electrical penetration assemblies for Davis-Besse were considered capable of withstanding the high temperatures and pressures that could result from a severe accident.

The sealing material providing the pressure boundary for the 48" containment vessel purge and exhaust butterfly-type isolation valves is made of ethylene propylene, an elastomer compound which is less durable than silicon rubber at elevated temperatures. However, the seal life for 350 F is approximately 50 hours (Ref. 29). Small break LOCAs without containment heat removal are representative of calculations using the MAAP computer code which suggest that a containment bulk temperature of 350°F would not be reached until about 25 hours after the start of the accident. Therefore, if seal failure were to occur, it would occur well after 50 hours. In addition, there is also another isolation valve in this line outside containment which would not be directly subjected to the same temperature as the interior

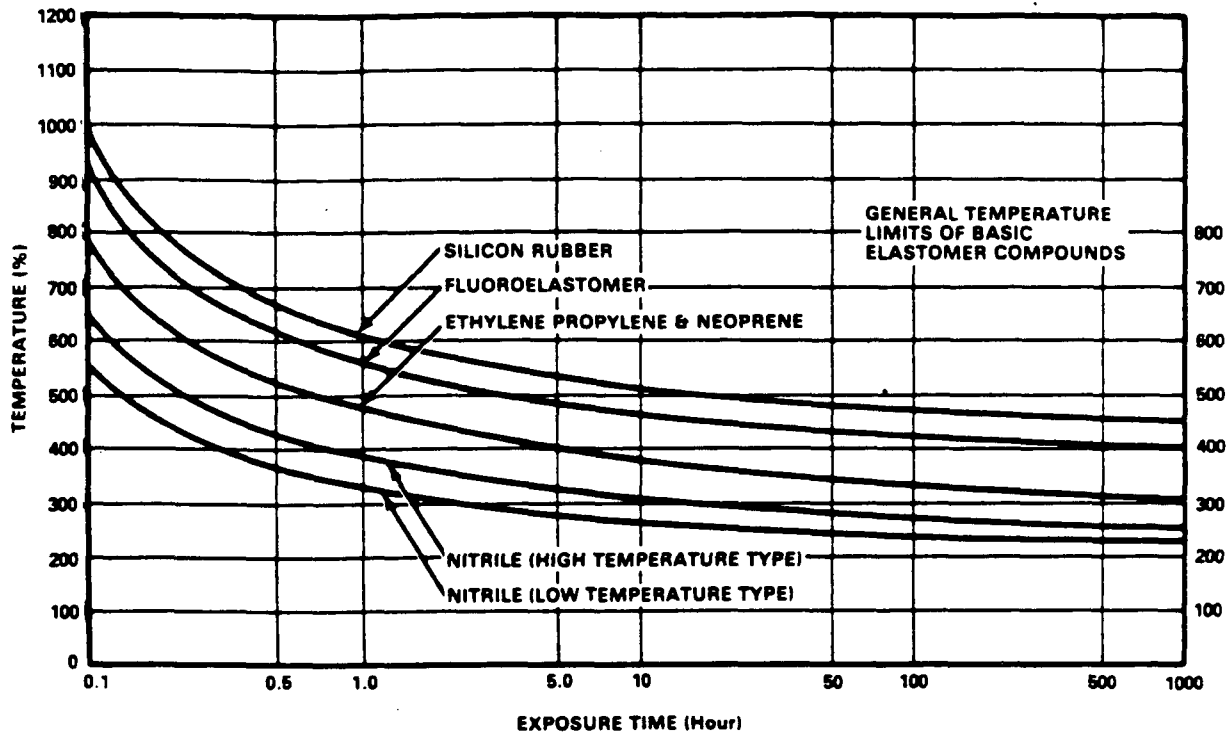


Figure 4-2. Seal Life as a Function of Time at Temperature

valve. This is due to ambient temperature losses from the large surface area and length of pipe in between the two valves. Equipment heat sink temperatures could also be lower than the bulk containment vapor temperature. Only long exposures to elevated superheated vapor temperatures could bring the equipment temperature above the maximum value of T_{sat} for the existing partial pressure of steam (Ref. 30). As such, the containment purge and exhaust penetrations were also considered capable of withstanding the high temperatures and pressures that could result from a severe accident.

4.3 OVERALL CONTAINMENT FAILURE CHARACTERIZATION

From the foregoing analysis and discussion, it is therefore concluded that the limiting pressure component is the hemispherical head of the containment vessel, with a mean failure pressure of 85.2 psig. This failure pressure takes into account elevated temperature conditions of the vessel wall which could arise during prolonged accident conditions and tend to lower the yield strength of the metal. At normal room temperature conditions, the mean failure pressure was calculated to be 95.3 psig. Other potential failure mechanisms such as penetrations and attachments to the containment vessel listed under Section 4.2 were investigated and found to have higher pressure capacities than the vessel itself. This failure location and pressure is consistent with other free-standing steel cylindrical containment vessels without reinforcements or stiffener geometry (Ref. 18).

Section 5 CONTAINMENT EVENT TREE

For most types of severe core-damage accidents, the potential consequences with respect to the response of containment cannot be predicted with certainty. To permit various outcomes to be investigated, a containment event tree (CET) was constructed. This event tree defines, at a relatively high level, the general types of containment response (or containment failure modes) that could lead to releases of different levels of severity. The overall structure of the CET and the events that comprise it are described in Section 5.1. The manner in which the CET events were evaluated is detailed further in Section 5.2.

5.1 DEVELOPMENT OF THE CONTAINMENT EVENT TREE

The CET was used to consider various outcomes with respect to containment response given a core-damage accident, and it served as a framework to quantify the frequencies of those outcomes. The overall structure chosen for the CET was a relatively small event tree. Phenomena that could have a significant impact on RCS integrity, containment response, and eventual releases from containment were included as CET top events. Failure of each of these top events was developed further in the form of fault-tree logic. It was in this supporting logic that various phenomenological possibilities were assigned appropriate probabilities. The scenarios input to the CET were the plant-damage states (PDSs) defined previously in Section 3.4.

As a starting point for the plant-specific CET, a CET developed for a generic B&W plant (Ref. 31) was reviewed and determined to be useful as a framework for developing plant-specific logic. One of the first revisions performed was to rework the overall generic logic from a success logic system to a failure logic system. This was done for consistency with fault-tree logic used in the front-end analyses, serving to minimize difficulties with the interface between the front-end and back-end analyses.

Changes were also made to the event tree and the logic supporting it to delete events that did not directly apply given plant-specific considerations (e.g., the top event referring to the potential that an overpressurization of containment could be "benign" was deleted, since it was applicable to a concrete containment, but not necessarily to a steel containment such as Davis-Besse's). Some top events were added to incorporate consideration of additional phenomena (e.g., to develop scenarios involving prevention of vessel failure after the onset of core damage). Figure 5-1 shows the original generic CET, and Figure 5-2 shows the final, plant-specific CET.

To describe the overall development of the event tree, each top event indicated in Figure 5-2 is summarized below, with emphasis on its branch points and role in the CET structure. Section 5.2 discusses the supporting logic and probabilistic treatment of applicable phenomena and other events in detail.

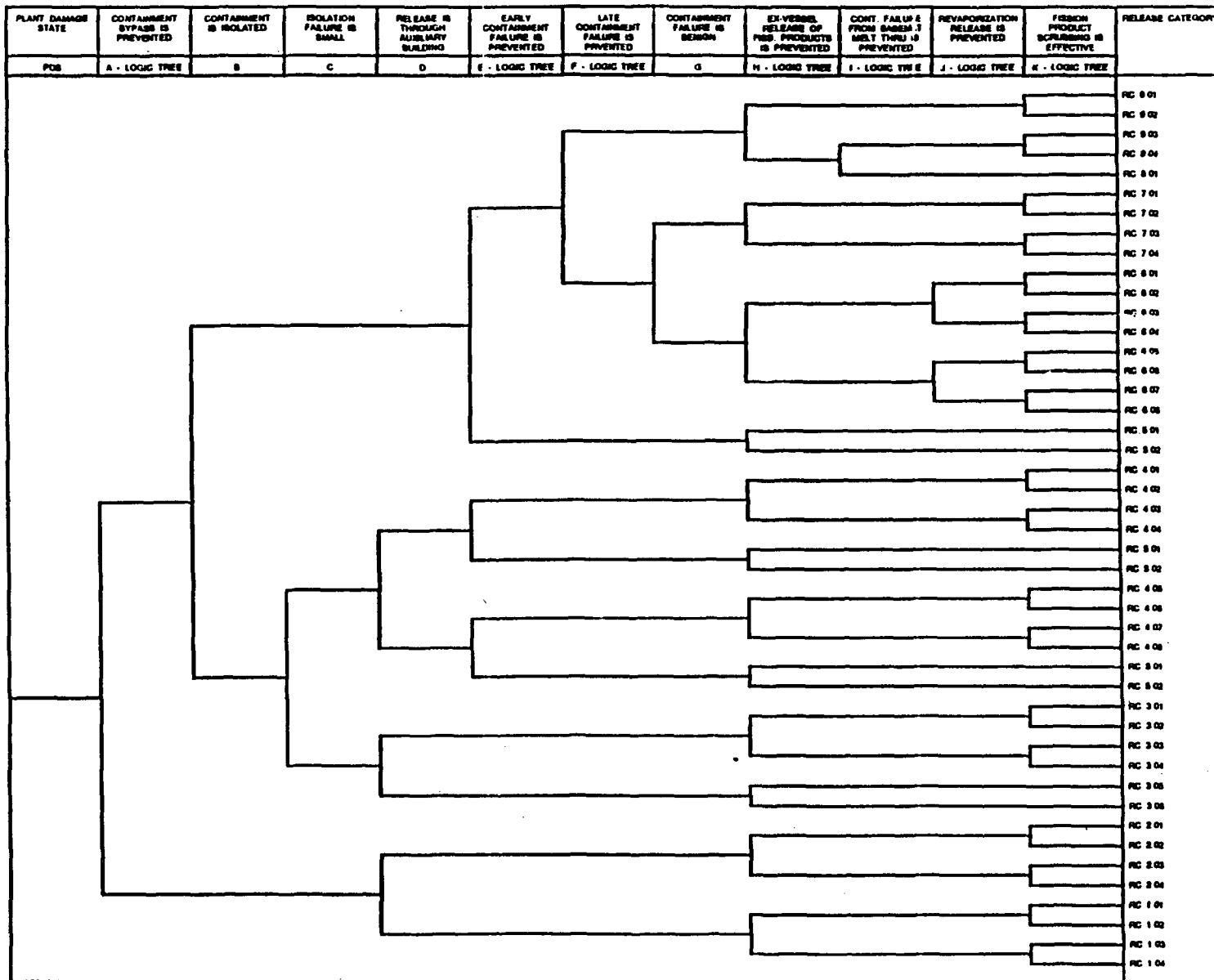


Figure 5-1. Generic B&W Containment Event Tree

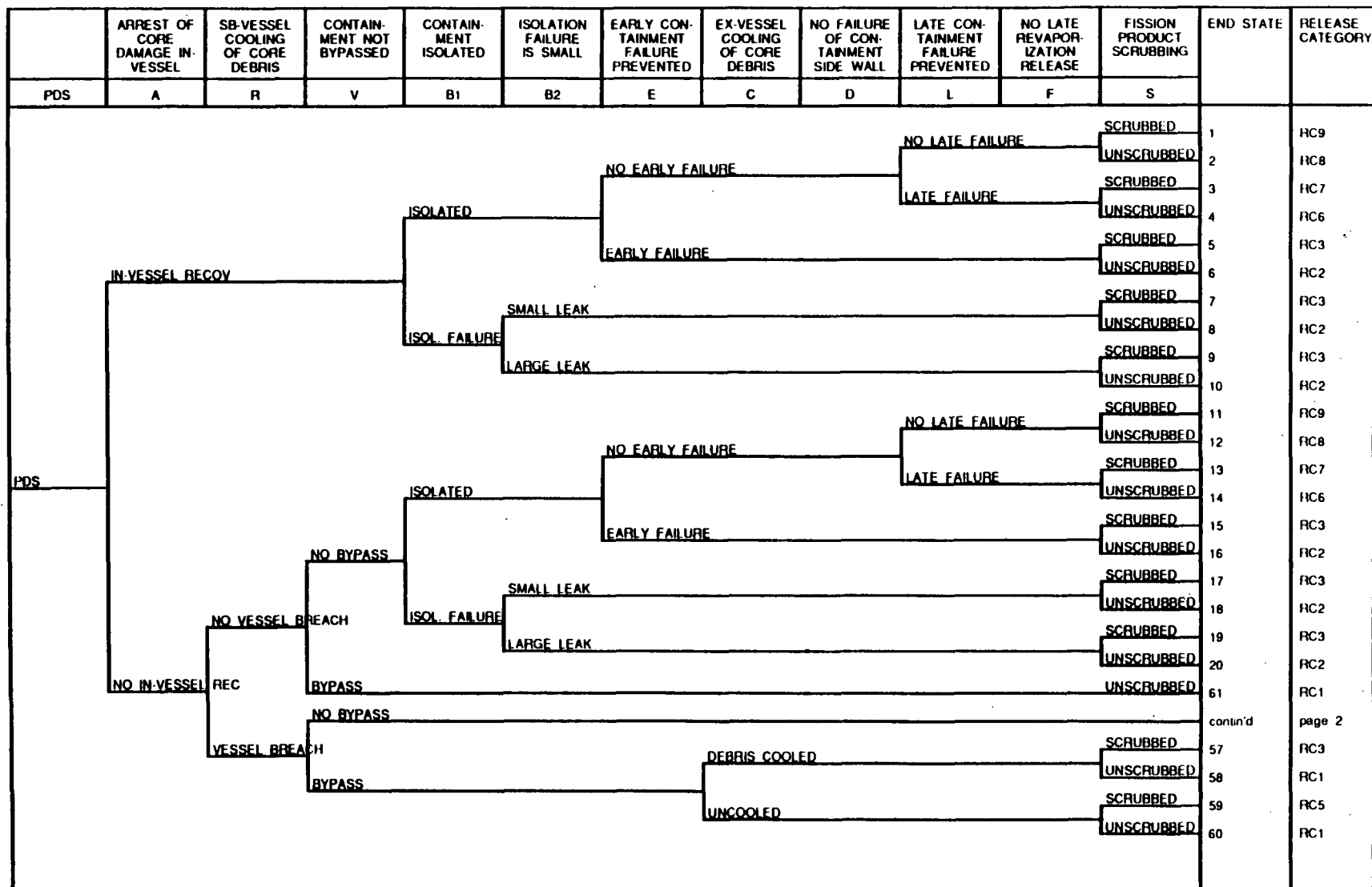


Figure 5-2. Davis-Besse Containment Event Tree (page 1 of 2)

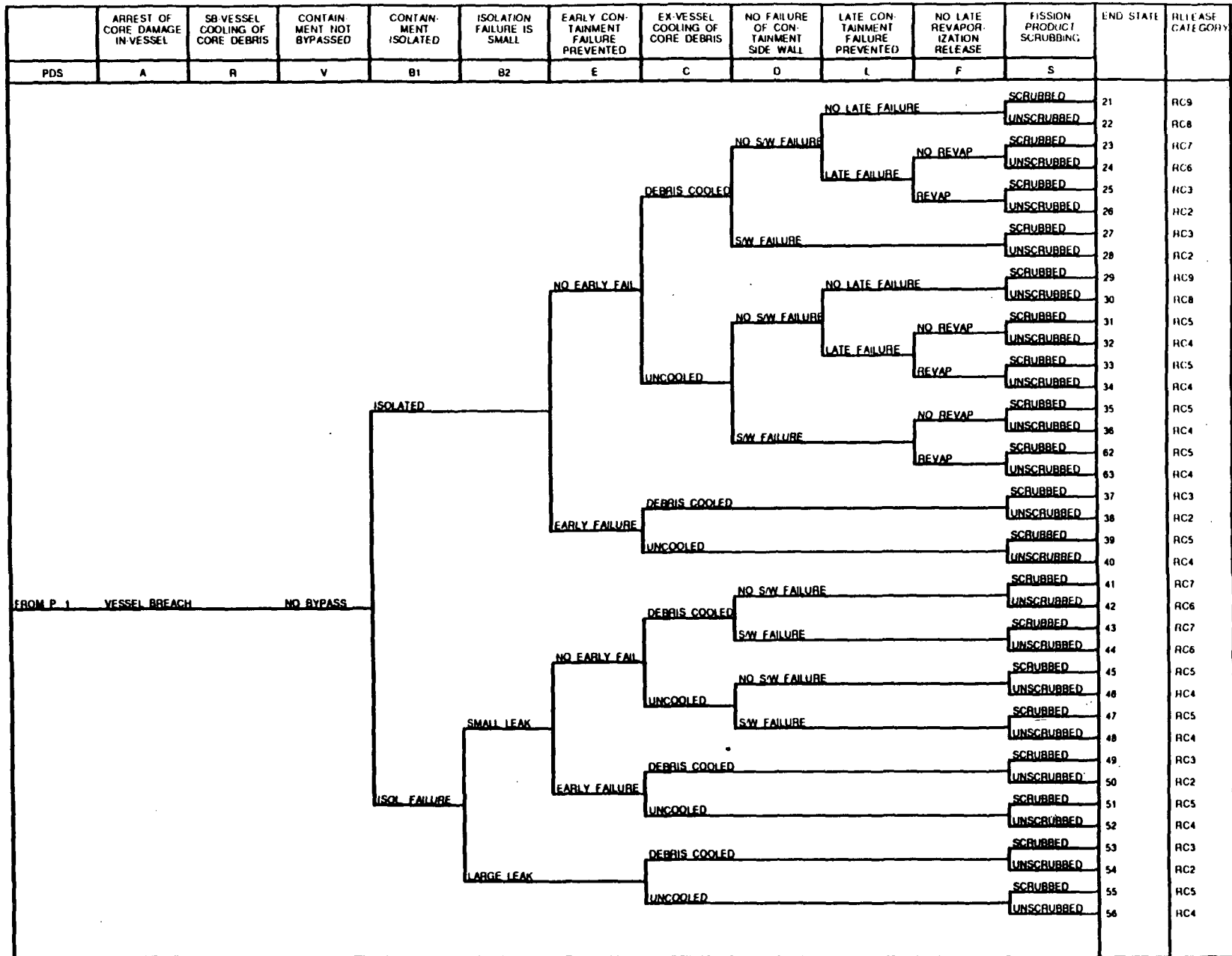


Figure 5-2. Davis-Besse Containment Event Tree (page 2 of 2)

Event A: Arrest of Core Damage In-Vessel

This event was included to account for the possibility that, after significant uncovering of the core occurs, injection may be regained and the fuel may be prevented from causing a reactor vessel failure. If core damage is arrested in-vessel, there is still the potential for certain failure modes of containment, including early containment failure (e.g., due to hydrogen burns) and late overpressurization. Therefore, appropriate branch points in the CET are retained for such considerations. On the other hand, if vessel failure is prevented, core-concrete interactions would also be prevented. Therefore, no branch points are indicated for events C and D in the CET given success for event A. By definition, for success of event A core cooling must be restored before there is sufficient overheating to cause creep rupture of one or more of the tubes in the steam generators. Therefore, no branch point is indicated for event V given success of event A as well. If event A is not successful, all of the subsequent events in the CET are relevant.

Event R: Submerged-Vessel Cooling of Core Debris

Event R was included to account for the possibility that a failure of the reactor vessel, after substantial fuel damage, could be prevented by the cooling effect of water around the exterior of the vessel, if the reactor cavity were deeply flooded. The Davis-Besse geometry is such that with the BWST contents injected, the reactor vessel would be surrounded by water to a level just below the bottom of the hot legs.

As in the case of top event A, if reactor-vessel integrity were maintained, phenomena associated with vessel failure and core-concrete interactions would not be relevant, but some failure modes would still apply. In addition, since melting of the core to the extent that there would be slumping into the bottom head of the reactor vessel is implied, the potential is retained that there might be a failure of a steam generator tube due to creep rupture (i.e., there is a branch point for event V given success of event R).

Event V: Containment Not Bypassed

This top event tracked whether or not the release of radionuclides from the primary system took place within the containment, or bypassed the barrier that the containment represents (note that a containment bypass is different from a containment failure). Sequences that constituted bypass events were interfacing-systems LOCAs, steam generator tube ruptures (as initiating events), and steam generator tube ruptures induced by creep rupture.

Bypass sequences represented a major part of potential fission-product releases from containment, given the potential for a direct release to the environment. Additionally, for bypass sequences where the reactor vessel was breached, ex-vessel fission product releases from core-concrete interactions were more likely given the concurrent loss of water inventory from containment. Other failure modes, such as overpressurizations or isolation failures, were not important given containment bypass. Therefore, the only branch points given failure for event V were those pertaining to whether there was an ex-vessel release of fission products

(implied by the status of event C), and whether there was scrubbing of the releases associated with the bypass (event S).

Event B₁: Containment Isolated

A direct function of the PDS, this top event indicated whether or not containment leakage rates were above the normal plant Technical Specification-allowed rate. Examples of potential leakage paths included normally open penetration lines which fail to close on an isolation signal, lines which could fail open after containment pressurization, etc. Specific discussion of credible isolation failures is contained in Section 3.3.1. For success of this event, the containment would be assumed to be isolated. If there were a failure, it could be either large or small, as discussed for the next event.

Event B₂: Isolation Failure Is Small

For failure of top event B₂, it was important to consider if the containment leakage path was large or small. A failure was "small" if containment did not depressurize appreciably given the leak, and "large" if it did.

Isolation failures could be important for fission-product releases since they would constitute a containment release prior to other potential containment failures. Earlier releases not only may allow more total leakage, but also provide less opportunity for scrubbing, aerosol settling, and other mechanisms for fission-product removal.

Event B₂ would be precluded if event B₁ were successful. For failure of event B₁ but success of event B₂, a small isolation failure would be implied. Branch points are included for early containment failure, to account for the possibility that an overpressurization or other early failure that would not be precluded by a small isolation failure could produce a more serious release than that associated with the isolation failure. Given both events B₁ and B₂ unsuccessful, a large isolation failure is implied. Branch points are provided in that case only for the events that would determine the magnitude of release, including whether ex-vessel releases occur due to core-concrete interactions (event C), whether there is a late revaporization from the RCS (event F), and whether the release is scrubbed (event S). Note that in quantifying event S, it was assumed that early, large isolation failures would not be subject to fission-product removal via the containment sprays.

Event E: Early Containment Failure Prevented

This top event accounted for containment failures before or early after reactor vessel breach, other than due to bypass or isolation failures.

Prior to vessel breach, potential hydrogen burns and in-vessel steam explosions were the major phenomena of concern. Early after vessel breach, applicable phenomena included the immediate pressure loading of containment, ex-vessel steam explosions, missiles generated at vessel breach, and hydrogen burns.

Prevention of early containment failure would allow fission products to settle in containment, and to have a chance to be removed by any sprays in operation. It would also allow short-lived isotopes to decay and would minimize the possibility of core-concrete interactions by preventing uncontrolled boiloff of water overlying ex-vessel core debris. Given failure for event E, side wall failure and late containment failure would not be relevant, but branch points are provided for the remainder of the events in the event tree.

Event C: Ex-Vessel Cooling of Core Debris

This top event examined whether or not corium released ex-vessel would be maintained at a temperature less than the melting point of concrete, thereby preventing significant core-concrete interaction.

Important considerations for determining the success or failure of debris coolability were the location and volume of core debris after vessel breach (i.e., reactor cavity or lower containment elevation), the amount of water overlying core debris, and the area of corium spread. Another important consideration was the determination of concrete composition (i.e. "limestone-limestone" for Davis-Besse).

If significant core-concrete interaction were to occur, important differences in fission-product releases would result. These would include the release of tellurium and other radionuclide species which would not have been released if concrete ablation had not occurred. Interaction of concrete decomposition gases with corium also results in significant quantities of carbon monoxide being formed which are then available for possible combustion.

Failure to cool ex-vessel corium in the reactor cavity region would result in a basemat failure, while failure to cool in the lower containment elevation would result in the corium-concrete eutectic ablating to a depth sufficient to cause containment side wall failure at the lower containment elevation.

Event D: No Failure of Containment Side Wall

This top event was included to account for the possibility that corium which relocated to the lower containment elevation might eventually interact with the containment vessel, given the proximity of the incore tunnel to the containment vessel. Of particular interest are the consequences of significant quantities of corium which relocate along a concrete curb that protects the containment vessel wall. Technical considerations included the coolability of corium, both when covered with water and when dry, the distribution of ejected corium, and corresponding potential corium depths.

If eventual contact of the containment wall with the corium-concrete eutectic was not prevented, containment failure would result, with an accompanying release of fission products. Success for event D would be assured if event C were successful. If event C were not successful, failure for event D would be implied if there was substantial dispersal of corium from the reactor cavity to the lower containment elevation.

Event L: Late Containment Failure Prevented

Failure for this top event would occur for sequences in which the containment was calculated to fail well after the arrest of core damage in-vessel or long after reactor vessel failure. Phenomena associated with a late containment failure included hydrogen/carbon monoxide burns, long-term steam generation, buildup of noncondensable gases, and thermal degradation of containment penetrations.

With the delay in containment failure, mitigation of associated fission-product releases was possible by a variety of removal modes including aerosol deposition, potential removal by spray operation, pool scrubbing, and isotopic decay.

Note also that if the containment did not fail by any other mechanism, including success for event L, but ex-vessel cooling of core debris failed (i.e., event C was unsuccessful), it was assumed that the outcome would correspond to basemat melthrough.

Event F: No Late Revaporization Release

This top event accounts for possible long-term revaporization of fission products which were initially deposited on various internal surfaces of RCS components, and would then have the potential for release late in the accident.

Important considerations for revaporization included the availability of secondary side cooling (ensuring availability of large, cool deposition surface areas) and the particular RCS break characteristic of the plant-damage state. Note that this top event was only applicable to late containment failures, since fission-product releases associated with early containment failures were not significantly affected by late revaporization phenomena.

Fission-product releases were characterized by the transport of various radionuclides from the RCS into containment over the long term.

Event S: Fission Product Scrubbing

This top event is applicable to almost all of the CET end states, accounting for a variety of fission-product removal mechanisms. Removal mechanisms of importance which were modeled included potential removal by containment sprays, plateout via several modes in containment, pool scrubbing and isotopic decay. For those sequences in which significant scrubbing would be expected to occur, fission-product releases were analytically lower, or adjusted by reduction factors appropriate for the mode of removal.

5.2 TOP EVENTS IN THE CET

To define the various combinations of phenomena and conditions that could lead to its occurrence, each of the top events in the CET was further developed through logic in the form of fault trees. The development was carried to the level necessary to provide proper coordination among the top events and with the front-end analysis (via the plant-damage

states) and to support the quantification of phenomenological and other events relating to the top events. This logical development and the corresponding probabilistic treatment are described for each top event in the following sections.

Some aspects of accident response are important to more than one of the top events. For such cases, one set of common logic was developed to ensure consistency and continuity among the top events. This logic is described in Section 5.2.11.

The supporting logic for each of the CET events is developed down to the level of basic events of various kinds, including the following:

- Events that make the connection between an element of a plant-damage state and that element's effect on containment response (for example, whether or not the systems needed to provide containment heat removal are available).
- Events that account for the potential for containment failure conditional on the internal pressure loading.
- Other events that reflect uncertainty in the occurrence or level of severity of a phenomenon.

The first of these types is identified as a "house" event, and is set to true or false to allow relevant portions of the CET logic to be used or discarded according to the plant-damage state. For the other types, probabilities are estimated by a variety of methods, including sensitivity studies, reference to other studies (especially those performed for NUREG-1150), and the application of analyst judgment. Where analyst judgment was applied to characterize the probability for an uncertain phenomenon, the relevant event was first assessed qualitatively. A probability corresponding to this qualitative assessment was then assigned to permit the event to be treated in the quantification of the CET. The probability scale that was used is one adapted from the work supporting the first draft of NUREG-1150 (Ref. 32), and is summarized in Table 5-1. In all cases, the point estimates provided are intended to represent mean values, consistent with the point estimates developed in the front-end analyses. The rationale for the selection of probabilities, whether based on other assessments or on analyst judgment relative to Davis-Besse, is provided along with the description of the logic development in the sections that follow.

5.2.1 Event A: Arrest of Core Damage In-Vessel

Event A of the containment event tree is the first of two events relating to the potential that failure of the reactor vessel might be prevented even though there had been some damage to the core. In this case, the potential was considered that a supply of injection to the reactor vessel sufficient to quench the core might be made available in time to terminate damage prior to substantial melting of the core (although there could be substantial structural damage). Two primary (and related) means by which core cooling might be restored were considered:

- The operators might succeed in establishing core cooling after the core was uncovered but before melting had progressed to the point at which it would

Table 5-1
Probability Scale for CET Basic Events

Qualitative Descriptor	Probability Range	Nominal Value
Certain to occur	—	1
Almost certain	$0.995 < \text{prob} < 1$	0.999
Very likely	$0.95 < \text{prob} < 0.995$	0.99
Likely	$0.7 < \text{prob} < 0.95$	0.9
Indeterminate	$0.3 < \text{prob} < 0.7$	0.5
Unlikely	$0.05 < \text{prob} < 0.3$	0.1
Very unlikely	$0.005 < \text{prob} < 0.05$	0.01
Remotely possible	$0 < \text{prob} < 0.005$	0.001
Impossible	—	0

be irreversible. This could occur, for example, if equipment were restored in a timely manner, offsite power were recovered, etc.

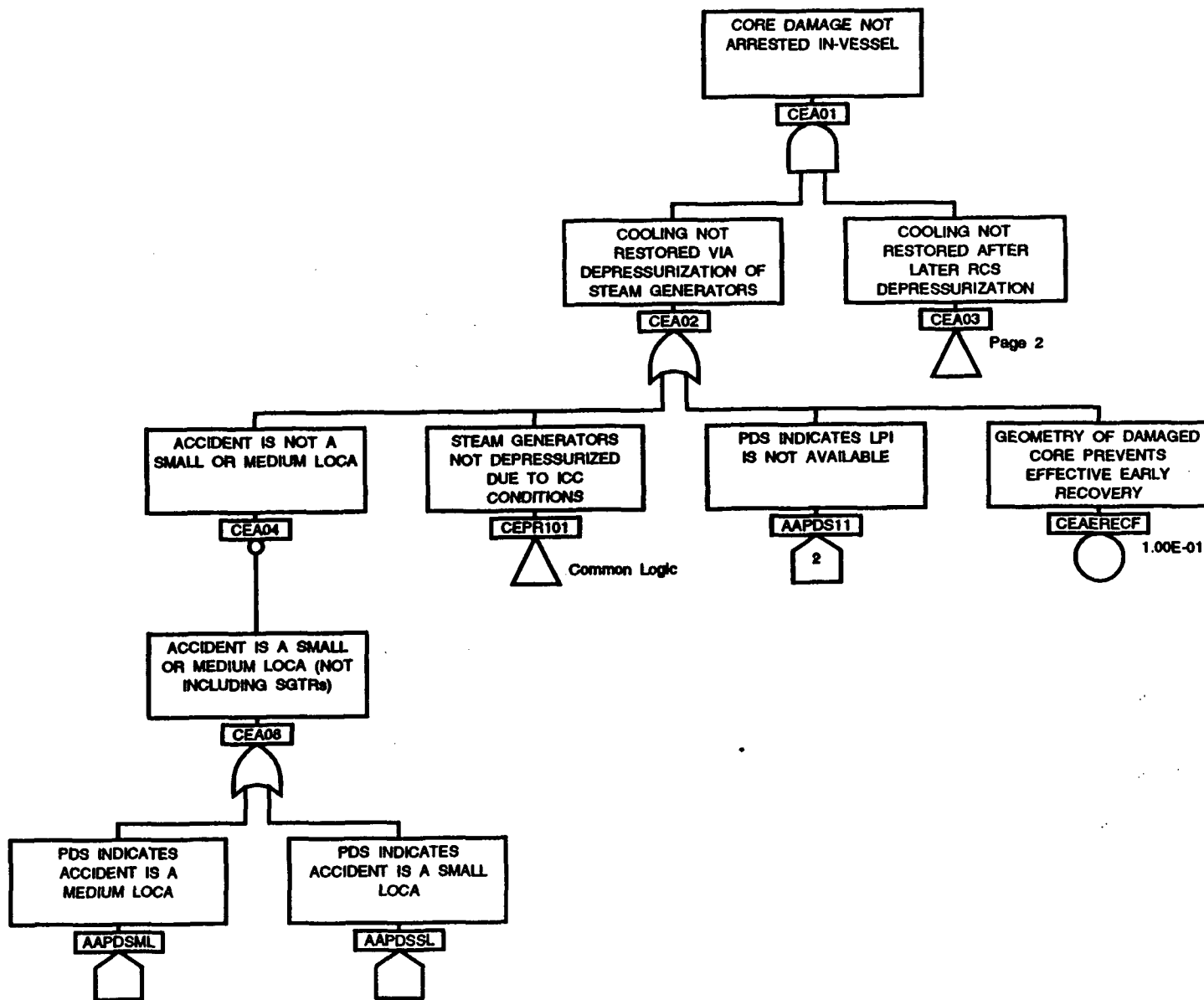
- Conditions in the RCS could change, such that systems that were available but that were not previously providing cooling might be capable of doing so. The most important case in this category would be the possibility of depressurizing the RCS sufficiently to permit injection by the HPI or LPI systems.

In the first of these cases, actions that could be taken to restore core cooling prior to uncovering of the core have been investigated in some detail in the front-end analyses. Successful restoration at this point would require some action between the time when the core began to heat up but before there was substantial melting. For most sequences, this would represent a relatively small increment beyond the time already considered for restoration of core cooling before the core began to uncover. Therefore, this case was not investigated in detail.

In the second case, it is possible for several types of sequences that the RCS would be depressurized before the reactor vessel failed due to attack by core debris. This depressurization could take one of the following forms:

- Operator action to depressurize the steam generators, as called for early in the inadequate core cooling (ICC) guidance in the emergency procedure (Ref. 33). This would be most effective in reducing RCS pressure if it were to be attempted when there was a small or medium LOCA, since the leak in the RCS and the depressurization of the steam generators would cause the most rapid decrease in RCS pressure.
- Operator action to open the PORV. Later instructions in the ICC guidelines call upon the operators to open the PORV if depressurization via the steam generators had not been effective in permitting core cooling to be restored. As it is applied in the ICC guidelines, the primary goal of this step is to reduce RCS pressure sufficiently to maximize the amount of any injection flow that might be available.
- Repeated cycling of the pressurizer safety-relief valves (PSVs) at elevated temperature and pressure could cause one or both to stick open. This would be relevant for accidents in which core damage occurred at very high pressure.
- Failure of a RCS hot leg or the pressurizer surge line due to creep rupture. As the core heated up, gases in the reactor vessel would reach very high temperatures. It is possible that these hot gases could be circulated sufficiently to cause other portions of the RCS to heat up as well. With the RCS pressurized, this could lead to creep rupture elsewhere in the system.

These options are reflected in the logic for event A, which is shown in Figure 5-3. The first of the two cases noted above is considered to be a viable option for arresting core damage in-vessel, at least for small and medium LOCAs. If the initiating event were a large LOCA, depressurization of the RCS would be implicit, and restoration of core cooling would be considered only in the context of the front-end analyses. For transients in which no LOCA



Page 2

Figure 5-3. Logic for Failure of CET Event A—Core Damage Not Arrested In-Vessel (page 1 of 2)

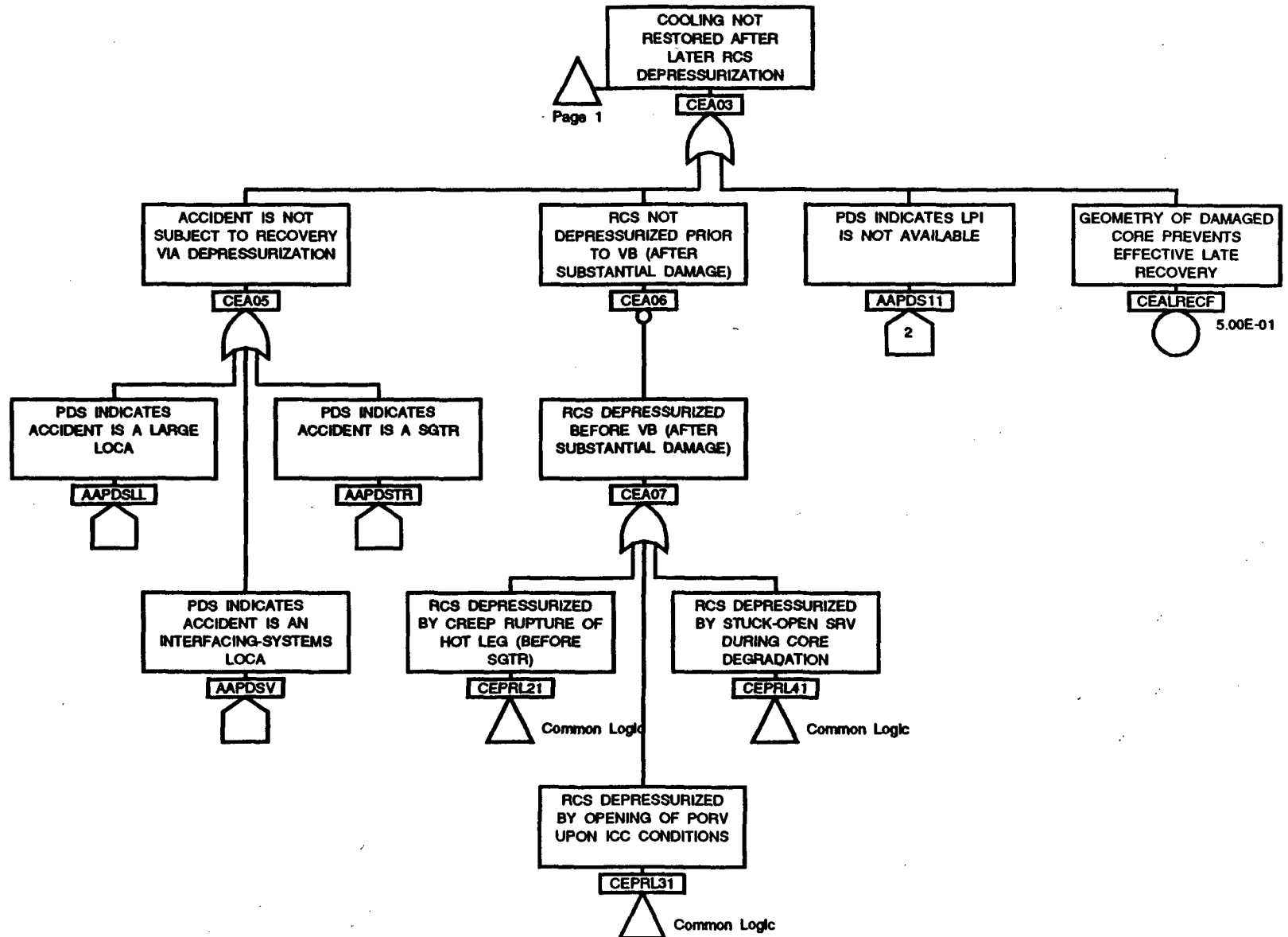


Figure 5-3. Logic for Failure of CET Event A—Core Damage Not Arrested In-Vessel (page 2 of 2)

developed core damage would only occur for cases in which feedwater was not available (with the exception of the special case of a transient without scram and with failure to provide emergency boration). For these cases, depressurization of the steam generators would not be relevant.

Failure to restore core cooling via this mode for small or medium LOCAs could result from any of the following:

- Failure to accomplish depressurization. As described in Section 5.2.11, the development for gate CEPR101 includes consideration of the unavailability of feedwater or of a means to depressurize the steam generators, and the potential for failure of the operators to act in a timely manner.
- The unavailability of LPI. This is addressed explicitly in the plant-damage states for both small and medium LOCAs.
- The possibility that the geometry of the core might have been sufficiently disrupted during early heatup that there would be insufficient ingress of water to permit effective cooling (event CEAERECF in the logic).

If the operators were successful in depressurizing the RCS, there remains a degree of uncertainty with respect to whether the core geometry would support core cooling without substantial melting of the fuel. The accident at TMI-2 provides some evidence that cold injection could be successful in terminating core damage, even though there might be substantial relocation of cladding and fuel within the reactor vessel. The technical work supporting NUREG-1150 also considered recovery of core cooling before vessel breach, although only for cases in which the loss of core cooling was the result of loss of ac power. In that assessment, successful restoration of cooling flow before vessel failure was assumed to arrest core damage (Ref. 34). In light of the limited experimental and analytical evidence to support a determination that restoration of cooling would succeed with assurance in this case, however, some uncertainty remains. Therefore, the failure to arrest core damage given restoration of cooling following depressurization of the steam generators is judged to be "unlikely" for this assessment.

The remaining means for depressurization noted above would be relevant for scenarios in which there was further heating of the core, such that either the operators were required to open the PORV, a PSV stuck open, or a rupture of the RCS was induced by creep rupture. The development of these possibilities is discussed in Section 5.2.11 as well.

Calculations of various high-pressure scenarios made using MAAP indicate that, by the time conditions in the RCS reach the point at which the operators would open the PORV under the ICC guidelines or there could be a temperature-induced failure in the RCS, it might be difficult to prevent core degradation from progressing to the point that the vessel was breached. The version of MAAP used for this assessment, however, has very limited models for consideration of in-vessel core cooling. Other assessments indicate that the failure to form a coolable geometry could range from unlikely to indeterminate (Ref. 35). It seems reasonable to assume that the formation of a coolable geometry would be less likely in this

case than in the previous case, in which core cooling was restored earlier (i.e., by depressurizing the steam generators, for which failure of the reactor vessel given restoration of core cooling was assessed to be "unlikely"). Therefore, in the absence of more definitive information, the probability of failure to form a coolable debris bed for late restoration of core cooling is taken to be "indeterminate." The basic events for event A are summarized in the tabulation below.

Quantification of Basic Events for Top Event A

PDS/Case	Description	Assessment	Probability
CEAERECF: geometry of damaged core prevents effective early recovery			
All	All relevant plant-damage states	unlikely	0.1
CEALRECF: geometry of damaged core prevents effective late recovery			
All	All relevant plant-damage states	indeterminate	0.5

5.2.2 Event R: Submerged-Vessel Cooling of Core Debris

Event R refers to a second method by which the damaged core might be cooled sufficiently to prevent a breach of the reactor vessel. In this case, the cooling would be established after the core had slumped into the lower head of the reactor vessel. Because the reactor cavity could be deeply flooded by this time (if the contents of the BWST had been injected), it is possible that there might be sufficient convective cooling at the surface of the reactor vessel to prevent its meltthrough.

The potential that this mode of cooling might succeed has been discussed extensively, and is of significant interest with respect to accident-management considerations. The version of MAAP used for this study does not have the capability to model this mode of cooling, although such models have been developed and are incorporated into MAAP version 4.0 (Ref. 35). An attempt was made to make a separate-effects study of this phenomenon for Davis-Besse based on the models for MAAP 4.0, but this study was inconclusive. Among the important issues that were not resolved in a satisfactory manner based on the limited evaluation that could be made was the question of whether the bottom-head penetrations could retain their integrity. It appeared that a strong case might be made for adequate heat transfer through the wall of the reactor vessel to limit the ablation of the vessel material. The penetrations present discontinuities in the large heat-transfer surface, and could be subject to local heating sufficient to cause them to fail. Once they failed, the openings created could lead to discharge of the core debris and additional ablation of the reactor vessel.

Even if this mode of cooling were to be viable, the benefits with respect to the potential for preventing containment failure for Davis-Besse could be somewhat limited. The core would still be sufficiently damaged that much of the fission products could be released

from the fuel matrix. There would be substantial radiative and convective heating of the upper internals of the reactor vessel and possibly of other portions of the RCS that could lead to a large release path to containment, if one were not already available. Decay heat would still cause substantial steaming to the containment which, in the absence of containment heat removal, could threaten to cause overpressurization. There could still be significant production of hydrogen in the reactor vessel as well. The primary benefits would be the elimination of any potential for failure of containment due to phenomena associated with the blowdown from the reactor vessel or as a consequence of core-concrete interactions. With one exception, neither of these was an important source of containment failure for Davis-Besse. The exception would involve scenarios in which there was a pressurized ejection of debris from the reactor vessel to the containment basement. If the debris were not cooled, the side wall of containment could be failed after the debris ablated the concrete curb protecting it. This would be most likely for situations in which the basement was not flooded by injection of the BWST; without injection of BWST water, submerged vessel cooling would not be possible at all.

The logic corresponding to failure for event R is shown in Figure 5-4. As the logic indicates, submerged-vessel cooling was assessed to be unable to prevent vessel failure if the reactor vessel were not deeply flooded prior to vessel breach (as determined by the plant-damage states), or if the cooling were not adequate to prevent vessel breach (designated by event CEREVHTF). In the base-case analyses, it was assumed to be "certain" that this mode of cooling would not be adequate (i.e., a probability of 1.0 was assigned to the event). A sensitivity study was also made to examine the impact of this assessment; the study and its results are described further in Sections 6.2 and 6.3.

5.2.3 Event V: Containment Bypass Is Prevented

Event V represents the potential for a direct release path to exist from the RCS that would bypass the containment boundary. Two types of accidents were considered in the context of containment bypass: interfacing-systems LOCAs, in which the initiating LOCA would lead to both core damage and a release outside containment, and a SGTR. The SGTR may be either the initiating event in an accident sequence, or may be induced by creep rupture in the steam generator tubes during core degradation as a result of a different type of accident. Thus, the plant-damage state may directly indicate that there is a bypass of containment, or there may be a bypass due to phenomena during meltdown of the core.

The logic for failure of event V is shown in Figure 5-5. If the plant-damage state is indicated by either a "V" or by "R" as the first letter, the accident involves a bypass. Otherwise, the potential for a temperature-induced tube rupture is considered (under gate CEV02).

The potential for a temperature-induced failure within the RCS is discussed in Section 2.2.3, and in more specific terms related to the containment event tree in Section 5.2.11. For a temperature-induced tube rupture to occur, the RCS would have to be at high pressure, since the possibility of creep rupture would be significantly reduced without a substantial

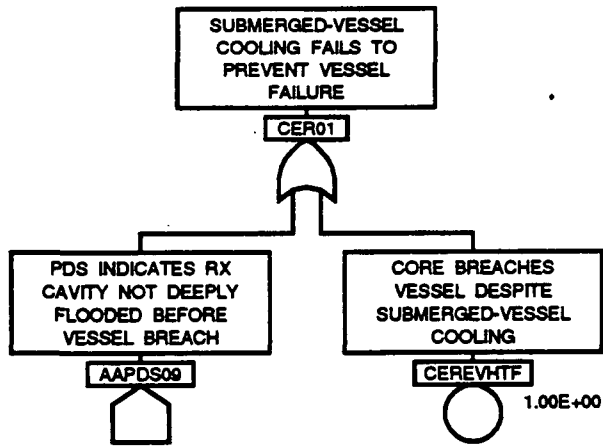


Figure 5-4. Logic for Failure of CET Event R—Submerged-Vessel Cooling of Core Debris Fails

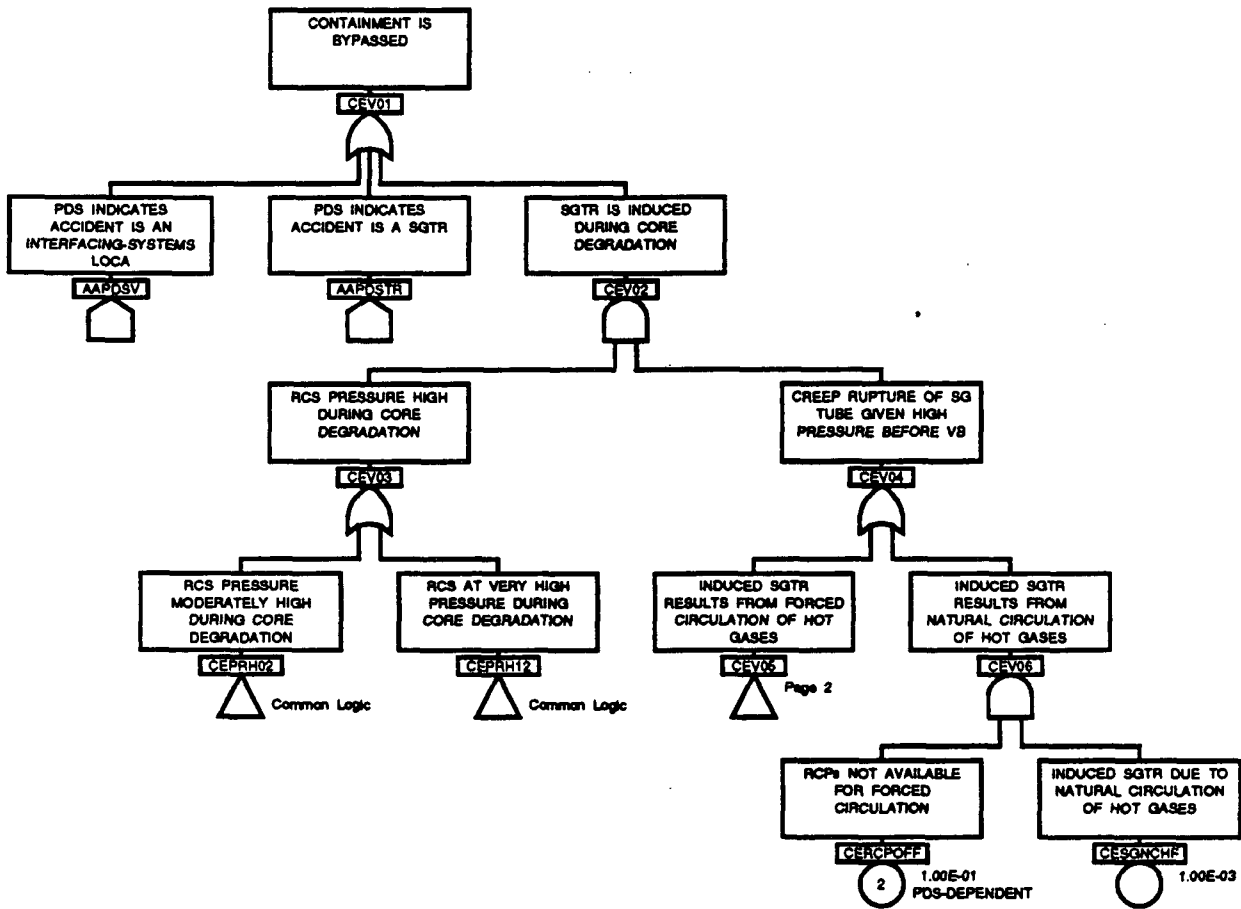


Figure 5-5. Logic for Failure of CET Event V—Containment Bypass (page 1 of 2)

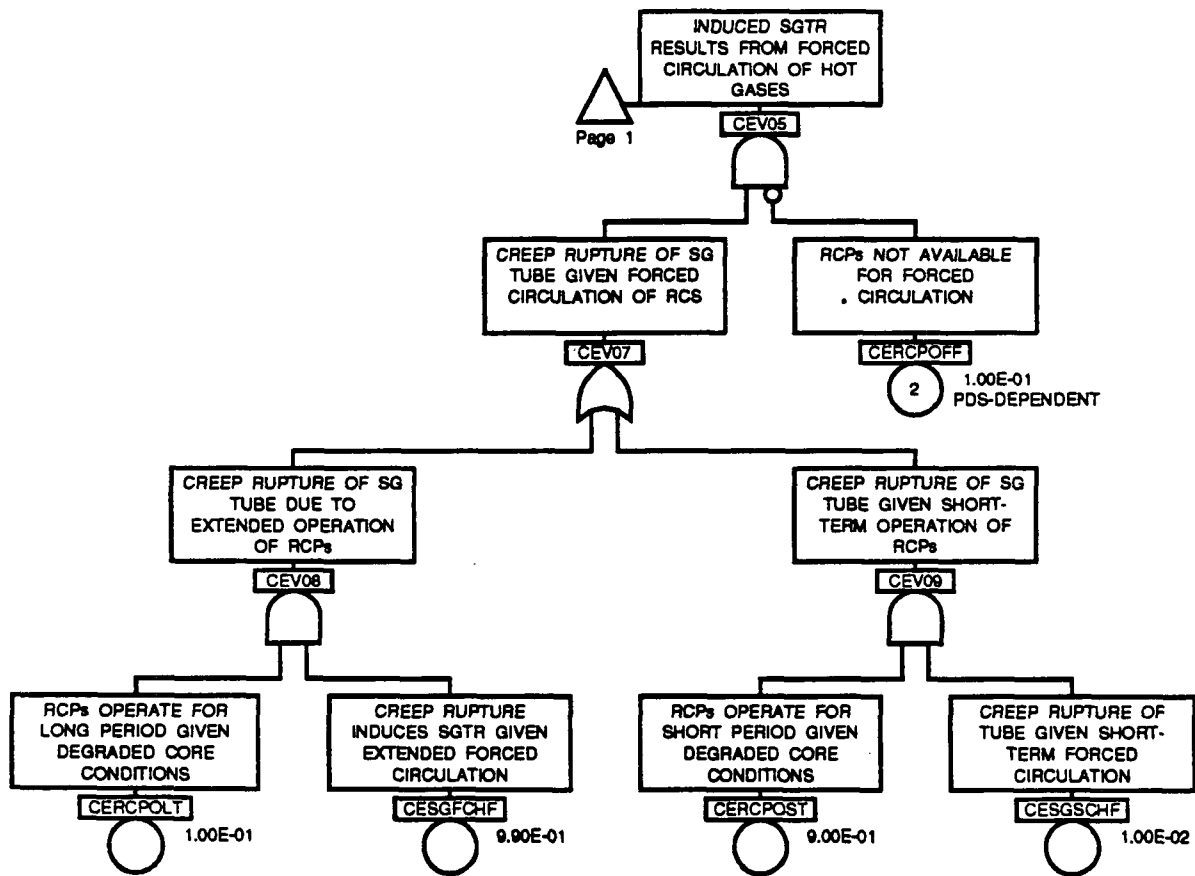


Figure 5-5. Logic for Failure of CET Event V—Containment Bypass (page 2 of 2)

pressure driving force. Thus, only accidents involving small LOCAs or transients would be of concern. Moreover, it is expected that the potential for creep rupture of a tube could be neglected for cases in which feedwater was available to the steam generators for several reasons. First, for small LOCAs and, to a lesser extent for transients, the availability of feedwater to the steam generators would cause RCS pressure to be lower than if feedwater were not available. Second, with feedwater available, the steam generators would tend to remain pressurized, reducing the pressure differential across the tubes. In addition, feedwater would provide cooling of the hot gases transported to the steam generators, limiting the temperature rise of the tubes. As a practical matter, core damage would not occur for important sequences involving transients (i.e., with no induced LOCA), provided feedwater was available.

A key consideration with respect to the potential for hot gases to threaten the tubes would be the ability to transport the gases to the steam generators. Without the RCPs and with no feedwater to the steam generators, there would be very little circulation of the gases through the tubes. The hot legs would be exposed to gases at very high temperatures. For temperatures that approached 1700 F, which may occur during a core-damage accident, the time required for creep rupture of either a hot leg or a tube is very short. Because of the thickness of the piping used for the hot legs, however, it would take a period of half an hour or more for the high temperature to be attained throughout the pipe wall. Without forced circulation, the hot legs would almost certainly be heated to a much greater extent than the tubes, so that failure of a hot leg would be expected before that of a tube (even considering that some of the tubes might be thinned prior to the accident). It is therefore judged to be only remotely possible that creep rupture of a tube could result under conditions of natural circulation.

The ICC guidelines call for the RCPs to be restarted, as a last means to induce some amount of cooling of the core (Ref. 33). If this were done, the water collected in the bowls of the RCPs would be forced into the core region. Immediately after RCP restart it was judged that there would be sufficient mixing of resultant steam and upper plenum gases in the lengthy raised loop hot legs to initially substantially cool the upper plenum gases prior to reaching the steam generator tubes. After continued pump operation, the gases would begin to heat back up. As discussed in Section 2.2.3, the MAAP code does not explicitly model the effects of the RCPs if they are restarted in a (largely) voided RCS. It was estimated, however, that an extended period of RCP operation would be required for the gases to return to the initial very high temperatures previously present in the upper plenum region.

There is substantial uncertainty with respect to whether the RCPs would continue to operate for an extended period. The pump motors are not qualified for the severe environment they would experience during a core-damage accident. Furthermore, the seals would be severely heated by the hot gases circulating through them; cooling with a steam medium on the RCS side of the seals would tend to be very ineffective, even if the systems providing seal cooling were available. If the seals were to fail, there would be further

depressurization of the RCS, which would lead to a reduction in the potential for creep rupture.

To reflect these considerations, the potential for a tube failure has been divided into three categories, as shown under gate CEV04 in Figure 5-5:

- If the RCPs were to operate for an extended period of time, the gases would have time to heat up and to cause exposure of both the hot legs and tubes to very high temperatures. Because of the relatively thin walls of the tubes, there would be a much smaller lag in conducting heat through the wall than for the hot legs. Therefore, it is considered to be "very likely" that creep rupture of a tube would occur before a hot leg failed. Based on the considerations noted above, it is judged to be "unlikely" that the RCPs would operate for such an extended period of time.
- If the RCPs were to operate for an intermediate period of time (e.g., on the order of 1/2 hour) before failing, sufficient circulation could be established that there would be a lower, but not necessarily negligible, chance of tube failure. It is considered to be "likely" that the RCPs would operate for up to about 1/2 hour, and "very unlikely" that the resulting circulation would lead to a tube failure. It should be noted that the result for this condition corresponds roughly to the mean value of the distribution generated by the expert elicitation for this issue for NUREG-1150 (Ref. 36).
- If the RCPs were not available, or failed almost immediately after being started, it is expected that there would be a very small residual potential for an induced failure. The event in this case is taken to be "remotely possible."

The types of accidents that would correspond to pressures that could lead to creep rupture of the tubes are developed under gates CEPRH01 and CEPRH11. These are described in Section 5.2.11. The probabilities of the basic events referred to above are summarized in the tabulation on the following page.

5.2.4 Events B₁ and B₂: Containment Isolation

Events B₁ and B₂ refer to the status of containment isolation. For cases in which event B₁ is successful, there is no pre-existing leakage path from the containment. If event B₁ fails but event B₂ succeeds, there is a small isolation failure. This implies that there may be an increased rate of leakage of fission products from containment, but that the leak is too small to arrest pressurization due to other phenomena. For cases in which event B₂ fails as well, there is a large leak from containment. This leak is assumed to be sufficient to prevent slow pressurization of containment (e.g., due to steaming from cooled core debris), but would not necessarily prevent more severe failures due to other loadings, such as due to hydrogen burns.

The status of events B₁ and B₂ is determined directly by the plant-damage states. Therefore, no supporting logic has been developed for these events. The cases of interest are summarized on the following page. For scenarios in which event B₁ fails but event B₂ is successful, a small isolation failure is implicit.

Quantification of Basic Events for Top Event V

PDS/Case	Description	Assessment	Probability
CERCPOLT: RCPs operate for long period given degraded core conditions			
All	All relevant plant damage states	unlikely	0.1
CERCPOST: RCPs operate for short period given degraded core conditions			
All	All relevant plant damage states	likely	0.9
CERCPOFF: RCPs not available for forced circulation			
SINYLYYN	Small LOCA plant-damage state	per cut sets	0.13
TINYFYDD	Transient plant-damage state	per cut sets	0.67
TINYNINN and TINBININN	Transient plant-damage state	per cut sets	1.0
TRNYFYDD	Transient plant-damage state	per cut sets	0.15
All others	All other plant-damage states	per cut sets	0.0
CESGNCHF: induced SGTR due to natural circulation of hot gases			
All	All relevant plant damage states	remotely possible	0.001
CESGFCHF: creep rupture induces SGTR given extended forced circulation			
All	All relevant plant damage states	very likely	0.99
CESGSCHF: creep rupture induces SGTR given short-term forced circulation			
All	All relevant plant-damage states	very unlikely	0.01

Quantification for Top Events B₁ and B₂

PDS/Case	Description	Assessment	Probability
Failure for event B ₁ : isolation failure			
PDS with "Y" as 4th character	successful containment isolation	impossible	0.0
All other PDS	isolation failure	certain	1.0
Failure for event B ₂ : large isolation failure			
PDS with "B ₂ " as 4th character	large isolation failure	certain	1.0
All other PDS	successful isolation or small isolation failure	impossible	0.0

5.2.5 Event E: Early Containment Failure Prevented

The possibility of early containment failure, as represented in event E, reflects the potential for loadings to cause failure of containment during the period from the start of core degradation to shortly after vessel failure. The failure modes considered include the following:

- Overpressurization due to a hydrogen burn prior to vessel breach,
- Overpressurization due to steaming to containment prior to vessel breach,
- An in-vessel steam explosion sufficient to cause a missile to penetrate containment,
- Overpressurization due to the loadings associated with the discharge of core debris from the reactor vessel,
- Other missiles generated following vessel failure,
- Overpressurization due to a hydrogen burn soon after vessel breach,
- The impulse loading caused by an ex-vessel steam explosion, and
- The possibility of direct attack of core debris on the containment vessel.

Two of these failure modes were determined not to be directly relevant for Davis-Besse. The first is the potential for overpressurization due to steam generation prior to vessel breach. Even without containment heat removal, passive heat sinks combined with the very large free volume of containment (about 2.8×10^6 ft³) would result in very slow pressurization, especially while relatively cold water from the BWST was being injected into the RCS. Thus, this mode of failure was neglected. The second relates to failure due to direct contact of core debris. The incore instrument tunnel at Davis-Besse provides a possible pathway for the transport of significant amounts of core debris up to the basement level (also referred to as the lower elevation) in the event that the RCS was still at high pressure at the time of vessel breach. The debris would be dispersed near the containment wall, but the wall is protected by a concrete curb that is 2.5 ft high and 1.5 ft thick. While ablation of this concrete may be a possible mode for failure in the longer term, the likelihood of rapid failure due to direct contact is judged to be negligible.

The remaining failure modes are each addressed in the logic for failure of event E, as shown in Figure 5-6. Each type of threat to containment integrity is discussed below.

Overpressurization Due to Early Hydrogen Burn

During the heatup of the core, the exothermic oxidation of the zircaloy cladding and core-support structure by steam would result in the generation of hydrogen gas. Additional hydrogen might be generated if some level of cooling were restored to the core or as the core interacted with water in the vessel's bottom head. If a sufficient concentration of hydrogen were present in containment, a deflagration or detonation could result, depending on the containment conditions. These burns could occur due to the hydrogen released prior to vessel

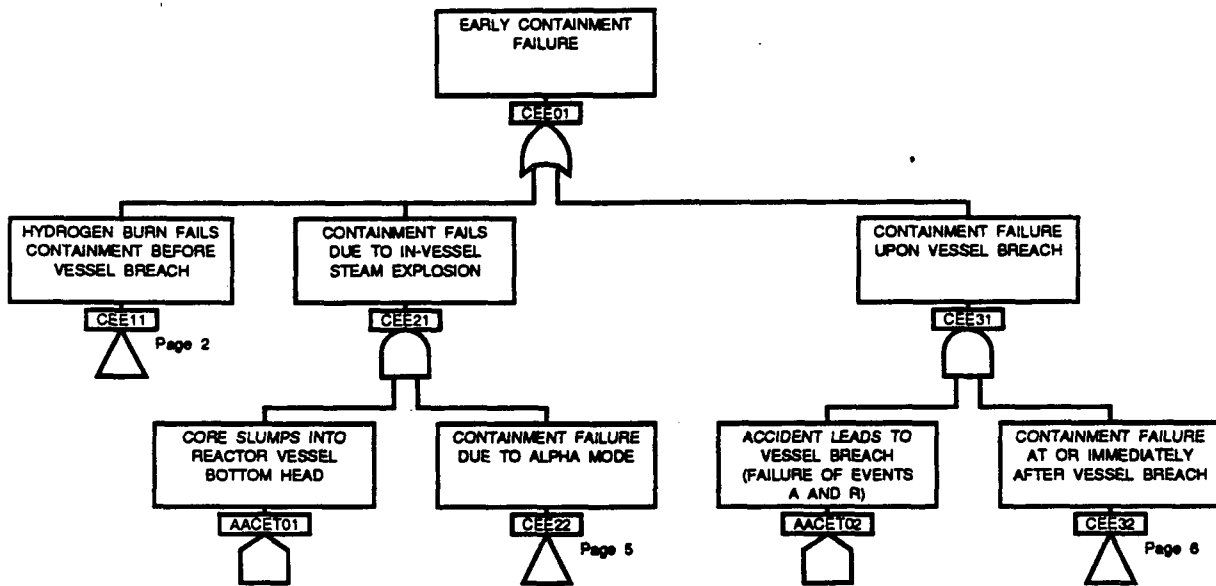


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 1 of 9)

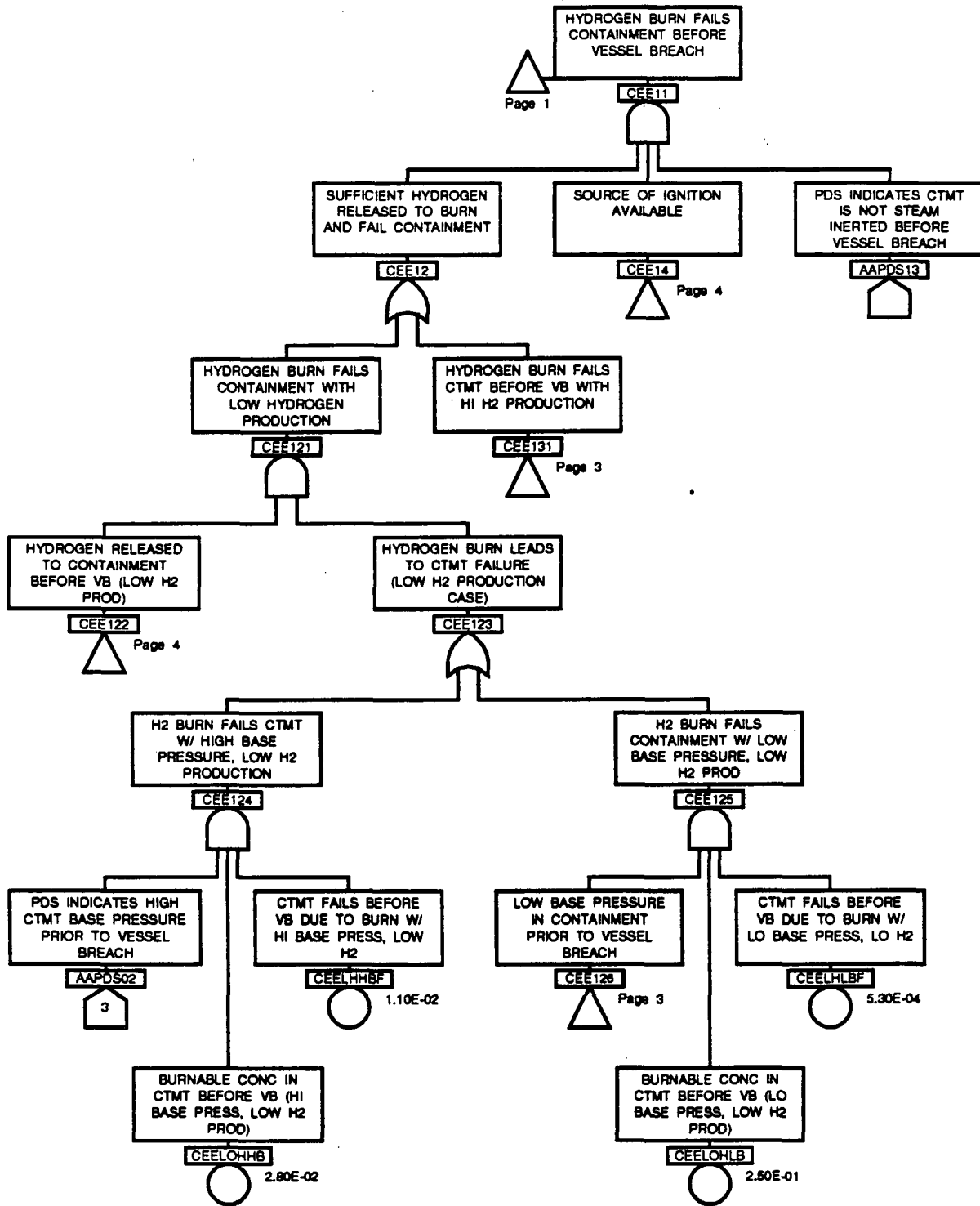


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 2 of 9)

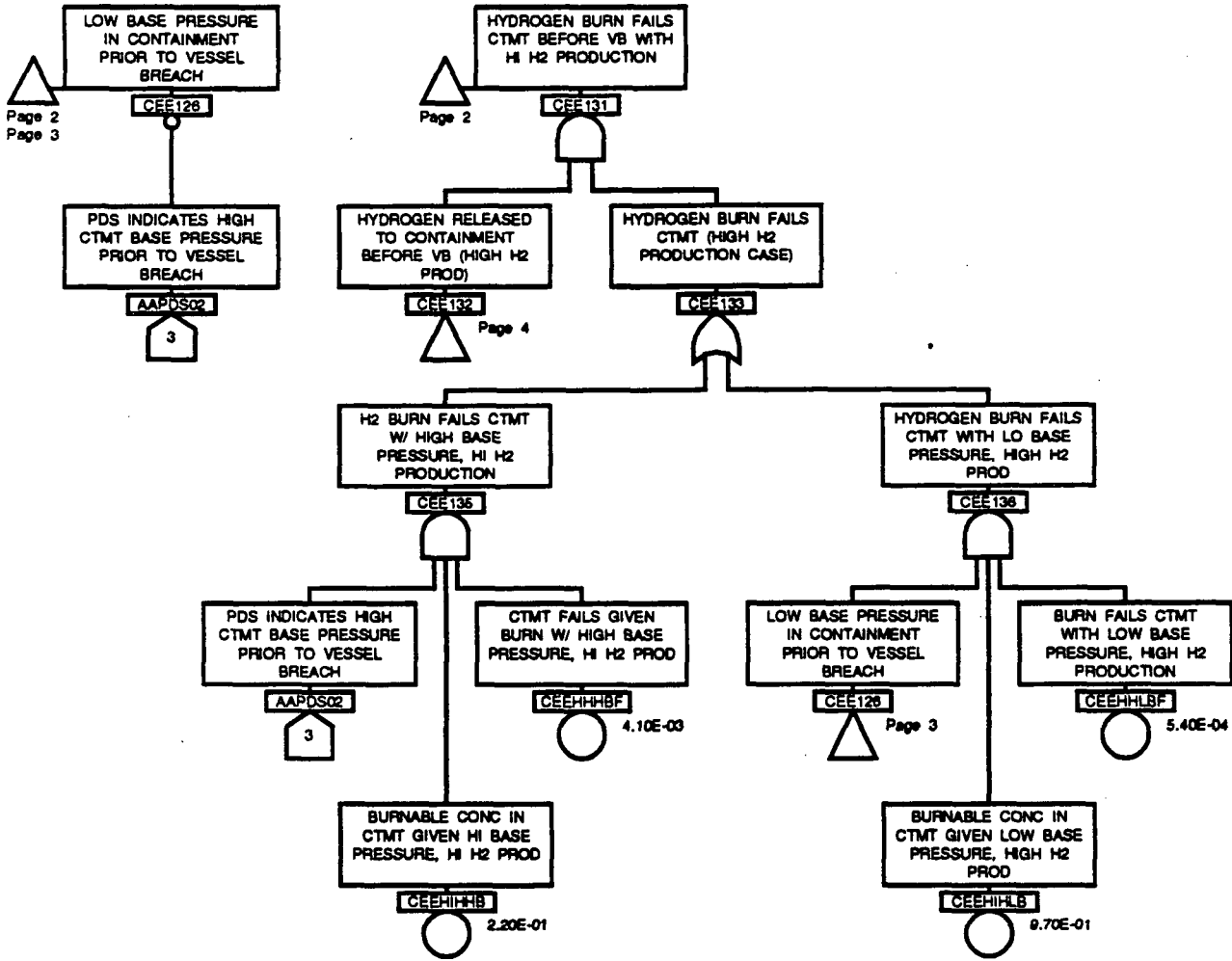


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 3 of 9)

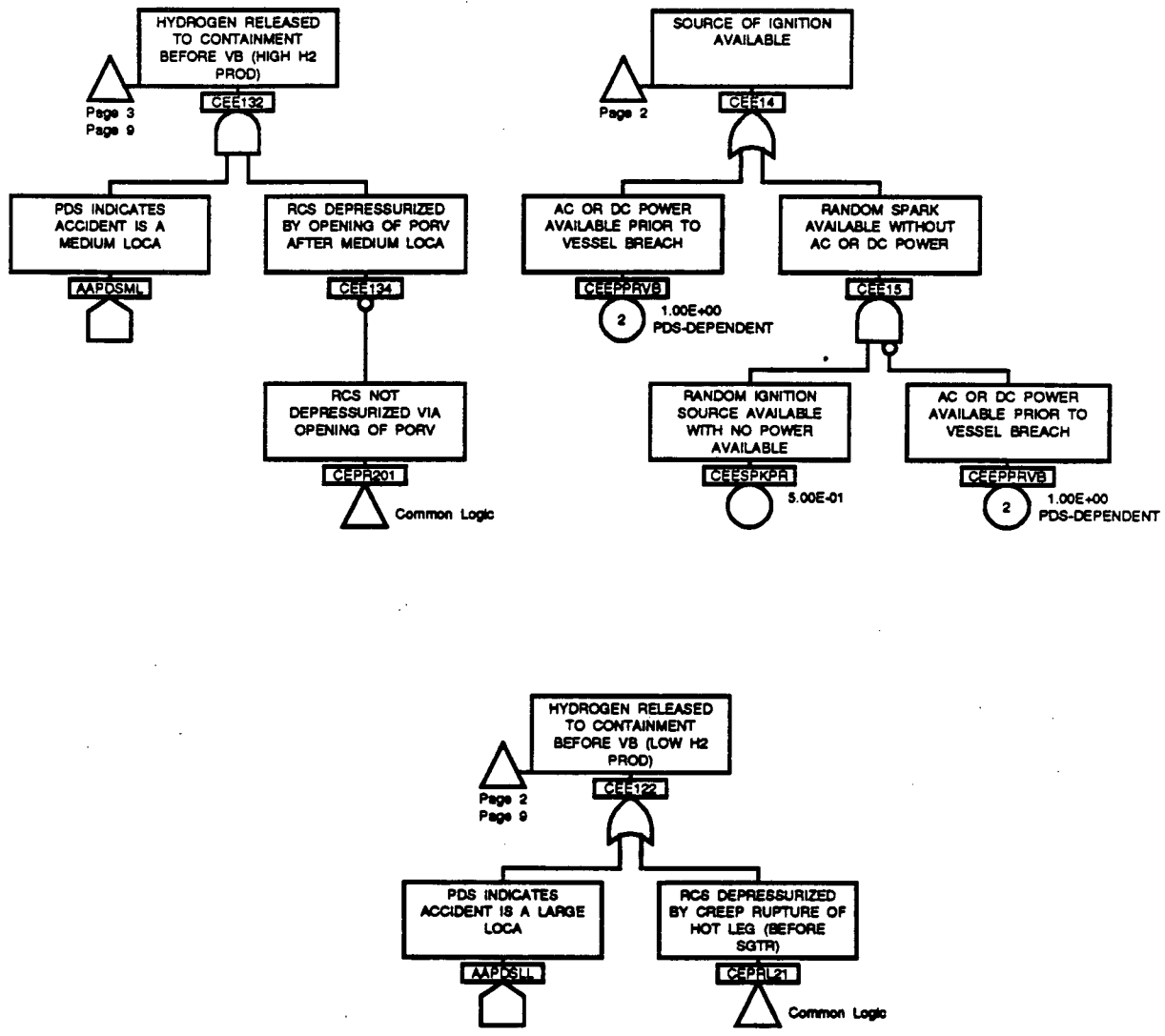


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 4 of 9)

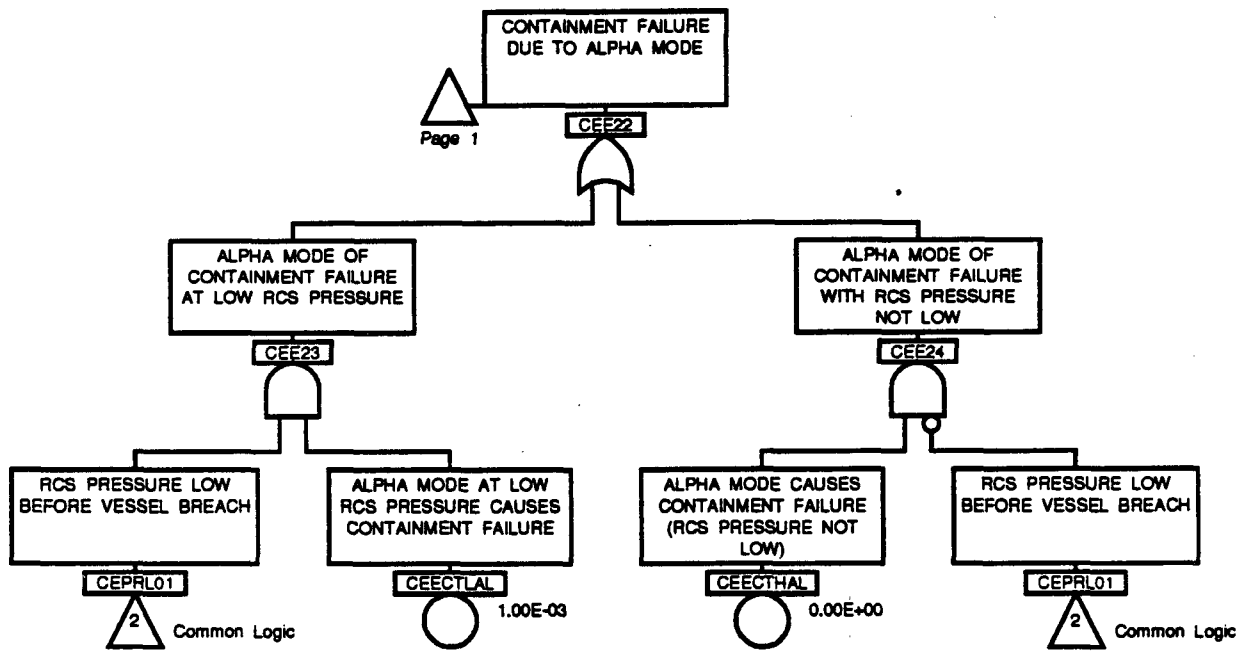


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 5 of 9)

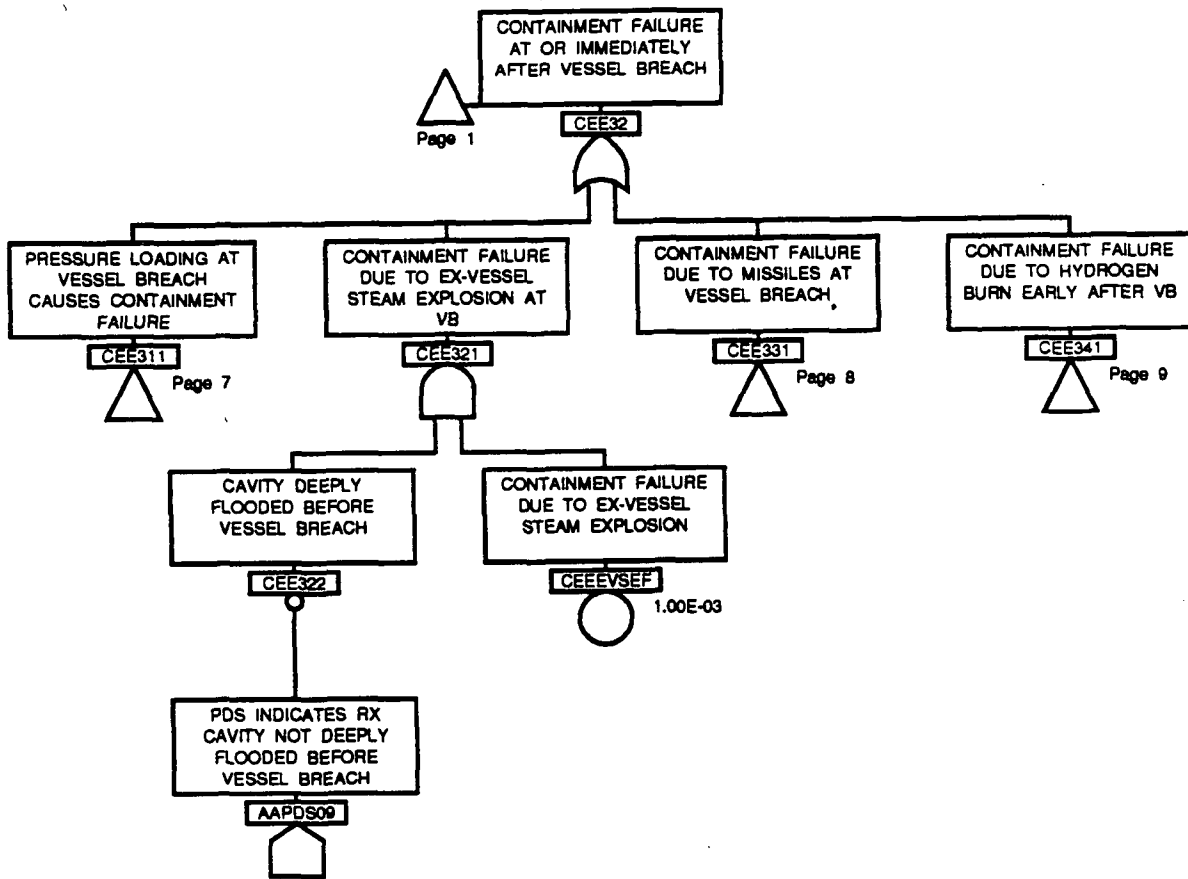


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 6 of 9)

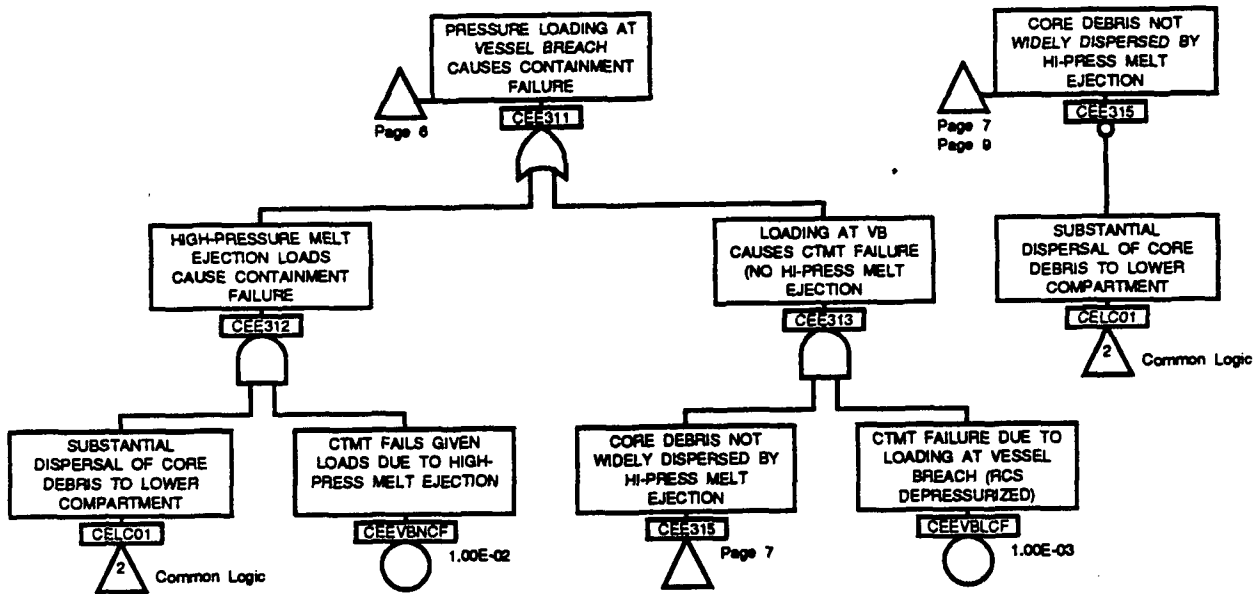


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 7 of 9)

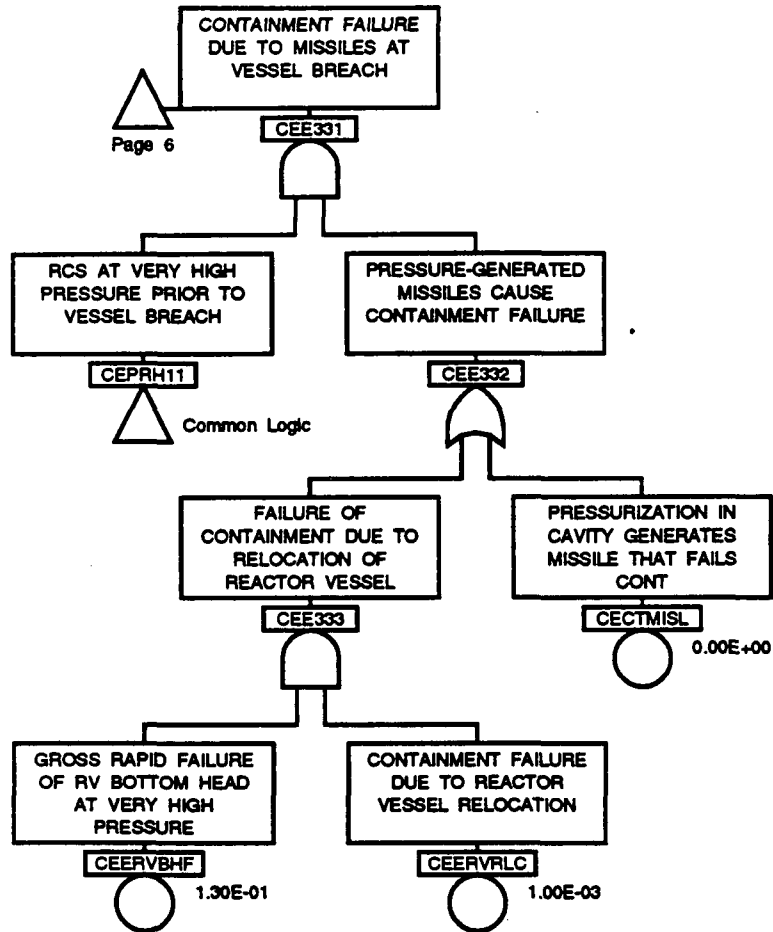


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 8 of 9)

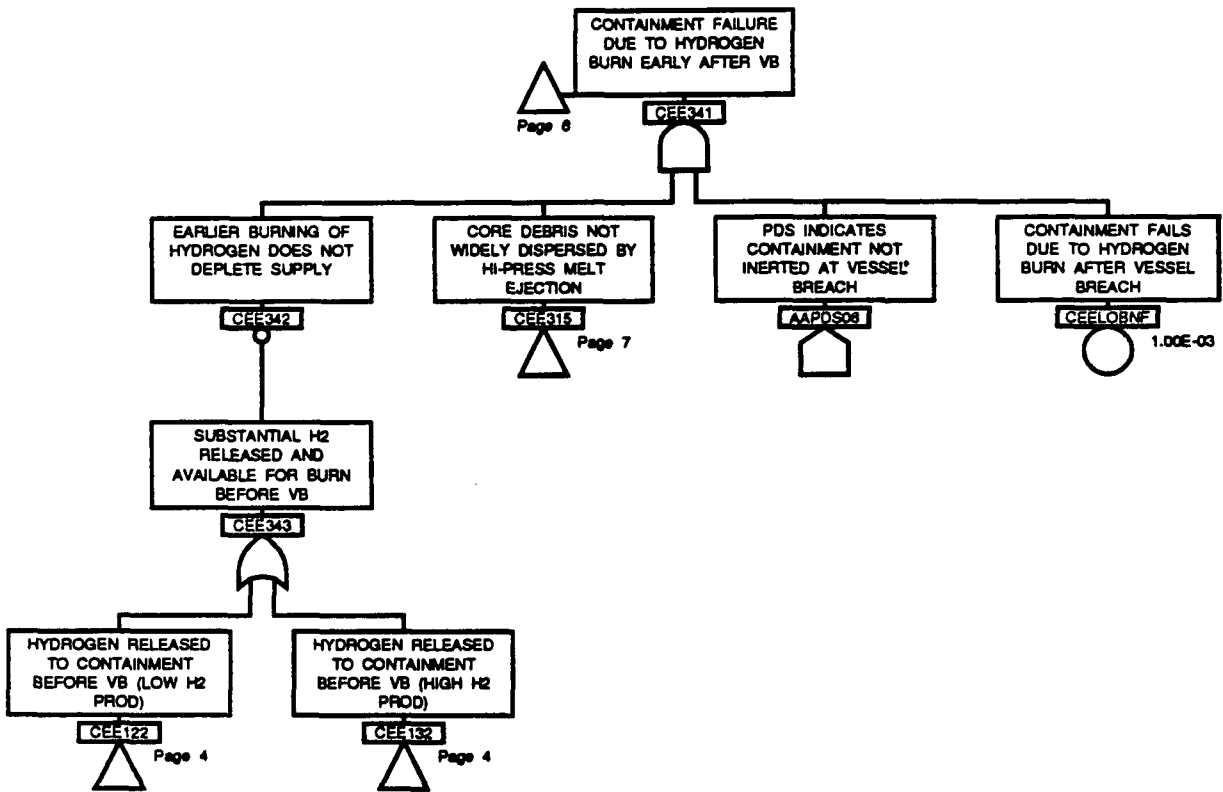


Figure 5-6. Logic for Failure of CET Event E—Early Containment Failure (page 9 of 9)

failure, during the blowdown at the time of vessel failure, or soon after vessel failure due to the additional hydrogen released.

The possibility and magnitude of hydrogen burns depend on many factors, including the amount of hydrogen generated, the timing of the release of this hydrogen from the RCS, the degree to which the containment is inerted by the presence of steam, the degree of mixing of the hydrogen within the containment environment, and the presence of a source of ignition. Each of these factors is discussed in order.

An estimate of the amount of hydrogen generated during core degradation is provided by the MAAP calculations. The amount of hydrogen that could be generated would depend on the amount of time the core materials were exposed to steam at high temperatures, the amount of steam present, and the degree to which the zirconium was exposed to the steam. The MAAP code uses a relatively simplistic choice of models for the meltdown processes, one in which damage to the core results in blockage of the channels between the fuel assemblies relatively early in the degradation process and another in which there is much less blockage. The core-blockage model tends to predict lower generation of hydrogen than the other model, since steam would be inhibited from reaching the cladding to a much greater extent. In the base-case analyses using MAAP, the no-blockage model was used. The predictions of hydrogen generation were found to fall into one of two ranges, depending on the type of accident. For most accidents, an amount of hydrogen equivalent to reaction of 25 to 35% of the zirconium in the reactor vessel was predicted by MAAP. For some accidents, in which there was collapse of the core geometry before there had been substantial melting of the fuel, an amount equivalent to reaction of about 55% of the zirconium was predicted. This was usually the case for accidents involving medium LOCAs in which core cooling was initially successful but was lost later on.

The MAAP results are judged to be representative of nominal values for the respective types of sequences. As discussed in Section 2.2.5, current assessments suggest an upper bound of 75% equivalent zirconium reaction for a broad range of accident types. To account for the range of possible values of hydrogen generation, these values were fit to a pair of lognormal distributions. These distributions were developed and applied as follows:

- For accidents that fall into the higher range, the median value of the distribution was taken to be 55% equivalent clad oxidation, and 75% was taken to be the 95th percentile. All sequences initiated by a medium LOCA were included in this category.
- For accidents that fall into the lower range as predicted by MAAP, a value of 30% zirconium reaction was assumed to represent the median value of the distribution, and 75% reaction was taken to correspond to the 99th percentile of the distribution. This distribution was applied for all other types of accidents.

The resulting distributions are shown in Figure 5-7. For purposes of comparison, two of the distributions developed based on the expert elicitations for NUREG-1150 are shown as well (Ref. 36). Cases 2c and 1b represent the lowest and highest cases, respectively, for

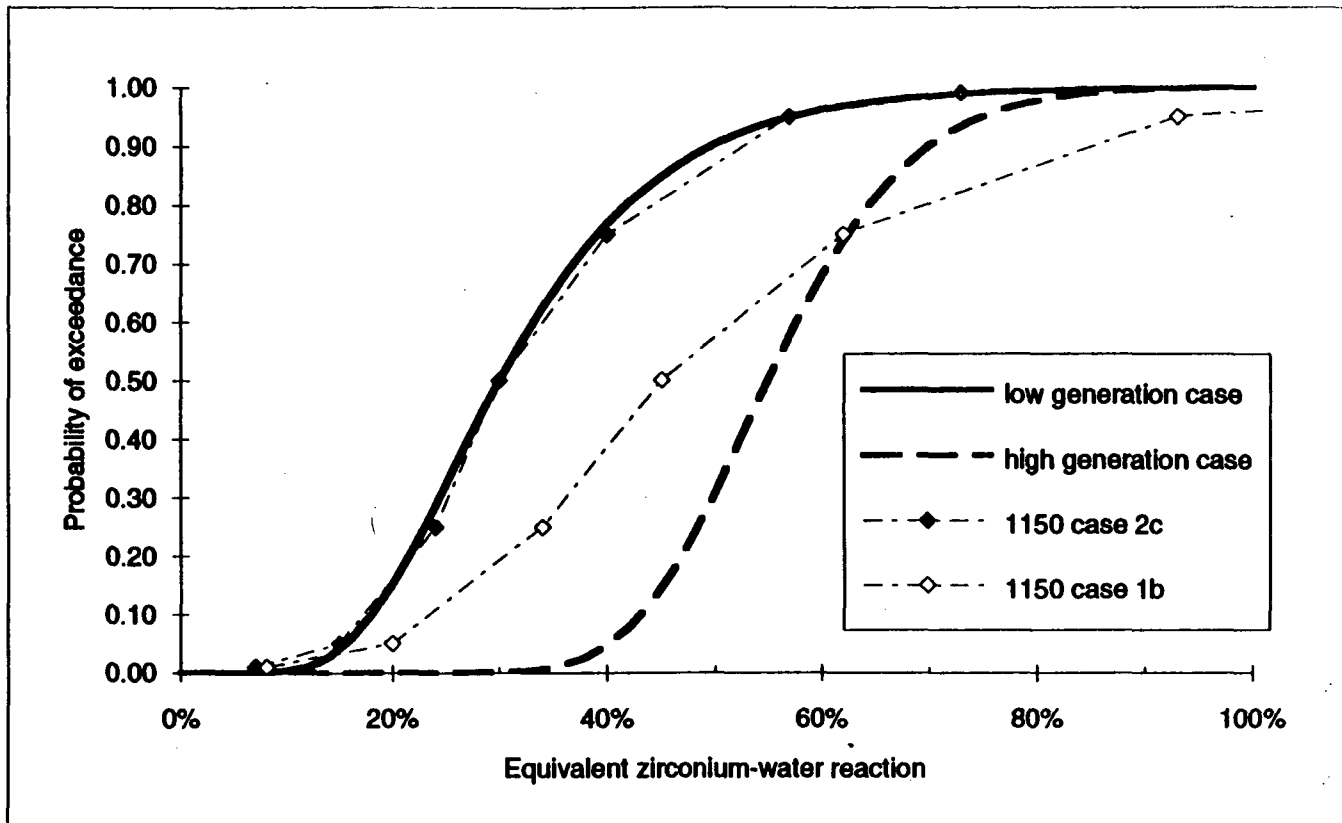


Figure 5-7. Cumulative Probability Distributions for In-Vessel Generation of Hydrogen

generation of hydrogen as assessed by the experts. Note that case 2c corresponds almost exactly to the low-generation case used for Davis-Besse. Case 1b is characterized by a broader distribution, with more weight at both lower and higher percentages of hydrogen generation. Based on the available technical information and the comparisons to these cases, the two cases selected to represent hydrogen production for Davis-Besse were judged to be appropriate.

Even at 100% zirconium reacted, the maximum concentration of hydrogen in the containment would be only about 13% (i.e., in a nominally dry containment), because of the large volume of the containment. This is below the minimum detonable quantity. The degree of mixing in the containment should be relatively high, and there are no volumes in which a large volume of hydrogen should preferentially concentrate (refer to Section 2.2.5 for further discussion of this issue). Therefore, failure of containment due to a detonation was not analyzed further.

The timing for the release of hydrogen would be determined largely by the pressure of the RCS. For cases in which RCS pressure was low prior to vessel breach (e.g., for large LOCAs), it was assumed that most hydrogen would be released prior to vessel breach. For high-pressure scenarios, it was assumed that insufficient hydrogen would be released prior to vessel breach to cause a burn, unless there was depressurization due to a stuck-open relief valve, creep rupture, etc. It was assumed that the bulk of the hydrogen would be released at vessel breach for those cases.

The possibility that the containment might be steam-inerted was evaluated based on the amount of hydrogen in containment and the conditions in the containment. For each plant-damage state, the fraction of steam in the containment atmosphere and the containment pressure were identified. Based on these conditions, the appropriate distribution for hydrogen generation was truncated at the lower limit of flammability. For a number of plant-damage states, the containment would be inerted at one or more of the time phases of interest for the CET. This was accommodated in the logic for the CET through the use of flags, as noted in the introduction to this section (e.g., event AAPDS13 under gate CEE11 in Figure 5-6). The flammability limits were determined from reported experimental data (Ref. 37).

If a flammable mixture were to be present in containment, it would remain for the mixture to be ignited. Ignition could occur due to a spark from an electrical component, if ac or dc power were available, from static electricity (e.g., due to operation of dampers), or from hot surfaces or hot core debris. For cases in which power was available, it was assumed that there would be a source of ignition at a time when a flammable mixture would exist. For cases with no power, the existence of a source of ignition was taken as "indeterminate."

To estimate the total pressure associated with the burning of hydrogen, a series of calculations was made for a range of hydrogen concentrations over each of several different sets of containment pressure and temperature conditions (inferring steam concentrations). These calculations were made using a separate computer program referred to in Section 2.2.4. As noted in Section 2.2.4, the degree of combustion was taken to be a step function, with

50% of the hydrogen assumed to be consumed for containment concentrations between 4 and 6%, 66% consumed for concentrations up to 8%, and complete combustion for concentrations in excess of 8%.

To calculate the conditional probability of containment failure as a function of the pressure due to hydrogen burns, the distribution of pressures calculated as described was combined with the cumulative distribution function for containment failure pressure. This produced a total probability of failure due to hydrogen burning for the case of interest. The probability of having a burn of any magnitude was inferred from the probability of having sufficient hydrogen generated to exceed the lower flammability limit for that case. The conditional probability of containment failure was then back-calculated by taking the ratio of the total probability of failure due to the burn to the probability of the burn.

This set of calculations was performed for various plant-damage states for conditions both before and after vessel breach. Relatively small probabilities of containment failure due to hydrogen burns were calculated, primarily because of the combination of the following two considerations:

- A relatively low containment base pressure prior to the hydrogen burn would be required to support a global burn; higher pressures would correspond to high concentrations of steam, such that the containment would be inerted. With low base pressures, a very large hydrogen burn would be required for total pressure to approach the containment capacity.
- The large volume of the containment limits the global concentration of hydrogen. For example, at a modest steam fraction of about 30%, burning would be of interest only for concentrations between about 6% (near the lower flammability limit) and about 11% (corresponding to 100% equivalent reaction of zirconium). Even using the distribution for high hydrogen generation, the likelihood of concentrations on this order for such conditions would be very low.

Because of the relatively low threat to containment integrity of hydrogen burns before vessel breach, the full set of plant-damage states that might involve release of hydrogen before vessel breach was consolidated into four cases: low base pressure for both low and high hydrogen production rates, and high base pressure (but still low enough such that the containment was not steam-inert) with low and high hydrogen production rates. The plant-damage states (other than those for which steam inerting would be implied) were grouped into these four categories, and the highest overall probability of containment failure due to hydrogen burn in each category was used to characterize the plant-damage states for that category. These conditions are developed under gate CEE12 of the supporting logic. As indicated, they would apply only for cases in which most of the hydrogen was released from the RCS to containment prior to vessel breach (e.g., a large LOCA or a transient with creep rupture of a hot leg), the containment was not steam-inert, and there was a source of ignition available. It should also be pointed out that the choice of high vs. low base containment pressure makes relatively little difference to the probability of containment failure. Burns at somewhat higher pressures tend to be mitigated to some extent by the additional steam

available to absorb energy. High base pressure was taken to be true for all cases in which the pressure was above 28 psia prior to the burn.

Following vessel breach, hydrogen that was previously held up in the RCS could be released to containment and could be available for burning. In the case of a high pressure melt ejection, rapid oxidation of finely fragmented core debris could also produce additional hydrogen. The burning of hydrogen in this case is discussed later, along with the other loads at vessel breach.

For cases in which the RCS was at sufficiently high pressure that much of the hydrogen might only be released at vessel breach, but for which a high pressure ejection did not cause substantial dispersal of core debris into the basement elevation, the considerations of hydrogen burns are very similar to the cases before vessel breach. If the containment were not inerted by steam in the period after vessel breach, a burn could lead to containment failure. Because the relatively detailed investigations of burn pressures prior to vessel breach indicated such a low overall probability of containment failure, the treatment of failure following vessel failure was less detailed. Containment failure due to a hydrogen burn following vessel failure was assessed to be "remotely possible" based on the following considerations:

- The highest overall probability of containment failure for any plant-damage state prior to vessel breach was calculated to be less than 0.001.
- During ejection from the vessel, it is possible that some additional hydrogen might be generated due to further oxidation of core materials. Although the quantity might not be very large, it could be sufficient to cause slightly higher burn pressures. Thus, there is additional uncertainty regarding the potential magnitude of a burn.
- The containment would tend to be steam-inert for a larger fraction of plant-damage states after vessel breach than before. Thus, use of what might be a bounding (but still small) probability for containment failure for those cases that were not steam-inert would not produce unacceptable results.

The logic for this case is provided under gate CE341 in event E. The probabilities for the basic events associated with hydrogen burns before or soon after vessel breach are summarized on the next page.

In-Vessel Steam Explosion and Pressure-Generated Missiles

It has been postulated that large dry containments could be failed by direct impact as a result of missiles generated during a severe accident. Based on previous analyses (Refs. 34 and 38), three types of missiles were considered for Davis-Besse:

- A steam explosion could occur inside the reactor vessel. This could result when the molten core slumped into the bottom head of the vessel and interacted with the water remaining there. If such a steam explosion were to occur and if it were sufficiently energetic, it is conceivable that the energy released could cause the generation of a missile (e.g., the vessel head) that could fail the containment on impact. This is traditionally referred to as the alpha mode of containment failure.

Quantification of Basic Events for Failure Due to Early Hydrogen Burns (Top Event E)

Basic Event	Base Pressure	Hydrogen Production	Probability
Combustible concentration in containment before vessel breach			
CEELOHHB	high	low	0.028
CEELOHLB	low	low	0.25
CEEHIHBB	high	high	0.22
CEEHIHLB	low	high	0.97
Containment fails before vessel breach due to hydrogen burn			
CEELHHBF	high	low	0.011
CEELHLBF	low	low	0.00053
CEEHHHBF	high	high	0.0041
CEEHHLBF	low	high	0.00054
PDS/Case	Description	Assessment	Probability
CEESPKPR: random ignition source available with no power available			
All	All relevant plant damage states (i.e., with no ac or dc power)	indeterminate	0.5
CEELOBNF: containment failure due to hydrogen burn after vessel breach			
All	All relevant plant damage states (no earlier burn, no dispersal to lower elevation)	remotely possible	0.001

- For cases in which the reactor vessel fails at high pressure, the thrust generated by the blowdown forces might be sufficient to cause the piping connected to the reactor vessel to shear off and for the reactor vessel itself to become a projectile.
- High-pressure blowdown could also cause other components outside the reactor vessel to be displaced with sufficient energy to become missiles.

Available research indicates that the pressure in the RCS may affect the potential for an in-vessel steam explosion. The Steam Explosion Review Group (SERG) assessed the probability of an in-vessel steam explosion that could lead to containment failure for pressures below about 200 psig to have a mean value of 0.008 (Ref. 36). Higher pressures were considered to have the potential to suppress the steam explosion, although the SERG did not

quantify the corresponding probability. The reference value was therefore reduced by an order of magnitude in analyses supporting NUREG-1150 (Ref. 34).

Other assessments (e.g., Ref. 39) have concluded that pressures above about 75 psig could suppress a steam explosion in the absence of an external trigger for the explosion. They have further concluded that there is no mechanism by which fuel-coolant interactions can result in a steam explosion in the reactor vessel of sufficient force to cause failure of both the reactor vessel and the containment. As a result, some PRAs have neglected this as a credible containment failure mode altogether.

In consideration of these inputs, it was judged that the probability of an in-vessel steam explosion capable of leading directly to containment failure could be adequately characterized as "remotely possible" for accidents progressing at low pressure. For cases in which core degradation would occur at intermediate or higher pressures, occurrence of the alpha failure mode was assessed to be "impossible."

Both of the other two failure modes are developed under gate CEE331 (conditional on the breaching of the reactor vessel). The possibility that the reactor vessel could become a projectile was also evaluated for the NUREG-1150 analyses. Conservative calculations were made that indicated that the thrust could be sufficient to cause shear failure of the piping. For Sequoyah, separate probabilities were assessed for the possibilities of directly causing containment failure and for causing the vessel to damage the missile shield but not to cause containment failure (the latter is of interest for Sequoyah because of the possibility that a pathway for bypassing the ice condenser might be created). For containment failure to occur, two conditions were required: the RCS pressure would have to be very high, and there would have to be a gross, rapid failure of the bottom head of the reactor vessel. The mean probability of the bottom-head failure was assessed to be 0.13, and the conditional probability of containment failure given this failure mode was assessed to be 0.01 (Ref. 34). Davis-Besse has a very large cavity area and large vent paths between the cavity and other areas in containment, which would tend to mitigate the potential for this failure mode even further. Therefore, the potential for containment failure given gross failure of the bottom head at very high RCS pressure was assessed to be "remotely possible."

The possibility that rapid pressurization of the cavity during vessel failure could lead to generation of other missiles was addressed primarily because it was a factor for the CET developed for a generic Babcock & Wilcox design, which was largely based on the Oconee configuration (Ref. 31). At Oconee, reactor shield plugs could become missiles during rapid pressurization of the reactor cavity. No such potential missiles were identified in the Davis-Besse design. Therefore, this event was assessed to be "impossible."

The probabilities for the basic events associated with this category of potential causes of early containment failure are summarized below.

Quantification of Basic Events for Failure by Missiles (Top Event E)

PDS/Case	Description	Assessment	Probability
CEECTLAL: alpha mode at low RCS pressure causes containment failure			
All low	All relevant plant-damage states (i.e., without in-vessel recovery and at low pressure)	remotely possible	0.001
CEECTHAL: alpha mode at high RCS pressure causes containment failure			
All others	All other plant-damage states	impossible	0.0
CEERVBFH: gross rapid failure of reactor vessel bottom head at very high pressure			
All very high	All relevant plant-damage states (i.e., at very high pressure prior to vessel breach)	unlikely	0.13
CEERVRLC: containment failure due to reactor-vessel relocation			
All very high	All relevant plant-damage states (i.e., at very high pressure prior to vessel breach)	remotely possible	0.001
CECTMISL: containment failure due to pressure-generated missile			
All	All plant-damage states	impossible	0.0

Failure Due to Pressure Rise at Vessel Breach

If the core debris were to breach the reactor vessel, the discharge of debris and steam from the RCS would lead to further pressurization of the containment. This pressure loading could result from several sources, including the steam released from the RCS at vessel breach, from the rapid transfer of heat from the core debris to water in the reactor cavity, and from direct heating of the containment atmosphere by widely dispersed debris.

If the debris were to exit the vessel via high pressure melt ejection, it could be dispersed to the lower elevation. Depending on the amount of debris that was finely fragmented, there could be a rapid direct transfer of energy to the containment atmosphere. Further exothermic oxidation of the fuel could also add energy to the atmosphere. There could also be burning of hydrogen simultaneous with this pressurization. This burning could involve both hydrogen generated during core degradation, and that produced during the oxidation in the containment atmosphere. Local burning at the site of oxidation could occur throughout the area in which the debris was dispersed.

The pressure rise at vessel breach was calculated using the MAAP code for a representative set of plant-damage states. These pressure rises tended to be quite small when compared to the estimates provided by the experts for NUREG-1150 (Ref. 40.). A sensitivity

case was evaluated, in which a parameter representing the fraction of debris that would be finely fragmented at vessel failure was increased from the nominal value of 0.03 to 0.33. The value of 0.33 was considered to be a realistic upper bound (Ref. 41). This sensitivity case was performed for an accident involving a high pressure core melt due to station blackout (plant-damage state TINYNINN). In this case, the pressure rise at vessel breach was about 37 psi, compared to about 24 psi in the base case. In neither the base case nor the sensitivity study was a hydrogen burn predicted to occur at the time of vessel breach.

For cases involving high pressure melt ejection, with the potential for direct containment heating and associated hydrogen burns (as described above), the probability of containment failure was calculated by developing a probability distribution for pressure rise at vessel breach based on the MAAP results, and adding to that pressure rise the pressure associated with a simultaneous hydrogen burn. The pressure rise calculated for the nominal fragmentation parameter (24 psi for FCMDH = 0.03) was assumed to represent the median of a lognormal distribution, with the pressure corresponding to a value of 0.33 (37 psi) assumed to be the 95%-tile.

Added to this distribution was a pressure rise associated with simultaneous burning of hydrogen. The quantity of hydrogen available for burning was assumed to be comprised of the following two components:

- The hydrogen generated during core degradation, as described earlier for hydrogen burns before and after vessel breach. For accidents in which RCS pressure remained high prior to vessel breach (as would be the case for all accidents with the potential for pressurized melt ejection), it was assumed that a large portion of the hydrogen would not be released until after vessel breach. Therefore, this quantity (defined by the distribution described earlier) was assumed to be available for burning.
- The hydrogen generated by oxidation of finely fragmented fuel in the containment atmosphere. It was assumed that an amount of zirconium oxidation would take place equivalent to the fraction of fuel that was finely fragmented (adjusted to account for the cladding previously oxidized in-vessel).

Thus, a distribution for the amount of hydrogen available for burning at vessel breach was developed that was a function both of the initial production and the amount of fuel that was finely fragmented. These correlated distributions were combined to produce a composite distribution for total pressure at vessel breach. This composite distribution is shown in Figure 5-8. The composite distribution was then multiplied by the distribution for probability of containment failure to provide an estimate of the total probability of containment failure due to a high pressure melt ejection. The overall probability of failure at vessel breach given dispersal of core debris to the lower elevation was calculated in this manner to be 0.009. Therefore, for all cases involving pressurized ejection of core debris beyond the reactor cavity, containment failure was judged to be "very unlikely."

Also shown in Figure 5-8 is the distribution for the case from the NUREG-1150 assessment for Zion that most closely corresponds to this case (Ref. 40). The expert

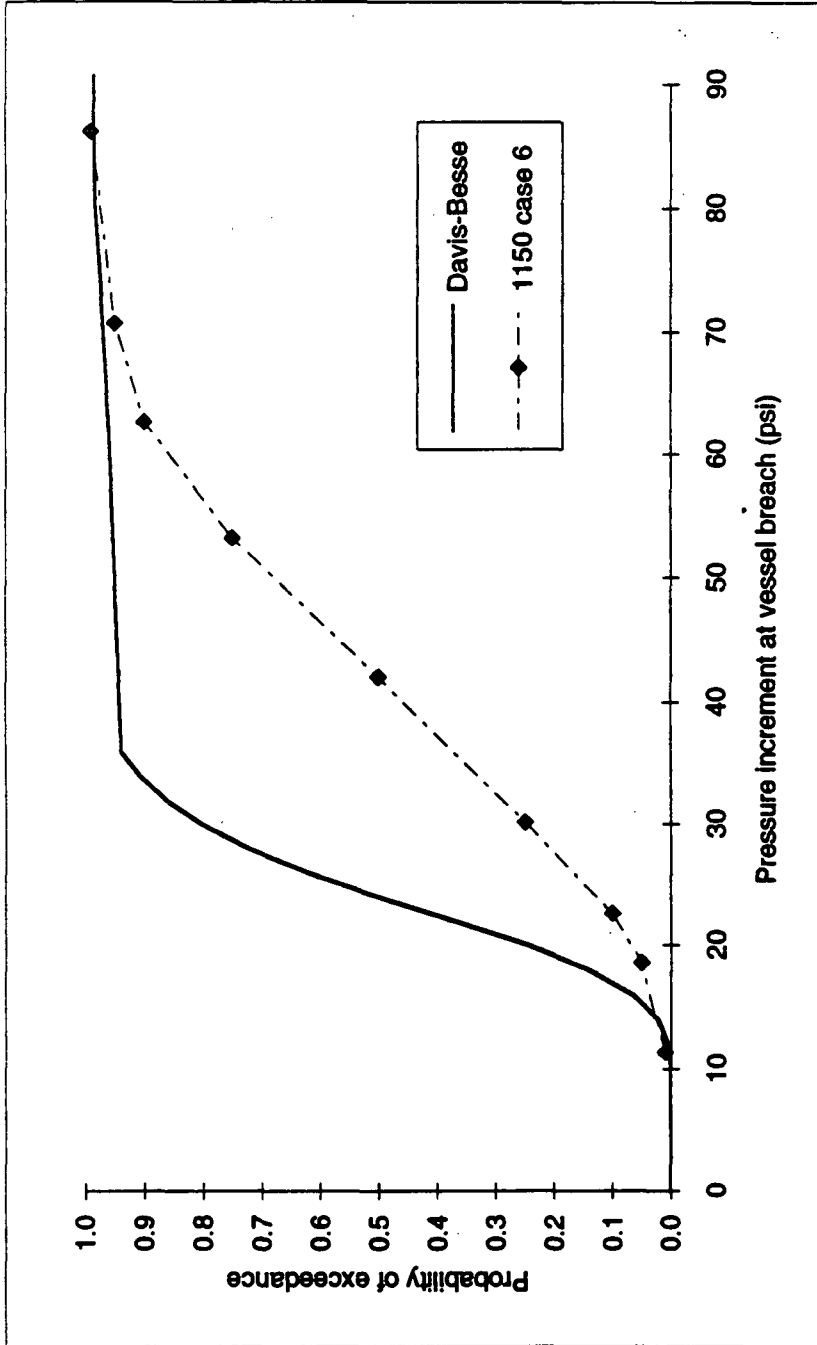


Figure 5-8. Cumulative Probability Distribution for Pressure Rise at Vessel Breach Due to Pressurized Melt Ejection

elicitation for Zion indicated somewhat higher probabilities of higher pressure increments, although the two distributions converge at higher pressures. Because there is a substantial conditional probability of containment failure only at pressures above about 80 psia, the important parts of these curves are relatively close together. Two factors tend to minimize the potential for a failure of the containment due to the pressurization immediately following vessel breach at Davis-Besse:

- (1) The containment volume is quite large, and can therefore accommodate significant amounts of energy with relatively small corresponding pressure rises. The free volume for Davis-Besse is nearly 10% larger than that for Zion (for a nominal power level for Davis-Besse that is about 15% lower than Zion).
- (2) The arrangement of the pathways between the lower and upper compartments would tend to limit the transport of large amounts of the core debris to the upper compartment in the event of pressurized ejection from the reactor vessel. This could reduce the degree to which direct heating of the containment atmosphere would take place.

Other accidents would not lead to significant dispersal of debris beyond the reactor cavity, either because the RCS pressure was not high enough to cause dispersal, or because deep flooding of the cavity caused the debris to be retained in the cavity (refer to the discussion of dispersal beyond in the reactor cavity in Section 5.2.11). For these cases, the pressure rise at vessel breach was calculated by MAAP to be relatively small, and none presented a serious threat to containment integrity. A more detailed assessment, as was performed for cases of pressurized ejection, was not judged to be warranted. Instead, containment overpressurization at vessel breach for these cases was judged to be "remotely possible." Note that the contribution due to hydrogen burns following vessel breach for cases other than those involving pressurized ejection are treated separately, as described earlier.

The probabilities for the two basic events relating to the potential for overpressurization due to the loads at vessel breach are summarized in the tabulation below.

Quantification of Basic Events for Failure Due to Pressure Rise at Vessel Breach (Top Event E)

PDS/Case	Description	Assessment	Probability
CEEVBNCF: containment fails given loads due to high pressure melt ejection			
All	All relevant plant damage states (i.e., with ejection of debris from reactor cavity at vessel breach)	very unlikely	0.01
CEEVBLCF: containment fails due to loads at vessel breach (no ejection from cavity)			
All	All relevant plant damage states (i.e., with retention of core debris in reactor cavity)	remotely possible	0.001

5.2.6 Event C: Ex-Vessel Cooling of Core Debris

Event C of the CET defines whether or not a coolable debris bed forms after the debris is ejected from the reactor vessel. The potential that the debris may be cooled is important with respect to long-term containment response. If the debris bed were cooled, and if containment heat removal was available, a condition could be reached in which containment integrity might be maintained in the long term. If the debris bed were coolable but there were no containment heat removal, the containment would eventually be overpressurized. If the debris bed were not cooled, core-concrete interactions could lead to overpressurization of the containment (by pressurization due to the generation of non-condensable gases or by burning of hydrogen and carbon monoxide), ablative failure of the side wall of the containment vessel (if the debris had been transported into the lower elevation), or penetration of the containment basemat. In these latter cases, additional fission products could be released during the core-concrete interactions.

The logic for failure to achieve ex-vessel cooling of the core debris is shown in Figure 5-9. Three possibilities for failure are indicated:

- For a plant-damage state involving a bypass scenario in which there was essentially no water retained in the containment, the only water available to cool the debris would be that released from the vessel when it failed. In this case, it is assumed that the relatively dry debris would not be cooled (after being cooled initially), and that core-concrete interactions would take place.
- The debris might be largely dispersed up to the basement elevation, where it could fail to form a coolable bed, or there could be insufficient overlying water to assure long-term coolability.
- The debris might be retained in the reactor cavity, where there might be a different probability for forming a coolable bed, with either deep or relatively shallow flooding.

The first case encompasses interfacing-systems LOCAs and some events involving SGTRs. SGTRs involving long-term failures of core cooling would be assumed to leave the cavity relatively dry. SGTRs in which there was a failure of high pressure injection could eventually involve a wet cavity, depending on the availability of low pressure injection when the RCS was depressurized.

For the second case, the possibility that the debris would be dispersed to the lower elevation is developed separately under gate CELC01 (described in Section 5.2.11). If the contents of the BWST were injected into containment, the reactor cavity would be deeply flooded, and the lower elevation would be flooded to a depth of a few feet. In this case, it would be likely that the debris would spread over a wide area. It was judged that a best estimate of the spread area would correspond to a depth of corium of approximately 6 inches. Based on current understanding, there is significant confidence that debris beds less than 10 inches in thickness can be cooled (Ref. 42). There is uncertainty, however, regarding

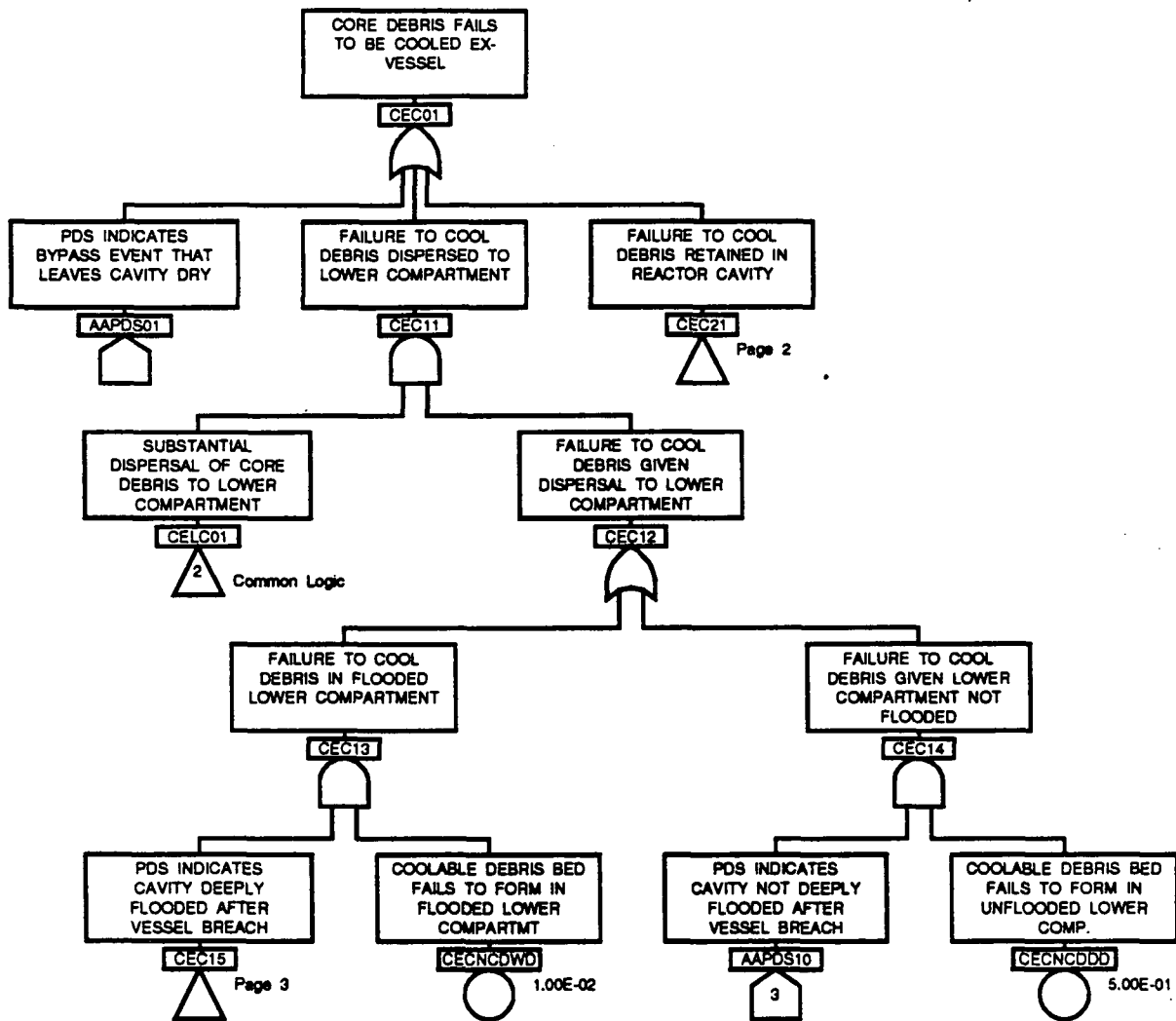


Figure 5-9. Logic for Failure of CET Event C—Core Debris Fails to be Cooled Ex-Vessel (page 1 of 3)

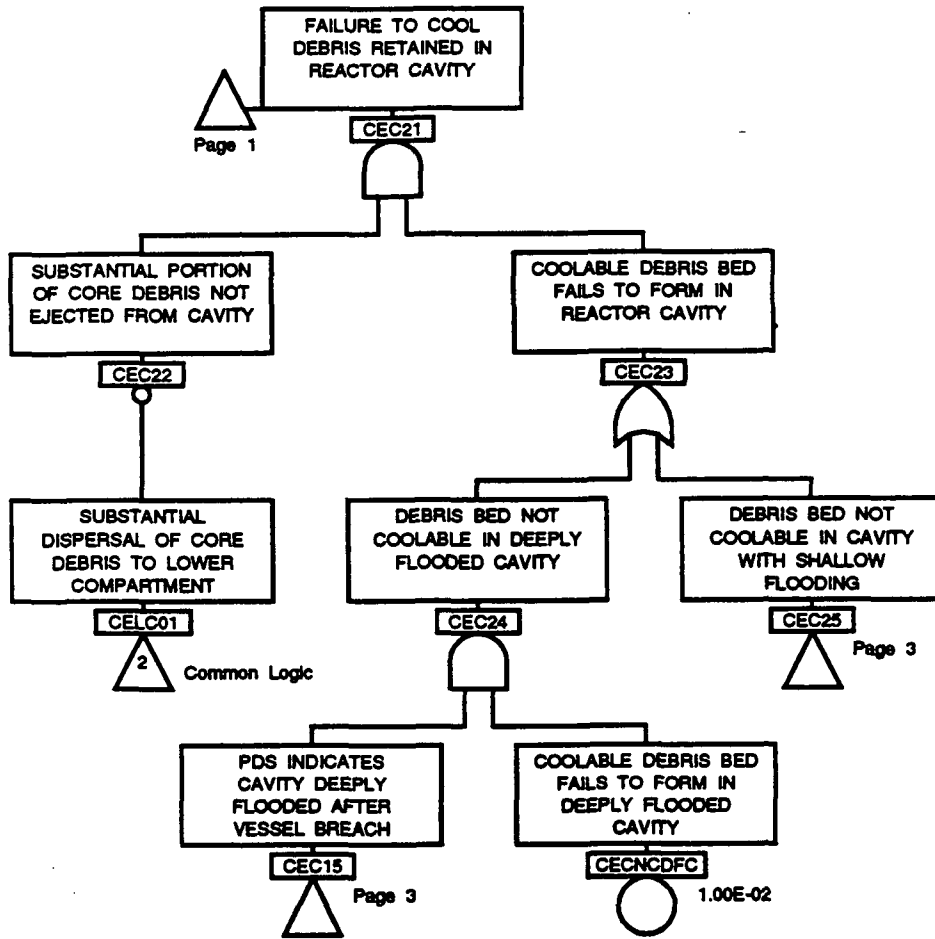


Figure 5-9. Logic for Failure of CET Event C—Core Debris Fails to be Cooled Ex-Vessel (page 2 of 3)

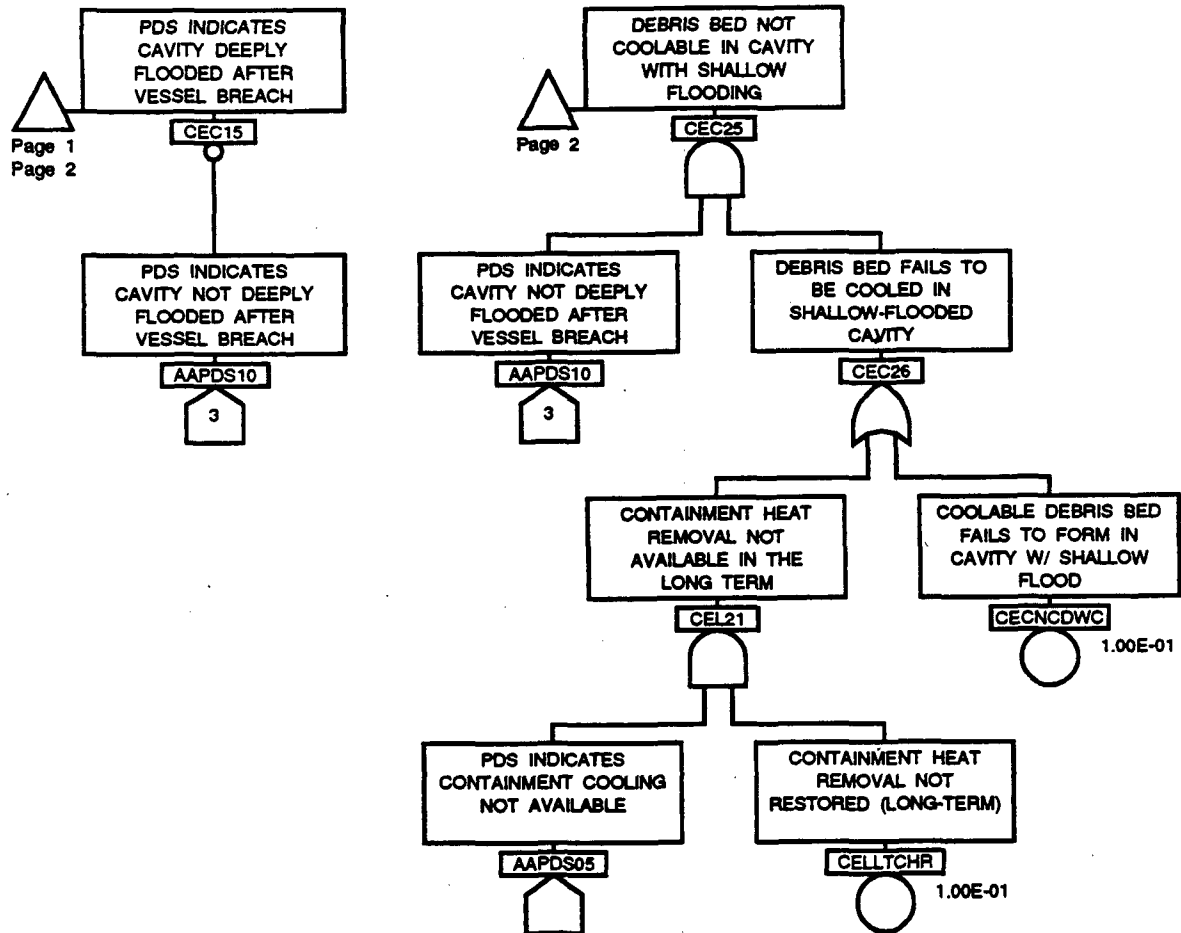


Figure 5-9. Logic for Failure of CET Event C—Core Debris Fails to be Cooled Ex-Vessel (page 3 of 3)

the extent to which the debris would spread after transport to the lower elevation. If it were arbitrarily assumed that the debris spread over only half the nominal area, a depth greater than 1 ft would result, and the debris bed might not be coolable. To account for uncertainty both in the potential for forming a coolable debris bed and in the assessment of the spread area, it was assumed that the failure to form a coolable debris bed in the lower elevation with overlying water was "very unlikely," rather than impossible.

For the cases in which the BWST contents were not injected into containment, the only water in the lower elevation would be that entrained with the core debris as it was transported through the instrument tunnel. This water could cause the debris to be quenched initially, but it would tend to dry out and heat up. Calculations using MAAP indicate that, in this circumstance, decay heat would typically be low enough that convective cooling and radiative heat transfer would be sufficient to prevent ablation of the concrete floor in the lower elevation. There is substantially more uncertainty regarding the degree to which the corium would remain frozen under these conditions. In most prior assessments, it was assumed that a debris bed with no overlying water would not be coolable. In this case, the probability of a coolable debris bed was taken as "indeterminate" to reflect uncertainty in the MAAP models for heat transfer and debris-bed configuration.

The third case cited above involves conditions in which the corium was largely retained in the reactor cavity. At Davis-Besse, the drains from the basement lead to the containment normal sump, which is located at the cavity elevation. Therefore, unless the accident involved a bypass that left the cavity essentially dry, there would be a substantial amount of water overlying the debris, even if the contents of the BWST were not injected. The spread area for the cavity is relatively large, and the nominal depth of debris would be expected to be about 10 inches. There is, however, uncertainty with respect to whether the debris bed would be in a coolable configuration, since the nominal depth could be slightly higher than 10 inches. It was judged that the probability of failure to form a coolable debris bed for this case, with a deeply flooded cavity, could be characterized as "very unlikely."

If the cavity were flooded only by the water originally in the RCS and core flood tanks (i.e., if the contents of the BWST were not injected), there would be a much shallower overlying depth of water. There would be good pathways for the transfer of heat from the cavity to the containment. If containment heat removal were available, the steam generated by cooling of the debris would tend to condense and drain back to the cavity. It was judged that this would be less likely to produce a coolable debris bed than for the case in which the cavity was deeply flooded. Therefore, the failure to form a coolable debris bed given shallow flooding in the cavity was taken to be "unlikely." If containment heat removal were not available, the debris in the cavity would tend to dry out (before or after overpressurizing containment). It was assumed that, for the case in which debris was retained in the cavity, the cavity was not deeply flooded, and containment heat removal was not available, ablation of the concrete would initiate when the debris dried out. The probabilities for the basic events associated with top event C are summarized below.

**Quantification of Basic Events for Failure
of Debris Bed Coolability (Top Event C)**

PDS/Case	Description	Assessment	Probability
CECNCDWD: coolable debris bed fails to form in flooded lower elevation			
All	All relevant damage states (i.e., with dispersal to basement and injection of BWST)	very unlikely	0.01
CECNCDDD: coolable debris bed fails to form in unflooded lower elevation			
All	All relevant damage states (i.e., with dispersal to basement but no injection of BWST)	indeterminate	0.5
CECNCDFC: coolable debris bed fails to form in deeply flooded reactor cavity			
All	All relevant damage states (i.e., with retention in cavity and injection of BWST)	very unlikely	0.01
CECNCDWC: coolable debris bed fails to form in reactor cavity with shallow flooding			
All	All relevant damage states (i.e., with retention in cavity and containment heat removal but no injection of BWST)	unlikely	0.1

5.2.7 Event D: No Failure of Containment Side Wall

If core debris were dispersed from the reactor cavity into the basement, it would be possible for sufficient debris to come into contact with the containment pressure boundary to cause failure. At Davis-Besse, the lower elevation of containment which would receive much of the dispersed debris (via the incore instrument tunnel) is near the wall of the containment vessel. The containment emergency sump is also located in this area. The steel containment vessel is protected by a concrete curb at the basement floor. This curb is 1.5 ft thick and 2.5 ft high. Therefore, for a substantial amount of debris to come into contact with the steel vessel directly, it would have to be blown preferentially against the wall and remain there. Given the velocity and viscosity of the debris and entrained water as it is postulated to leave the instrument tunnel, this is judged to have a negligible probability.

If a coolable debris bed were to fail to form, however, the concrete curb could be ablated, and the containment vessel would then be exposed to direct attack by the molten debris. This could lead to failure in a relatively long time; i.e., it would take a period of at least a few hours to heat up the debris (which would be quenched initially after ejection from the reactor vessel) and to ablate 1.5 ft of concrete. If the containment vessel were to be breached at that level, there would be a release path near the bottom of the annulus between the containment and shield building. Thus, as indicated in Figure 5-10, for cases in which the

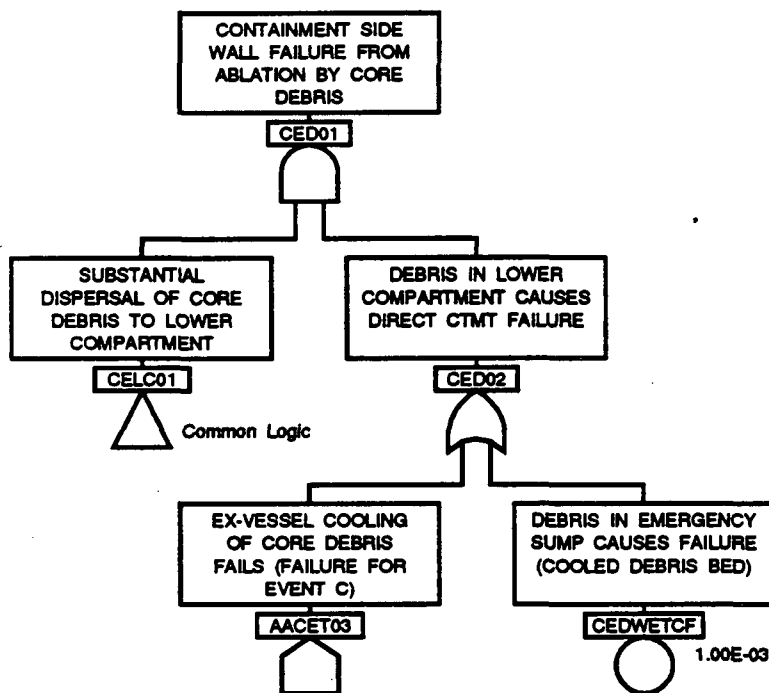


Figure 5-10. Logic for Failure of CET Event D—Containment Side Wall Failure from Ablation by Core Debris

debris was dispersed to the lower elevation and a coolable debris bed failed to form, direct, ablative failure is assumed to occur eventually (i.e., failure for event D).

Another possibility for failure due to contact with core debris would be due to a failure within the emergency sump. Steel plate forms a seal between the emergency recirculation piping and a guard pipe that surrounds it. The guard pipe passes through the foundation of the shield building, and is therefore embedded in concrete. The pressure boundary is extended to a point beyond the shield building, where the recirculation piping enters the auxiliary building. For core debris to cause failure at that point, there would have to be a pool of debris in the emergency sump sufficiently deep that it could not be cooled, and that would cause failure of the sealing flange inside the sump, permit molten debris to flow down to the point at which the pressure boundary would be reached, and to cause failure at that point (some 10 ft from the entrance to the guard pipe in the sump). This distance relative to the length of piping would provide a very limited view factor for radiative heating of the pressure boundary. In addition, it would be extremely unlikely that there would be sufficient debris present in the sump such that it could flow to a point near the outer end of the guard pipe without freezing. Therefore, this potential for failure, given there is substantial debris in the lower compartment that is otherwise cooled, is assessed to be "remotely possible.". The corresponding probability for event CEDWETCF is 0.001.

5.2.8 Event L: Late Failure of Containment Prevented

If the containment were to remain intact through the phenomena described in the preceding sections, there would still be the chance that continued interactions could lead to a late failure. As shown in the supporting logic provided as Figure 5-11, three primary possibilities were investigated with respect to late failure of containment (failure for event L).

The first possibility would result from the unavailability of containment heat removal. Decay heat generated by the core debris would continue to cause steam to be generated (if the debris were being cooled), or would cause non-condensable gases to build up (in the case of core-concrete interactions). Without containment cooling, the containment would eventually be overpressurized. Because it would take a very long time for this to occur (on the order of tens of hours, depending largely on the length of time for which core cooling was initially available following the initial shutdown), there would typically be an opportunity for heat removal to be restored if it was initially unavailable. The dominant causes of failure of cooling via the containment air coolers included loss of service water and unavailability of electric power. Recovery of each as a function of time was considered in the front-end analyses, but generally for periods much shorter than would be of interest with respect to containment response. The distribution of non-recovery times for ac power would not be directly applicable, since it is likely that dc power would have to be restored before recovery of ac power could be attempted. Therefore, a single event was defined to reflect failure to recover core cooling in the long term. It was judged to be "unlikely" that heat removal would not be recovered in time to preserve containment integrity during long-term heatup.

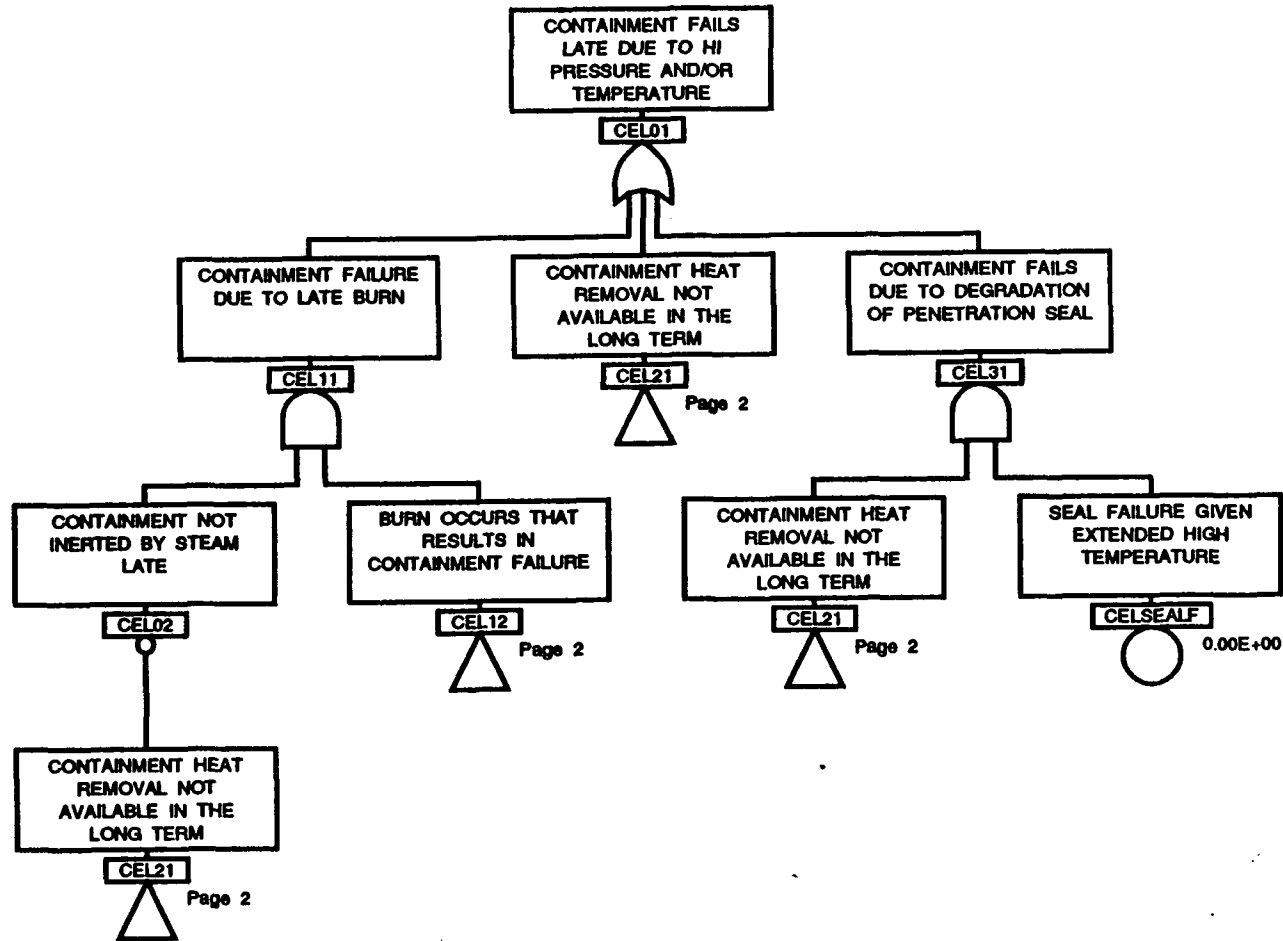


Figure 5-11. Logic for Failure of CET Event L—Late Containment Failure (page 1 of 2)

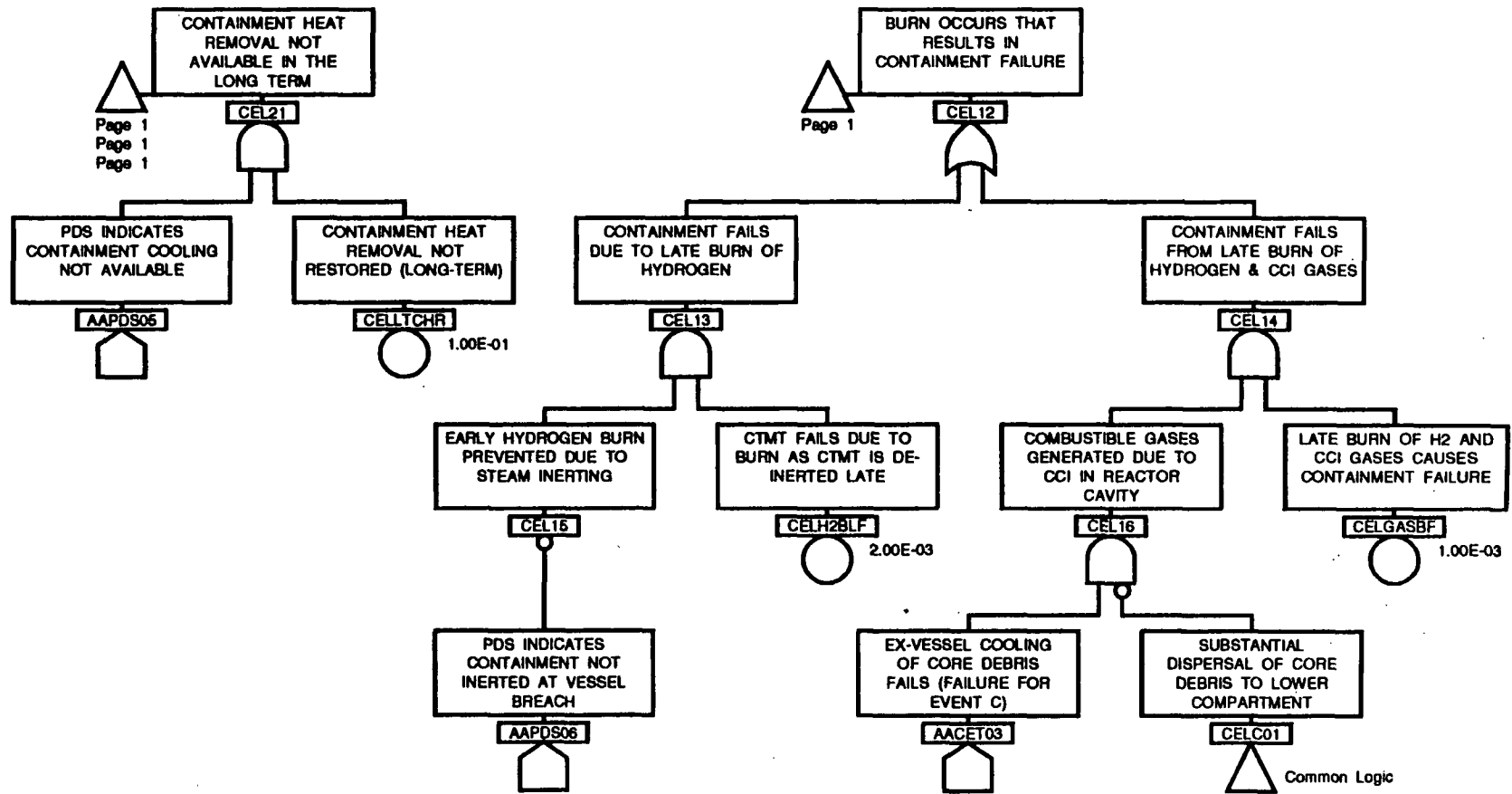


Figure 5-11. Logic for Failure of CET Event L—Late Containment Failure (page 2 of 2)

The possibility that the effects of a severe accident could cause failure of the containment air coolers was also considered. For some plants, the potential for a hydrogen burn to lead to failure of fan coolers has been addressed. For Davis-Besse, the likelihood of large global burns is very low, and the impact on the containment air coolers is expected to be small. The probability of failure of the air coolers is therefore judged to be negligible compared to the fraction of the plant-damage states for which they would be unavailable due to other causes. The effectiveness of the air coolers in preventing overpressurization of the containment as a consequence of the buildup of non-condensable gases generated by core-concrete interactions was also considered. It is possible that the non-condensable gases could cause the air coolers to operate at significantly reduced efficiency. The air coolers, however, have substantial margin above their design basis. Therefore, it is expected that they would provide sufficient heat removal from containment that the containment would not be overpressurized by non-condensable gases before meltthrough of the basemat.

The second possibility for late containment failure is for a burn to lead to overpressurization of containment. Two types of burns were considered. If the containment were inerted by steam early in the accident, it is possible that the availability (or restoration) of containment heat removal could lead eventually to condensation of sufficient steam that inerting would be lost. If this were the case, a global burn of the hydrogen in the containment could occur that might overpressurize containment. To investigate this potential, burn calculations were performed for a postulated set of containment conditions in which the containment atmosphere would be at relatively high temperature and pressure, but not inert due to steam. The resulting distribution was combined with the distribution for containment capacity. In this case, the distribution associated with the potential reduction in the strength of the steel containment vessel due to elevated temperature was applied (refer to Section 4 for a discussion of the effects of extended elevated temperature on containment strength). A combined probability of a late burn and resulting containment failure of about 0.002 was calculated for this condition. This probability was used to bound all of the cases in which the containment was predicted to be inert at the time of vessel breach, but for which containment heat removal was available late.

The other way in which a burn might threaten containment could be the case in which the core debris was not cooled, such that the ablation of concrete produced carbon monoxide. The carbon monoxide, in combination with hydrogen generated by the oxidation of core materials, could burn late and lead to overpressurization. For this to be of concern, containment heat removal would typically need to be available (since there would otherwise be sufficient steam in the containment atmosphere to ensure inerting, even without injection of the BWST contents). In addition, sufficient combustible gases would have to accumulate to produce a burn large enough to threaten containment (i.e., there would have to be little or no localized burning of combustible gases as they were generated). It is considered to be very unlikely that the containment would fail due to the burning of a large quantity of hydrogen and carbon monoxide, especially since base pressure would need to remain relatively low to permit a flammable mixture to form. Moreover, the lower flammability limits for carbon monoxide

are higher than those for hydrogen. Therefore, an effectively larger concentration would be required for the mixture of combustible gases in containment for global burning to take place. It is considered to be unlikely that a large quantity of combustible gases would collect before at least a portion was ignited locally (e.g., in the cavity or other location where the gases were produced). Therefore, the overall probability of failure due to a late burn of hydrogen and carbon monoxide was assessed to be "remotely possible."

The final possibility for late containment failure involved consideration of the potential for degradation of penetration seals due to long-term exposure to high temperatures. As described in Section 4, this was investigated and determined not to be a limiting failure mechanism for the containment. Therefore, the corresponding event in the supporting logic was assessed to be "impossible." The basic events for event L are summarized below.

Quantification of Basic Events for Late Containment Failure (Top Event L)

PDS/Case	Description	Assessment	Probability
CELSEALF: penetration seal failure due to extended exposure to high temperature			
All	All plant-damage states	impossible	0.0
CELH2BLF: containment fails due to hydrogen burn as containment is de-inerted			
All	All relevant damage state (i.e., early inerting and containment heat removal available late)	calculated	0.002
CELGASBF: late burn of hydrogen and gases generated by core-concrete interactions causes containment failure			
All	All relevant damage state (i.e., containment heat removal and failure of ex-vessel core cooling)	remotely possible	0.001
CELLTCHR: failure to restore containment heat removal (long-term)			
All	All relevant damage state (i.e., with containment heat removal not initially available)	unlikely	0.1

5.2.9 Event F: No Late Revaporization Release

During core degradation, it is expected that much of the fission products released from the fuel would tend to plate out on the relatively cooler surfaces of the RCS. These fission products might, later in the accident, revaporize and be released from the RCS, with the potential for a larger release to the environment. The revaporization could occur as a result of the self-heating of the fission products as they decay, and may be promoted by the flow of very hot gases past the surfaces to which they adhere. Event F is included in the CET to

reflect the potential for an increase in the magnitude of release due to this revaporization, although it has no bearing on the manner of containment failure.

Based on the MAAP calculations for Davis-Besse, substantially diminished retention of fission products in the RCS was predicted for a broad range of accidents. These accidents all shared two characteristics: (1) there was a breach in the RCS, and (2) feedwater was not available.

This appears to be generally consistent with the treatment of potential revaporization releases in the analyses supporting NUREG-1150 (Ref. 34). Revaporization was considered to be relevant in that assessment for accidents in which pathways through the RCS existed that would promote natural circulation through the reactor vessel after vessel breach. This flow of gases could cause the revolatilized fission products to be released to the containment. It was judged in that assessment that the primary requirement for this phenomenon was the existence of two substantial holes in the RCS, close enough to each other for natural circulation patterns to develop. The breach of the reactor vessel would be one such hole, and a break elsewhere in the RCS would constitute the second hole. Very small LOCAs were not expected to produce adequate natural circulation to sweep fission products out of the RCS, and an interfacing-systems LOCA was expected to be too far from the breach in the reactor vessel to support natural circulation.

In the calculations specific to Davis-Besse, all accidents in which there was at least a small LOCA provided the necessary flowpath for natural circulation. The only exception was the case in which the small LOCA was the result of seal failures for all four reactor coolant pumps (i.e., four small leaks which, taken together, comprised a very small LOCA). The availability of feedwater appeared to ensure that surfaces remained sufficiently cool that fission products were retained, despite the existence of the flowpath.

The logic supporting occurrence of event F (i.e., that a revaporization release from the RCS does occur late in the accident) is shown in Figure 5-12. In the logic, the two requisites identified above are indicated: there must be a substantial hole in the RCS separate from the vessel breach, and feedwater must fail to support the retention of the fission products.

Existence of an adequate hole is inferred from the pressure in the RCS prior to vessel breach (under gate CEF02). Through the logic under gate CEF05, small LOCAs are discriminated according to whether or not they are the result of seal failures. Event CELSLOCA accounts for the fraction of the core-damage bins involving small LOCAs that are seal LOCAs.

In addition to identifying whether feedwater is available, a basic event is included to reflect uncertainty in the phenomena that could lead to a late revaporization release. There may be some chance that such a release could occur, despite the provision of feedwater to the steam generators (e.g., due to the specific location of the break in the RCS). It is judged that it is "unlikely" that the cooling available in the steam generators would fail to cause significant retention of fission products in the RCS (event CEFRVSGC). The probabilities for the basic events associated with top event F are summarized in the tabulation that follows.

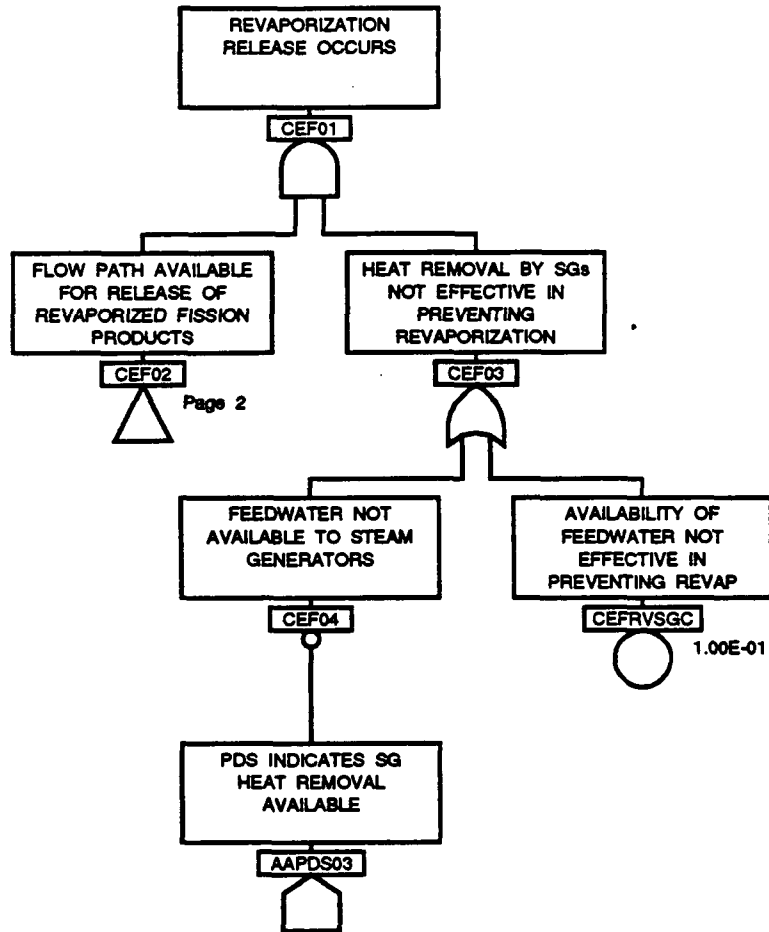


Figure 5-12. Logic for Failure of CET Event F—Late Revaporization Release from RCS (page 1 of 2)

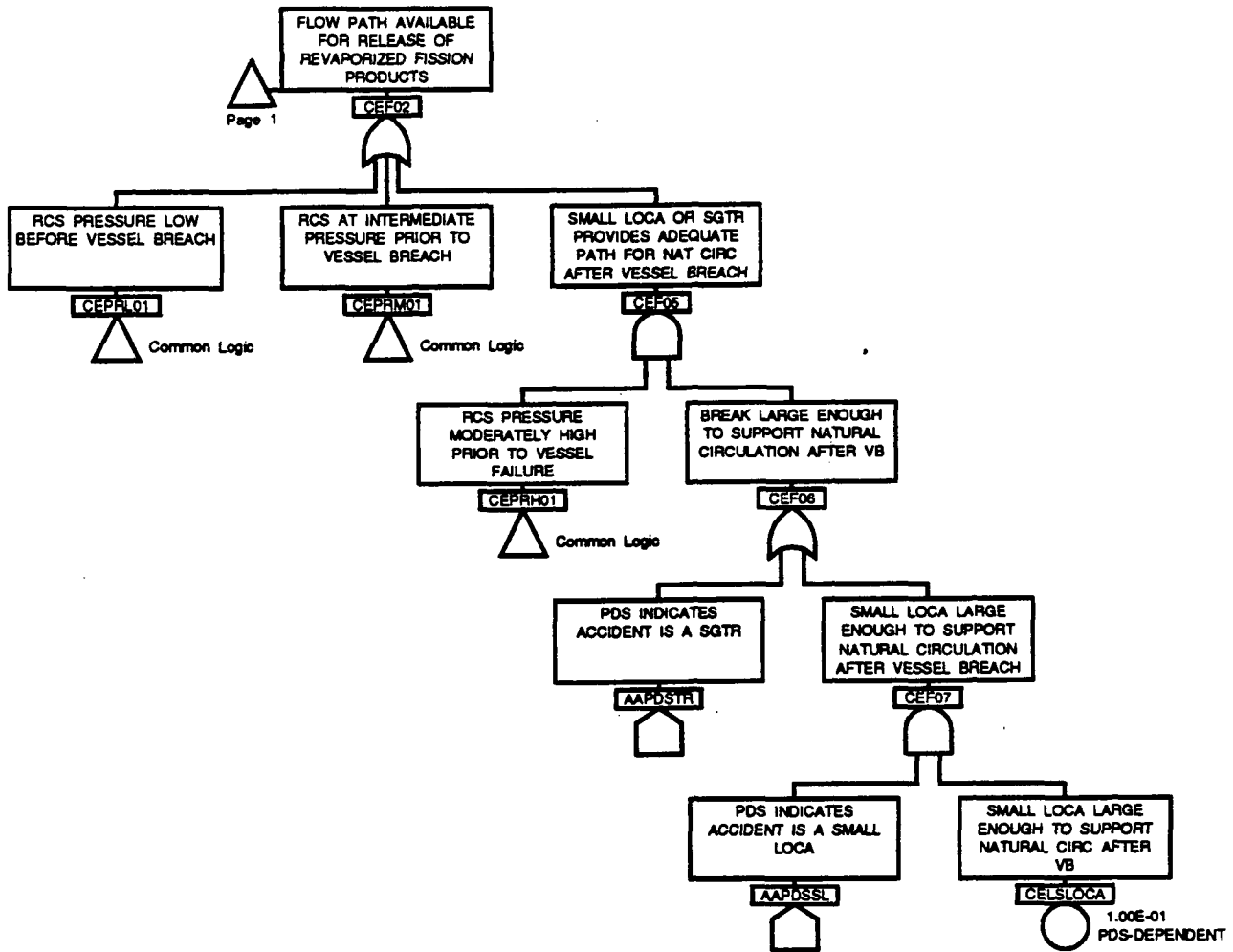


Figure 5-12. Logic for Failure of CET Event F—Late Revaporization Release from RCS (page 2 of 2)

**Quantification of Basic Events for Occurrence
of Late Revaporization Release (Top Event F)**

PDS/Case	Description	Assessment	Probability
<u>CESLOCA: small LOCA large enough to support natural circulation after vessel breach</u>			
SRYYFYCD	Small LOCA damage state	per cut sets	0.02
SRYYFYD	Small LOCA damage state	per cut sets	0.46
SRYYFYYN	Small LOCA damage state	per cut sets	0.02
SRYYFRCD	Small LOCA damage state	per cut sets	0.30
SRYYFRYD	Small LOCA damage state	per cut sets	0.11
SIYYFYCD	Small LOCA damage state	per cut sets	0.92
SIYYFIND	Small LOCA damage state	per cut sets	1.0
SIYYFINN	Small LOCA damage state	per cut sets	0.17
SIYYNINN	Small LOCA damage state	per cut sets	0.01
SIYYFICD	Small LOCA damage state	per cut sets	0.92
SINYFYCD	Small LOCA damage state	per cut sets	0.16
SINYFYYN	Small LOCA damage state	per cut sets	0.01
Other small LOCAs	All other plant-damage states involving small LOCAs	per cut sets	0.00
All others	All plant-damage states except small LOCAs	irrelevant	—
<u>CEFRVSGC: availability of feedwater not effective in preventing late revaporization release</u>			
All	All relevant damage states (i.e., two substantial breaches in the RCS)	unlikely	0.1

5.2.10 Event S: Scrubbing of Fission Products

Like event F, event S is included in the CET to distinguish the magnitudes of various releases from containment, rather than to identify the nature of a containment failure mode. Scrubbing of the fission products released from the fuel is considered in two contexts. First, for cases in which there was a release to the containment atmosphere, operation of the containment spray system could remove some fission products from the containment atmosphere. For interfacing-systems LOCAs, the largest release would be expected to take place through the RCS break directly to the auxiliary building. In this case, scrubbing could

effectively be provided either by submergence of the break location, or by holdup and removal processes within the auxiliary building.

The logic for failure of scrubbing (i.e., failure for event S) is provided in Figure 5-13. If the containment sprays were operating, there should be substantial removal of the fission products from the containment atmosphere. This would not be as effective, however, for cases in which there was a large isolation failure. In that case, the containment would not tend to pressurize sufficiently to cause the spray system to be activated. Moreover, fission products could be transported directly to the break from the time they were first released to the containment atmosphere, so that there might be limited holdup and opportunity for scrubbing.

For interfacing-systems LOCAs, it is expected that the break locations would generally be flooded. Core damage for these events would occur after the contents of the BWST were injected. It is judged to be "unlikely" that the break location would not be sufficiently submerged to provide scrubbing. Other removal processes within the auxiliary building were not investigated in detail, and for the fraction of interfacing-systems LOCAs judged not to be submerged, no scrubbing was assumed. While this may tend to overstate the source term somewhat, the frequency of such releases would be dominated by unscrubbed releases resulting from a steam generator tube rupture.

Failure due to ablation of the curb at the lower elevation and resulting contact of debris with the side wall of containment would cause the release to occur into the annular region between the containment vessel and the shield building. Containment failures due to overpressurization would also release to this region. Gases released to this annulus could be filtered by the emergency ventilation system, which draws air from the annulus and penetration rooms and discharges through filters. No reduction in the release fractions, however, was assessed as a consequence of this mechanism for scrubbing.

Thus, the only basic event for which quantification was required with respect to top event S was event CESISLNS, which was assessed a probability of 0.1 for all plant-damage states in which the spray system was available.

5.2.11 Common Supporting Logic for Top Events

Several of the phenomena and conditions associated with the response of containment to a severe accident affect more than one of the top events in the containment event tree. To ensure that the logic associated with these phenomena or conditions is consistent for the different top events, a single set has been assembled, and is described in this section. Specifically, the logic that reflects the various pressure regimes in the RCS prior to failure of the reactor vessel and that for dispersal of core debris to the lower elevation (or basement) are addressed in this section.

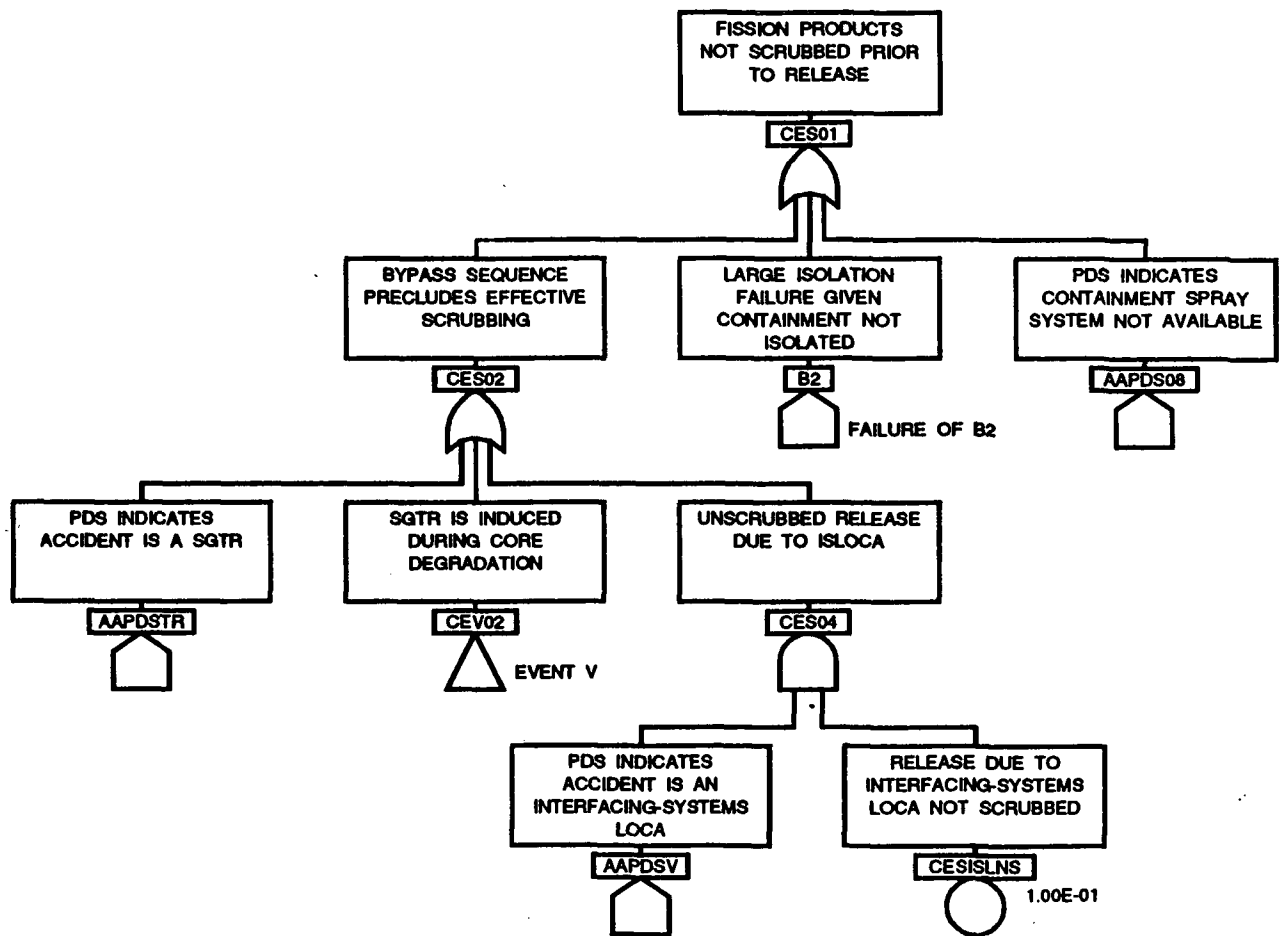


Figure 5-13. Logic for Failure of CET Event S—Fission Products Not Scrubbed Prior to Release

RCS Pressure Prior to Vessel Breach

The pressure in the RCS prior to failure of the reactor vessel due to a severe accident can influence several important aspects of subsequent containment response. For purposes of this analysis, accidents have been assigned to four ranges of pressure:

- Very high, with the pressure at or near the setpoint for the pressurizer relief valves (i.e., about 2500 psig);
- Moderately high, with pressure about 1500 to 2000 psig;
- Intermediate, nominally at about 1000 psig; and
- Low, a few hundred psig or less.

The types of accidents that fall into each of these ranges and their implications with respect to the containment event tree are summarized in Table 5-2. These implications are discussed further in previous sections, as they relate to particular top events of the containment event tree.

The potential that the accident would progress at low pressure is developed under gate CEPRL01, as shown in Figure 5-14. As this logic indicates, low pressure prior to vessel breach would result from a large LOCA or from other events in which the RCS was depressurized after the initiator. Three alternatives for depressurizing the RCS are developed in the logic under gate CELPR02:

- Depressurizing the steam generators to reduce RCS pressure,
- Failure of the RCS pressure boundary due to creep rupture, or
- Opening of the PORV for certain types of accidents.

Only for medium and small LOCAs (including SGTRs and transient-induced LOCAs) would the first alternative be relevant with respect to reducing RCS pressure sufficiently to correspond to the low category for pressure prior to vessel failure. For large LOCAs, as already noted, depressurization would be implicit. For transients which would not result in LOCAs prior to core damage, core damage would only result if feedwater were not available. Therefore, depressurization using the steam generators would be precluded.* For medium and small LOCAs, depressurization could fail in the event of either the unavailability of feedwater to the steam generators or the failure to accomplish the depressurization in a timely manner.

The availability of feedwater is addressed explicitly in the core-damage bins for small LOCAs and SGTRs. It was not considered explicitly for medium LOCAs, but it is very likely

*One core-damage sequence in which feedwater might be available would entail a failure to achieve shutdown, including failure of emergency boration. The relatively high power level would, however, preclude substantial depressurization of the RCS prior to vessel breach.

**Table 5-2
RCS Pressure Ranges of Interest Prior to Vessel Breach**

Category	Nominal Range	Types of Accidents Included	Implications in Containment Event Tree
Very high	2500 psig	<ul style="list-style-type: none"> • Transients and no feedwater, or failure to scram 	<ul style="list-style-type: none"> • Maximum potential for pressurized melt injection • Maximum potential for inducing creep rupture of RCS hot leg or steam generator tube • Retention of hydrogen in RCS prior to vessel breach • Potential to suppress in-vessel steam explosion
Moderately high	1500 - 2000 psig	<ul style="list-style-type: none"> • Small LOCA without feedwater • SGTR without feedwater 	<ul style="list-style-type: none"> • Potential for pressurized melt ejection • Potential for inducing creep rupture of RCS hot leg • Potential to suppress in-vessel steam explosion
Intermediate	1000 psig	<ul style="list-style-type: none"> • Medium LOCA • Small LOCA and feedwater, or opening of PORV • SGTR and feedwater, or opening of PORV • Transient and opening of PORV, or stuck-open PSV 	<ul style="list-style-type: none"> • Potential for pressurized melt ejection • Small potential for inducing creep rupture in RCS • Potential to suppress in-vessel steam explosion
Low	<300 psig	<ul style="list-style-type: none"> • Large LOCA • Medium LOCA and blowdown of steam generators, or opening of PORV • Small LOCA and feedwater and opening of PORV, or blowdown of steam generators, or induced hot leg rupture • SGTR and feedwater and opening of PORV, or blowdown of steam generators, or induced hot leg rupture • Transient with induced hot leg rupture 	<ul style="list-style-type: none"> • No potential for pressurized melt ejection • No potential for inducing creep rupture in RCS • Increased potential for in-vessel steam explosion • Potential for earlier release of hydrogen in containment • Reduced holdup of fission products in RCS

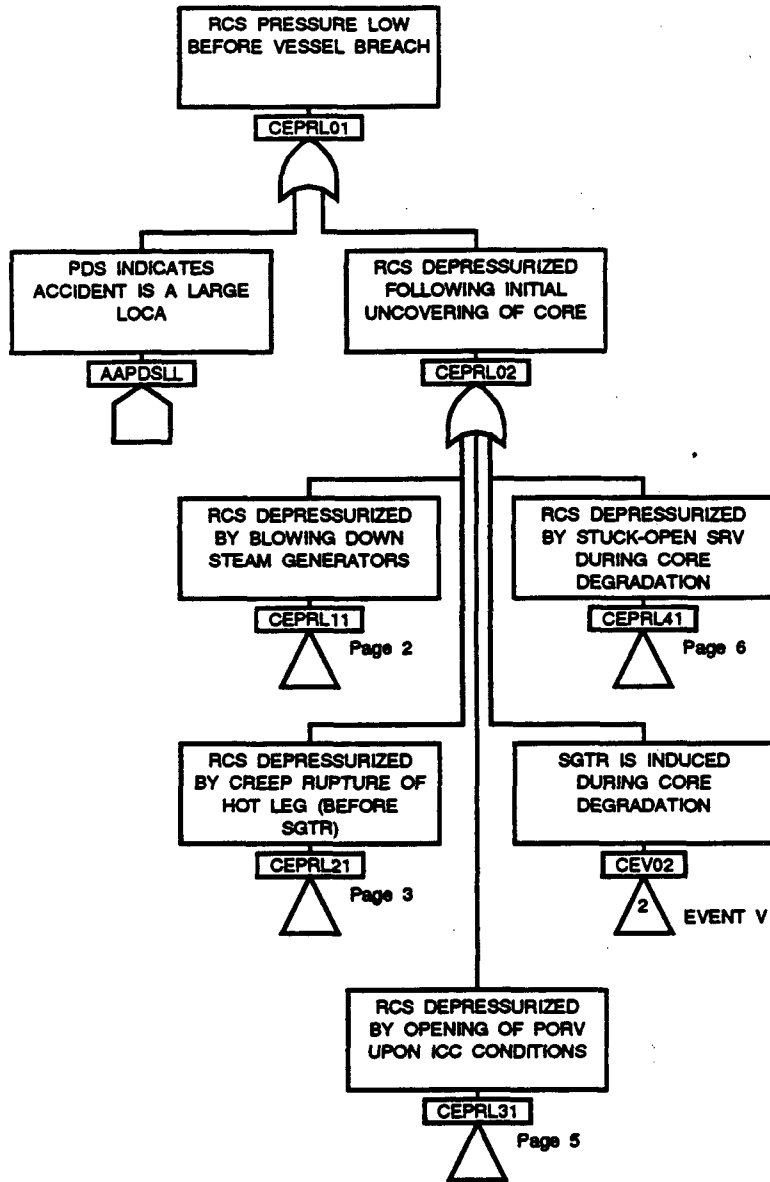


Figure 5-14. Common CET Supporting Logic for Low RCS Pressure Prior to Vessel Breach (page 1 of 6)

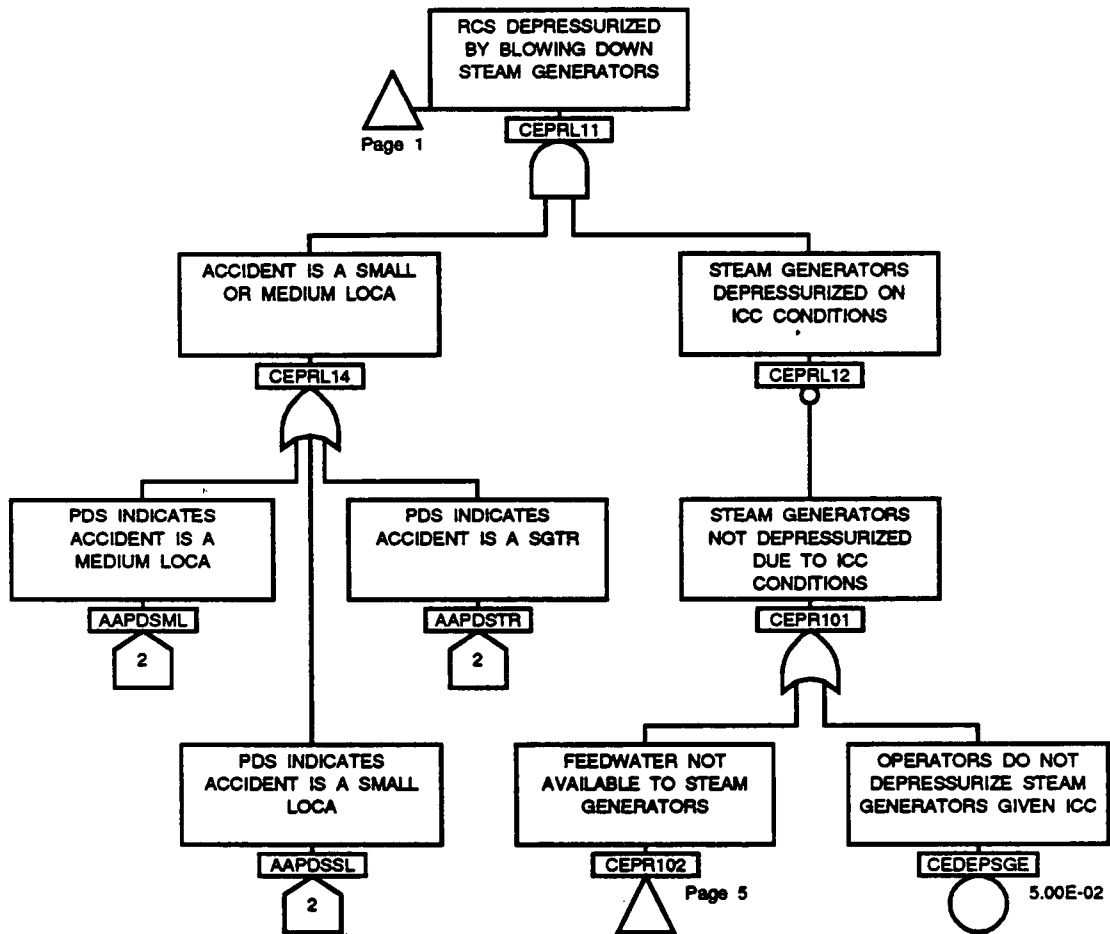


Figure 5-14. Common CET Supporting Logic for Low RCS Pressure Prior to Vessel Breach (page 2 of 6)

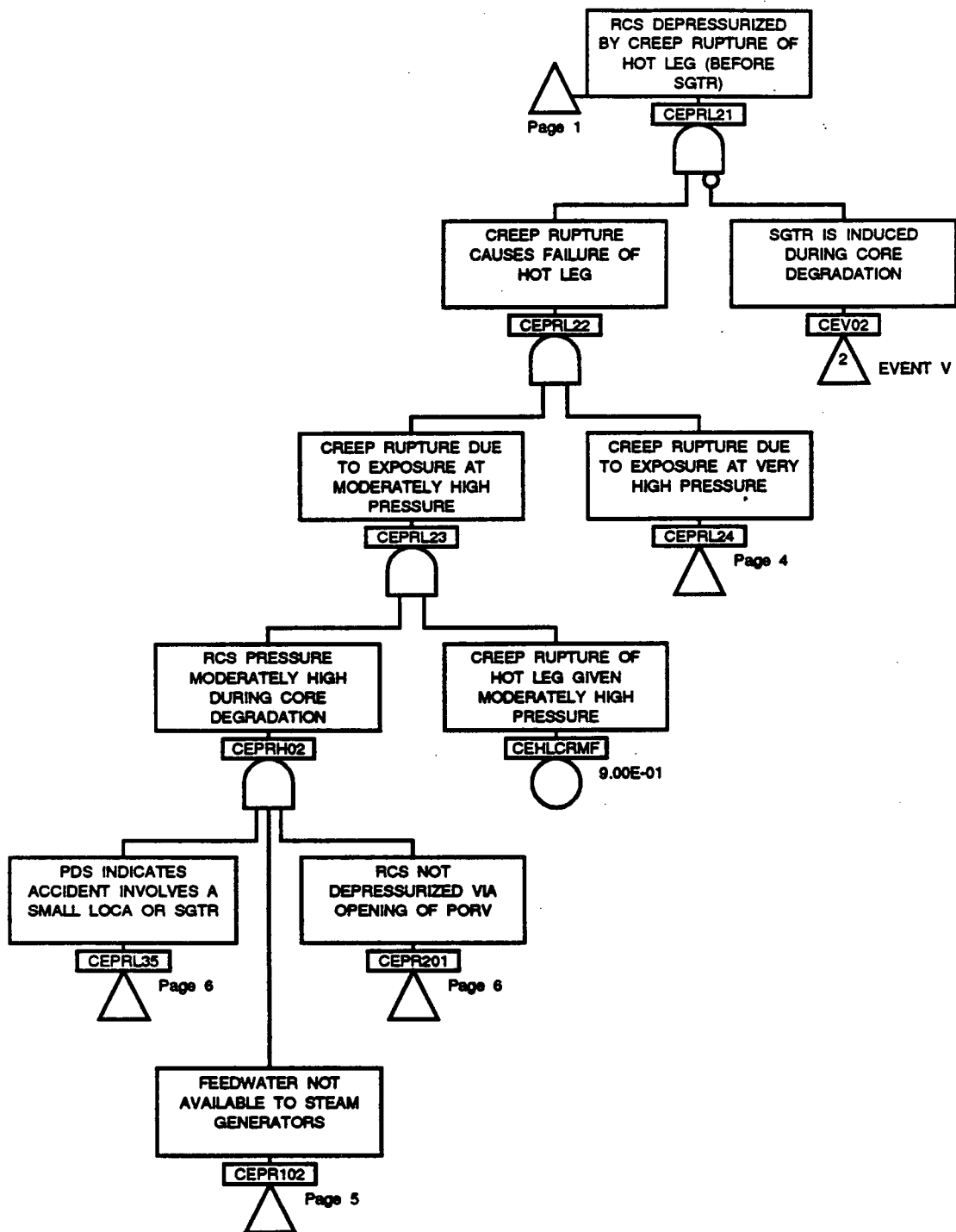


Figure 5-14. Common CET Supporting Logic for Low RCS Pressure Prior to Vessel Breach (page 3 of 6)

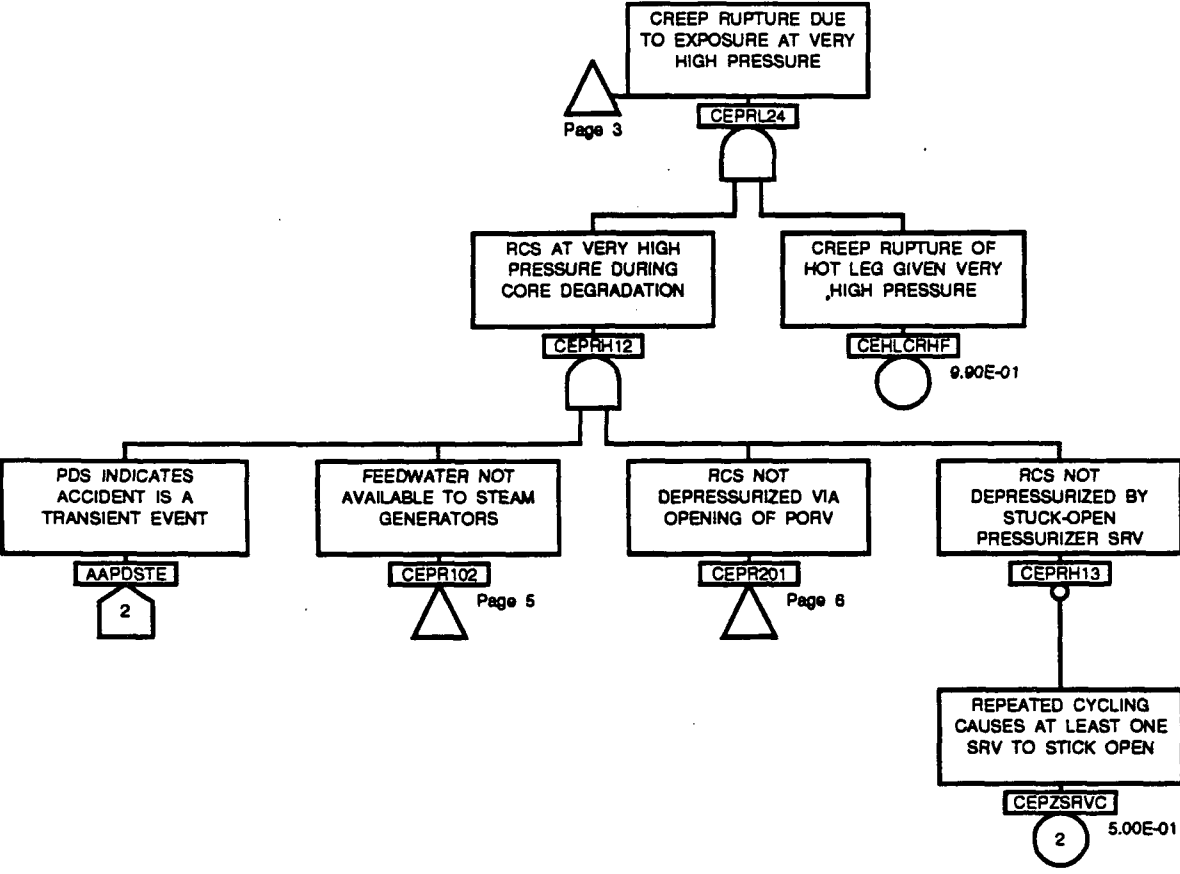


Figure 5-14. Common CET Supporting Logic for Low RCS Pressure Prior to Vessel Breach (page 4 of 6)

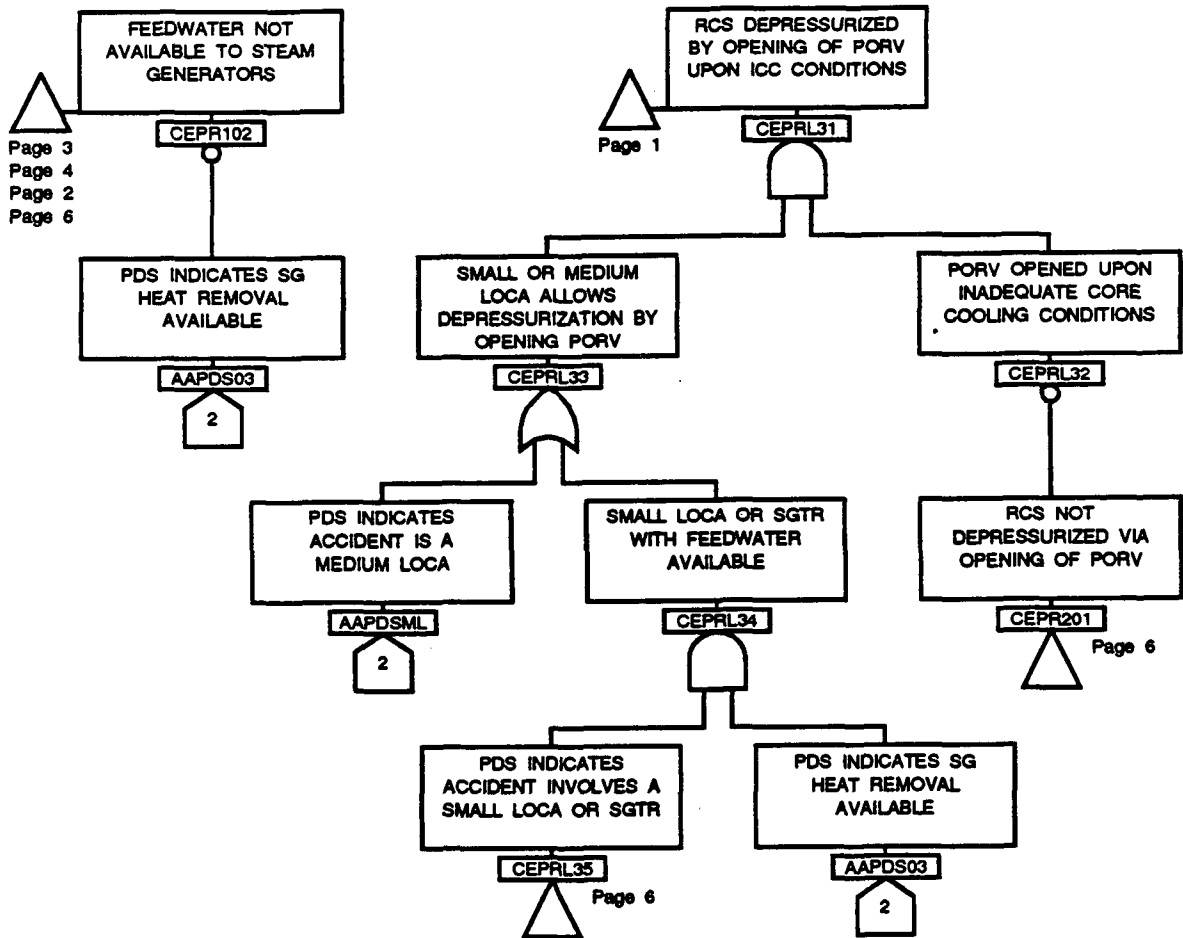


Figure 5-14. Common CET Supporting Logic for Low RCS Pressure Prior to Vessel Breach (page 5 of 6)

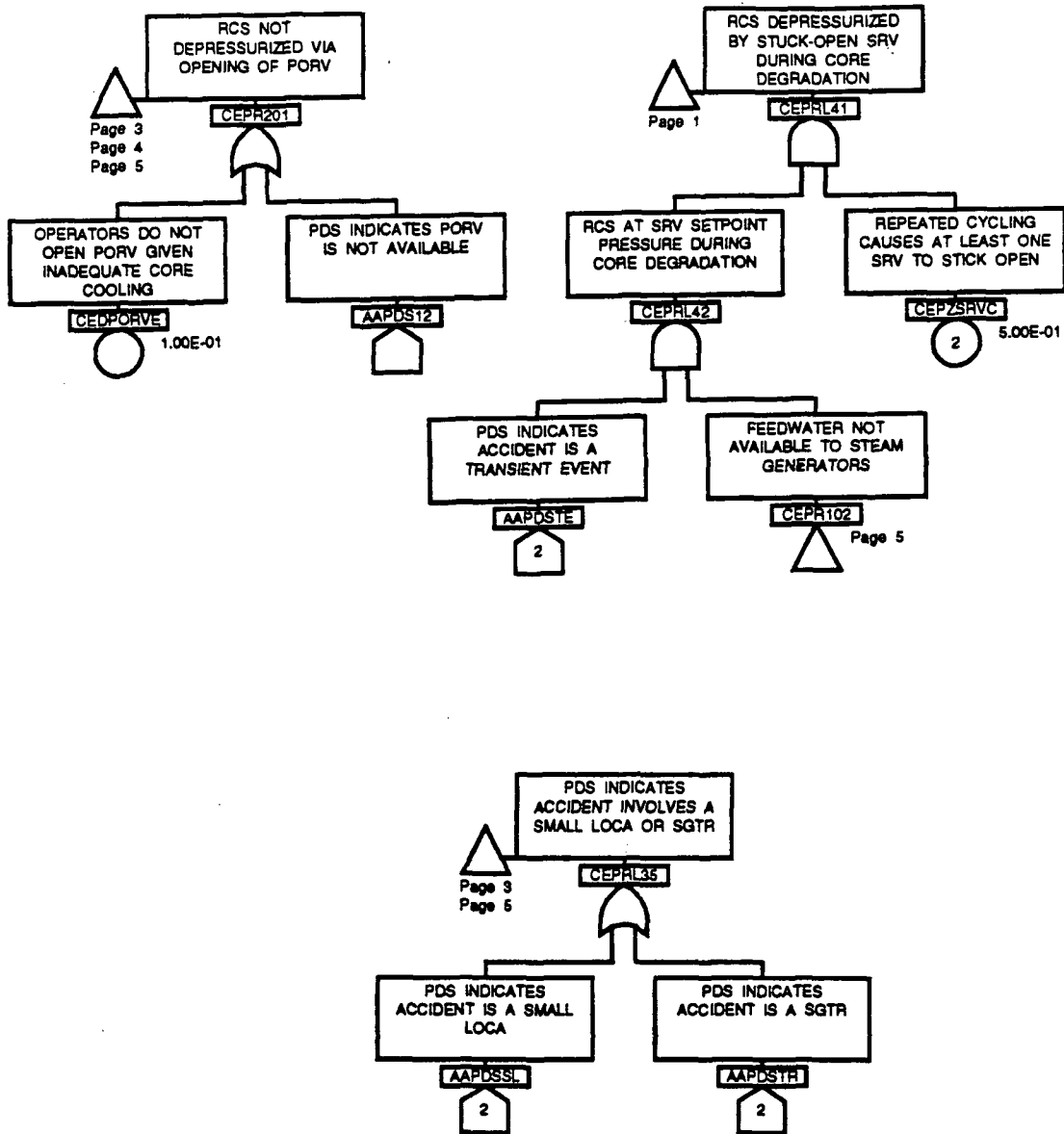


Figure 5-14. Common CET Supporting Logic for Low RCS Pressure Prior to Vessel Breach (page 6 of 6)

that AFW flow would be available for these sequences. Given the availability of feedwater, it is expected that some means would be available to the operators to depressurize the steam generators, so that failure of the operating crew to act was judged to be the dominant contributor to failure to depressurize (i.e., the additional hardware failures were assumed to be negligible).

The failure of the operators to act is indicated in the logic development by event CEDEPSGE. This event refers specifically to actions in response to instructions in the emergency procedure for inadequate core cooling (ICC) to initiate depressurization (Ref. 33). The indications of ICC conditions and the procedural instructions are both reasonably clear, so that the operator action should be relatively reliable. For most small LOCAs, however, at least some level of credit for operator action to maintain or recover core cooling is already reflected in most of the sequence cut sets. Considering the additional opportunities for action presented by the ICC procedure and the additional time available to initiate depressurization, it is judged that failure of the operator action is, in general, coupled to the sequence cut sets via low dependence. Based on the methods discussed in Section 3.2 of Part 3, this implies a conditional probability of failure of the operator action no lower than 0.05. For medium LOCAs, there are relatively few operator actions represented in the sequence cut sets for failure of injection. It is judged to be "very unlikely" that the operators would fail to attempt depressurization of the steam generators under these conditions.

The second mechanism for depressurization of the RCS is associated with creep rupture of the RCS. The potential exists for exposure to elevated temperatures and pressures for a significant period of time to lead to creep rupture of the RCS pressure boundary prior to failure of the reactor vessel. The potential for a creep rupture of the RCS depends on the temperatures of the gases in the RCS, on the degree to which these gases are circulated through the RCS, and on RCS pressure. As described in Section 2.2.3, an assessment was made of the susceptibility of various portions of the RCS to creep rupture. The focus of this assessment was on the RCS hot legs and the tubes in the steam generators. In other studies of PWRs, the pressurizer surge line has also been considered as a potential location for creep rupture prior to vessel breach. At Davis-Besse, it is judged that the surge line would be less susceptible to creep rupture than are the hot legs, because it is constructed of stainless steel, which is less susceptible to creep rupture than is carbon steel (of which the hot legs are constructed), and because the surge line would not be exposed to the high temperatures necessary to threaten its integrity unless at least one of the hot legs were as well. The discussion in this section is of the potential for failure of a hot leg that could lead to depressurization of the RCS. The logic and probabilistic treatment associated with creep rupture leading to a SGTR are discussed in Section 5.2.3, which addresses event V of the containment event tree.

For accidents that progressed at relatively high pressures, the temperatures of hot gases would tend to be sufficiently high to cause creep rupture of the hot legs. As indicated in Section 2.2.3, a temperature of 1700 F could cause creep rupture relatively quickly. Because of the thickness of the hot leg piping, a period of 1/2 or more might be required for the outer

portion of the piping to heat up sufficiently to lose strength. It is not certain that this would occur prior to vessel failure. Furthermore, as described in Section 5.2.3, the assessment of the potential for an induced SGTR was made based on the potential for creep rupture of the steam generator tubes prior to failure of a hot leg. Therefore, depressurization by other means or by creep rupture of steam generator tubes would preclude creep rupture of a hot leg. If the RCS were at very high pressure (i.e., about 2500 psig) and not depressurized due to some other mechanism, it was judged to be "very likely" that creep rupture of a hot leg would occur prior to vessel breach. If the pressure were moderately high (1500 to 2000 psig), there is somewhat less confidence that creep rupture would take place before vessel failure. Therefore, creep rupture was assessed to be "likely" for this case.

The possibility that the operators would depressurize the RCS by opening the PORV depends on both the availability of the PORV and the successful decision on the part of the operating crew to open the valve under the ICC guidelines in the emergency procedure. The question of PORV availability is addressed explicitly in the definition of plant-damage states. With respect to operator reliability under these circumstances, the probability of failure would be at least somewhat coupled to the events in the core-damage cut sets since, for virtually all of the accidents that might progress at high RCS pressure, some level of credit would already be reflected for operator action to prevent core damage. As in the previous case, it is judged that at least low dependence would apply, suggesting a minimum probability of failure of 0.05. It is also reasonable to assume that, by this point in the accident, the level of stress on the operators could be higher than would be the case during earlier phases of the accident. Therefore, it is reasonable to characterize the probability that the operators would fail to open the PORV when instructed to do so under the inadequate core cooling guidelines as "unlikely." A more detailed breakdown according to the details of the cut sets for the plant-damage states is not judged to be warranted, in light of the degree of uncertainty that would be inherent to any such assessment.

Accidents that would progress at intermediate pressure (nominally about 1000 psig) would include medium and small LOCAs for which feedwater was available but there was no further attempt to depressurize the RCS by reducing steam pressure or opening the PORV. The logic for this case (using top event CEPRM01) is shown in Figure 5-15. Note that the development in this case simply indicates that if the pressure does not correspond to one of the other three levels of interest, it must be intermediate.

Moderately high pressure (about 1500 to 2000 psig) would exist for small LOCAs or SGTRs for which feedwater was not available and no other means of depressurization existed. The logic corresponding to this pressure condition is shown in Figure 5-16. RCS pressure could be lowered by either opening of the PORV or by a creep rupture.

Very high pressure (nominally about 2500 psig, near the setpoints for the PORV or pressurizer safety valves) would only exist for a transient condition with no feedwater. In this case, in addition to the potential that the RCS could be depressurized due to a creep rupture or opening of the PORV, it is possible that continued cycling of the pressurizer safety valves could cause at least one to stick open. Because of the very high temperatures of the steam

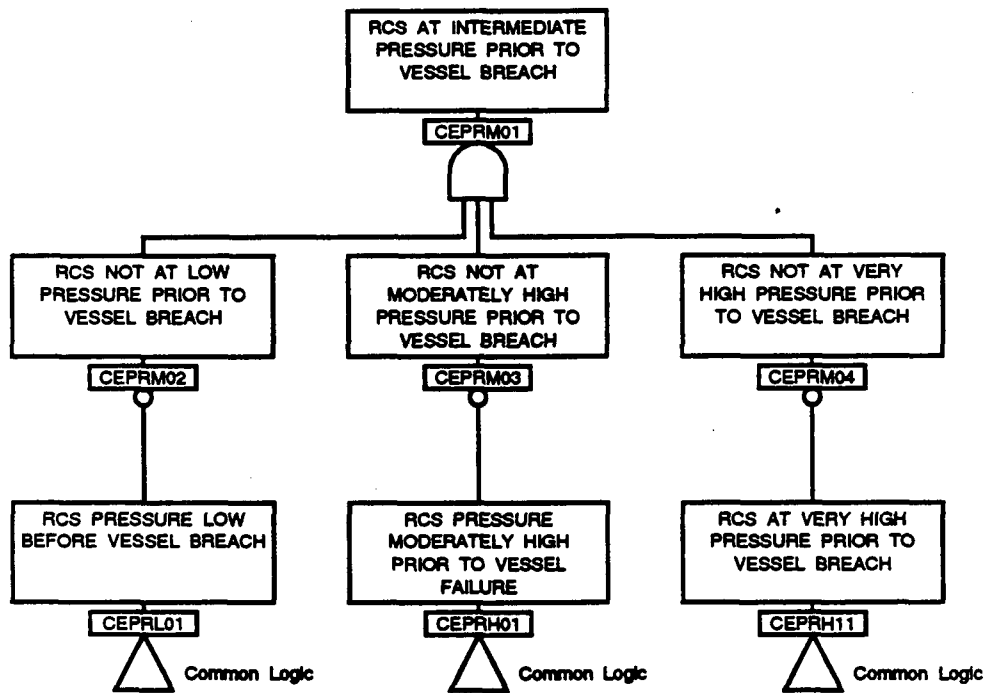


Figure 5-15. Common CET Supporting Logic for Intermediate RCS Pressure Prior to Vessel Breach

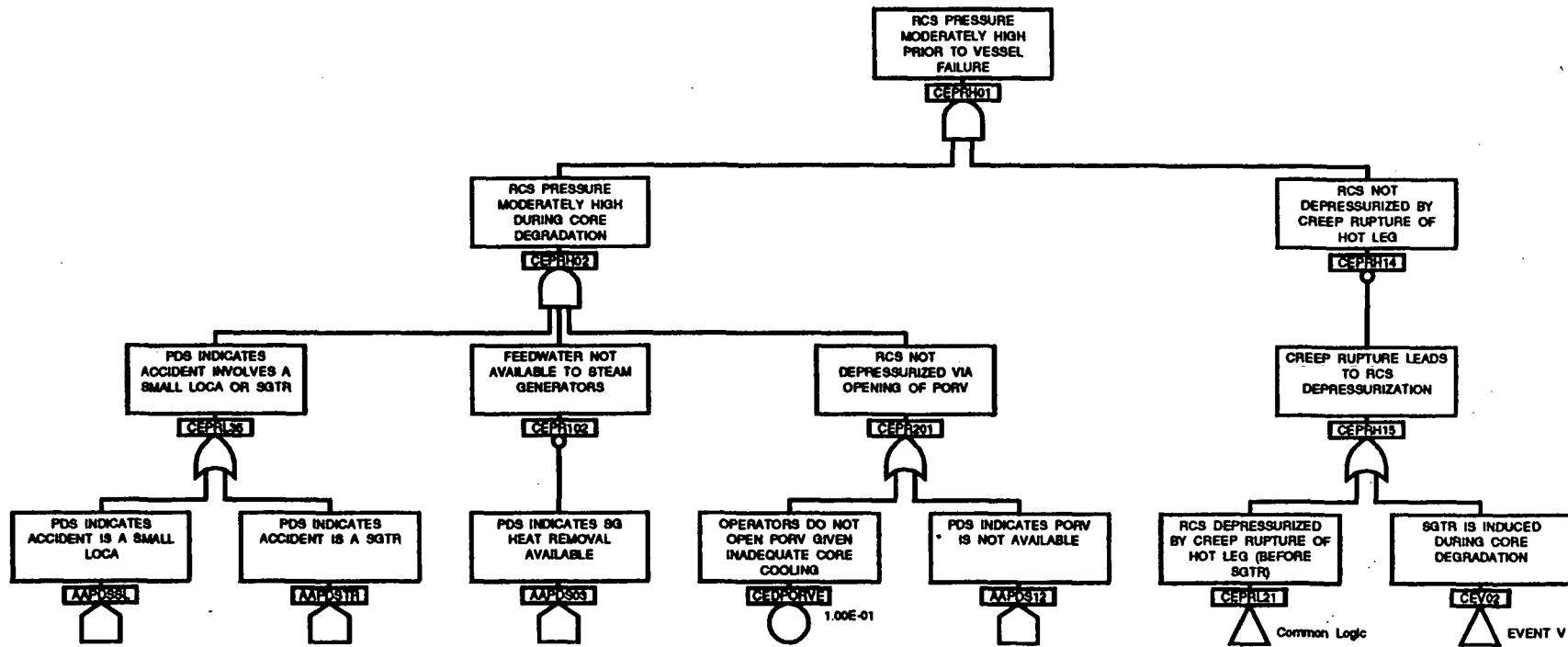


Figure 5-16. Common CET Supporting Logic for Moderately High RCS Pressure Prior to Vessel Breach

that would be exiting the relief valves during core degradation and the large numbers of cycles they could experience, the likelihood that one or more valves might stick open is assessed as "indeterminate." These possibilities are represented in the logic for this event, which is shown in Figure 5-17.

The basic events and corresponding probabilities associated with the logic defining pressure conditions in the RCS are summarized in the tabulation below.

Quantification of Basic Events Relevant to RCS Pressure Prior to Vessel Breach

PDS/Case	Description	Assessment	Probability
CEDEPSGE: operators do not depressurize steam generators given inadequate core cooling			
All	All relevant plant-damage states (i.e., with feedwater available)	unlikely	0.05
CEDPORVE: operators do not open PORV given inadequate core cooling			
All	All relevant plant-damage states (i.e., with PORV available)	unlikely	0.1
CEPZSRVC: repeated cycling causes at least one PSV to stick open			
All	All relevant plant-damage states (i.e., RCS at very high pressure)	indeterminate	0.5
CEHLCRMF: creep rupture of RCS hot leg given very high pressure			
All	All relevant plant-damage states (i.e., RCS at moderately high pressure)	likely	0.9
CEHLCRHF: creep rupture of RCS hot leg given moderately high pressure			
All	All relevant plant-damage states (i.e., RCS at very high pressure)	very likely	0.99

Dispersal of Core Debris Beyond Reactor Cavity

The potential for the pressurized ejection of core debris beyond the reactor cavity is important chiefly because of the possibility that the ejection may be accompanied by direct containment heating, because of the impact on coolability of the core debris, and because of the possibility that sufficient debris may come into contact with the containment pressure boundary to cause failure. The logic corresponding to the cases of interest is described in this section.

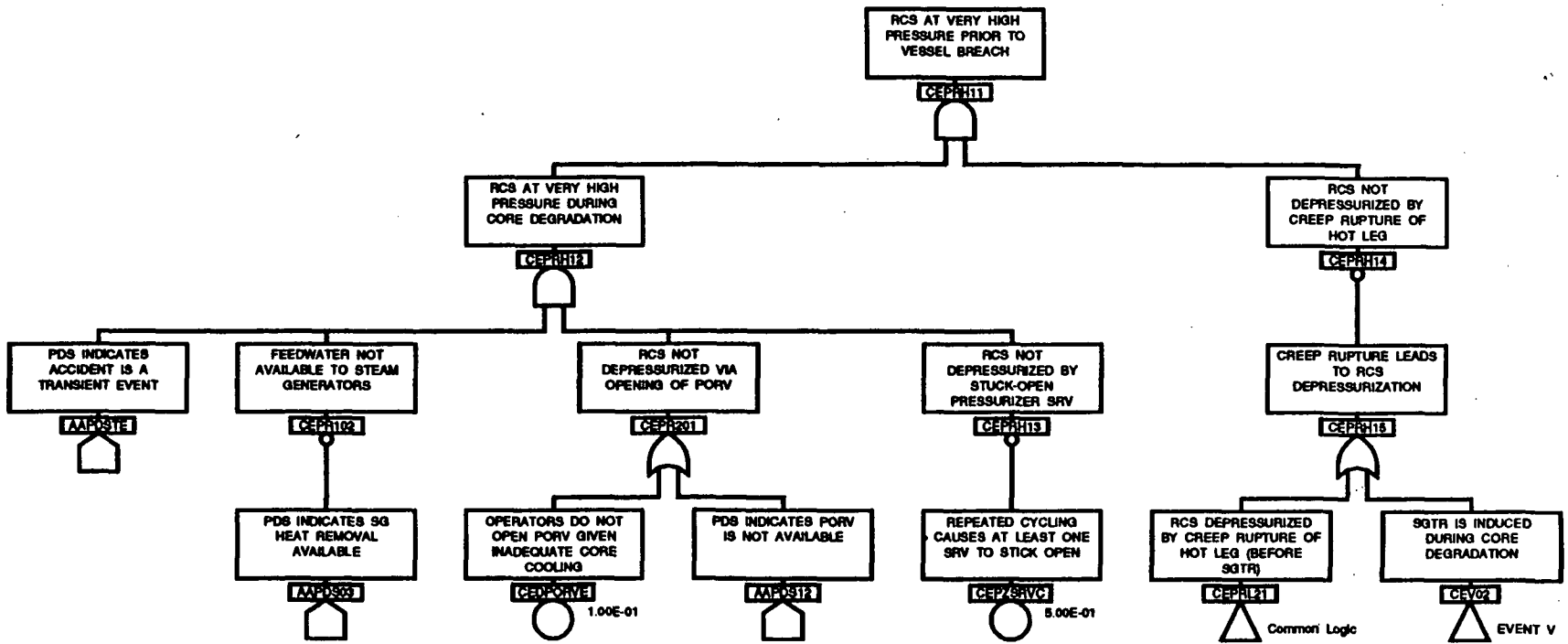


Figure 5-17. Common CET Supporting Logic for Very High RCS Pressure Prior to Vessel Breach

The logic for dispersal of debris beyond the reactor cavity (i.e., to the lower elevation) is shown in Figure 5-18. The logic differentiates between cases in which the reactor cavity is deeply flooded prior to vessel breach and those in which the cavity is not deeply flooded. The reason for this distinction is that previous assessments have postulated that deep flooding could prevent significant dispersal beyond the cavity. For example, the analyses of the Sequoyah plant for NUREG-1150 assumed that it was impossible to disperse debris through a deeply flooded cavity to other areas of the containment (Ref. 34).

The MAAP calculations provide results that are substantially different from that assessment. Using MAAP, most of the core debris is predicted to be transported through the instrument tunnel up into the lower elevation for any case in which RCS pressure is more than about 500 to 600 psig prior to vessel breach. For such pressures, the expansion of fluid exiting the RCS via the vessel breach into the reactor cavity is calculated to result in sufficient velocities to sweep the debris through the tunnel, irrespective of the amount of water in the cavity or instrument tunnel.

Research and experimentation in this area since publication of NUREG-1150 have been largely inconclusive with respect to the effects of deep water on pressurized ejections from the reactor vessel (Ref. 43).

The plant-specific analyses for Davis-Besse were weighted heavily in the assessment of the events relating to the conditional probability of dispersal. It was judged to be "likely" that the debris would be dispersed to the lower elevation for cases in which the debris was ejected from the reactor vessel at very high or moderately high pressure (i.e., about 1500 psig or greater) and the reactor cavity was deeply flooded. For cases in which the pressure in the RCS was intermediate (nominally about 1000 psig), it was judged that dispersal of a substantial fraction of the core debris through a deeply flooded cavity might be less likely. Therefore, this case was taken to be "indeterminate." For cases in which the cavity was not deeply flooded prior to vessel breach, dispersal was assumed to be certain for all cases of intermediate or higher pressure prior to vessel breach.

The likelihood of pressurized ejection from the reactor vessel was assessed to be a function of RCS pressure in the analyses supporting NUREG-1150 (Ref. 34). For accidents above about 2000 psig, the mean probability of failure of the vessel by pressurized ejection was assessed to be 0.79. For somewhat lower pressures, the probability was assessed to be 0.6. Therefore, the logic was developed to include the conditional probabilities of pressurized ejection, and the mean values from the reference analyses were applied. This is reflected in the logic under gates CELC07 and CELC08.

The results for the basic events associated with the dispersal of core debris beyond the cavity are summarized below.

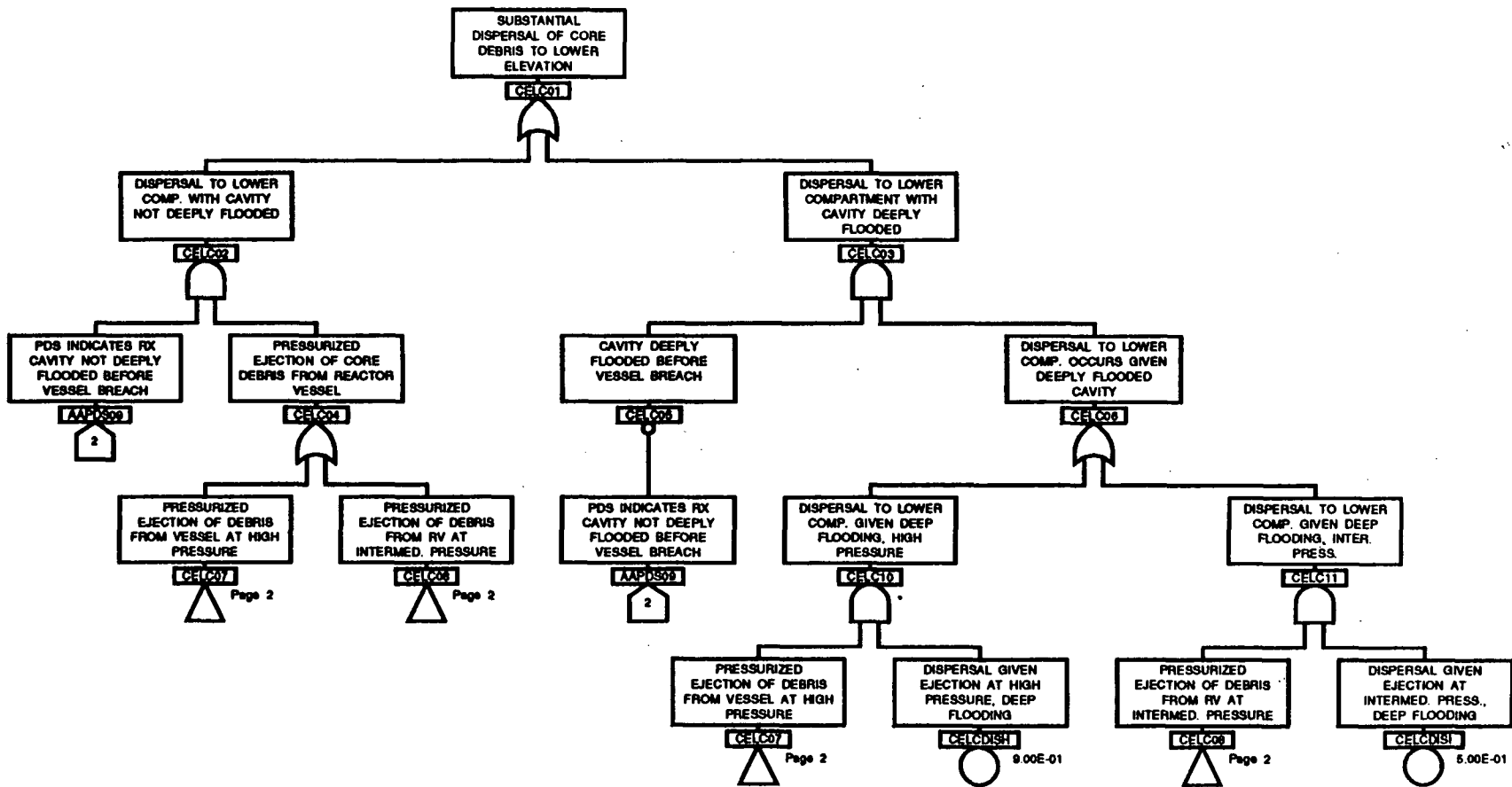


Figure 5-18. Common CET Supporting Logic for Debris Dispersal to Lower Elevation (page 1 of 2)

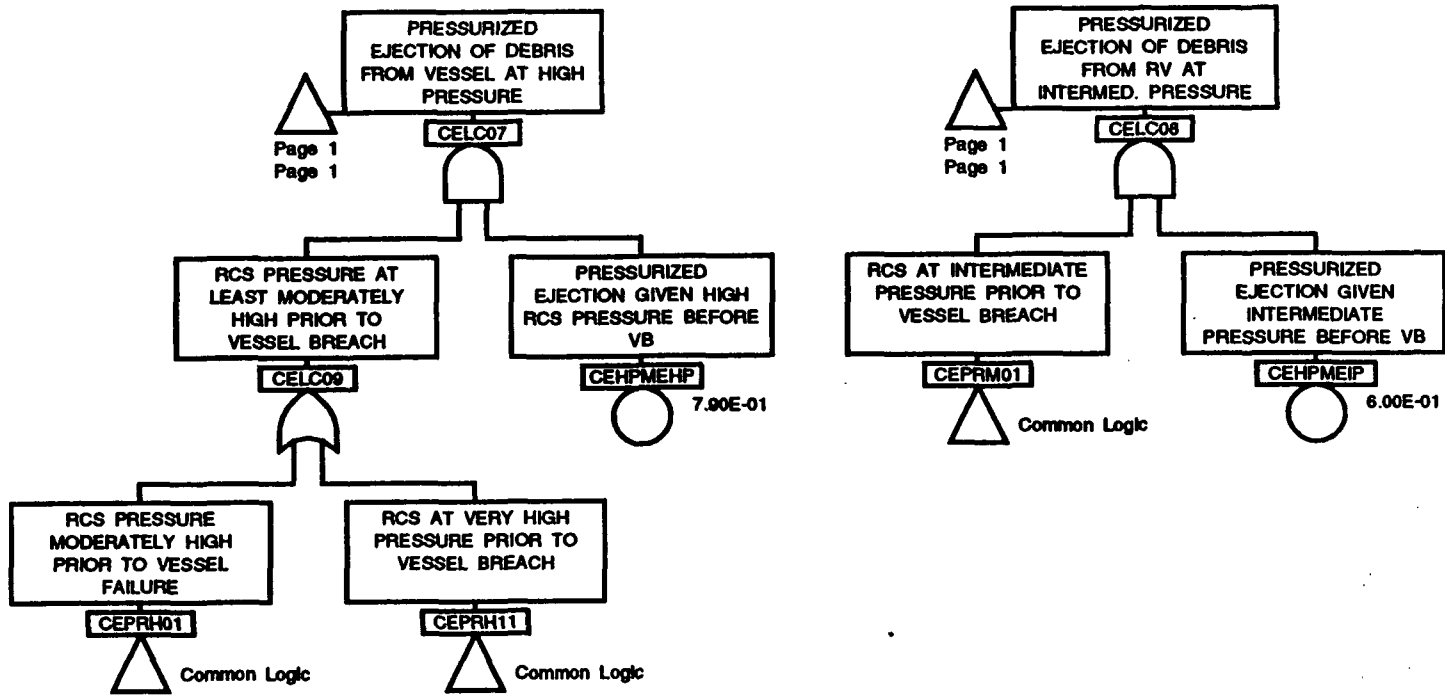


Figure 5-18. Common CET Supporting Logic for Debris Dispersal to Lower Elevation (page 2 of 2)

Quantification of Basic Events for Dispersal of Debris Beyond Cavity

PDS/Case	Description	Assessment	Probability
CELCDISH: dispersal given ejection at high pressure, deep flooding			
All at high pressure	All cases with very high pressure prior to vessel breach	likely	0.9
All at moderately high pressure	All cases with moderately high pressure prior to vessel breach	likely	0.9
CELCDISI: dispersal given ejection at intermediate pressure, deep flooding			
All at intermediate pressure	All cases with intermediate pressure prior to vessel breach	indeterminate	0.5
CEHPMEHP: pressurized ejection given high RCS pressure before vessel breach			
All at high pressure	All cases with very high pressure prior to vessel breach	likely	0.79
All at moderately high pressure	All cases with moderately high pressure prior to vessel breach	likely	0.79
CEHPMEIP: pressurized ejection given intermediate RCS pressure before vessel breach			
All at intermediate pressure	All cases with intermediate pressure prior to vessel breach	indeterminate	0.6

Section 6 ACCIDENT PROGRESSION AND QUANTIFICATION FOR THE CONTAINMENT EVENT TREE

Section 2 described the models that were developed to permit analysis of the progression of core-damage accidents for Davis-Besse using the MAAP 3.0B computer code. The results of those assessments are described below, in Section 6.1. The possibilities for containment responses other than the nominal responses predicted by MAAP were considered through the construction of a containment event tree (CET), as described in Section 5. The manner in which the CET outcomes were quantified is summarized in Section 6.2. Section 6.3 provides a description of the results of that quantification.

6.1 CONTAINMENT RESPONSE FOR REPRESENTATIVE ACCIDENTS

The response of the RCS and containment to a core-damage sequence and the subsequent fission product release would be dependent on sequence characteristics that lead to fuel damage as well as the status of containment safeguards. However, it is sufficient to divide the entire set of sequences into five general categories to provide representative containment responses: large, medium, and small LOCAs, transient-initiated sequences, and steam generator tube ruptures (SGTRs).

6.1.1 Large LOCAs

The containment response to large breaks is perhaps the most straightforward of all the core-damage sequences. To illustrate the containment response, plant-damage state ARXYFRYX will be discussed (Ref. 44): a 2.0 square foot break in the RCS piping near the discharge of a reactor coolant pump at sequence initiation; full ECCS injection followed by failure of all high pressure injection and low pressure injection pumps when switched to the recirculation mode; one train of containment spray available until recirculation, at which time it is also assumed to fail; and one containment air cooler assumed available throughout the analysis.

Given the large break, the RCS depressurizes quickly. With full injection and one containment spray pump in operation, the BWST reaches minimum level in 47 minutes. With failure of the recirculation phase of ECCS, water inventory is quickly lost, and full core melt/reactor vessel failure occurs at 3.3 hours. A value of 27% cladding oxidation is estimated, corresponding to a containment hydrogen concentration of just over 2%, given steam addition to containment during the sequence.

A containment hydrogen concentration of 2% is roughly half of the minimum necessary for a hydrogen burn to be initiated. It should also be noted that for this transient, containment steam concentration after reactor vessel failure (~ 55%) is very close to a level

sufficient to provide steam inertment for any amount of combustible gases in the containment atmosphere. Figures 6-1 and 6-2 summarize these parameters.

Containment pressure rises quickly after break initiation, reaching the containment spray actuation pressure setpoint in 31 seconds. The combination of passive heat sinks, containment air cooler operation, and containment spray actuation are sufficient to mitigate the pressure rise and begin a pressure reduction until the time at which the reactor vessel eventually fails and corium is released to the containment. Given the low RCS pressure at the time of reactor vessel failure and the presence of a flooded reactor cavity, all corium released remains in the reactor cavity. Given the corium spread area and water level in the cavity, the corium is quenched, with decay heat transferred to the cavity water. Following the increase resulting from reactor vessel failure, containment pressure rises slowly to approximately 42 psia, after which the heat removal rate for the containment air coolers is sufficient to initiate a slow reduction in pressure. Figure 6-3 summarizes the containment response.

For this class of accidents, operator actions based on inadequate core cooling conditions have little effect on system response. The RCS is decoupled from the secondary side very shortly after break initiation such that secondary side depressurization has a negligible effect. Restarting the RCPs provides only a minor amount of fluid to the core region and contributes little positive effect. With the RCS depressurized by the break, opening the PORV to depressurize the system also has a negligible effect on system response.

Overall, the peak containment pressure of 43.8 psia occurs at 60 seconds into the sequence, which is identical to the time of peak pressure calculated in the Davis-Besse design-basis analysis for containment response to a large break LOCA (Ref. 45).

Other large LOCA sequences present variations on this response. If no containment cooling is available, long term steaming will eventually overpressurize and fail the containment structure. For large LOCA sequences the corium always remains in the reactor cavity. Given the containment geometry, all water within the containment is drained by gravity to the reactor cavity and normal containment sump, and is therefore available for corium cooling. In all cases in which no containment cooling is available, the containment vessel will fail from steaming overpressure prior to dryout of the corium contained in the reactor cavity, based on the relationship between the amount of water overlying the debris in the reactor cavity and the free volume of the containment.

For a large LOCA case with a complete failure of all ECCS injection and containment cooling, reactor vessel failure occurs at 1.6 hours and the containment vessel fails at 17.5 hours. Additionally, it should be noted that a single containment air cooler in operation provides sufficient heat removal capability to prevent containment overpressure failures.

6.1.2 Medium LOCAs

To illustrate the RCS and containment response to a medium LOCA, plant-damage state MRXYFRYX will be discussed (Ref. 46): a 0.03 square foot break in the RCS piping

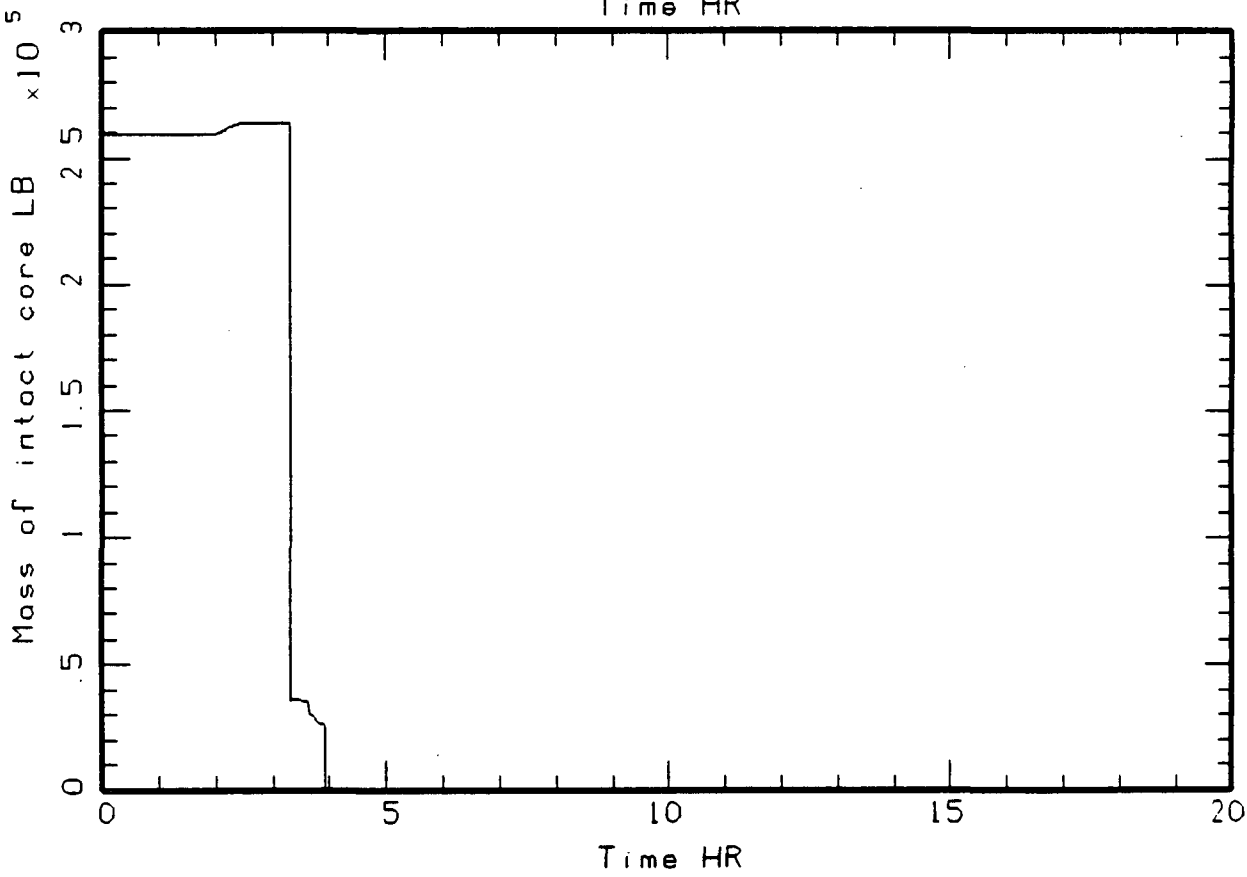
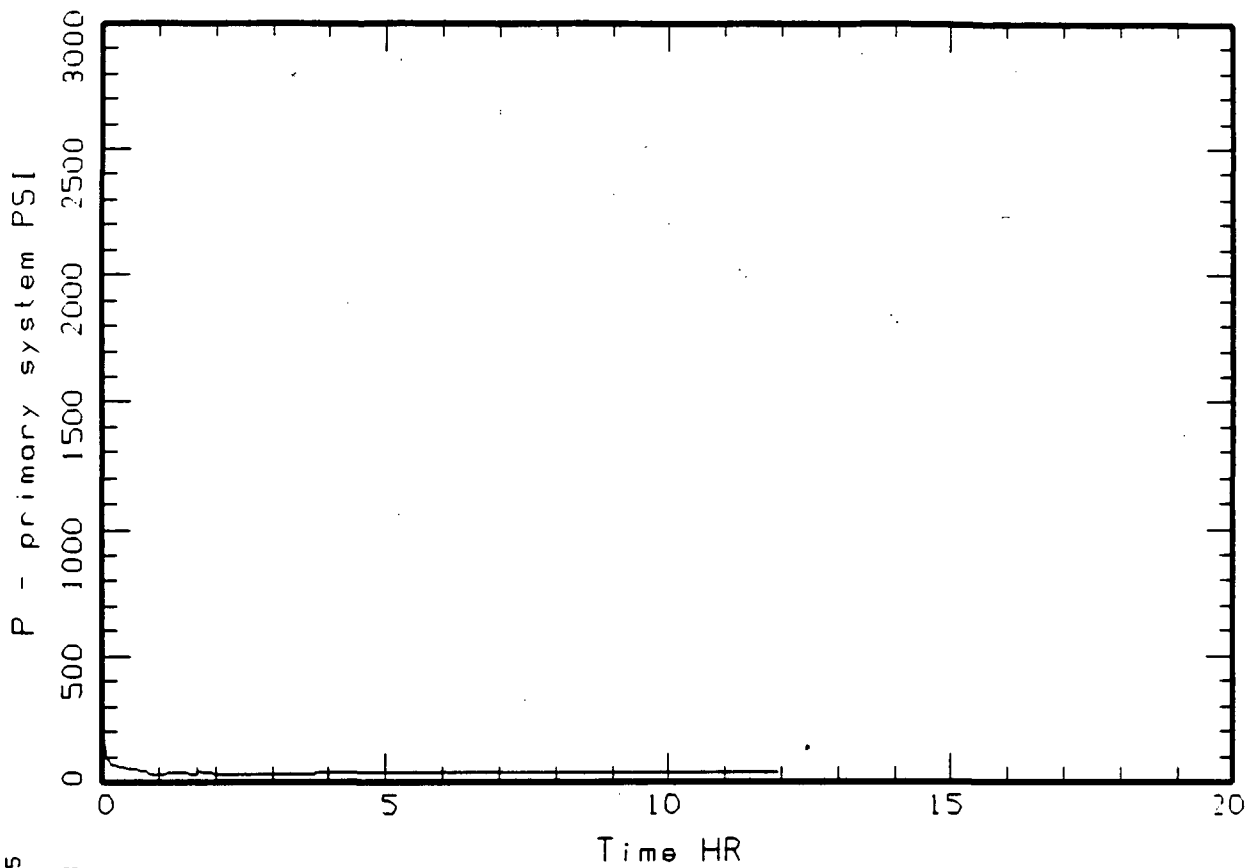


Figure 6-1 Large LOCA Response (1 of 3)

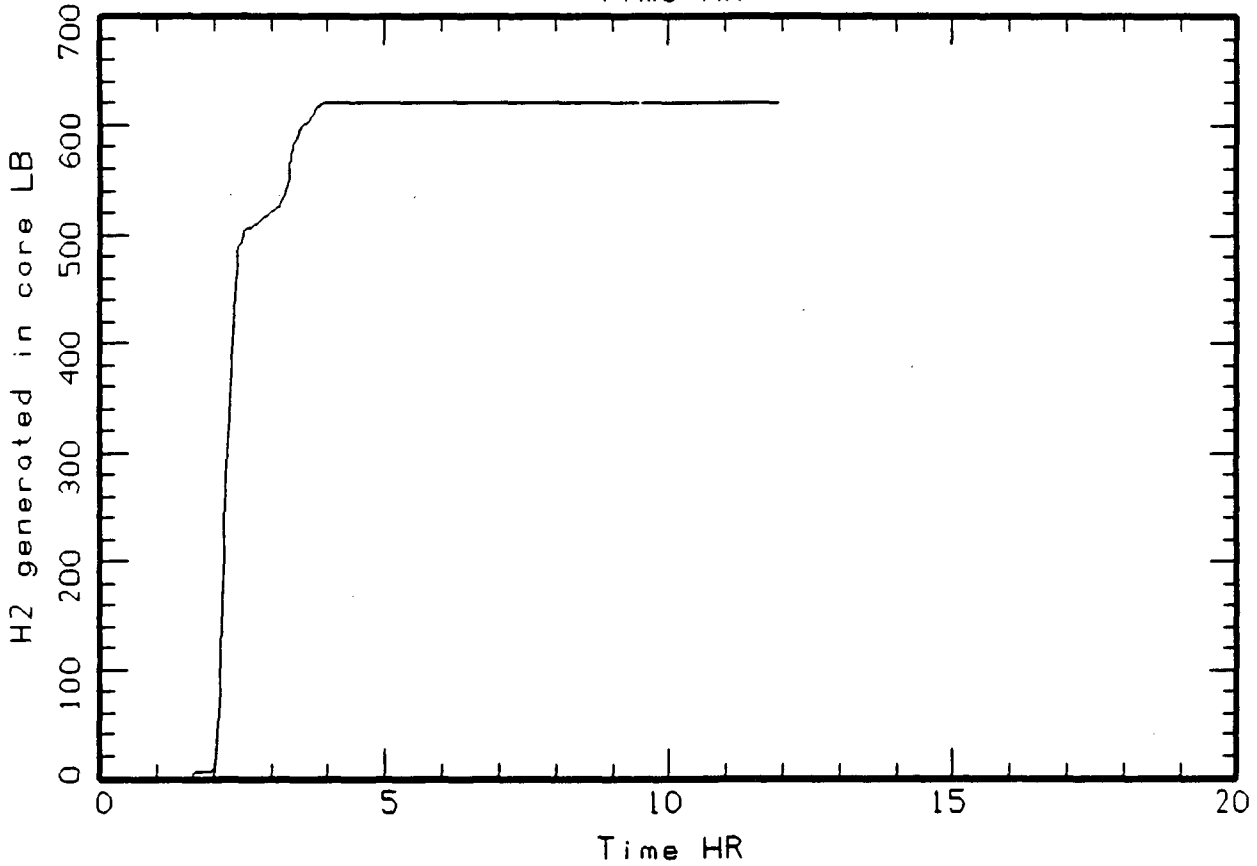
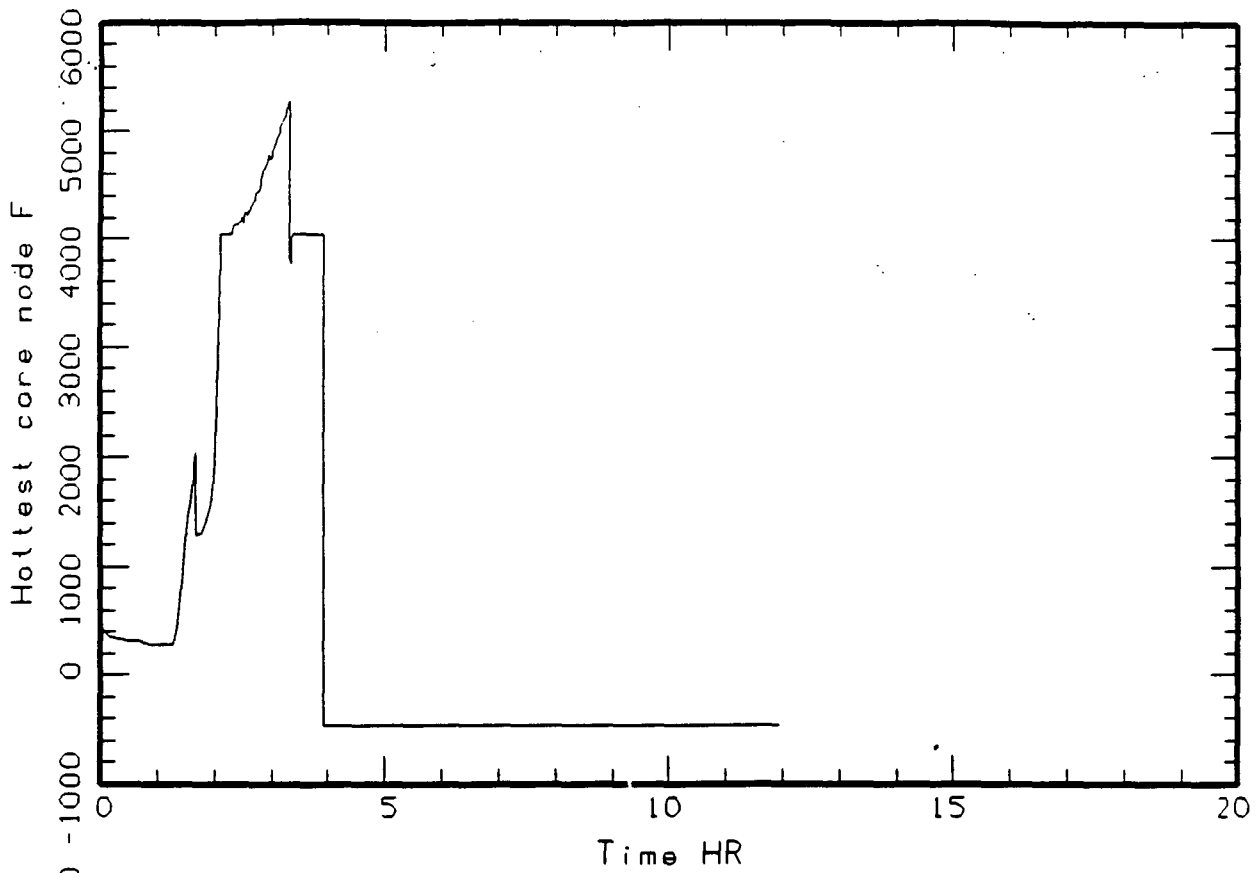


Figure 6-2 Large LOCA Response (2 of 3)

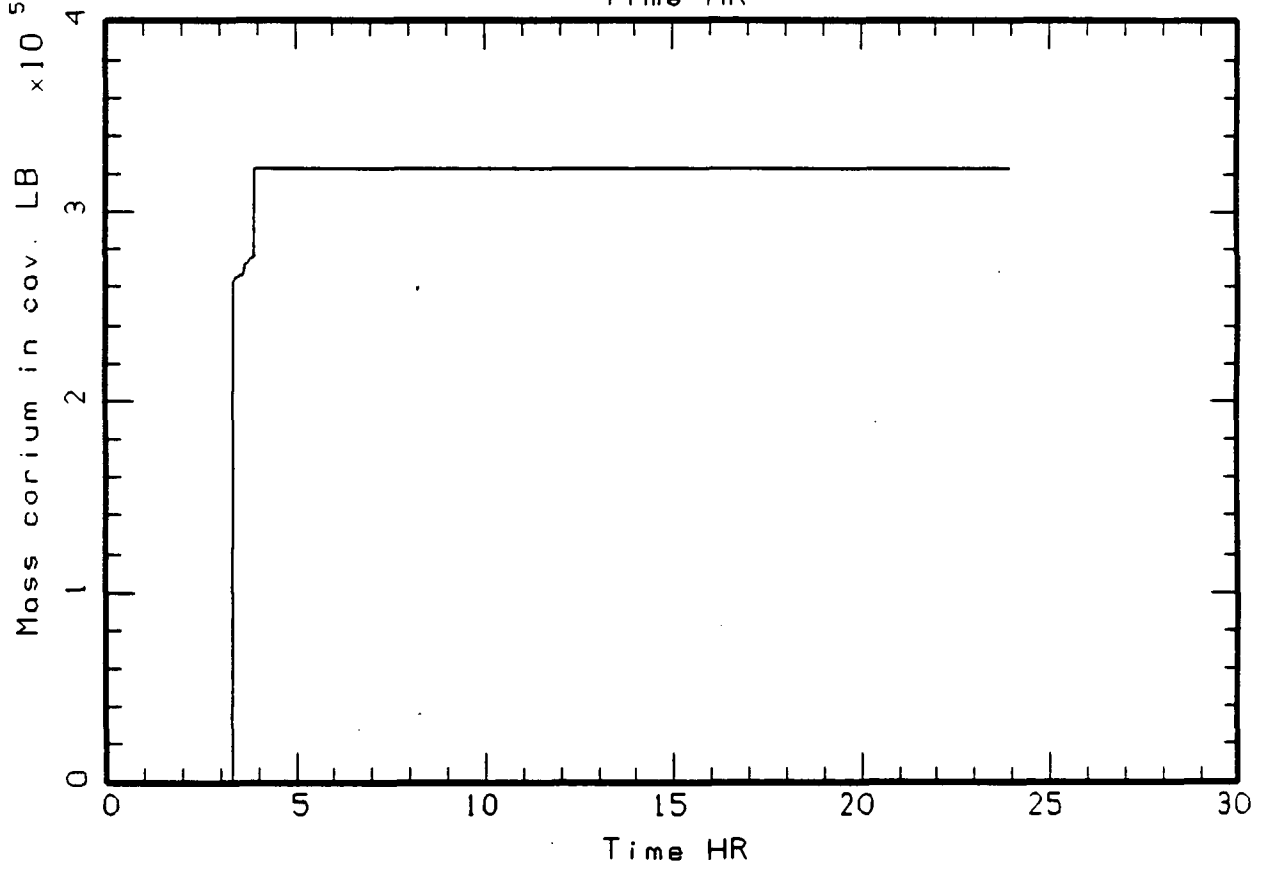
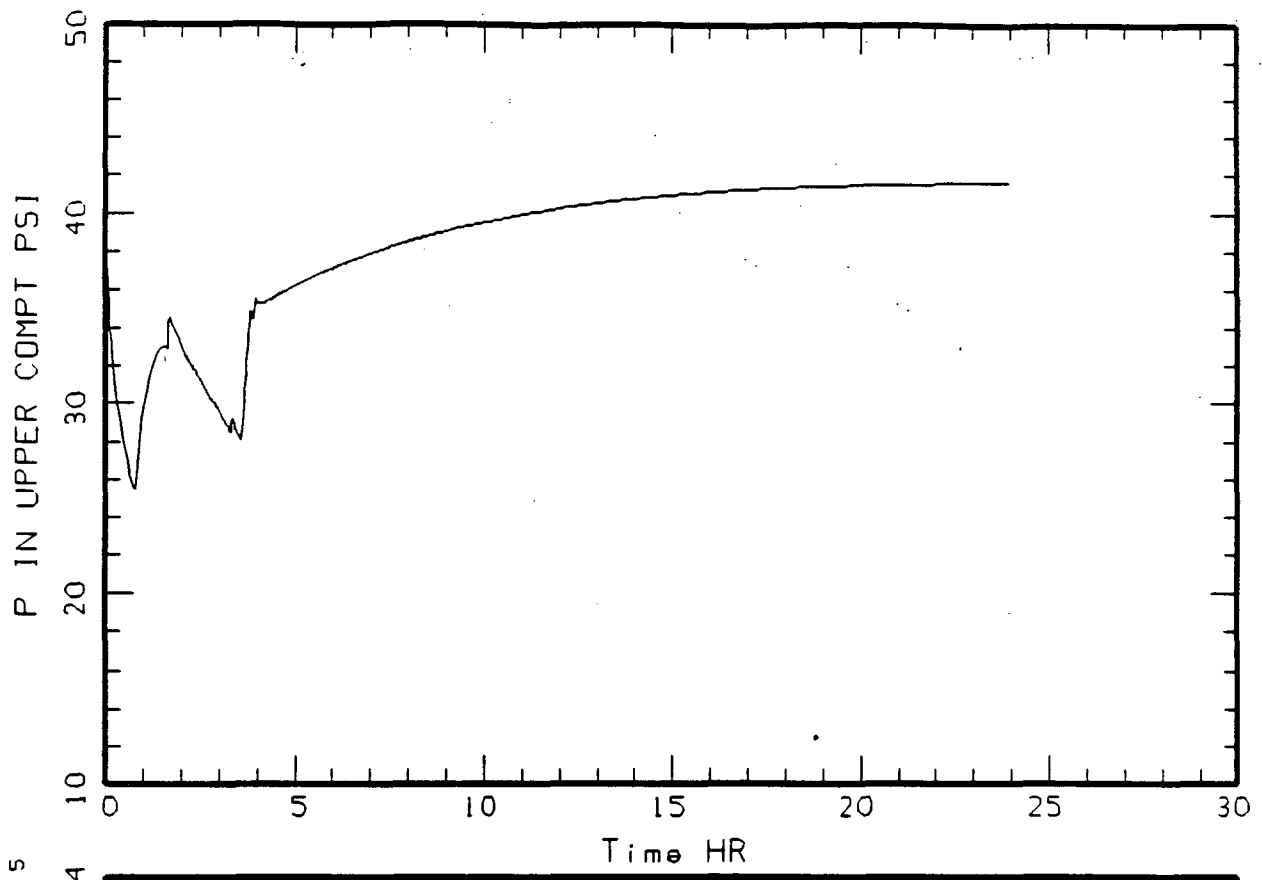


Figure 6-3 Large LOCA Response (3 of 3)

near the discharge of a reactor coolant pump at sequence initiation; full ECCS injection followed by failure of all high pressure injection and low pressure injection pumps when switched to the recirculation mode; one train of containment spray available until recirculation at which time it was also assumed to fail; and one containment air cooler assumed available throughout the analysis.

This break is at the smaller end of the IPE medium break range of 0.02 to 0.5 square feet. As such, the RCS depressurizes much more slowly than for breaks in the large break range. After initially holding up at approximately 1000 psi (secondary side heat sink pressure), the system continues to depressurize, eventually enabling use of low pressure injection until the BWST is depleted at 4.9 hours. Subsequent to failure of recirculation, the RCS repressurizes to about 500 psi. With uncovering of the core just after ten hours, the core region begins to become superheated, and the operators initiate actions associated with inadequate core cooling (ICC). After depressurizing the secondary side, operating RCPs, and eventually opening the pressurizer PORV, the RCS is depressurized when reactor vessel failure occurs at 13.6 hours.

For this particular transient, operation of RCPs given the fluid inventory contained in cold leg piping, the degree of core oxidation, and system pressure, a MAAP calculated collapse of core materials occurs. With the change of core geometry, a greater amount of cladding oxidation than for other LOCAs is calculated, with a value of 57%. The corresponding containment hydrogen concentration after reactor vessel failure is 4%. A hydrogen concentration of 4% is slightly less than the minimum concentration required to enable combustion given the presence of a significant quantity of steam. Post-reactor vessel failure steam concentrations (~ 57%) are very close to a level sufficient to provide inertment for any level of combustible gases, and are sufficient to prevent burns in the 4% range. Figures 6-4 and 6-5 summarize these parameters.

After break initiation, containment pressure rises at about 15 psi/hour until reaching a peak of about 33 psia prior to failure of the reactor vessel. At this point the combination of passive heat sinks and containment air cooler operation is sufficient to mitigate the pressure rise and begin a pressure reduction. After the BWST is depleted and containment recirculation fails, containment pressure begins to rise again in response to the heatup of the RCS. After reaching a peak of about 42 psia, pressure is again reduced due to continued action of the containment air coolers and lessened steaming from the RCS as the core is uncovered. Eventually, the reactor vessel fails with a resultant sequence peak pressure of 43 psia. Given the low RCS pressure at the time of reactor vessel failure and the presence of a flooded reactor cavity, all corium released remains in the reactor cavity, with decay heat transferred to the cavity water. Subsequently, the containment air cooler heat removal rate is sufficient to initiate a slow reduction in pressure. Figure 6-6 summarizes the containment response.

Other medium LOCA sequences present variations on this response. As for all medium and large LOCAs, if no containment cooling is available, long term steaming will

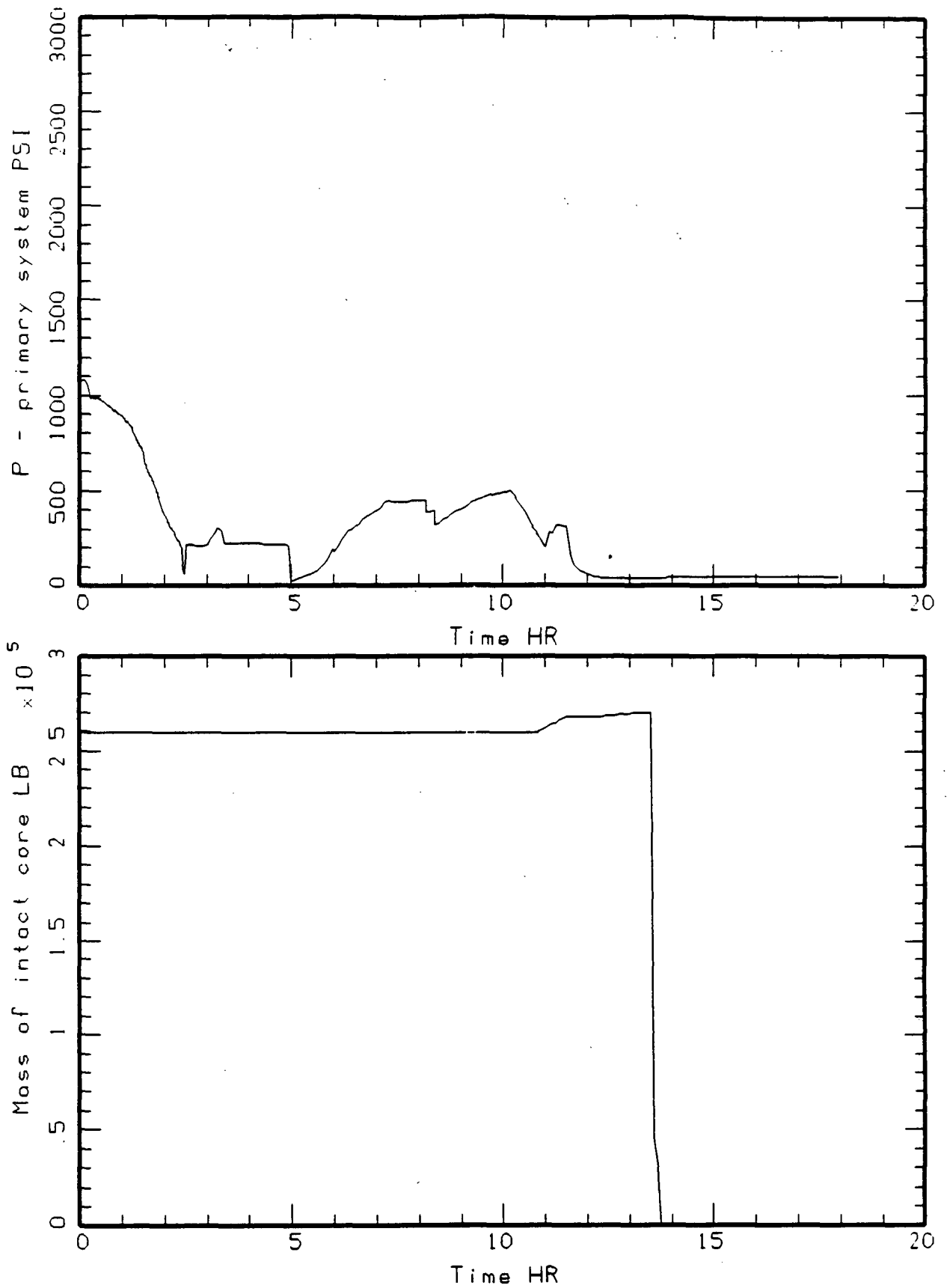


Figure 6-4 Medium LOCA Response (1 of 3)

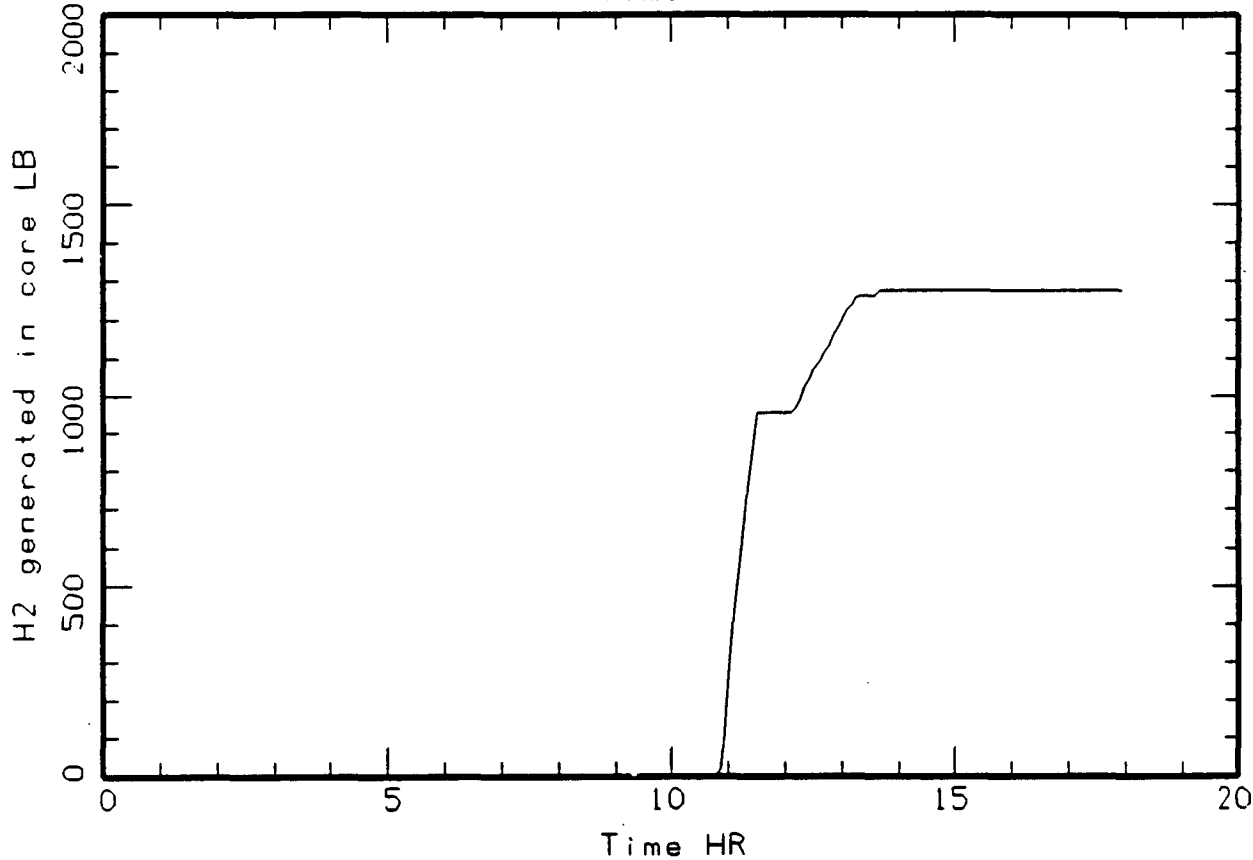
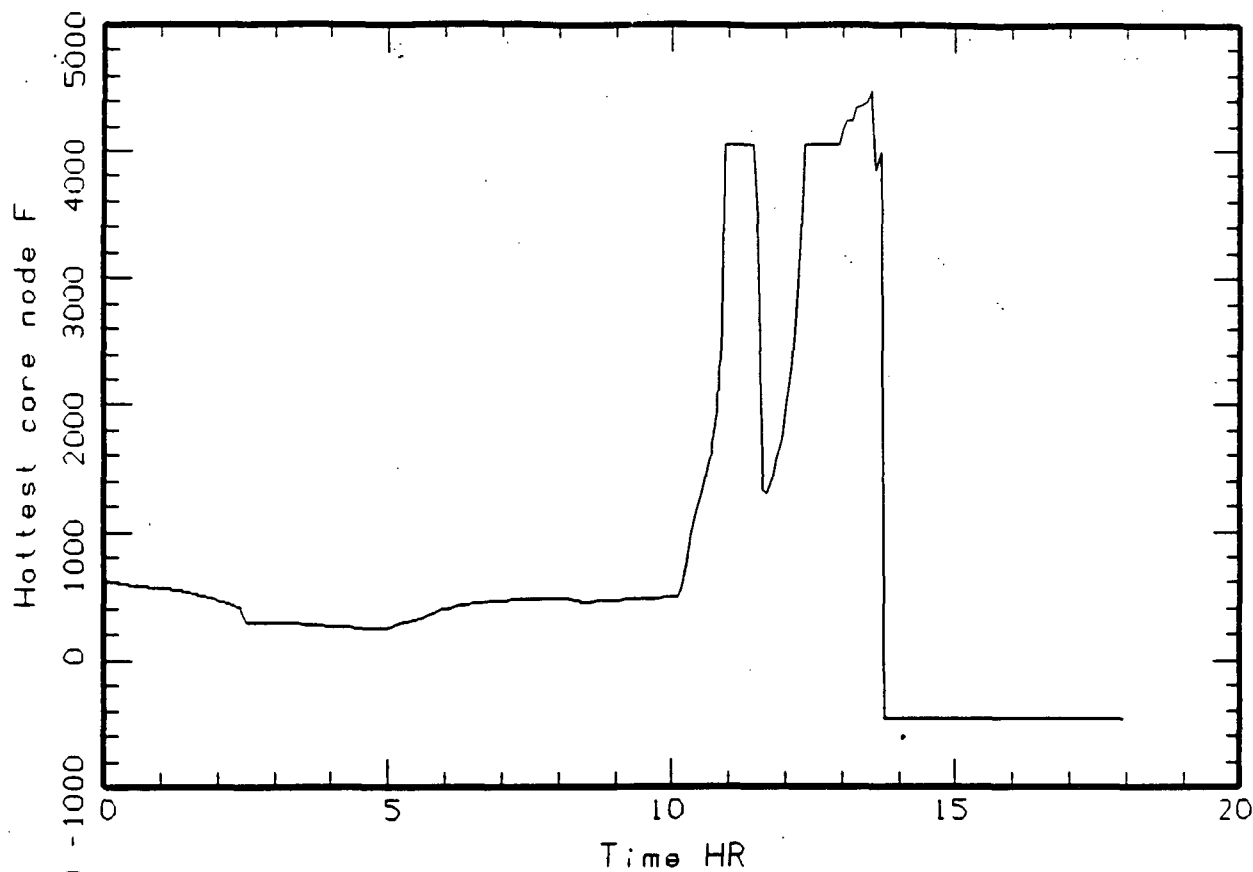


Figure 6-5 Medium LOCA Response (2 of 3)

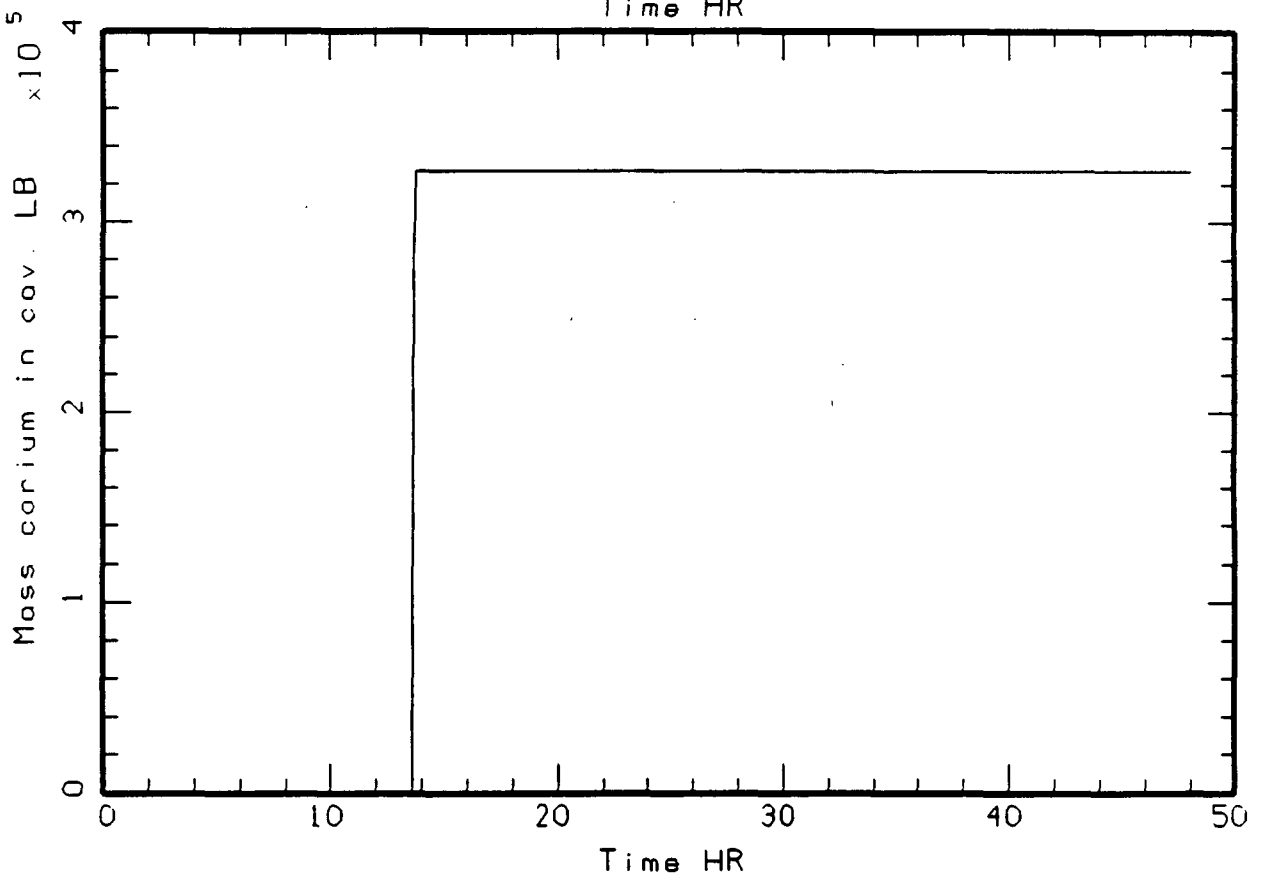
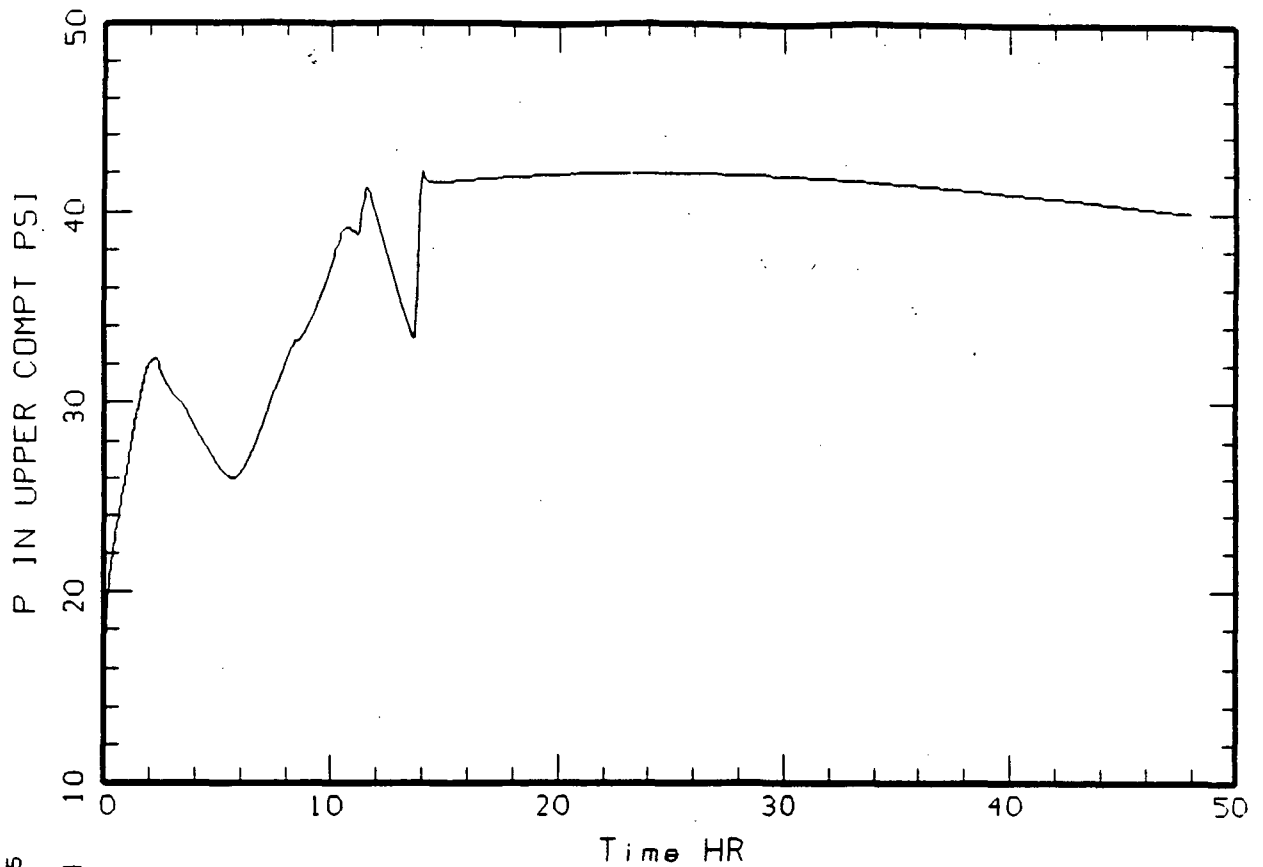


Figure 6-6 Medium LOCA Response (3 of 3)

eventually overpressurize and fail the containment structure. For medium break sequences the corium leaving the reactor vessel always remains within the reactor cavity/normal sump region of containment. RCS pressures are always sufficiently low that creep rupture of primary system piping is not applicable.

For a similar medium LOCA case with a complete failure of all ECCS injection and containment cooling, reactor vessel failure occurs at 6.1 hours and containment vessel failure at 23.4 hours. As noted for large break sequences, a single containment air cooler in operation provides sufficient heat removal capability to prevent containment overpressure failures.

6.1.3 Small LOCAs

To illustrate the RCS and containment response to a small LOCA, plant-damage state SRNYFRYD will be discussed (Ref. 47): a 0.0075 square foot break in the RCS piping near the discharge of a reactor coolant pump at sequence initiation; RCS injection with one makeup pump and one train of high pressure injection (no low pressure injection) until the BWST is depleted; complete failure of high pressure injection during the recirculation mode (makeup would not be available during this mode of ECCS); one train of containment spray available until the BWST is depleted; one containment air cooler operates throughout the analysis; main feedwater fails at sequence initiation; and loss of auxiliary feedwater pump control (i.e., the pump maintains constant maximum flow) on one train of AFW at sequence initiation.

This break falls within the IPE small break range of 0.003 to 0.02 square feet. After break initiation, the RCS depressurizes to approximately 1500 psi for the duration of ECCS injection. Due to loss of a dc bus, one train of auxiliary feedwater operates at constant maximum flow and overfills its steam generator (overflow criterion of 162,000 lbm) within about 40 minutes. At the time of overflow, both trains of the steam-driven AFW pumps are assumed to fail (the motor driven feedwater pump is also unavailable in this sequence). After failure of RCS injection at 6.9 hours, the RCS depressurizes to about 1000 psi (secondary side heat sink pressure). Consistent with design basis analyses of break sizes within this range (Ref. 48), the RCS then repressurizes as the combined effect of energy loss out the break and heat transfer to the secondary side is less than the energy addition from decay heat. This repressurization is enhanced as the secondary side approaches dryout, with the RCS repressurizing to a peak value of about 2250 psi. When uncovering of the core starts just after ten hours, the core region begins to become superheated, and the operators will initiate actions associated with ICC. Depressurizing the secondary side, operating the reactor coolant pumps, and opening the pressurizer PORV delays reactor vessel failure until 16 hours after sequence initiation. Figures 6-7 through 6-9 summarize these parameters.

For this sequence a value of 38% clad oxidation is calculated. The corresponding containment hydrogen concentration after reactor vessel failure is 2.6% which is less than the minimum concentration necessary to support combustion. The associated steam

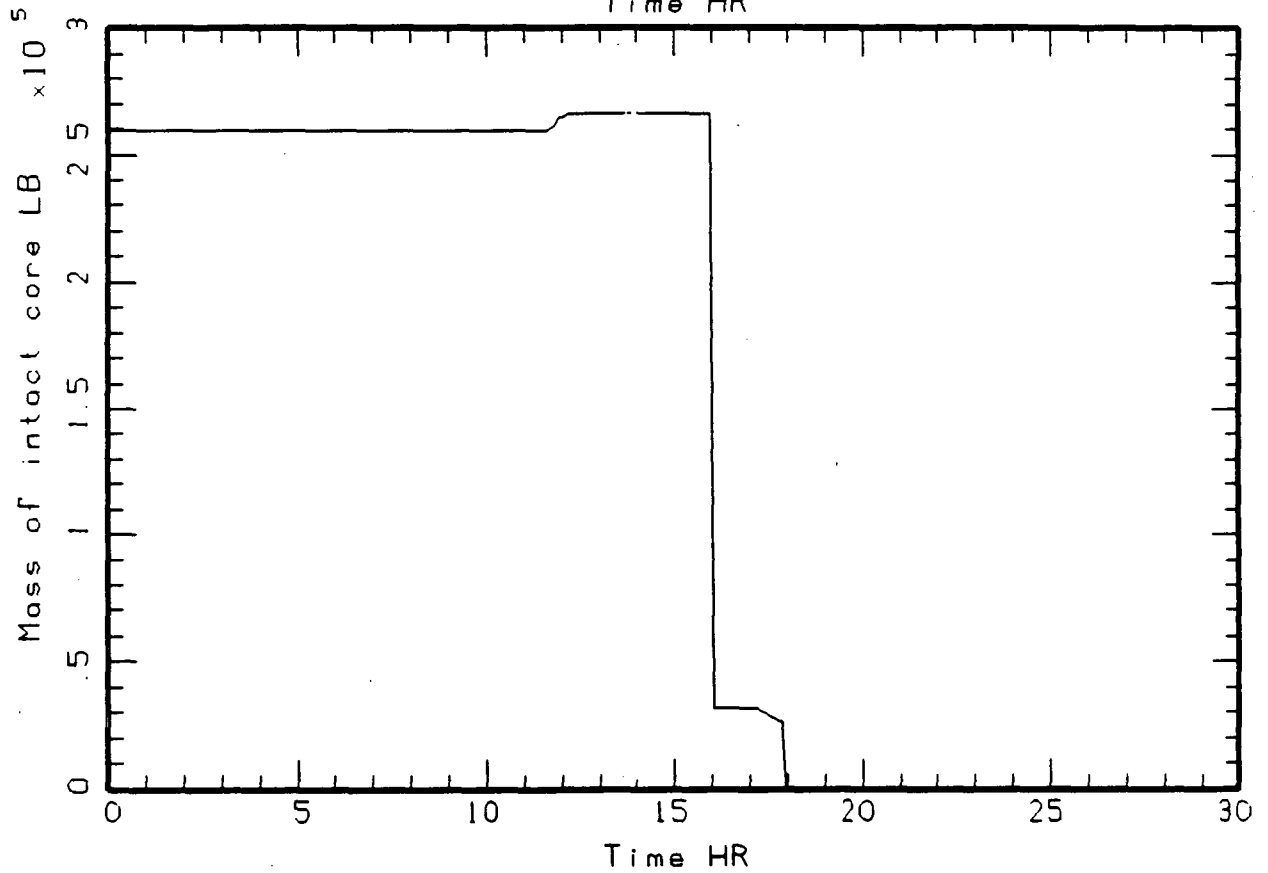
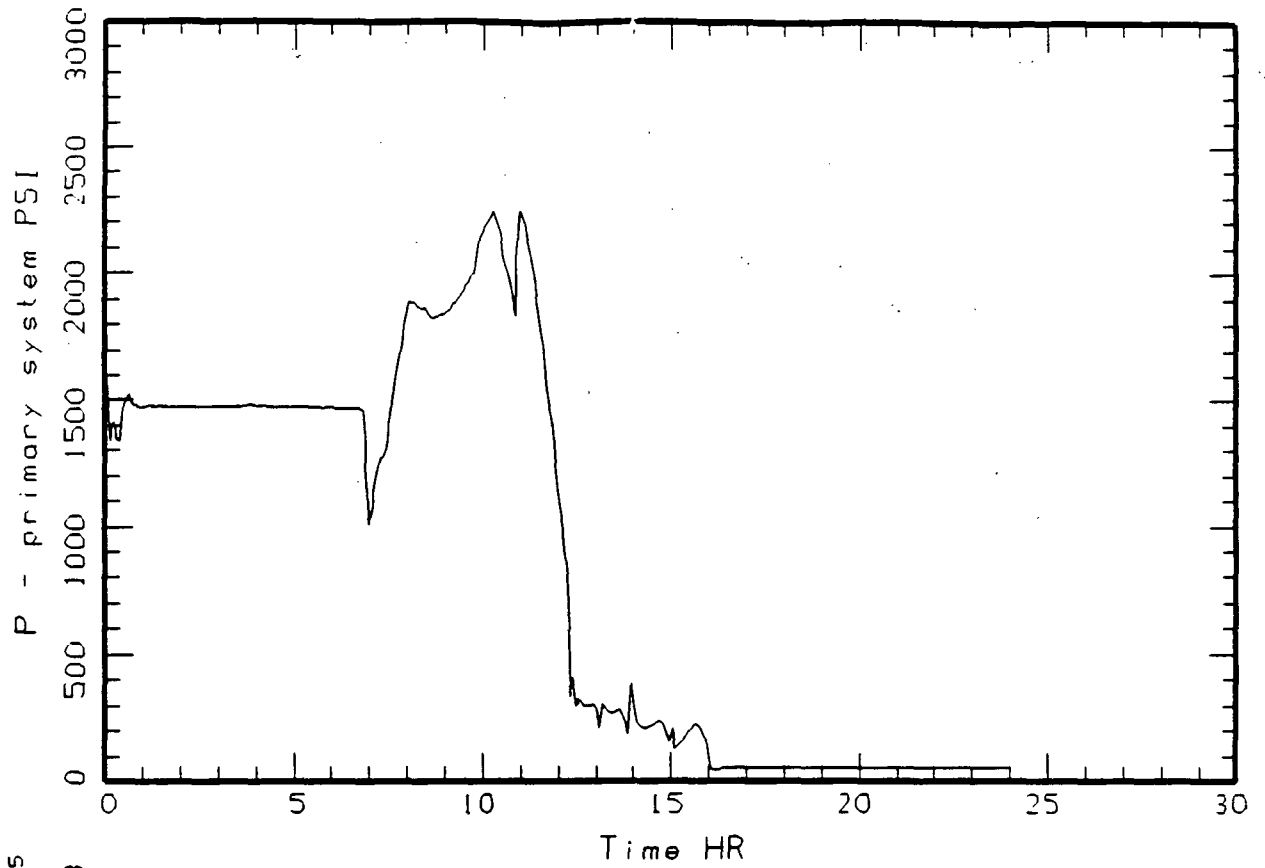


Figure 6-7 Small LOCA Response (1 of 4)

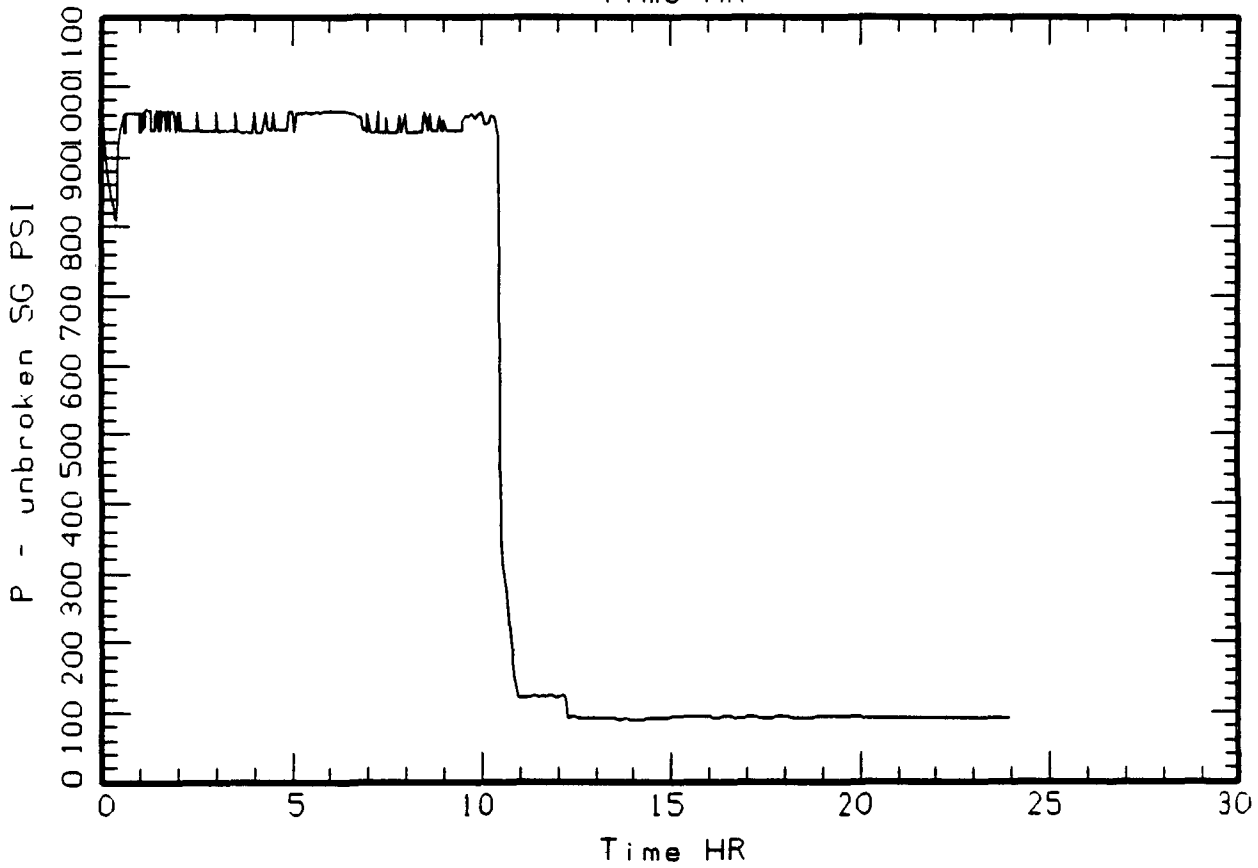
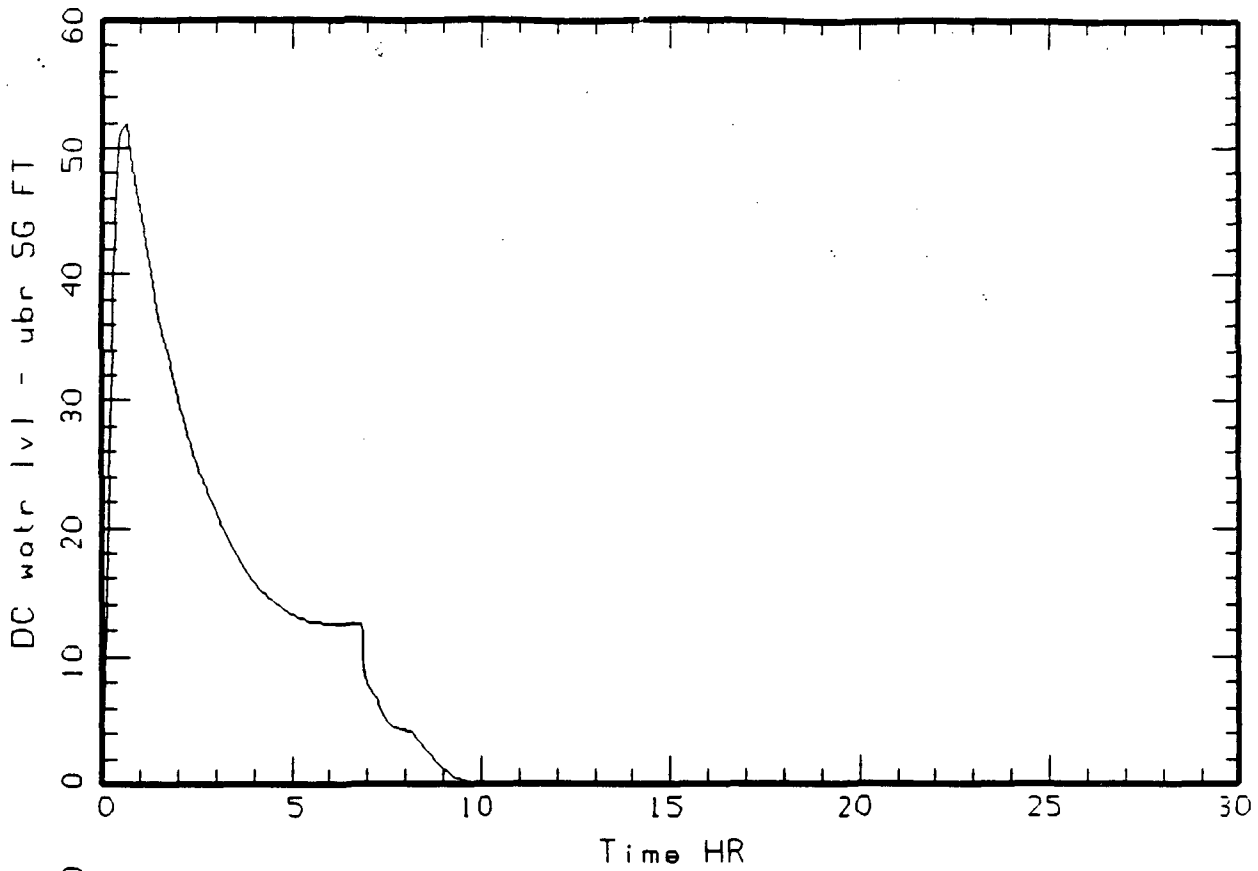


Figure 6-8 Small LOCA Response (2 of 4)

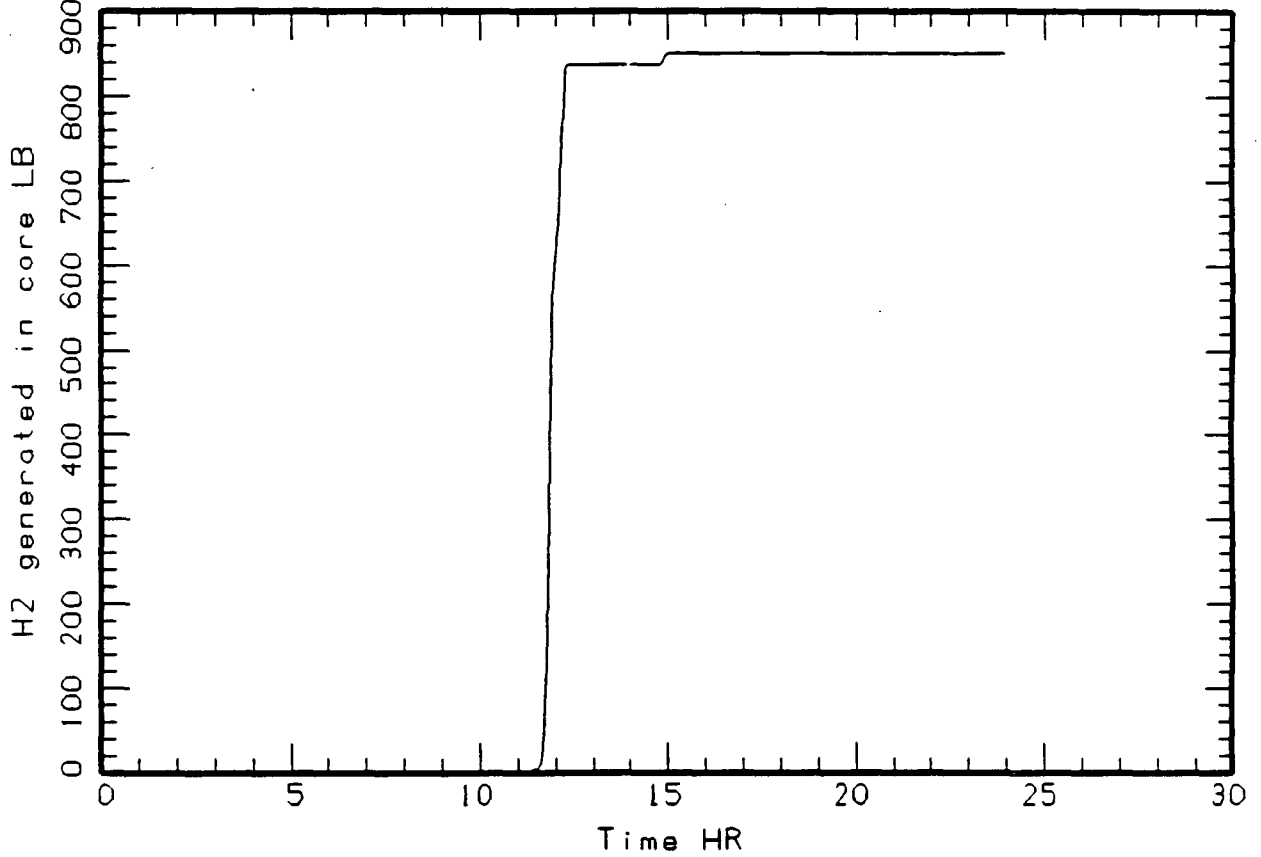
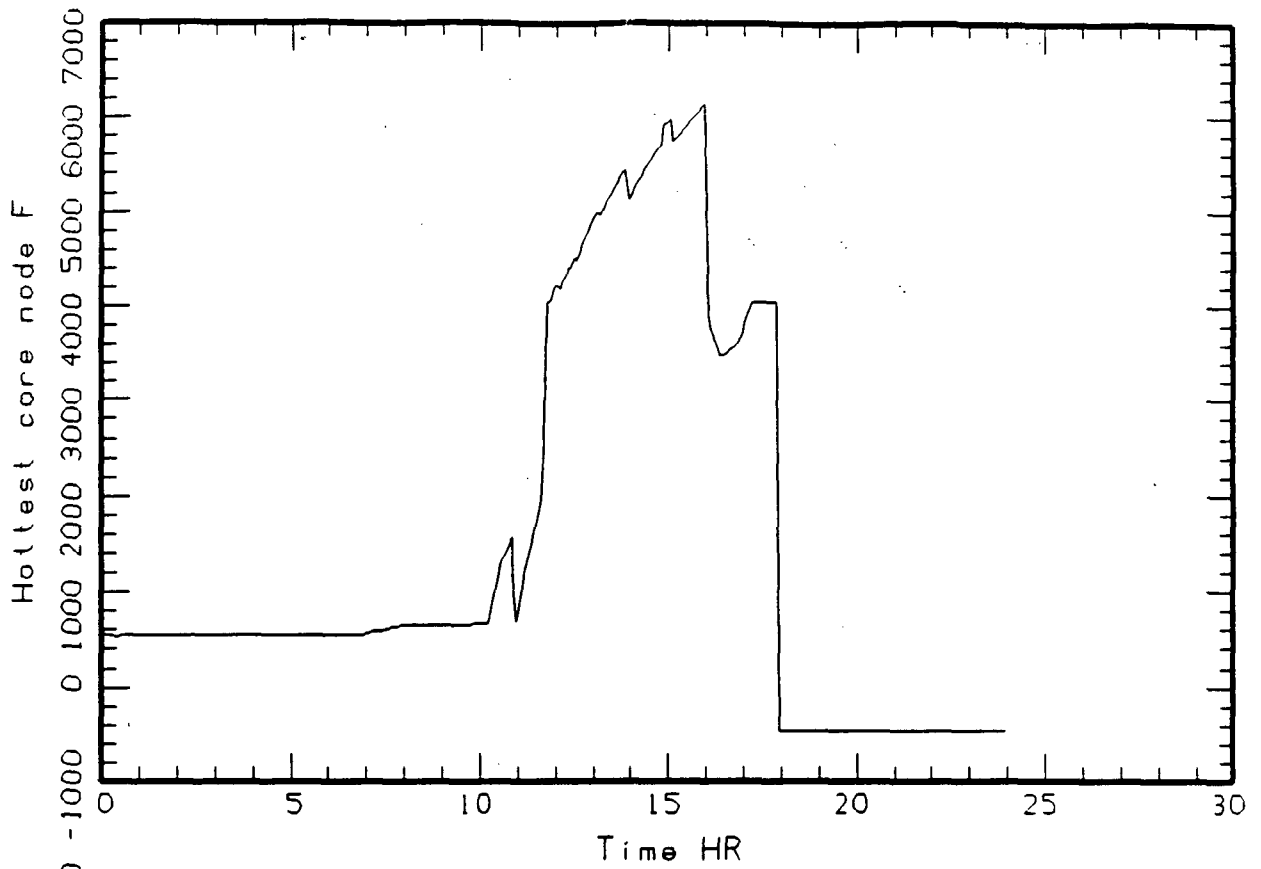


Figure 6-9 Small LOCA Response (3 of 4)

concentration is 59.5% which is sufficient to inert the containment for any concentration of combustible gases at the range of containment temperatures under consideration.

After break initiation, containment pressure rises at about 8.5 psi/hour until reaching an initial peak of about 34 psia. At this point the combination of passive heat sinks and containment air cooler operation is sufficient to mitigate the pressure rise and begin a pressure reduction. After the BWST is depleted and containment recirculation fails, containment pressure begins to rise again in response to the heatup of the RCS. After reaching a peak value of about 47 psia, pressure is again reduced due to continued operation of the containment air coolers and lessened steaming from the RCS as the core is uncovered. Eventually, the reactor vessel fails with a resultant sequence peak pressure of 55 psia. Given the low RCS pressure at the time of reactor vessel failure and the presence of a flooded reactor cavity, all corium released remains in the reactor cavity, with decay heat transferred to the cavity water. Subsequently, the containment air cooler heat removal rate is sufficient to initiate a slow reduction in pressure. Figure 6-10 summarizes the containment response.

Other small LOCA sequences present variations on this response. Of particular importance is the time of core flood tank injection and the effect on water level in the reactor vessel. In the majority of small LOCAs analyzed, reactor vessel failure time was greater than 25 hours into the sequence. Given the extended duration to reactor vessel failure, at the end of the nominal 48 hour sequence duration none of the small break cases reached containment pressures close to the ultimate pressure capability, even without any containment cooling systems in operation.

Another important consideration is the availability of auxiliary feedwater. For cases analyzed with eventual dryout of the secondary side, the time to reactor vessel failure was significantly reduced when compared to cases with nominal auxiliary feedwater system operation. Additionally, for all small break cases analyzed, gas temperatures in the upper reactor vessel region were insufficient if circulated into the RCS to cause creep rupture of primary system piping.

Seal LOCAs exhibit essentially the same behavior as small break LOCAs, since the total equivalent break size of 0.004 square feet (initial total volumetric break flow of approximately 400 gpm) is within the small break area range.

6.1.4 Transients

The following representative case of a transient initiated sequence analysis will be discussed (plant-damage state TINYNINN (Ref. 49): a loss of offsite power with all emergency diesel generators (including the station blackout diesel generator) failing to start resulting in a station blackout; eventual depletion of the batteries resulting in loss of auxiliary feedwater pump control (i.e., pumps maintain constant maximum flow) at two hours; and the pressurizer PORV fails closed (or remains closed).

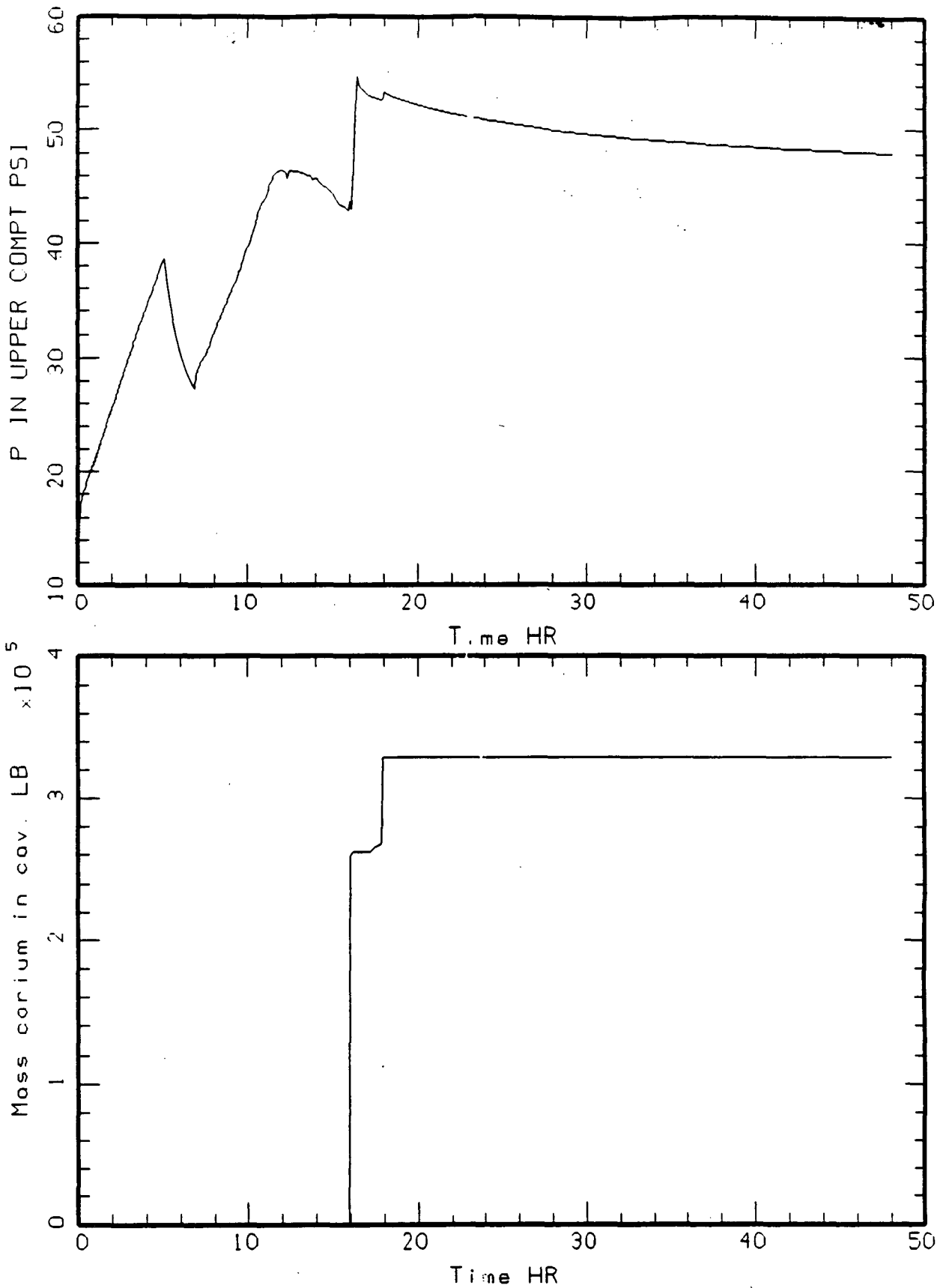


Figure 6-10 Small LOCA Response (4 of 4)

The characteristics of transient sequences are unique from those previously outlined for LOCA cases. With no immediate break in the RCS pressure boundary, system pressure stabilizes at nominal pressure with natural circulation maintained by normal auxiliary feedwater operation. When loss of auxiliary feedwater pump control occurs at two hours (causing sustained maximum feed flow), RCS pressure is sharply reduced until the resultant steam generator overfill leads to loss of the steam-driven auxiliary feedwater pumps. The system then slowly repressurizes, reaching the 2500 psig lift setpoint for the code safety valves after the steam generators boil dry. Without power available to operate the pressurizer PORV upon sufficient superheat conditions in the RCS, system pressure remains at code safety pressure until most liquid inventory is lost and the reactor vessel fails at 9.7 hours. Depressurization of the secondary side upon core superheat is possible by manually opening the steam generator atmospheric vent valves, but has a negligible effect, since at this point in the sequence the steam generators are thermodynamically decoupled from the primary side.

For this sequence a value of 31% clad oxidation is calculated. The corresponding containment hydrogen concentration after reactor vessel failure is 2%, which is less than the minimum concentration necessary to support combustion. The associated steam concentration is 66%, which is sufficient to inert the containment for any concentration of combustible gases at the range of containment temperatures under consideration. It should also be noted that the steam concentration for this case is higher than for the LOCA cases, due to RCS inventory being released to the containment at the higher enthalpy associated with primary system code safety valve actuation pressure. Figures 6-11 through 6-13 summarize these parameters.

Immediately after reactor vessel failure, containment pressure rises from just under 30 psia to a peak just under 54 psia. With a RCS pressure of 2500 psig at time of reactor vessel failure and minimal level of about 2.5 feet of water in the reactor cavity, approximately 88% of the corium is calculated to be forced up the incore tunnel into the lower level of containment. After a continued strong rise in containment pressure associated with steaming of water overlying corium in the lower level, pressure rises at a very slow rate (~ 0.7 psi/hr) for the remainder of the nominal 48 hour sequence time. Figures 6-14 and 6-15 summarize the containment response.

Other transient sequences present variations on this response. Given that most transient sequences which do not result in a seal LOCA involve a loss of main feedwater, the availability of auxiliary feedwater is very important. The longer auxiliary feedwater is available, the longer the time to reactor vessel failure. For cases where containment cooling is not available, an eventual overpressure failure of containment is more likely the earlier the time of reactor vessel failure (i.e., reactor vessel failure produces a higher base pressure for the long term pressure increase to begin from).

For sequences which remain at or near RCS safety valve relief pressures for significant lengths of time, the probability of creep rupture of RCS piping is much higher than for lower

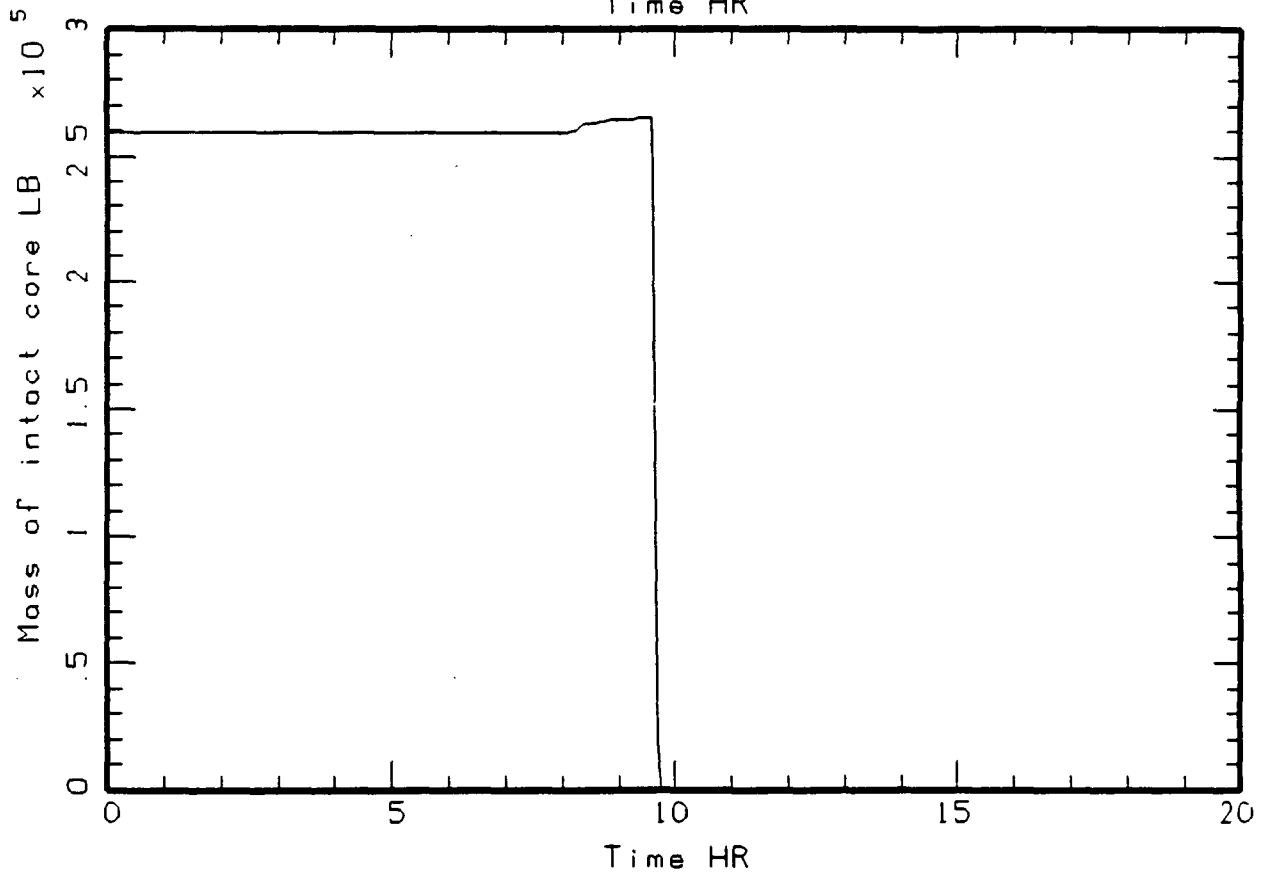
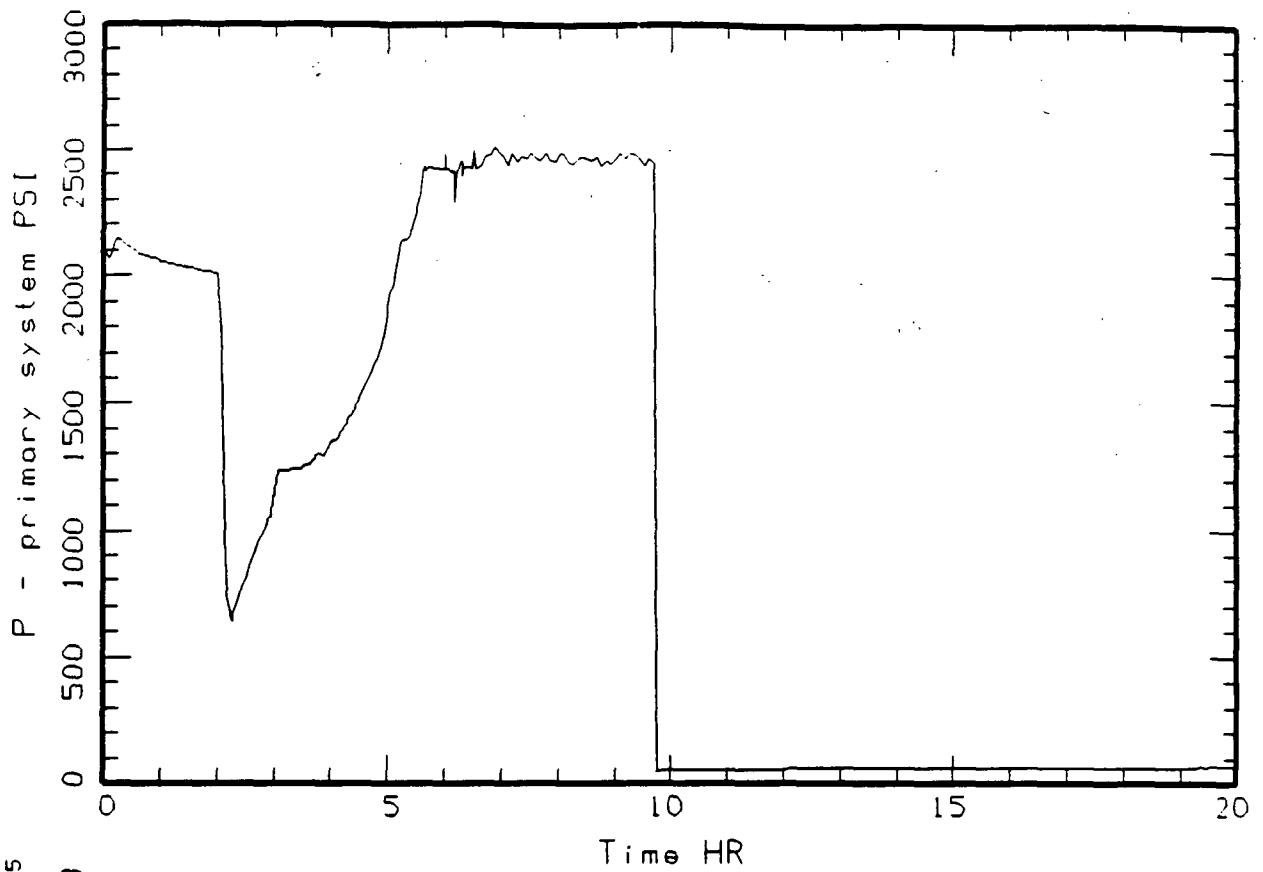


Figure 6-11 Transient Response (1 of 5)

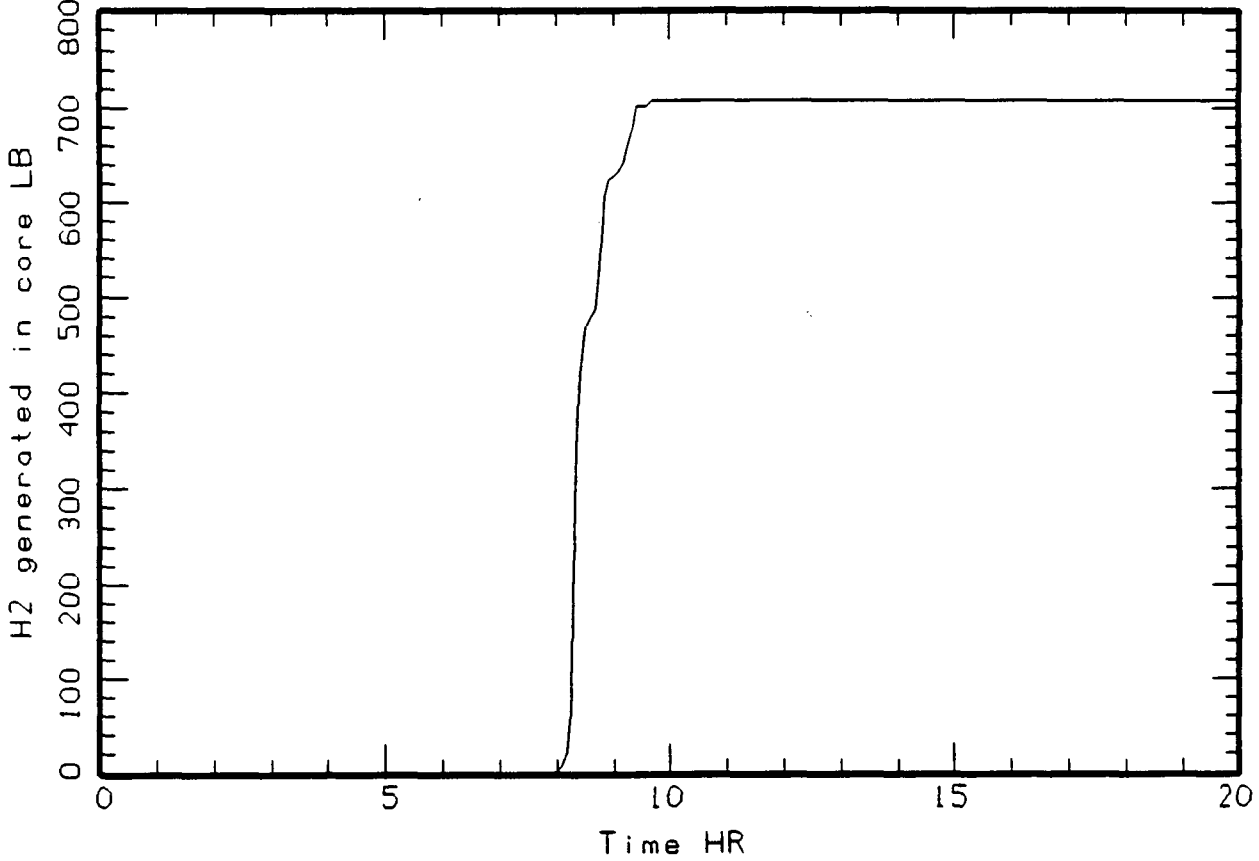
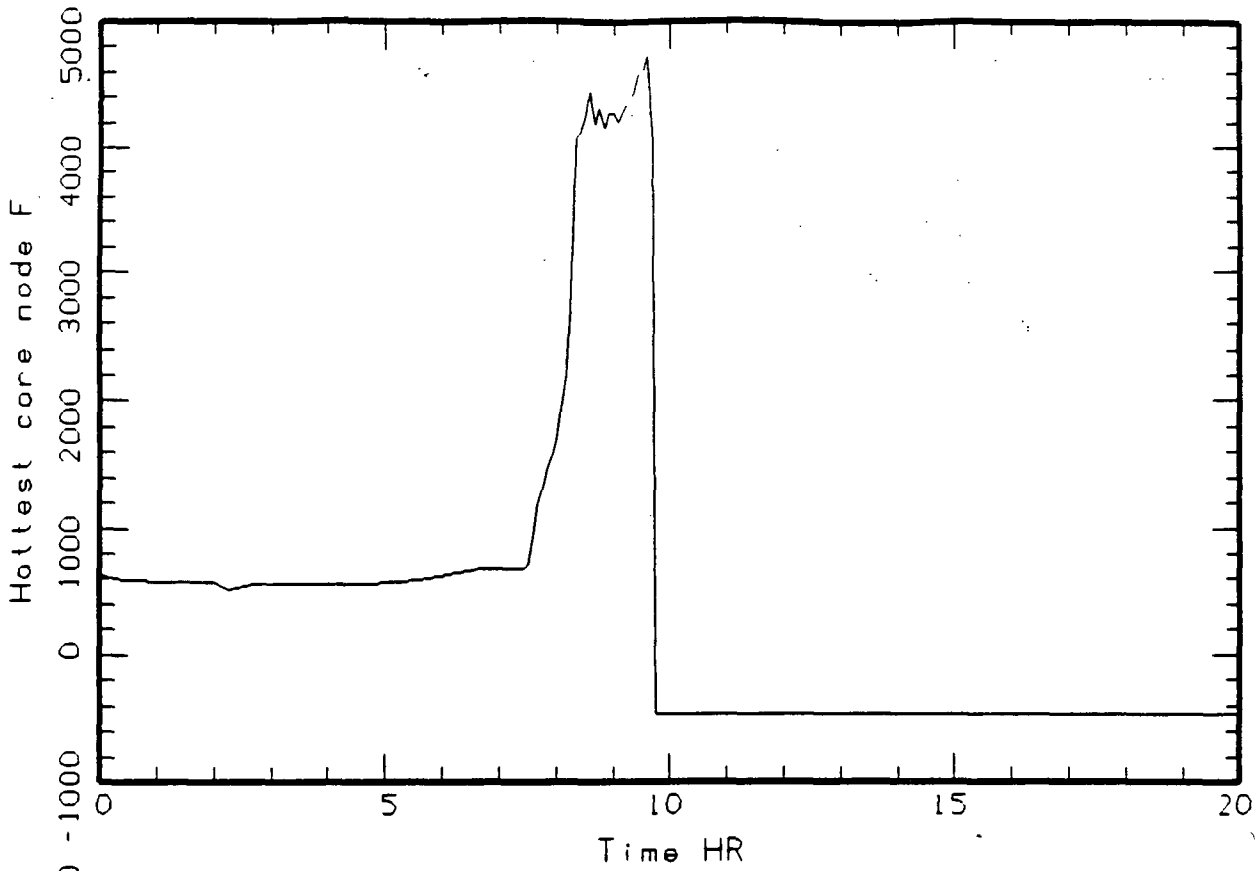


Figure 6-12 Transient Response (2 of 5)

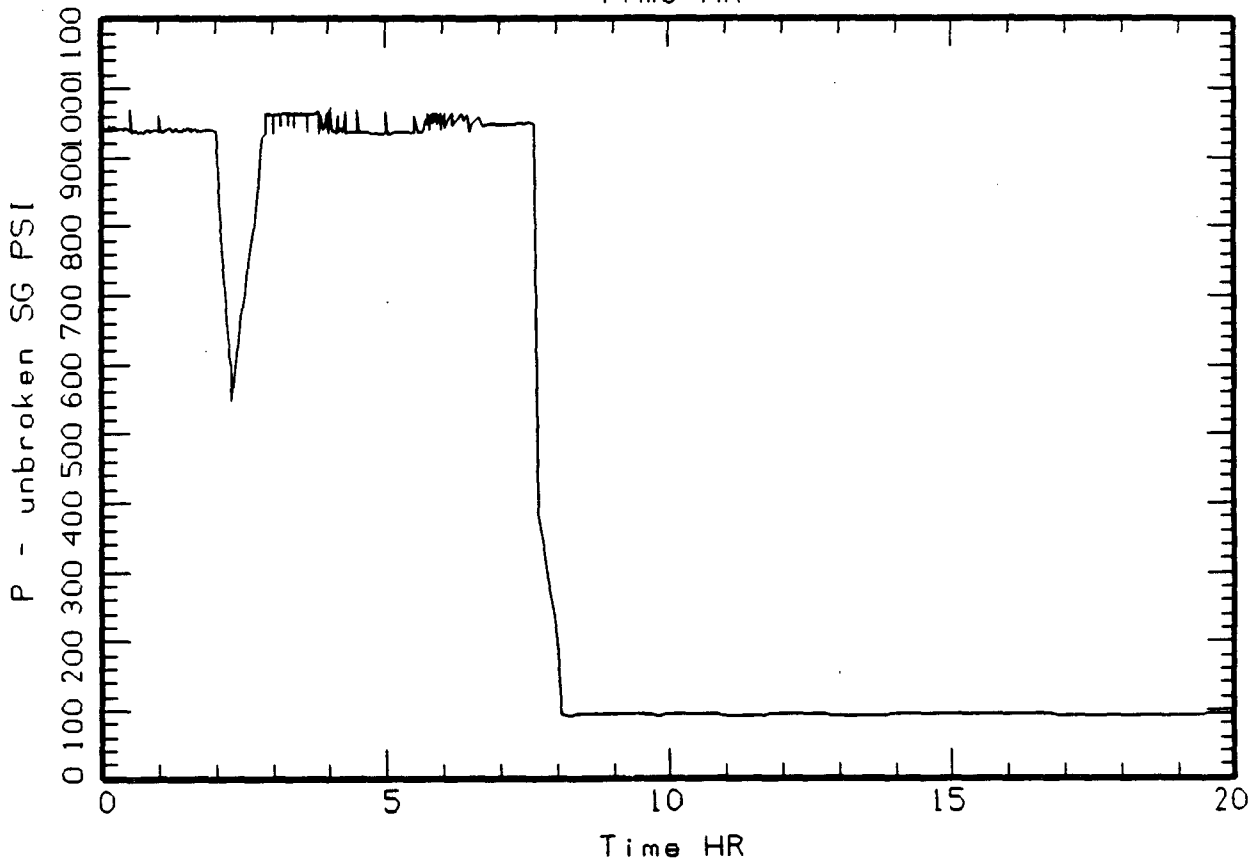
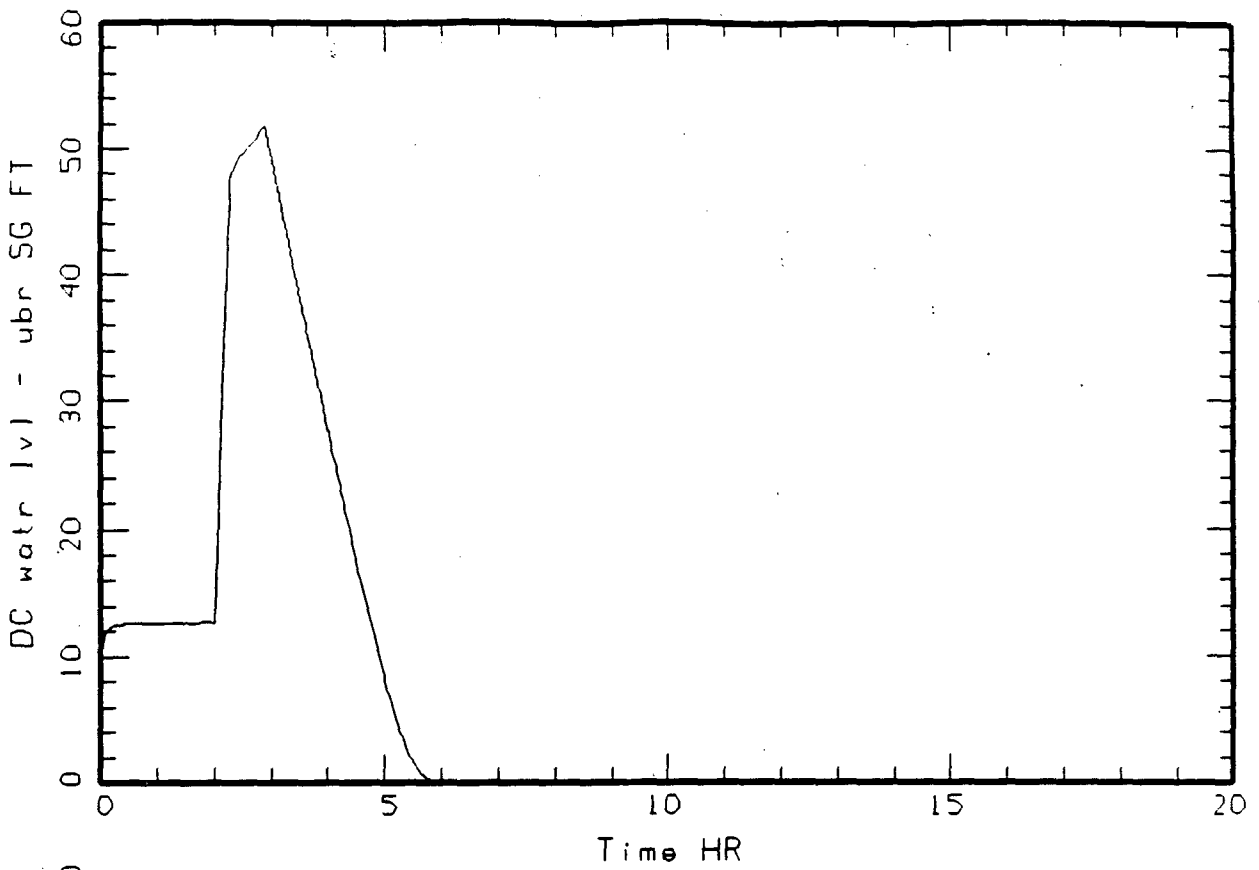


Figure 6-13 Transient Response (3 of 5)

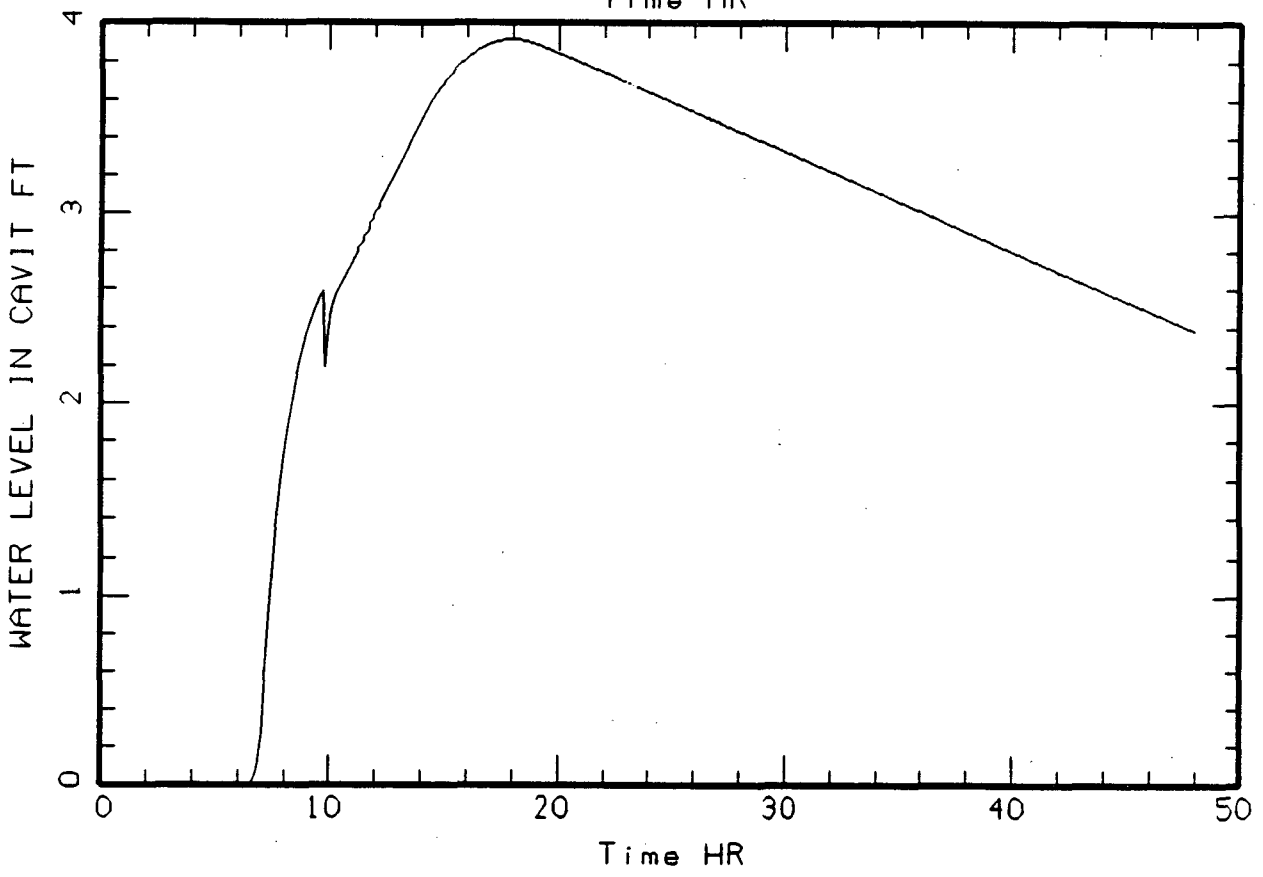
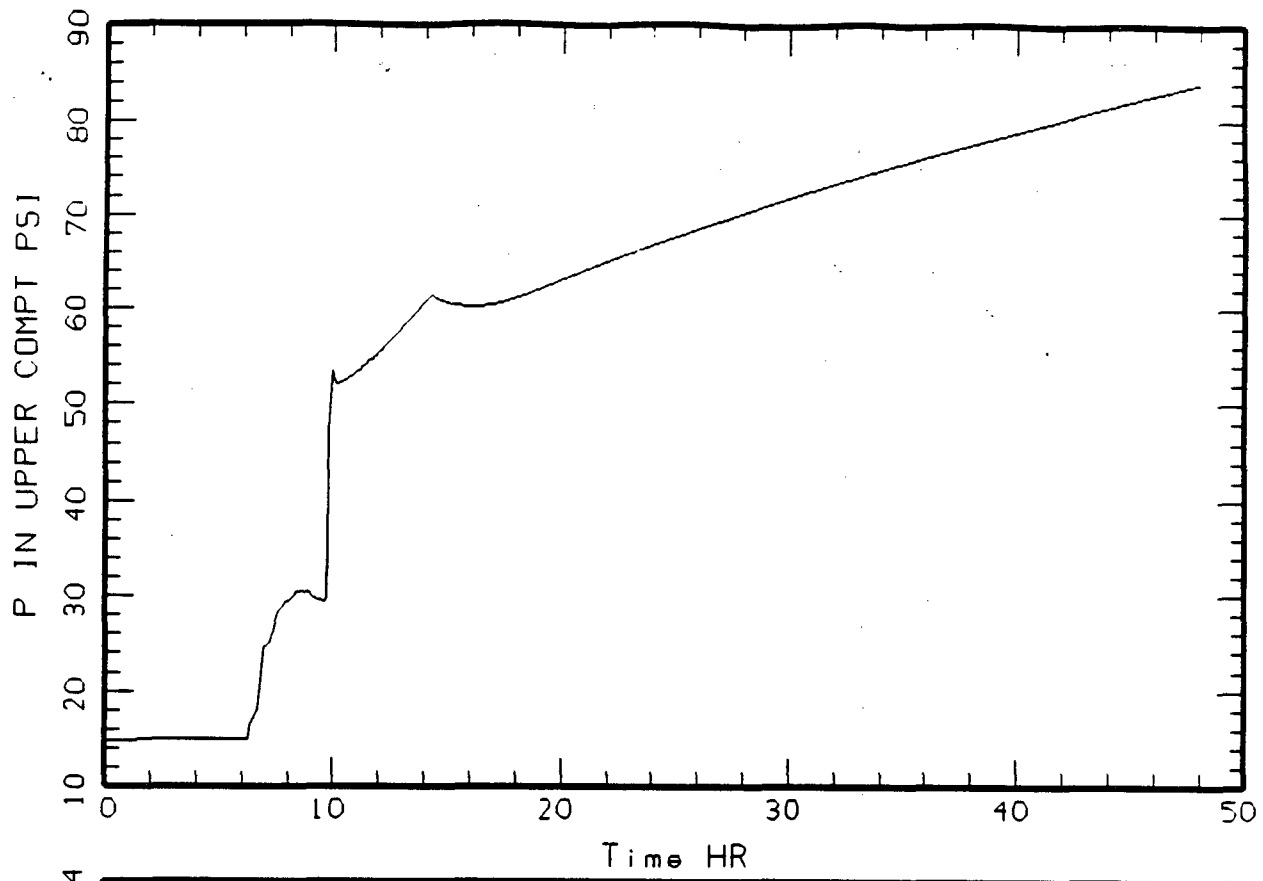


Figure 6-14 Transient Response (4 of 5)

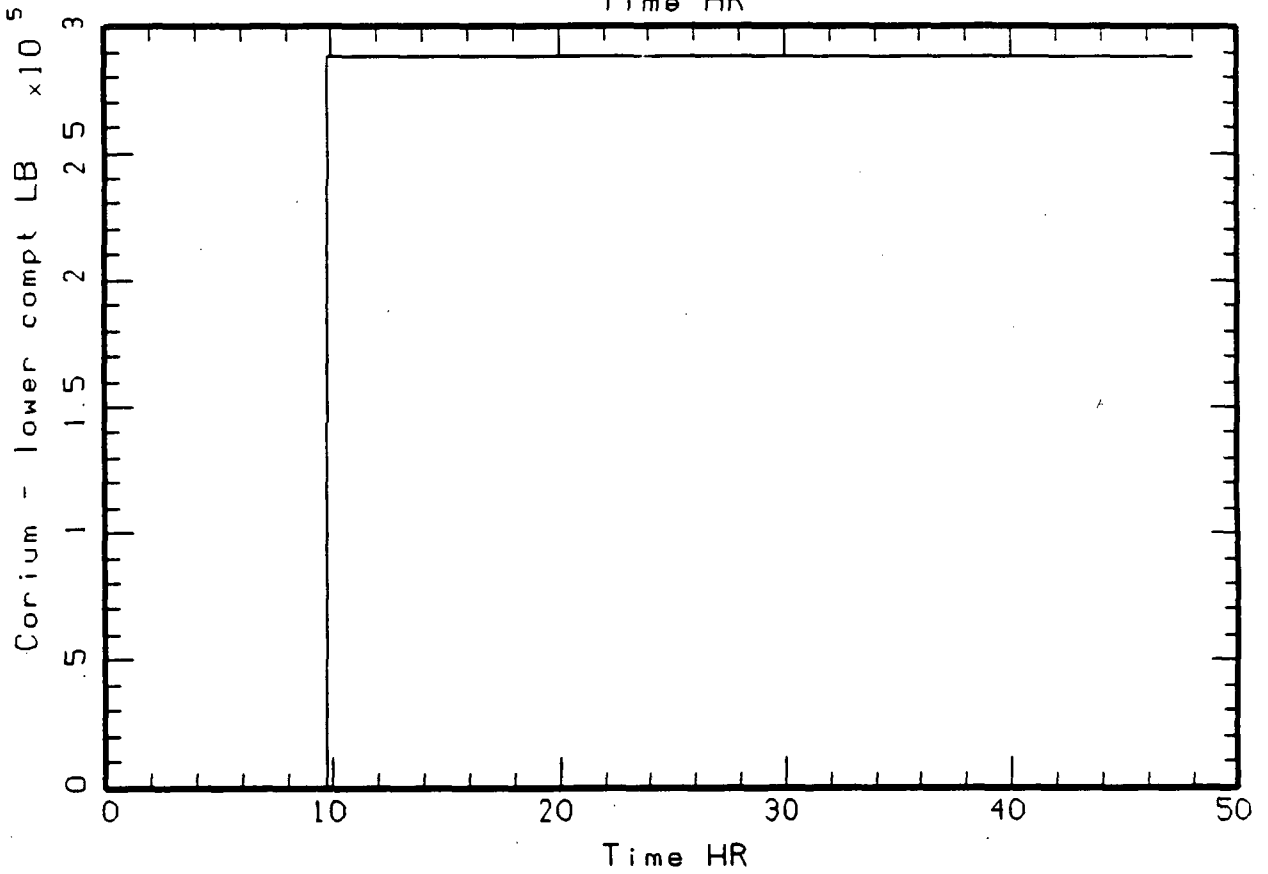
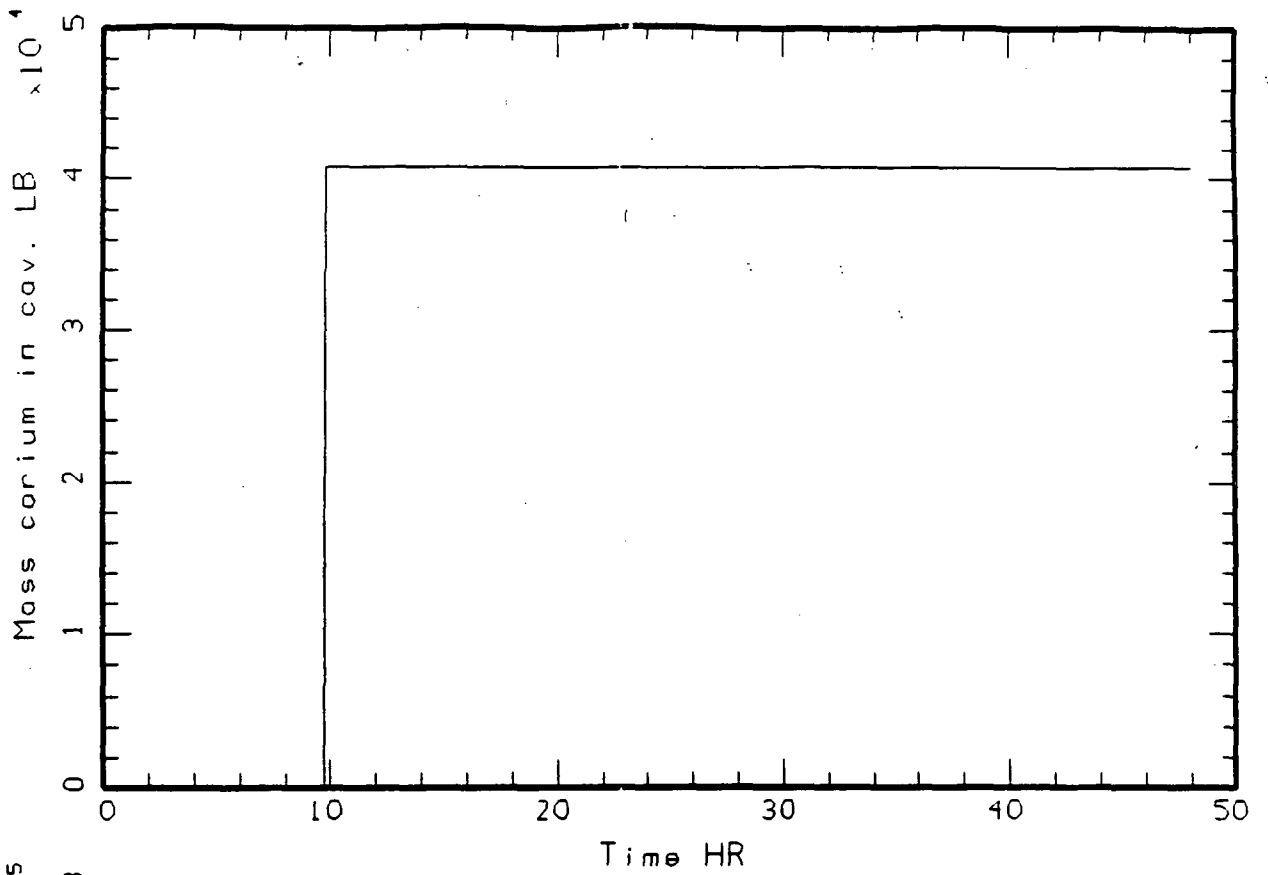


Figure 6-15 Transient Response (5 of 5)

pressure cases. For the Davis-Besse primary system piping arrangement and materials, the hot leg is the most likely portion of the pressure boundary to fail due to creep rupture. If this occurs, the RCS rapidly depressurizes and takes on characteristics very similar to a large LOCA.

6.1.5 Steam Generator Tube Ruptures

Steam generator tube rupture (SGTR) cases are unique in that they constitute a direct release path from the primary side to the secondary side, bypassing the containment. To illustrate the reactor system response to a SGTR, plant-damage state RIYVXINN will be discussed (Ref. 50): a double-ended tube rupture at sequence initiation; loss of offsite power at sequence initiation; failure of all emergency diesel generators to start (including the station blackout diesel); loss of all ECCS injection pumps and makeup pumps; loss of all containment cooling; and loss of auxiliary feedwater pump control (i.e., the pump maintains constant maximum flow) for both AFW trains at two hours into the sequence.

As for the transient sequences discussed previously, SGTR cases exhibit behavior unique from LOCA cases. The SGTR flow is equivalent to that calculated in previous detailed best-estimate RELAP5 analyses (Ref. 51) at approximately 39 lbm/second. After sequence initiation, RCS pressure initially drops due to the tube rupture, then repressurizes to just under 2200 psi due to the lack of injection and the small break size. At sequence time of two hours, system pressure is reduced sharply as both trains of auxiliary feedwater begin to maintain a constant maximum flow rate to their steam generators. After both steam-driven auxiliary feedwater pumps fail upon steam generator overfill and AFW flow is terminated, RCS pressure once again rises. After the secondary side boils dry, RCS pressure eventually reaches the pressurizer code safety valves lift pressure of 2500 psig. Although break flow is continuing into the broken steam generator and being released via steam generator safety valves, minimal heat transfer is achieved given the high enthalpy of the leak flow (as compared to feedwater). Without the pressurizer PORV, RCS pressure remains at code safety pressure until most liquid inventory is lost and the reactor vessel fails at 9.8 hours. Depressurization of the secondary side upon core superheat is possible by manually opening the steam generator atmospheric vent valves, but has negligible effect given the lack of effective heat transfer from leak flow, as noted above.

For this sequence a value of 30% clad oxidation is calculated. The corresponding hydrogen concentration after reactor vessel failure is 0.5%, which is an order of magnitude less than the minimum concentration necessary to support combustion. The associated sequence steam concentration of 47% is less than that required to inert the containment for some concentrations of combustible gases. Figures 6-16 through 6-18 summarize these parameters.

Prior to reactor vessel failure, containment pressure rises about three psi due to actuation of the RCS code safety valves. At reactor vessel failure, containment pressure rises sharply to about 30 psia. With a RCS pressure of 2500 psig and minimal level of less than 0.5

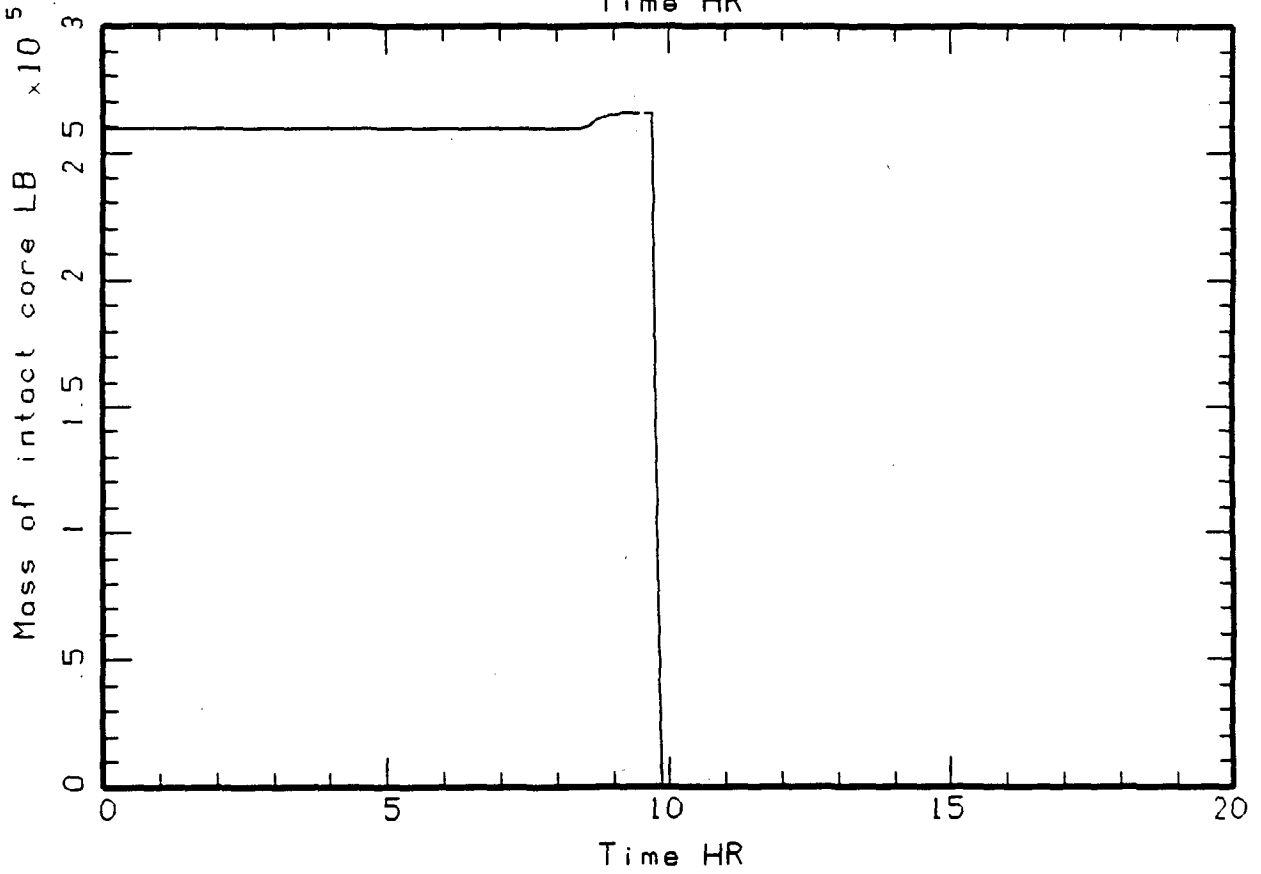
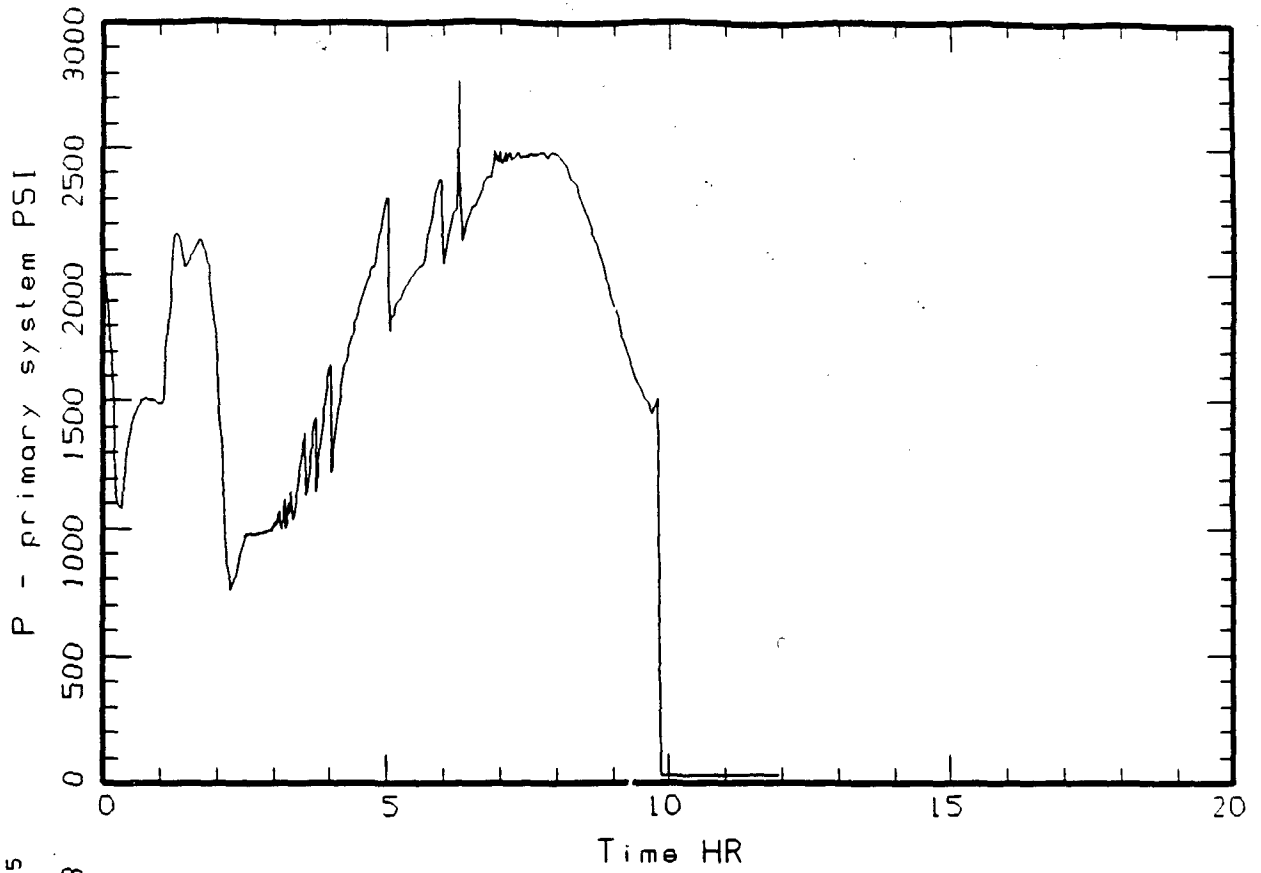


Figure 6-16 Steam Generator Tube Rupture Response (1 of 5)

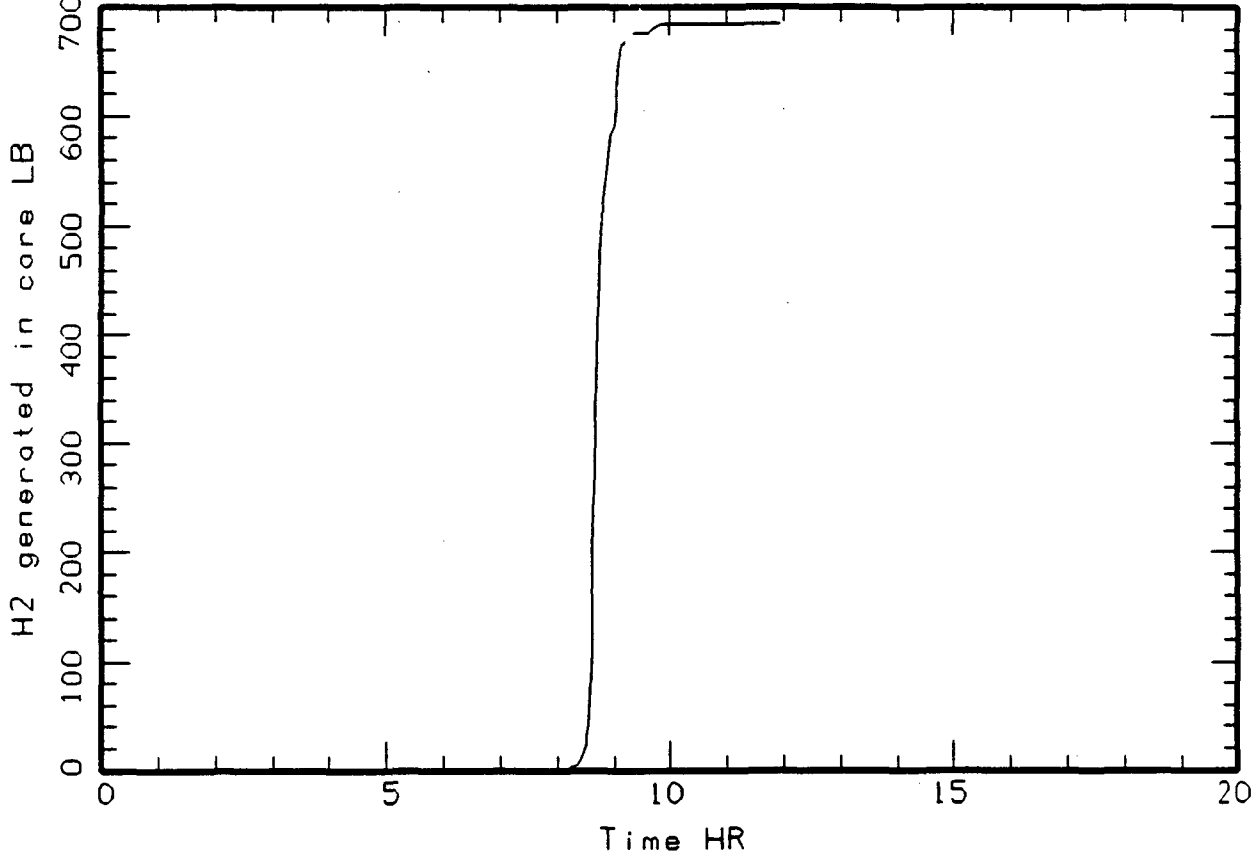
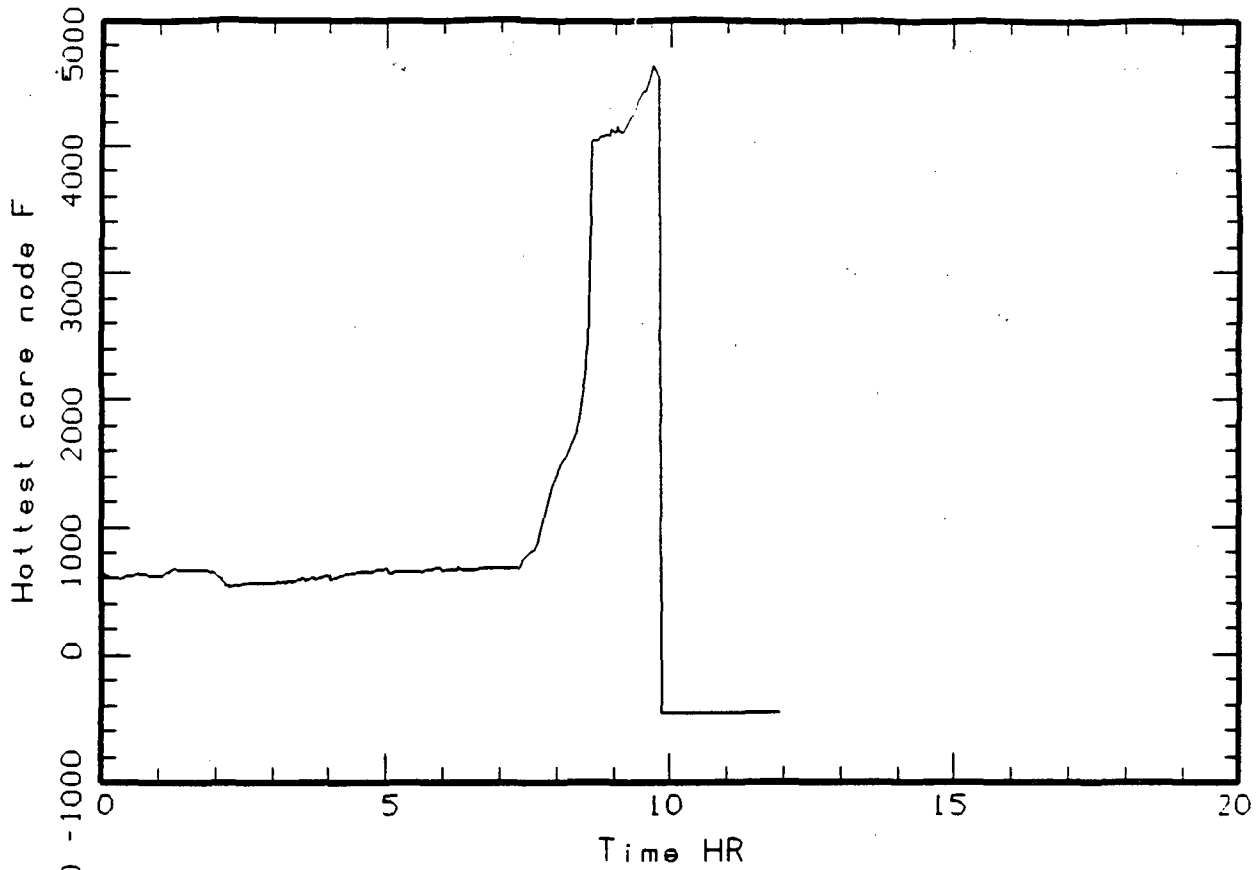


Figure 6-17 Steam Generator Tube Rupture Response (2 of 5)

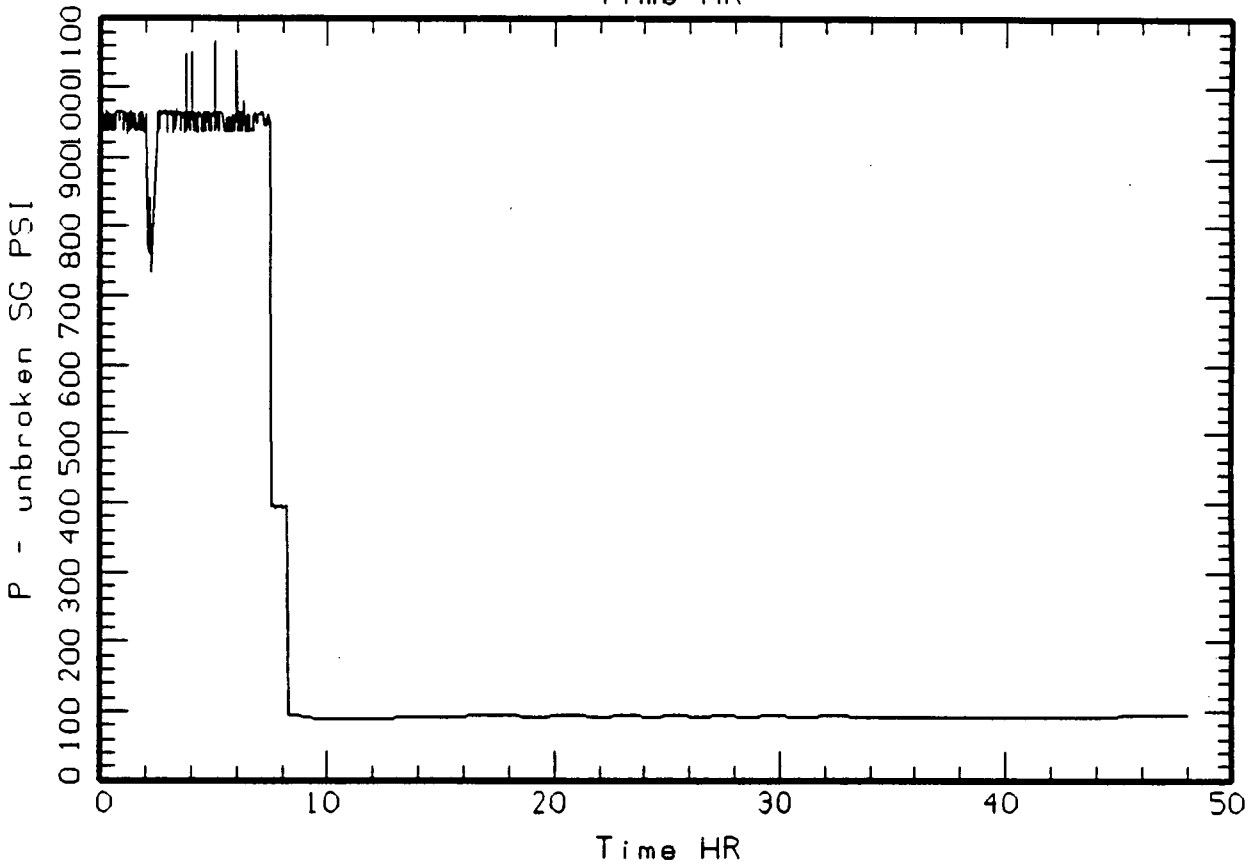
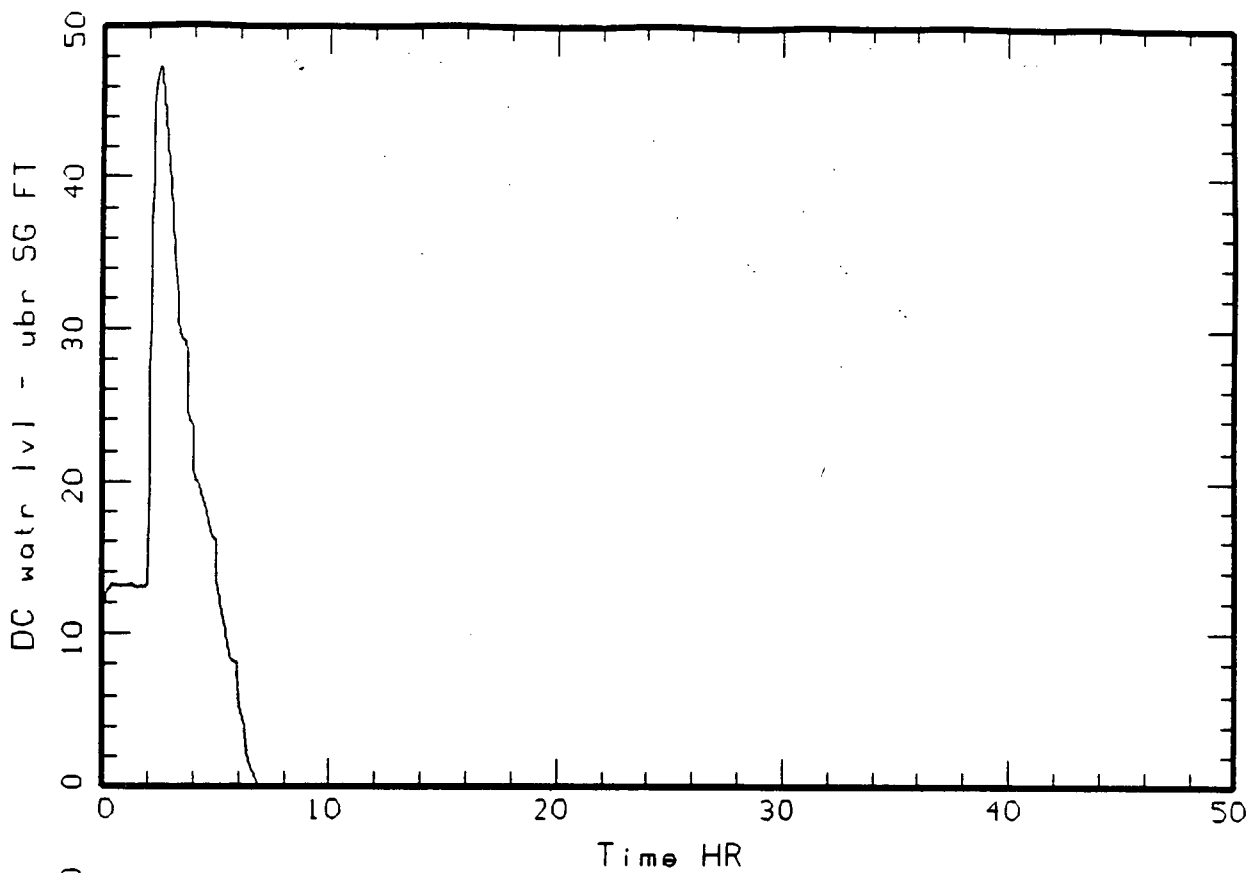


Figure 6-18 Steam Generator Tube Rupture Response (3 of 5)

feet of water in the reactor cavity, approximately 86% of the corium is forced into the containment lower level. Steaming of water overlying corium without the presence of any containment heat removal results in a continual slow rise in pressure (~ 1.0 psi/hour) for the remainder of the sequence analysis period. Although the containment pressurization rate is somewhat reduced by gas flow out of the ruptured tube, this also represents a direct path for radionuclides to bypass the containment. Figures 6-19 and 6-20 summarize the containment response.

Other SGTR cases present variations on this response. For many cases, the estimation of a credible core-damage sequence due to a SGTR is dependent on the ability to depressurize the RCS to about 1000 psig. At this pressure, the primary/secondary pressure differential is essentially non-existent and the leakage rate becomes minor. As such, the availability of auxiliary feedwater and the ability to steam the secondary side is of major importance. Even without injection, if the primary side pressure can be lowered to ~ 1000 psig, it takes much longer than 48 hours for the core to become uncovered if secondary side heat removal can be maintained.

For the case discussed above, RCS pressure is not maintained at high pressure for sufficient duration for creep rupture of the system pressure boundary to become probable. For any case where creep rupture might be probable, the RCS would depressurize rapidly and take on the characteristic of a large LOCA. The source term from such an event would be increased to some extent given the tube rupture bypass path.

6.2 QUANTIFICATION OF THE CET

The logic that comprises the CET and the probabilistic treatment for the basic events in that logic are described in Section 5.2. Once the probabilities were developed for the primary events represented in the supporting logic for the CET, the quantification of CET outcomes was a relatively straightforward process. The first step in the quantification process was to construct a fault tree that linked the top events in the CET according to the CET logic. To do this, a fault-tree top event was defined for each pathway represented in the CET. This top event was then developed as an "AND" gate of each of the CET top events relevant to the pathway; the supporting logic was used as the input for all CET top events that had failed according to the CET logic, and the complement of the supporting logic was used for successful top events.

The logic supporting each of the top events in the CET was constructed using the CAFTA computer workstation, in the same manner as for the system fault trees (refer to Section 2.1 of Part 3 for more information on that process). Therefore, CAFTA was used to assemble the logic for the CET pathways as well. The routines normally applied for fault-tree solution (i.e., by finding cut sets and approximating their probabilities) are not adequate for evaluating the CET outcomes, because of the need to track a large number of both success and failure states, and because of the use of relatively large probabilities for some events, such

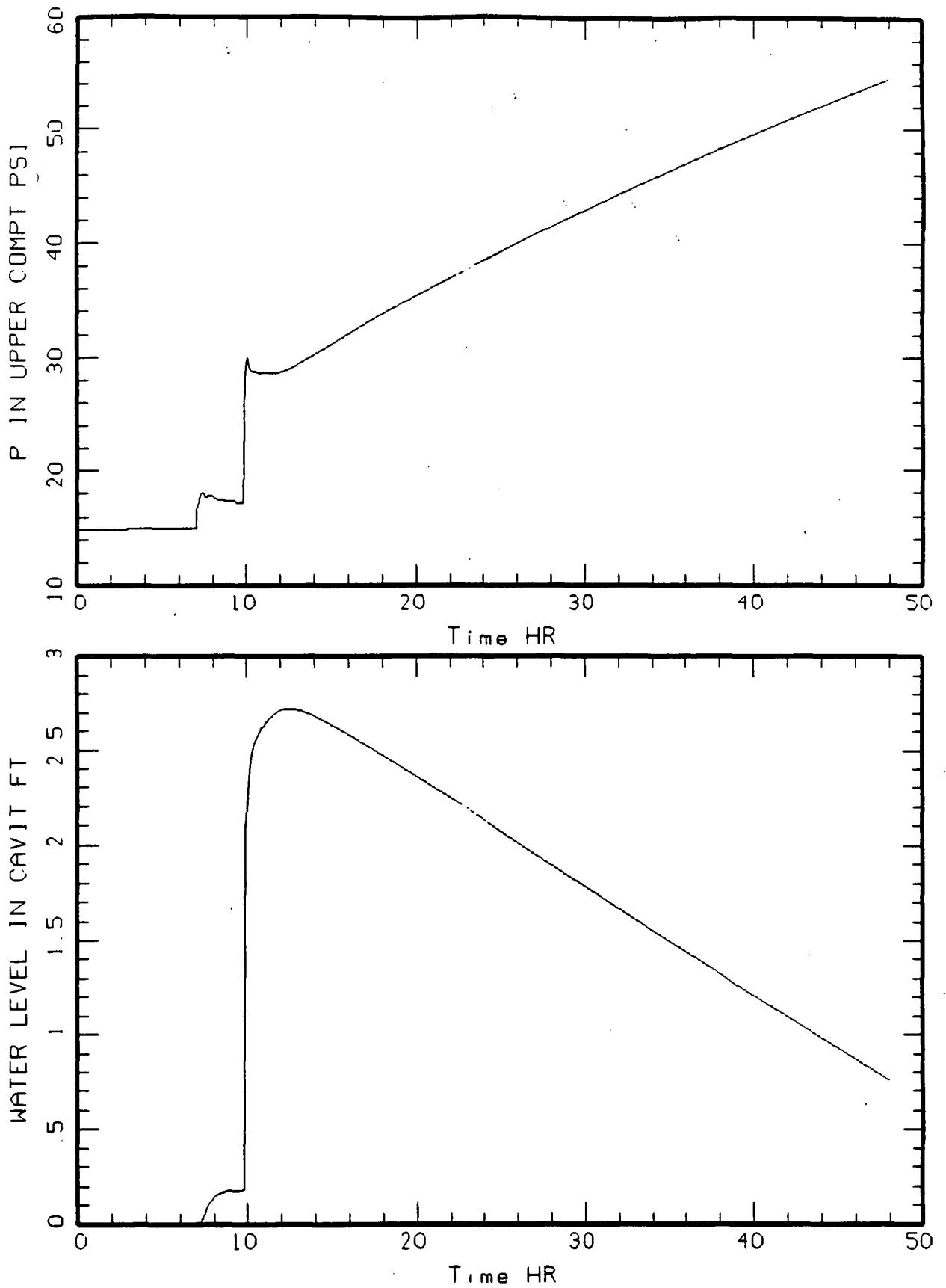


Figure 6-19 Steam Generator Tube Rupture Response (4 of 5)

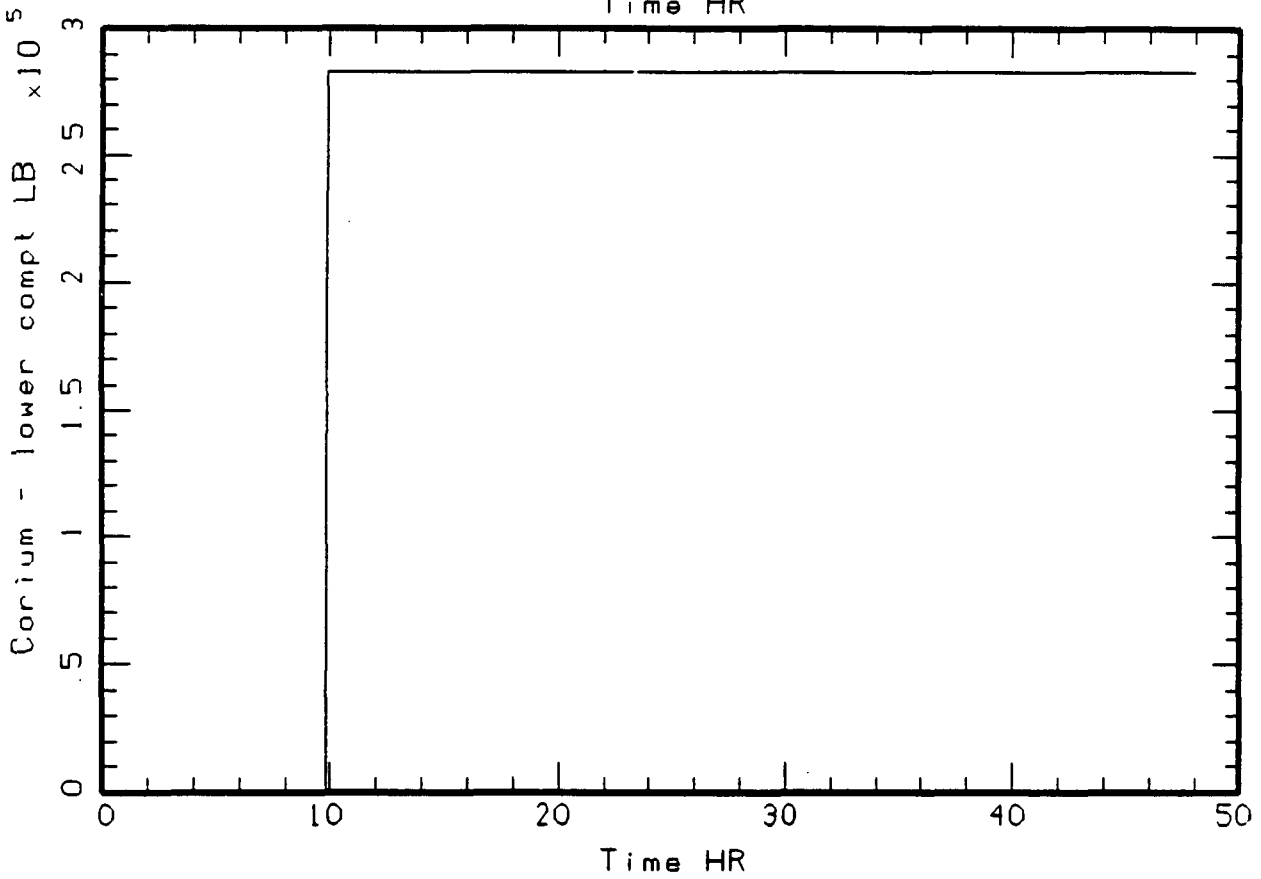
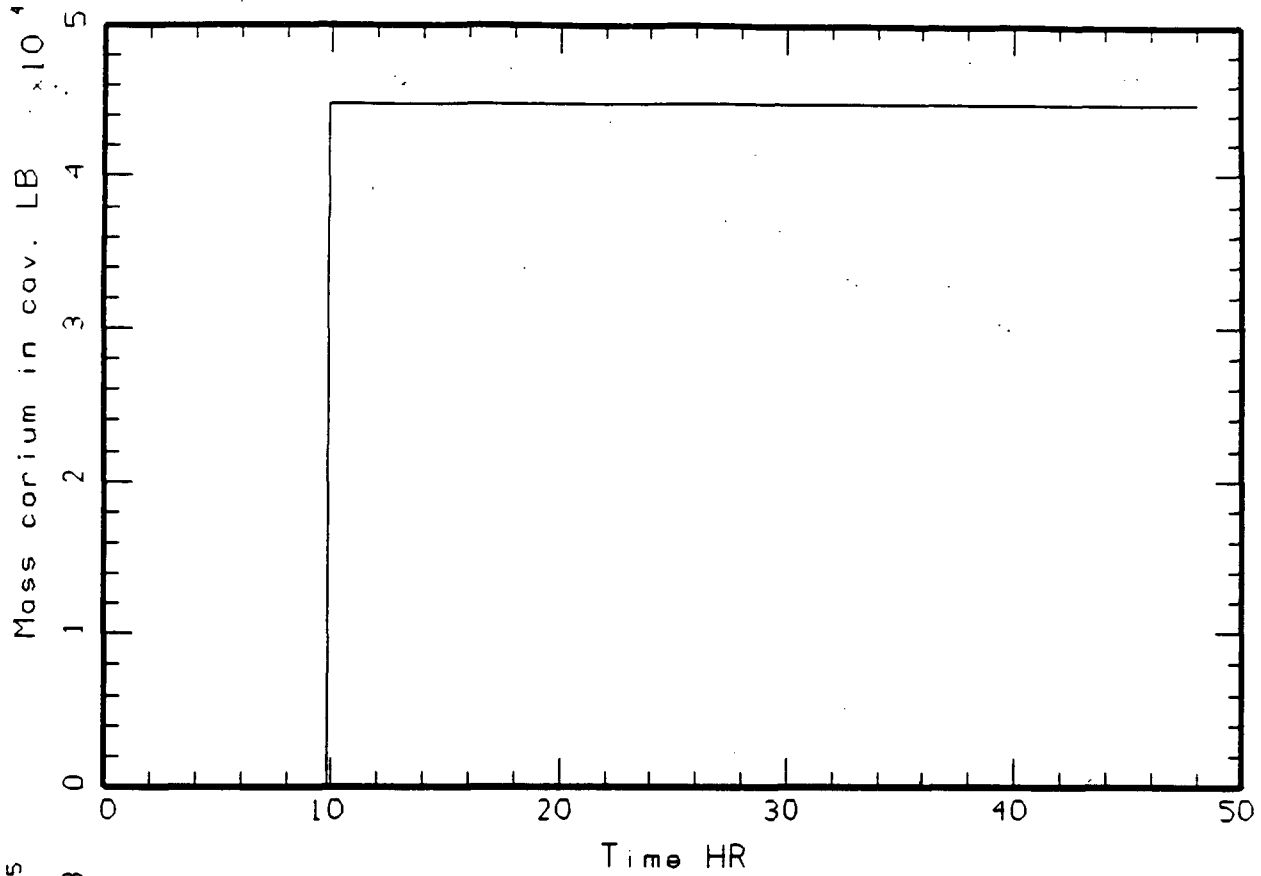


Figure 6-20 Steam Generator Tube Rupture Response (5 of 5)

that approximation methods do not apply. Consequently, the computer code GTPROB was used to perform the CET quantification (Ref. 52).

GTPROB is a supplement to CAFTA that permits direct quantification of fault trees by using a truth table expansion algorithm. GTPROB calculates the probability for every top gate and every intermediate gate in any set of fault-tree logic. Depending on the size of the fault tree being solved, GTPROB can calculate the exact probability for a fault-tree gate, or an approximation if it is necessary to apply a truncation value to make the solution tractable. The CET and supporting logic comprised a set of fault-tree logic that was not extremely complicated, so that it was possible to perform the quantification with a very low truncation value.

Because the probabilities for some of the events in the CET logic varied according to the plant-damage state being considered, it was necessary to assemble a separate data base for several of the damage states. Once this was done, GTPROB was exercised for the full set of CET logic for each plant-damage state, calling upon the appropriate data base. The results of this process were the probabilities for every gate in the logic, including those corresponding to the CET outcomes, conditional on occurrence of the plant-damage state. The calculation of probabilities for intermediate gates proved very valuable in tracing through the event tree to ensure that the probabilities for the end states appeared to be appropriate, and to understand the impact of various phenomena on the outcomes. The ability to perform the calculations quickly and efficiently also facilitated performance of several sensitivity studies. The base case results, as well as those of the sensitivity studies, are described in the following section.

6.3 FREQUENCIES FOR CET OUTCOMES

The basic results from the quantification of the CET are a set of probabilities for the CET outcomes, conditional on a particular plant-damage state. Because there are 61 CET outcomes and 64 plant-damage states, this produces a very large volume of information. Therefore, the results have been consolidated in various ways to provide better illustration of the important findings.

Table 6-1 provides a summary of the CET results for all plant-damage states with frequencies greater than 10^{-7} per year, organized according to general categories of CET outcomes. The general categories are as follows:

- Containment bypass, encompassing interfacing-systems LOCAs and SGTRs (including both those that initiated an accident sequence and those that resulted from creep rupture during core degradation);
- Early containment failure, including failure of containment isolation and failures due to phenomena such as hydrogen burns before or around the time of vessel failure;
- Failure of the containment side wall, which could occur due to ablation of the concrete curb at the basement level of containment, leading to containment failure in the intermediate to late time frame;

Table 6-1
Conditional Probabilities of Containment Failure Modes

Plant-Damage State	Frequency of Damage State	Containment Bypass	Early Failure	Side Wall Failure	Late Failure	Basemat Meltthrough	Intact Containment
AIXYFYYX	2.6×10^{-7}		0.0021			0.0100	0.9879
AIXYNINX	1.0×10^{-7}		0.0020		0.1017	0.0896	0.8068
ARXYFRYX	8.0×10^{-7}		0.0033		0.0020	0.0099	0.9848
ARXYFYYX	5.3×10^{-7}		0.0033		0.0020	0.0099	0.9848
MIXYFYCX	1.4×10^{-7}		0.0007	0.0015		0.0076	0.9902
MIXYFYYX	2.3×10^{-7}		0.0026	0.0015	0.0001	0.0993	0.8965
MRXYFRYX	1.5×10^{-6}		0.0036			0.0099	0.9865
RRYVXIND	1.7×10^{-7}	1.0000					
RRNVXIND	1.1×10^{-7}	1.0000					
SINYFYCD	7.9×10^{-7}	0.0107	0.0069	0.0066		0.0038	0.9720
SINYFYYN	2.0×10^{-6}	0.1071	0.0074	0.0077		0.0019	0.8759
SIYYFIND	6.9×10^{-7}		0.0030	0.0015	0.0001	0.0993	0.8961
SIYYFINN	1.1×10^{-7}		0.0032	0.0149	0.0001	0.0966	0.8852
SIYYFYCD	8.6×10^{-7}		0.0003			0.0008	0.9989
SIYYFYD	6.9×10^{-6}		0.0030	0.0015	0.0001	0.0993	0.8961
SIYYFYYN	6.6×10^{-7}		0.0032	0.0149	0.0001	0.0966	0.8852
SIYYNINN	6.9×10^{-6}		0.0022	0.0149	0.1001	0.0869	0.7959

Table 6-1 (continued)
Conditional Probabilities of Containment Failure Modes

Plant-Damage State	Frequency of Damage State	Containment Bypass	Early Failure	Side Wall Failure	Late Failure	Basemat Melthrough	Intact Containment
SRNYFRYN	2.2×10^{-7}	0.1071	0.0075	0.0069	0.0018	0.0026	0.8742
SRYYFIYD	8.9×10^{-7}		0.0040			0.0099	0.9860
SRYYFRYD	1.2×10^{-6}		0.0040			0.0099	0.9860
SRYYFRYN	6.2×10^{-7}		0.0041	0.0002		0.0098	0.9860
SRYYFYCD	1.1×10^{-6}		0.0003			0.0008	0.9988
SRYYFYD	1.3×10^{-6}		0.0040			0.0099	0.9860
SRYYFYYN	6.7×10^{-7}		0.0041	0.0002		0.0098	0.9860
TINININN	9.0×10^{-7}	0.0005	0.0051	0.1955	0.0814	0.0542	0.6633
TINYFYCD	1.3×10^{-5}	0.0054	0.0042	0.0033		0.0044	0.9828
TINYFYD	2.8×10^{-7}	0.0018	0.0050	0.0034		0.0069	0.9830
TINYFYYN	2.6×10^{-6}	0.0536	0.0053	0.0038		0.0059	0.9314
TINYLYYN	3.1×10^{-7}	0.0536	0.0046	0.0034	0.0019	0.0038	0.9328
TINYNINN	1.8×10^{-5}	0.0005	0.0051	0.1955	0.0814	0.0542	0.6633
TIYYFYYN	1.6×10^{-7}		0.0068	0.0065		0.0040	0.9827
TRNYFYYN	1.7×10^{-7}	0.0536	0.0059	0.0034		0.0063	0.9308
V	8.8×10^{-7}	1.0000					
Total	6.6×10^{-5}	0.026	0.0040	0.059	0.034	0.041	0.836

- Late containment failure, due to slow overpressurization or burns long after vessel failure;
- Basemat meltthrough, implied for cases in which containment was not predicted to fail by any other mechanism, but the core debris was not cooled; and
- Intact containment, in which it would be expected that containment integrity would be maintained in the long term.

The results were also weighted by the frequencies of the plant-damage states to provide an overall indication of the relative likelihood of the various containment failure modes. The overall conditional probabilities of the categories summarized above are illustrated in Figure 6-21. The factors that contribute to the results for each of the general categories of outcomes are described below. To aid in understanding the results, and particularly the potential impact of uncertainties in some phenomena, a set of sensitivity studies was also conducted. The nature of the sensitivity studies and their results are also described in conjunction with the breakdown of the overall results.

As this figure indicates, no containment failure would be expected for approximately 84% of the sequences that comprise the core-damage frequency. For those cases in which containment failure would not be expected to occur, the core debris would be in a cooled state and containment heat removal would be functioning to limit the pressure rise inside containment. The reasons for this relatively large fraction of outcomes that correspond to an intact containment are discussed in the context of the general categories of containment failure below.

6.3.1 Containment Bypass

It was calculated that about 2.6% of the plant-damage states would result in containment bypass. A breakdown of the plant-damage states that contribute to the bypass scenarios is provided in Figure 6-22. Approximately half the frequency of bypass is due to interfacing-systems LOCAs, and another 20% results from sequences initiated by a SGTR. The remaining 30% is due to creep ruptures of steam generator tubes for other accidents in which core damage was expected to progress at high pressure. Thus, less than 1% of the core-damage sequences that were not initially bypasses would lead to bypass failure of containment. This is due to several factors, including the need for operation of the RCPs (as discussed below), the likelihood that the accident would progress at pressures low enough that they would not lead to creep rupture in a relatively short time, and the availability of feedwater which, in addition to aiding in keeping RCS pressure low, could cool the hot gases from the core.

One of the factors that contributes to limiting the potential for an induced tube rupture is the need for extended operation of the RCPs to transport hot gases from the reactor vessel to the steam generators. The communication between the core and the steam generators would be relatively poor if only natural processes would be available to support heating of the

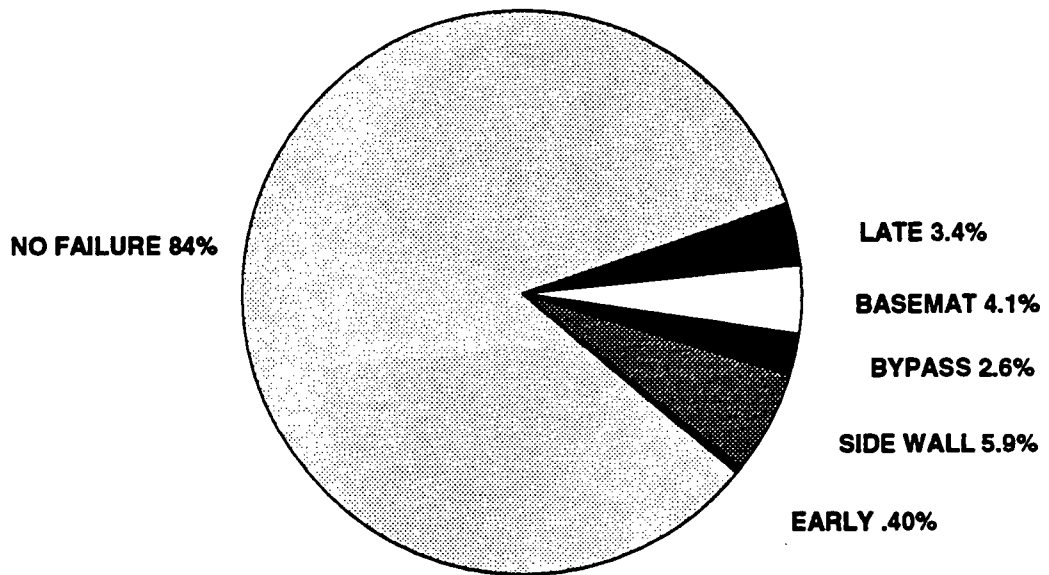


Figure 6-21. Overall Summary of Conditional Probabilities for Containment Failure Modes

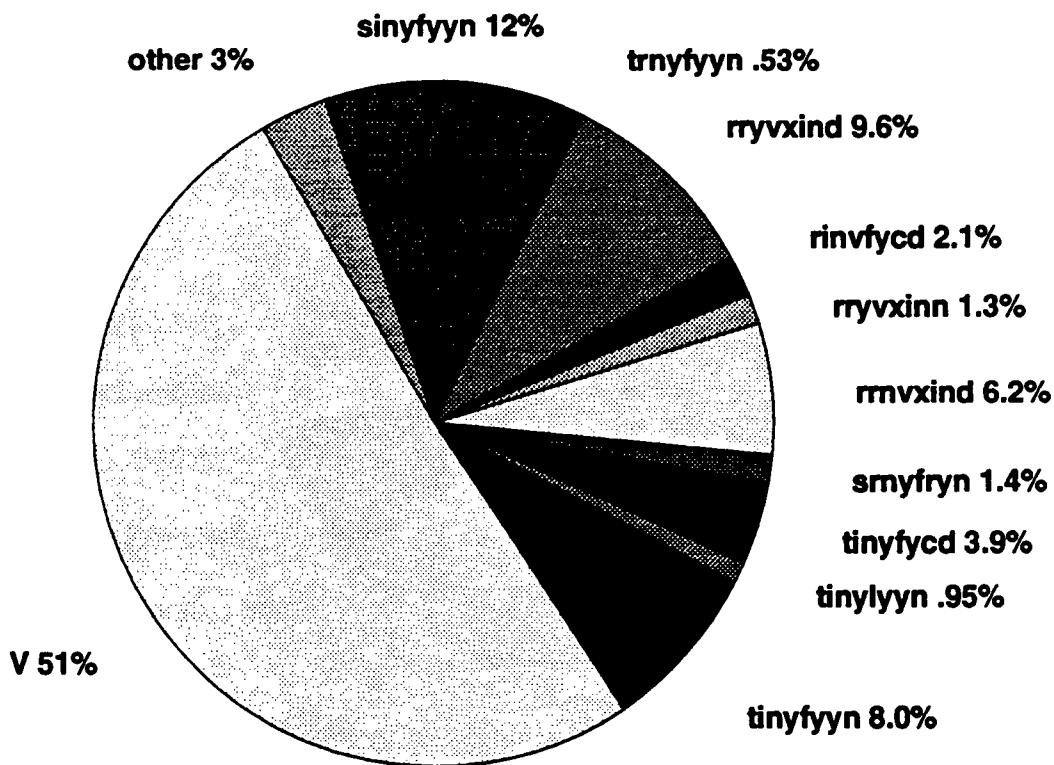


Figure 6-22. Contributions of Plant-Damage States to Frequency of Containment Bypass

tubes, and creep rupture of a hot leg would be expected long before a tube might fail. The RCPs would generally be idle at the onset of core degradation (either because the pumps would be unavailable, such as due to loss of offsite power or of cooling water, or because the operators would trip them when subcooling margin was lost). The portion of the emergency procedure that provides guidance for inadequate core cooling calls for restarting the pumps to attempt to restore cooling flow to the core (Ref. 33). This would tend to cause water in the pump bowls to be transferred to the core, resulting in a short-lived reduction in gas temperatures in the RCS. The mass remaining in the RCS would then heat back up, potentially threatening the tubes in the steam generators. It was judged, however, that the RCPs would be unlikely to operate for very long under these conditions. To examine the impact of this judgment, a sensitivity case was evaluated in which it was assumed to be likely that the pumps would operate for a sufficient period of time to permit creep rupture of the tubes (if the RCPs were available). In this sensitivity study, the overall conditional probability of bypass given core damage increased from 2.6% to about 8.2%. This indicates that the assumptions regarding RCP operation under degraded core conditions are moderately important. As described in Part 6, the instructions for restarting the pumps and allowing them to continue operating are being re-examined.

6.3.2 Early Containment Failure

The relatively small fraction (about 0.4%) of outcomes that correspond to early failures is spread among several categories of low-probability challenges, including early hydrogen burns, in-vessel and ex-vessel steam explosions, and the loading at vessel breach due to steam generation and direct containment heating. Isolation failures were assessed to contribute a negligible amount to the potential for releases from containment for all plant-damage states. The plant-damage states that contribute most to the potential for early containment failure are identified in Figure 6-23.

About 37% of the contribution to early containment failure results from plant-damage states TINYNINN and TINB1NINN, in which there is a transient without heat removal via the steam generators and with failure of containment heat removal and containment sprays. These damage states result almost entirely from sequences involving station blackout. They are important (relative to early containment failure) because they could involve core damage at high pressure (unless, for example, creep rupture of a hot leg were to occur), the contents of the BWST would not flood the reactor cavity deeply prior to vessel breach, and because they comprise a substantial fraction (about 29%) of the core-damage frequency. The remaining contributions are distributed among many other plant-damage states, as indicated in Figure 6-23. To investigate further the uncertainties associated with containment response to high pressure melt ejection, the conditional probability of containment failure given pressurized ejection from the reactor cavity was increased from 0.01 to 0.1 in a sensitivity study. The impact was to increase the conditional probability of early containment failure

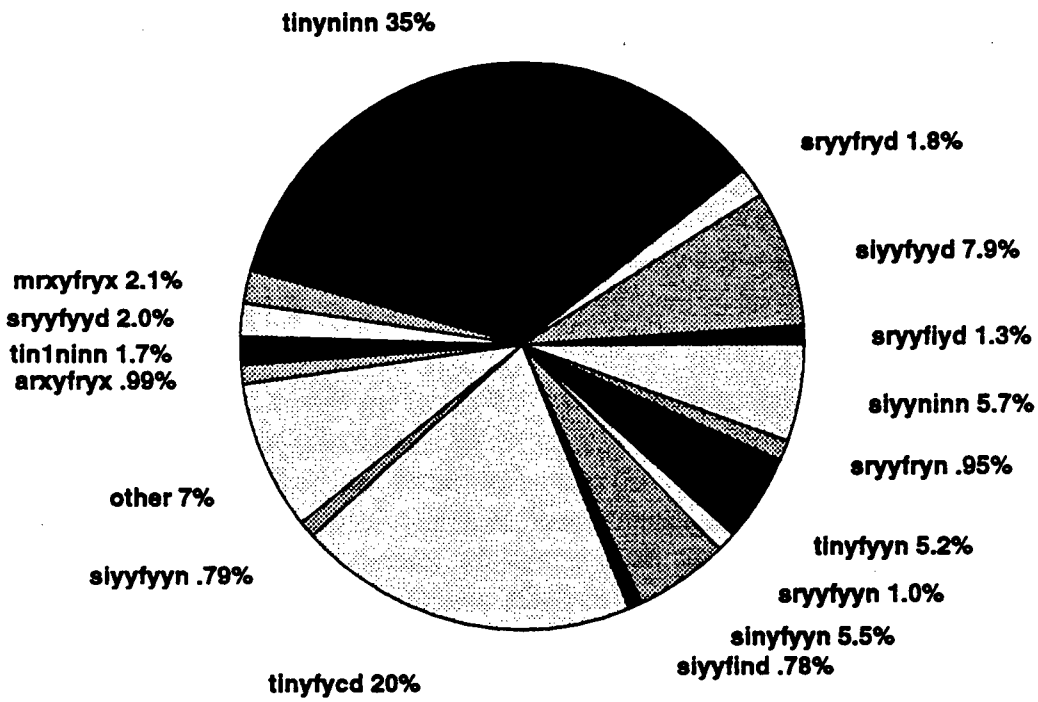


Figure 6-23. Contributions of Plant-Damage States to Frequency of Early Containment Failure

from about 0.4% to about 2.5%. Thus, although the overall probability of early failure would still be low, the results are sensitive to this parameter. As described in Section 5.2.5, the conditional probability of failure given pressurized ejection for the base case was calculated in a manner that took into account uncertainties in the phenomena, and the value used is considered to be appropriate for Davis-Besse.

6.3.3 Side Wall Failure

The largest fraction of containment failures was estimated to be associated with the potential for side wall failure of containment, at about 6%. This might result in containment failure on the order of several hours after vessel failure (i.e., after the core debris dried out in the basement, heated up sufficiently to begin attacking the concrete, and ablated the 1.5-ft thick curb in the basement). The fraction of plant-damage states that result in this outcome is due to the strong potential that a substantial fraction of the core debris would be transported up into the basement for scenarios in which core damage progressed at pressures of 500 to 600 psig or higher, coupled with the possibility that the debris would not be covered by overlying water if the contents of the BWST had not been injected.

As shown in Figure 6-24, plant-damage state TINYNINN is also the most important contributor for this containment failure mode, contributing about 90% to the fraction of outcomes that lead to side wall failure. The same factors that lead to its relative importance with respect to early containment failure make it dominant for side wall failure as well (i.e., the large contribution to overall core-damage frequency, the likelihood of core damage at high pressure, and the lack of injection of the BWST contents).

A sensitivity study was also performed in which the conditional probabilities for events relating to failure of debris-bed coolability in the presence of overlying water were increased to 0.2 (from 0.01 or 0.1, depending on the specific case). In this case, there was a modest increase in the fraction of results leading to side wall failure (from 5.9% to 8%). The relative contribution of plant-damage state TINYNINN, however, was reduced substantially. This was due to the rise in the importance of the large fraction of damage states in which the basement would be flooded by water from the BWST.

6.3.4 Late Containment Failure

Late failure of containment was estimated to occur for about 3.4% of the total core-damage frequency. Late failures include long-term overpressurization due to the absence of containment heat removal and the possibility of burning of hydrogen or other combustible gases long after vessel breach.

Late failure was assessed to be relatively unlikely largely because heat removal would be available for many plant-damage states, or would be recovered well within the time necessary to prevent long-term overpressurization. Late burns that would fail containment were assessed to be relatively remote possibilities due to the limited source terms for

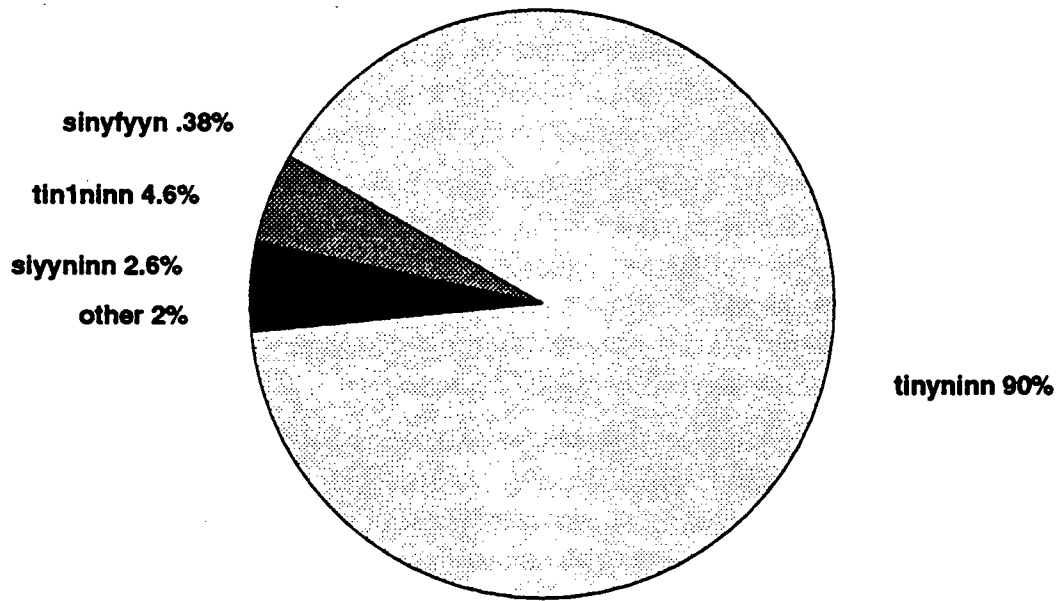


Figure 6-24. Contributions of Plant-Damage States to Frequency of Side Wall Failure of Containment

combustible gases and the large volume of containment that could accommodate even large burns without exceeding the containment pressure capacity.

The breakdown of plant-damage states that contribute to occurrence of late containment failure is provided in Figure 6-25. Once again, damage state TINYNN is most important, contributing about 65% for this failure mode. This is due to the relatively large fraction of the core-damage frequency this damage state represents, coupled with the lack of containment heat removal.

In the base case, it was judged to be likely that containment heat removal would be recovered prior to long-term overpressurization for plant-damage states in which it was not initially available (including damage state TINYNN). To examine the impact of this assessment, a sensitivity case was performed in which no credit was given to late recovery of heat removal. In that case, the fraction of outcomes leading to late failure was assessed to increase from about 3% to about 33%. This would correspond roughly to the fraction of damage states for which heat removal was not initially available. Thus, as would be expected, eventual recovery of heat removal is important for long-term maintenance of containment integrity following core damage.

6.3.5 Basemat Melthrough

Outcomes of the CET in which there was no other failure but the core debris was not cooled were assigned, by default, to the category of basemat melthrough. This assignment may be somewhat conservative, since, for many accidents, it would be expected that the debris would freeze long before the basemat was penetrated. Depending on where the debris was located, ablation through the full depth of the concrete could take on the order of 100 hours. The effect of this potential conservatism is lessened by the fact that these outcomes were assigned to the release categories for intact containment, since leakage from the containment would be expected to be the most important mode of release.

Overall, about 4% of the total core-damage frequency was estimated to result in basemat melthrough. As Figure 6-26 indicates, the plant-damage states that contribute are primarily those in which the BWST contents would not be injected, since successful debris cooling was much more likely if the debris was deeply flooded. Note also that these outcomes would only include scenarios in which the debris was retained in the reactor cavity, since if the debris were uncooled and in the basement, side wall failure of containment would be assumed.

As noted previously, a sensitivity study was performed in which a higher probability was assumed for failure of the debris to be cooled given there was overlying water. In this case, the conditional probability of basemat failure was calculated to increase to almost 13%. This outcome, together with the fraction associated with side wall failure (about 8%) account for the probability of 0.2 used for failure of coolability in the sensitivity case.

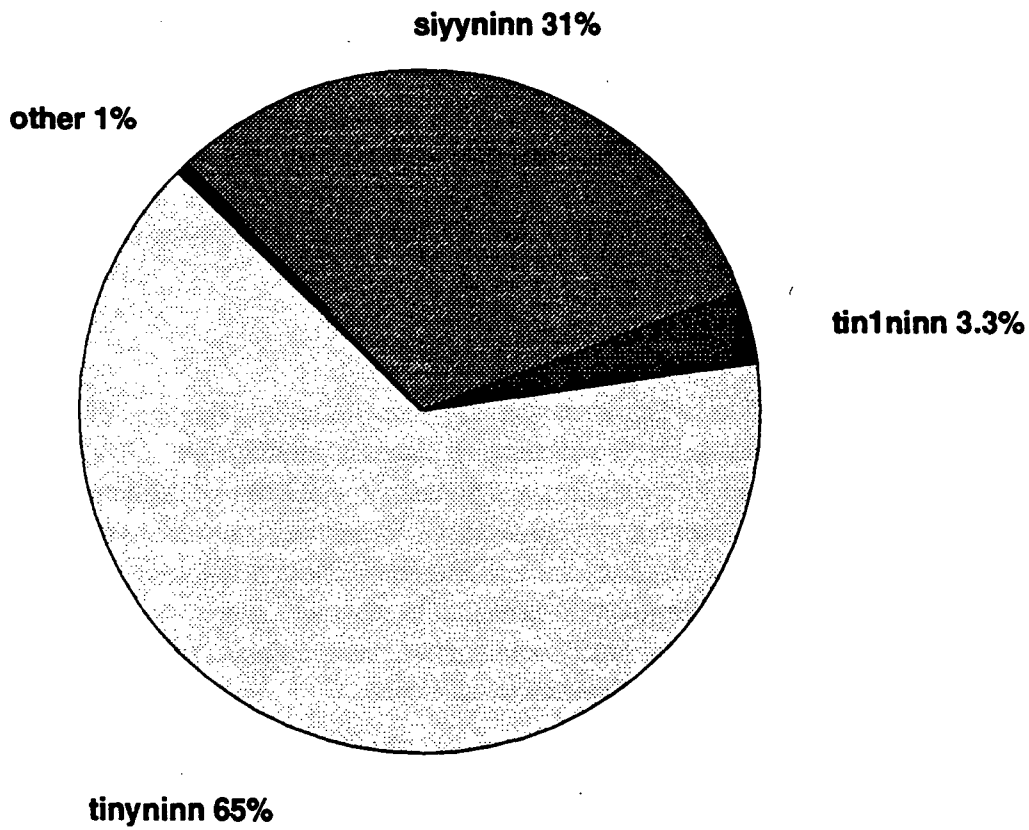


Figure 6-25. Contributions of Plant-Damage States to Frequency of Late Containment Failure

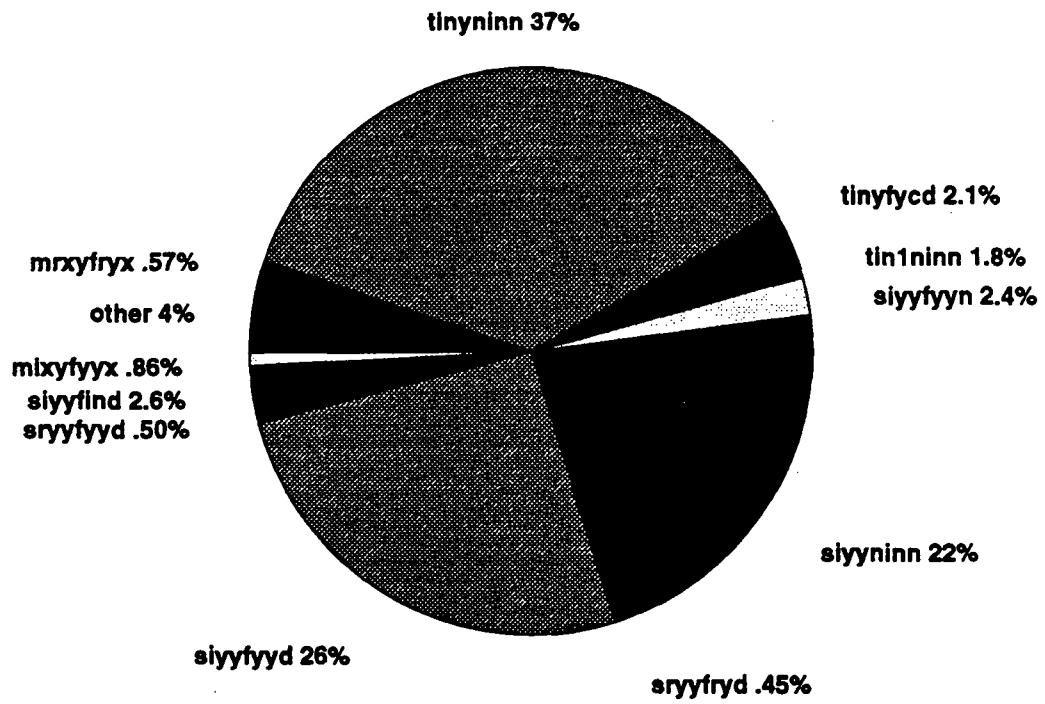


Figure 6-26. Contributions of Plant-Damage States to Frequency of Basemat Meltthrough

6.3.6 Prevention of Vessel Failure

The CET tracks scenarios in which the reactor vessel might not fail as a result of core damage. As described in Section 5, this could occur either due to recovery of cooling before the core slumped into the lower vessel head, or due to cooling of the debris in the lower head as a consequence of submergence of the vessel (although no credit was given to the latter possibility in the base case). It was estimated that, for about 8% of the frequency of the plant-damage states, cooling could be successfully restored after some core damage had occurred but core slump had not yet taken place. This would be the case when there was the potential for depressurization of the RCS and low pressure injection was available to supply cooling flow. The implication of this result is that either depressurization or injection would not be available for most of the plant-damage states.

The final sensitivity study that was performed addressed the potential for submerged-vessel cooling of the debris in the bottom head. The probability that the reactor vessel would fail despite submergence by water injected from the BWST was varied from 1.0 (i.e., no credit was given to prevention of vessel failure by submerged cooling in the base case) to 0.01. This provides an indication of the effect on containment response if submerged-vessel cooling is later determined to be a viable means of preventing vessel failure. In this sensitivity study, the fraction of outcomes that would not lead to vessel failure was estimated to increase from 8% to about 21%. This indicates that the BWST contents would be injected prior to vessel breach (flooding the reactor vessel) for a substantial fraction of the plant-damage states. As increased understanding of this mode of cooling is reached, the CET may be adjusted to give an appropriate level of credit to it.

It should be noted that cooling of the debris in-vessel would not preclude some modes of containment failure. Early hydrogen burns, bypass due to creep rupture of steam generator tubes, and late overpressurization in particular would still be possibilities. For cases in which the debris slumped into the lower head, in-vessel steam explosions would also be possible. These were all modeled explicitly in the CET and its supporting logic. On the other hand, failures at vessel breach, side wall failure, and basemat penetration would all be prevented if the vessel did not fail.

6.3.7 Summary of CET Results

The most important findings from the back-end analysis related to the reasons that the containment was likely to retain its integrity for most types of accidents. Chief among these reasons is the very large free volume available in the containment. At 2.8×10^6 ft³, there is substantial margin to accommodate severe accident loadings without approaching pressures that would be likely to result in containment failure.

The geometry of the reactor cavity was also important. The cavity area is relatively large, so that even if the core debris were to be retained in the cavity, it is likely that it would form a coolable geometry. In addition, all areas of the containment drain eventually to the

containment normal sump, which is located in the cavity region. Therefore, any water that is present in containment would be available for cooling debris in the cavity. If the contents of the BWST had been injected, a depth of water of approximately 25 ft would be present in the cavity. Even if only the original volume of the RCS and the core flood tanks were present, the debris would be covered by water at least 4 ft deep. This water would generally cause the debris to re-freeze, and with containment heat removal available, should allow a relatively stable condition to develop.

The cavity communicates with the containment basement mainly via the incore instrument tunnel. For accidents that would progress at relatively high pressure (several hundred psig or greater), it is possible that debris would be dispersed to the basement. At that level, there would be an area over which the debris could spread even larger than the cavity. If the contents of the BWST were injected, there would be several feet of overlying water in that area as well. Therefore, a stable condition could be achieved similar to that in the cavity.

Because of the large volume of the containment, it would be very difficult for sufficient hydrogen to be generated or to accumulate to support a burn that could challenge the containment capacity. Similarly, pressurization due to direct containment heating or steam generation at vessel breach would not be likely to cause the capacity to be exceeded. Direct containment heating could be further limited because there would not be direct pathways for finely fragmented fuel to be transferred efficiently from the cavity to the upper regions of containment.

Containment isolation was found to be a negligible contributor to the potential for releases from the containment. This is due in part to administrative controls, and particularly those that prevent using the containment purge lines during power operation. Other penetrations are generally well monitored.

Section 7 RADIONUCLIDE RELEASE CHARACTERIZATION

This section describes the characterization of fission-product releases for the Davis-Besse IPE. Based on an examination of the results of MAAP calculations and on consideration of the nature of the scenarios involving containment failures of various types, a set of release categories was defined to permit the large number of potential releases to be consolidated. It should be noted that these release categories were defined primarily on the basis of severity of release, with relatively little reflection of differences in timing among some scenarios. Therefore, the results may require further refinement before use in calculation of offsite consequences, if that should be undertaken in the future. The approach for estimating the release fractions is described in Section 7.1. The development and definition of the release categories are described in Section 7.2. Section 7.3 provides a summary of the results in terms of frequencies of release categories for each of the plant-damage states.

7.1 ESTIMATION OF RELEASE FRACTIONS

This section describes the method by which radionuclide releases were estimated and the release magnitude of each radionuclide group determined for different CET endpoints. The major factors impacting the radioactive releases were as follows:

- (1) The fraction of radioactivity released from the fuel to the reactor coolant system and then to the containment and other buildings.
- (2) The systems available for removal of radioactivity, such as containment sprays and containment air coolers, and natural removal processes, such as deposition and plateout on surfaces.
- (3) Availability of the containment and/or the containment failure mode.

Each of these factors was dependent on particular accident sequences which established the systems available to cool the core and the containment, which, in turn, determined the available time for fission product removal processes to become effective in reducing radioactive releases. The accident sequences were analyzed using an integrated computer analysis code, the Modular Accident Analysis Program (MAAP). The reactor coolant system, containment nodalization, and the safety systems modeled for Davis-Besse are described in Section 2.1. MAAP was designed to provide realistic assessments for core-damage accidents, including calculations of fission-product release, transport, removal and deposition.

Many of the accident sequences were similar in terms of the nature of the core-melt progression, status of removal mechanisms, and containment failure modes. Thus, a number of accident sequences could be represented by one radioactive release source term, normally referred to as a release category. A majority of the release categories defined in the following sections were derived directly from MAAP runs.

Over thirty accident sequences involving a spectrum of LOCAs, transients, and steam generator tube ruptures were analyzed using MAAP. In addition, several sensitivity runs were performed to further define the potential impact of uncertainties in release categories associated with phenomenological modeling in MAAP.

For release categories for which specific MAAP runs were not made, the release categories were estimated based on parameters of similar release categories and sensitivity runs. Ex-vessel releases were estimated based on sensitivity runs performed for some sequences for which the cavity area was adjusted downwards, which, in turn, resulted in increased core-concrete interactions.

The releases for various radionuclide groups were calculated using the Cubicciotti steam oxidation model and Kelly's correlations given in MAAP. The steam oxidation model of Cubicciotti assumes that release of fission gas and volatile fission products follow the kinetics of fuel oxidation when UO_2 is heated in steam. MAAP keeps track of the following radionuclide groups:

- (1) Noble gases (NG)
- (2) Iodines (I)
- (3) Cesium (Cs)
- (4) Tellurium (Te)
- (5) Antimony (Sb)
- (6) Strontium (Sr)
- (7) Molybdenum (Mo)
- (8) Lanthanum (La)
- (9) Cerium (Ce)
- (10) Barium (Ba)
- (11) Uranium Oxide (UO_2)

Based on similarity in the release fractions, antimony and tellurium releases were combined into one radionuclide group (Sb-Te) and cerium and lanthanum releases were combined into one radionuclide group (Ce-La). Additionally, the time and duration of release for each release category were estimated based on MAAP runs. For sequences which resulted in containment failure, releases were calculated for a period of 24 hours following the containment failure. For sequences that did not result in a containment failure, releases were calculated for the duration of the accident, nominally 48 hours.

In order to limit the release categories to a minimum number, the results of MAAP runs for different sequences with relatively similar core damage progression and containment systems availability were reviewed to determine whether the releases from these sequences could be combined. Additionally, this review also focused on similarity in releases for noble gases and iodines, which are dominant contributors to offsite risk. Based on this review, a

representative release for noble gases and iodines was selected for each release category. The releases for other radionuclides were taken as the maximum release fraction calculated by MAAP for sequences from which the representative noble gas and iodine source term was selected.

It should be noted that release categories were based on the magnitude of total fission products released, irrespective of their relative timing for applicable sequences. This was considered appropriate since a full level 3 study was not performed for the Davis-Besse IPE. Therefore, these release categories may be conservative and should not be directly applied to offsite consequence estimations.

7.2 DEFINITION OF RELEASE CATEGORIES

The sections that follow describe the categories that were developed to characterize the releases corresponding to the CET end states. The first part of the description for each release category defines the category as it relates to the applicable paths through the CET. The second part describes the representative sequences from which particular parameters were derived. Many sequences could follow the same path through the containment event tree and thus arrive at the same release category. The third part of the release category discussion provides some insights into the range of sequences that might result in a particular release category, and also the range of sequences for which the release category definition can be applied.

7.2.1 Release Category 1

This release category is characterized as a bypass of containment with releases directly going outside the auxiliary building. Ex-vessel fission products are not released. Fission product scrubbing is not effective. Representative releases are shown in Table 7-1.

The representative sequence for a containment bypass is a steam generator tube rupture accident. During this accident fission products could be directly released to the environment via the main steam safety valves (MSSVs). If one of the MSSVs sticks open, a majority of the release would bypass the containment. Core damage occurs due to failure of emergency core cooling systems. If the reactor vessel is breached during the accident, corium (molten reactor core) will be released to the containment. Dispersal of corium over a large area allows the corium to cool, thereby preventing ex-vessel release of fission products. A large amount of fission products released will be deposited or plated out on the surfaces of the reactor coolant system and the containment. Credit for scrubbing in the steam generators or containment is not considered.

The other sequences that could be represented by this release category are interfacing-systems LOCA sequences that involve containment bypass to the auxiliary building. For these sequences, however, releases for iodines and particulates will be significantly lower than the values given in Table 7-1 due to plateout and deposition in the auxiliary building. As such, this release category was not used for other sequences.

Table 7-1
Release Category 1

Description: Containment bypass, without ex-vessel release of fission products and no spray removal of fission products

Fission Product Group	Core Release Fractions
Noble Gases	1.0
I	0.6
Cs	0.6
Te-Sb	1.0×10^{-2}
Ba	5.0×10^{-5}
Ce-La	1.0×10^{-7}
Sr	1.0×10^{-5}

7.2.2 Release Category 2

This release category is characterized by releases due to a containment isolation failure or an early containment failure. Ex-vessel fission products are not released. Fission product removal via sprays is not effective. Representative releases are shown in Table 7-2.

The representative sequence is a LOCA with a failure of containment to isolate, or a containment failure during the sequence. For these sequences, fission products will be released to the containment with a majority of the iodine and particulate releases plated out on the reactor coolant system and containment surfaces.

Core damage occurs due to failure of emergency core cooling systems. When the reactor vessel fails, the corium will be dispersed over a large area of the containment floor. This allows corium to cool, thereby preventing ex-vessel release of fission products.

Since ex-vessel releases are not assumed to occur, this release category is also applicable to sequences that do not involve reactor vessel failure. This release category is also considered applicable to sequences involving late containment failures and revaporization of iodine from reactor coolant system surfaces.

7.2.3 Release Category 3

This release category is characterized as a bypass of containment with releases going directly to the auxiliary building or a containment isolation failure or an early containment failure. Ex-vessel fission products are not released. Fission product removal by containment sprays is effective. Representative releases are shown in Table 7-3.

The representative sequence for a containment bypass to the auxiliary building is an interfacing-systems LOCA. During this accident fission products could be directly released to the auxiliary building, bypassing the containment. A majority of fission products released will be deposited or plated out on the surfaces of the reactor coolant system and the auxiliary building.

For the sequences that involve containment isolation failures coincident with a LOCA, or sequences involving a very early containment failure, a majority of the iodine and particulate releases will be plated out on the reactor coolant system and containment surfaces.

Core damage occurs due to failure of emergency core cooling systems. When the reactor vessel fails, the corium will be dispersed over a large area of the containment floor. This allows corium to cool, thereby preventing ex-vessel release of fission products.

Based on the MAAP runs for a large break LOCA sequence with and without containment sprays, the effectiveness of sprays to remove fission products was estimated. The containment sprays will reduce cesium and iodine releases by a factor of 100 and particulate releases by a factor of 5. For interfacing-systems LOCA sequences, fission product removal is accomplished by water overlying the break location and/or removal by fire water spray, etc.

**Table 7-2
Release Category 2**

Description: Containment isolation failure or early containment failure, without ex-vessel release of fission products and no spray removal of fission products

Fission Product Group	Core Release Fractions
Noble Gases	1.0
I	0.1
Cs	0.1
Te-Sb	3.0×10^{-2}
Ba	2.0×10^{-4}
Ce-La	6.0×10^{-3}
Sr	1.0×10^{-4}

**Table 7-3
Release Category 3**

Description: Containment isolation failure, ISLOCA, or early containment failure, without ex-vessel release of fission products and with spray removal of fission products

Fission Product Group	Core Release Fractions*
Noble Gases	1.0
I	1.0×10^{-3}
Cs	1.0×10^{-3}
Te-Sb	6.0×10^{-3}
Ba	4.0×10^{-5}
Ce-La	1.0×10^{-3}
Sr	2.0×10^{-5}

*Based on Table 7-2 releases.

Since a majority of the iodine and particulate releases will be plated on the containment and reactor coolant system surfaces, this release category is considered applicable to SGTR sequences (containment bypass to environment) with fission product scrubbing.

Since ex-vessel releases are not assumed to occur, this release category is also applicable to sequences that do not involve reactor vessel failure. This release category is also considered applicable to sequences involving late containment failures and revaporization of iodine from reactor coolant system surfaces.

7.2.4 Release Category 4

This release category is characterized by releases due to a containment isolation failure or an early containment failure. Ex-vessel fission products are released. Fission product removal via sprays is not effective. Representative releases are shown in Table 7-4.

The representative sequence is a LOCA with a failure of containment to isolate, or a containment failure during the sequence. For these sequences, fission products will be released to the containment with a majority of the iodine and particulate releases plated out on the reactor coolant system and containment surfaces.

Core damage occurs due to failure of emergency core cooling systems. When the reactor vessel fails, the corium will be dispersed over a smaller area of the containment floor. The amount of coolant available in the containment cavity may also be minimal. This results in core-concrete interaction, which, in turn, results in release of certain fission products from the corium.

This release category is also considered applicable to sequences involving late containment failures and revaporization of iodine from reactor coolant system surfaces.

7.2.5 Release Category 5

This release category is characterized as a bypass of containment with releases directly going to the auxiliary building or a containment isolation failure or an early containment failure. Ex-vessel fission products are released. Fission product removal by containment sprays is effective. Representative releases are shown in Table 7-5.

The representative sequence for a containment bypass to the auxiliary building is a interfacing-systems LOCA. During this accident, fission products could be directly released to the auxiliary building, bypassing the containment. A majority of fission products released will be deposited or plated out on the surfaces of the reactor coolant system and the auxiliary building.

For the sequences that involve containment isolation failures coincident with a LOCA, or sequences involving an early containment failure, a majority of the iodine and particulate releases will be plated out on the reactor coolant system and containment surfaces.

Table 7-4
Release Category 4

Description: Containment isolation failure or early containment failure, with ex-vessel release of fission products and no spray removal of fission products

Fission Product Group	Core Release Fractions
Noble Gases	1.0
I	0.2
Cs	0.2
Te-Sb	0.1
Ba	8.0×10^{-4}
Ce-La	6.0×10^{-3}
Sr	2.0×10^{-3}

Table 7-5
Release Category 5

Description: Containment isolation failure, ISLOCA, or early containment failure, with ex-vessel release of fission products and with spray removal of fission products

Fission Product Group	Core Release Fractions*
Noble Gases	1.0
I	2.0×10^{-3}
Cs	2.0×10^{-3}
Te-Sb	2.0×10^{-2}
Ba	2.0×10^{-4}
Ce-La	2.0×10^{-3}
Sr	4.0×10^{-4}

*Based on Table 7-3 releases.

Core damage occurs due to failure of emergency core cooling systems. When the reactor vessel fails, the corium will be dispersed over a smaller area of the containment floor. The amount of coolant available in the containment cavity may also be minimal. This results in core-concrete interaction, which, in turn, results in release of certain fission products from the corium.

Based on the MAAP runs for a large LOCA sequence with and without containment sprays, the effectiveness of sprays to remove fission products is estimated. The containment sprays will reduce cesium and iodine releases by a factor of 100 and particulate releases by a factor of 5.

For interfacing-systems LOCA sequences, fission product removal is accomplished by water overlying the break location and/or removal by fire water spray, etc.

Since a majority of the iodine and particulate releases will be plated on the containment and reactor coolant system surfaces, this release category is considered applicable to SGTR sequences (containment bypass to environment) with fission product scrubbing.

This release category is also considered applicable to sequences involving late containment failures and revaporization of iodine from reactor coolant system surfaces.

7.2.6 Release Category 6

This release category is characterized as a late containment failure without revaporization. Ex-vessel fission products are not released. Fission product removal by sprays is not effective. Representative releases are shown in Table 7-6.

The representative sequence for a late containment failure is a transient or a LOCA resulting in an early reactor vessel failure followed by a late containment failure. Dispersal of the corium over a large area allows corium to cool preventing ex-vessel release of fission products. A majority of fission products released are deposited or plated out on the surfaces of the reactor coolant system and the containment. The containment spray system is not available to remove fission products effectively.

7.2.7 Release Category 7

This release category is characterized as a late containment failure without revaporization. Ex-vessel fission products are not released. Fission product removal by sprays is effective. Representative releases are shown in Table 7-7.

The representative sequence for a late containment failure is a transient or a LOCA resulting in an early reactor vessel failure followed by a late containment failure. Dispersal of the corium over a large area allows corium to cool, preventing ex-vessel release of fission products. A majority of fission products released are deposited or plated out on the surfaces of the reactor coolant system and the containment. The containment spray system is available to remove the fission products effectively.

Table 7-6
Release Category 6

Description: Late containment failure, without ex-vessel release of fission products and no spray removal of fission products	
Fission Product Group	Core Release Fractions
Noble Gases	1.0
I	4.0×10^{-3}
Cs	4.0×10^{-3}
Te-Sb	2.0×10^{-4}
Ba	5.0×10^{-6}
Ce-La	3.0×10^{-7}
Sr	5.0×10^{-7}

Table 7-7
Release Category 7

Description: Late containment failure, without ex-vessel release of fission products with spray removal of fission products	
Fission Product Group	Core Release Fractions*
Noble Gases	1.0
I	8.0×10^{-6}
Cs	8.0×10^{-6}
Te-Sb	4.0×10^{-5}
Ba	1.0×10^{-6}
Ce-La	6.0×10^{-8}
Sr	1.0×10^{-7}

*Based on Table 7-6 releases.

Based on the MAAP runs for a large LOCA sequence with and without containment sprays, effectiveness of sprays to remove fission products is estimated. The containment sprays will reduce cesium and iodine releases by a factor of 500 and particulate releases by a factor of 5.

7.2.8 Release Category 8

This release category is characterized as no containment failure. Ex-vessel fission products are not released. Containment sprays are not available for fission product removal. Representative releases are shown in Table 7-8.

The representative sequence for no containment failure is a transient or a LOCA resulting in a reactor vessel failure but no containment failure. Containment air coolers are available to cool the containment and maintain the pressure in containment well below its failure pressure. The fission products from the containment atmosphere are removed via the condensation of steam by containment air coolers. The intact containment also allows for natural processes to become more effective in removing fission products from the containment atmosphere. A majority of fission products are deposited or plated out on the surfaces of the reactor coolant system and the containment. The containment spray system is not available to remove fission products.

7.2.9 Release Category 9

This release category is characterized as no containment failure. Ex-vessel fission products are not released. The containment spray system is available for fission product removal from the containment atmosphere. Representative releases are shown in Table 7-9.

The representative sequence for no containment failure is a transient or a LOCA resulting in a reactor vessel failure and no containment failure. Containment air coolers and containment spray systems are available to cool the containment and maintain the containment pressure well below the its failure pressure. The fission products from the containment atmosphere are removed via the condensation of steam by containment air coolers and by the containment spray system.

The representative releases are based on MAAP runs in which containment failure did not occur and the containment spray system is available to cool the containment and remove fission products from the containment atmosphere.

7.3 ESTIMATED RELEASE FREQUENCIES

Each of the outcomes for the CET was assigned to one of the release categories, as indicated in Figure 5-2. The conditional probabilities for the outcomes were also combined according to the assigned release categories. The results, in terms of overall conditional probabilities of the release categories, are presented in Figure 7-1.

**Table 7-8
Release Category 8**

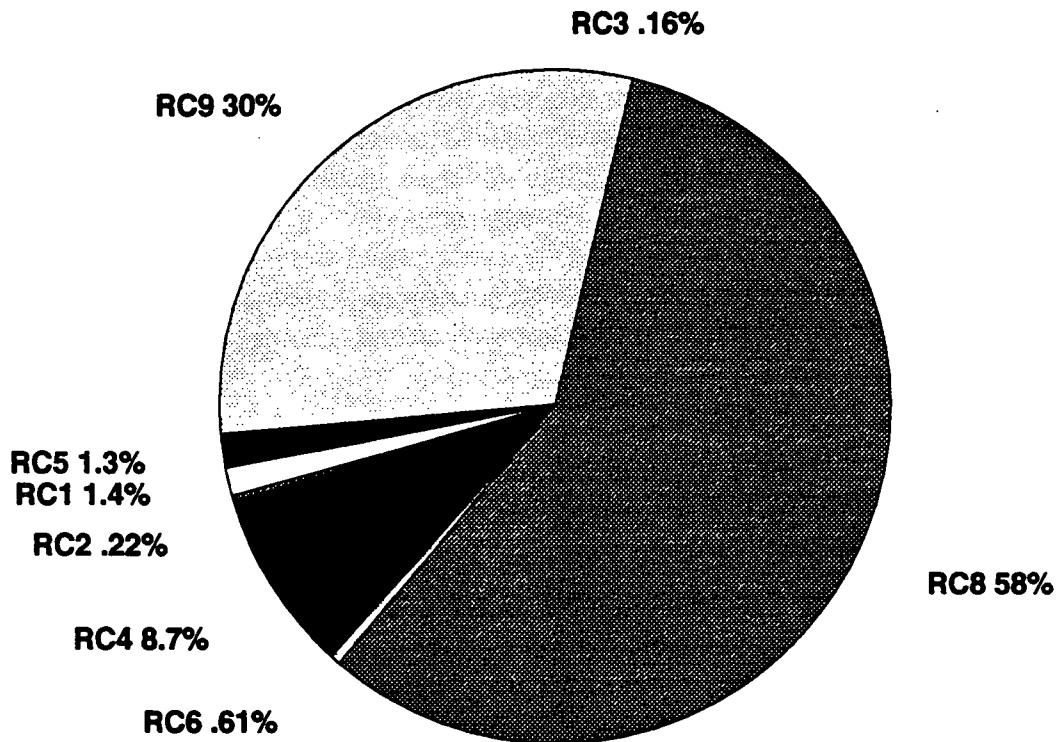
Description: No containment failure, without ex-vessel release of fission products and no spray removal of fission products

Fission Product Group	Core Release Fractions
Noble Gases	4.0×10^{-2}
I	3.0×10^{-4}
Cs	6.0×10^{-4}
Te-Sb	1.0×10^{-5}
Ba	3.0×10^{-7}
Ce-La	3.0×10^{-7}
Sr	1.0×10^{-7}

**Table 7-9
Release Category 9**

Description: No containment failure, with spray removal of fission products

Fission Product Group	Core Release Fractions
Noble Gases	4.0×10^{-2}
I	1.0×10^{-6}
Cs	1.0×10^{-6}
Te-Sb	1.0×10^{-6}
Ba	2.0×10^{-9}
Ce-La	5.0×10^{-12}
Sr	5.0×10^{-10}



Note: RC7 is .0032%

Figure 7-1. Overall Conditional Probabilities for Release Categories Given Core Damage

The results illustrated by this figure are consistent with those described in Section 6.3. Release categories 8 and 9, which are for scenarios in which the containment maintains its integrity (note that these categories also include basemat meltthrough cases), combine for approximately 88% of the overall frequency of core damage. Release category 8 includes those scenarios in which fission-product removal by the containment spray system would be effective, while release category 9 includes those in which spray removal would not be available. As the figure indicates, scrubbing would be available for about two-thirds of the intact containment cases.

Release category 1 includes bypass sequences in which there would be limited scrubbing of fission products, and is comprised primarily of steam generator tube ruptures (either as initiating events or due to creep rupture of tubes during core degradation) and of interfacing-systems LOCAs which were not effectively scrubbed. Most releases following interfacing-systems LOCAs would be subjected to scrubbing by overlying water in the auxiliary building; these scenarios have been assigned to release category 5. The remainder of the frequency of interfacing-systems LOCAs would be included in release category 1. It should be noted that the assignment to release category 1 of the fraction of interfacing-systems LOCAs not subject to scrubbing is conservative, since it assumes effectively no removal mechanisms outside the RCS. Since the interfacing-systems LOCA releases would be into the auxiliary building, however, substantial plateout and filtering prior to release from the building would be expected.

Release categories 2 and 3 would include early containment failures, without and with removal of fission products by containment sprays, respectively. The fractions of outcomes assigned to these release categories are relatively small, since early containment failures were assessed to be very unlikely.

Release category 4 encompasses CET outcomes in which there is an ex-vessel release of fission products due to core-concrete interactions and scrubbing of fission products would not be available. This release category includes a small contribution from early containment failures, as well as a portion of the late and side wall failures. As noted above, release category 5 includes interfacing-systems LOCAs in which scrubbing by overlying water is effective. The remainder of the late containment failures are assigned to release categories 6 and 7, which correspond to cases without and with fission-product scrubbing, respectively, and without ex-vessel release of fission products.

For reference purposes, the frequencies of the release categories and the fractions for each plant-damage state assigned to each release category are summarized in Table 7-10.

Table 7-10
Frequencies and Conditional Probabilities of Release Categories

Plant-Damage State	Frequency of Damage State	RC 1	RC 2	RC 3	RC 4	RC 5	RC 6	RC 7	RC 8	RC 9
AIXYFINX	3.0×10^{-8}		0.0020		0.0005		0.0016		0.9959	
AIXYFYYX	2.6×10^{-7}			0.0021						0.9979
AIXYNINX	1.0×10^{-7}		0.0018		0.1004		0.0015		0.8964	
ARXYFRYX	8.0×10^{-7}		0.0035		0.0001		0.0018		0.9947	
ARXYFYYX	5.3×10^{-7}			0.0035		0.0001		0.0018		0.9947
MIXYFINX	8.8×10^{-8}		0.0023		0.0019				0.9958	
MIXYFYCX	1.4×10^{-7}		0.0006		0.0015				0.9978	
MIXYFYYX	2.3×10^{-7}		0.0023		0.0019				0.9958	
MRXYFIYX	2.7×10^{-9}		0.0036		0.0001		0.0018		0.9945	
MRXYFRYX	1.5×10^{-6}		0.0035		0.0001				0.9964	
MRXYFYYX	7.6×10^{-8}		0.0035		0.0001				0.9964	
MRXYNYXX	1.3×10^{-9}			0.0130		0.0011		0.0904		0.8954
RINVFYCD	3.7×10^{-8}	1.0000								
RIYVFYCD	1.2×10^{-9}	1.0000								
RIYVNINN	8.2×10^{-9}	1.0000								
RINVNINN	4.9×10^{-9}	1.0000								
RRYVXIND	1.7×10^{-7}	1.0000								

Table 7-10 (continued)
Frequencies and Conditional Probabilities of Release Categories

Plant-Damage State	Frequency of Damage State	RC 1	RC 2	RC 3	RC 4	RC 5	RC 6	RC 7	RC 8	RC 9
RRYVXINN	2.3×10^{-8}	1.0000								
RRNVXIND	1.1×10^{-7}	1.0000								
RRNVXINN	5.1×10^{-9}	1.0000								
SINYFYCD	7.9×10^{-7}	0.0107		0.0074		0.0061				0.9758
SINYFYD	2.8×10^{-8}	0.0069		0.0088		0.0062		0.0002		0.9780
SINYFYYN	2.0×10^{-6}	0.1071		0.0080		0.0071				0.8778
SINYLYYN	4.8×10^{-8}	0.0933		0.0082		0.0072				0.8913
SIY1FYD	4.0×10^{-9}		0.0027		0.0019				0.9954	
SIY1NINN	4.3×10^{-8}		0.0020		0.1124		0.0028		0.8828	
SIYFYCD	8.6×10^{-9}		0.0003						0.9997	
SIYFYND	6.9×10^{-7}		0.0027		0.0019				0.9954	
SIYFYNN	1.1×10^{-7}		0.0028		0.0154				0.9818	
SIYFRYN	4.6×10^{-9}		0.0028		0.0154				0.9818	
SIYFYCD	8.6×10^{-7}		0.0003						0.9997	
SIYFYD	6.9×10^{-6}		0.0027		0.0019				0.9954	
SIYFYYN	6.6×10^{-7}		0.0028		0.0154				0.9818	
SIYNNINN	6.9×10^{-6}		0.0020		0.1124		0.0028		0.8828	

Table 7-10 (continued)
Frequencies and Conditional Probabilities of Release Categories

Plant-Damage State	Frequency of Damage State	RC 1	RC 2	RC 3	RC 4	RC 5	RC 6	RC 7	RC 8	RC 9
SIYYNYYN	6.9×10^{-9}			0.0131		0.0013		0.0888		0.8968
SRNYFRYD	7.2×10^{-9}	0.0107	0.0070		0.0034		0.0002		0.9787	
SRNYFRYN	2.2×10^{-7}	0.1071	0.0080		0.0064		0.0018		0.8768	
SRNYFYCD	4.2×10^{-8}	0.0107		0.0070		0.0034		0.0002		0.9787
SRNYFYD	2.4×10^{-9}	0.0107		0.0070		0.0034		0.0002		0.9787
SRNYFYYN	1.4×10^{-8}	0.1071		0.0080		0.0064		0.0018		0.8768
SRNYNIYN	2.4×10^{-9}	0.1071	0.0080		0.0066		0.0892		0.7891	
SRYYFIYD	8.9×10^{-7}		0.0040		0.0001				0.9959	
SRYYFRCD	4.8×10^{-8}		0.0003						0.9996	
SRYYFRYD	1.2×10^{-6}		0.0040		0.0001				0.9959	
SRYYFRYN	6.2×10^{-7}		0.0040		0.0002				0.9958	
SRYYFYCD	1.1×10^{-6}		0.0003						0.9996	
SRYYFYD	1.3×10^{-6}		0.0040		0.0001				0.9959	
SRYYFYYN	6.7×10^{-7}		0.0040		0.0002				0.9958	
SRYYNRYN	1.9×10^{-8}		0.0131		0.0012		0.0904		0.8953	
TINININN	9.0×10^{-7}	0.0005	0.0039		0.2581		0.0200		0.7175	
TINYFIYN	9.5×10^{-8}	0.0536	0.0050		0.0035		0.0014		0.9365	

Table 7-10 (continued)
Frequencies and Conditional Probabilities of Release Categories

Plant-Damage State	Frequency of Damage State	RC 1	RC 2	RC 3	RC 4	RC 5	RC 6	RC 7	RC 8	RC 9
TINYFRYN	6.4×10^{-8}	0.0536	0.0056		0.0035				0.9373	
TINYFYCD	1.3×10^{-5}	0.0054		0.0044		0.0031				0.9872
TINYFYVD	2.8×10^{-7}	0.0018		0.0052		0.0031				0.9899
TINYFYVN	2.6×10^{-6}	0.0536		0.0056		0.0035				0.9373
TINYLYVN	3.1×10^{-7}	0.0536		0.0053		0.0032		0.0014		0.9366
TINYNNN	1.8×10^{-5}	0.0005	0.0039		0.2581		0.0200		0.7175	
TIYFYVN	1.6×10^{-7}			0.0073		0.0060				0.9867
TRNYFRYD	9.2×10^{-8}	0.0054	0.0060		0.0017		0.0001		0.9868	
TRNYFRYN	3.0×10^{-8}	0.0536	0.0065		0.0032		0.0009		0.9359	
TRNYFYCD	1.1×10^{-8}	0.0054		0.0039		0.0004				0.9891
TRNYFYVD	1.4×10^{-8}	0.0046		0.0049		0.0017				0.9887
TRNYFYVN	1.7×10^{-7}	0.0536		0.0062		0.0032				0.9371
V	8.8×10^{-7}	0.1000				0.9000				
Overall conditional probabilities		0.0144	0.0022	0.0016	0.0865	0.0131	0.0061	0.00003	0.5809	0.2951
Total frequencies	6.6×10^{-5}	9.5×10^{-7}	1.4×10^{-7}	1.0×10^{-7}	5.7×10^{-6}	8.6×10^{-7}	4.0×10^{-7}	2.1×10^{-9}	3.8×10^{-5}	1.9×10^{-5}

REFERENCES FOR PART 4

1. Henry, R. E. and M. G. Plys, M.G. *MAAP-3.0B - Modular Accident Analysis Program for LWR Power Plants*. Electric Power Research Institute Report NP-7071-CCML, November 1990 (with updates).
2. Gabor, J. R., et.al. *MAAP Thermal-Hydraulic Qualification Studies*. Electric Power Research Institute Report TR-100741 (Final Report), June 1992.
3. "MAAP-3.0B PWR Revision 18 Transmittal." Fauske & Associates, Inc., Document FAI/92-21, April 1992.
4. *MAAP Users Guide—PWR Babcock & Wilcox*. Fauske & Associates Inc., April 1991 (with updates).
5. *MIPS Users Manual, Code Version 1.80*. Gabor, Kenton & Associates, Inc., May 1992.
6. Kenton, M. A., and J. R. Gabor. *Recommended Sensitivity Analyses For An Individual Plant Examination Using MAAP 3.0B*. Gabor, Kenton & Associates, Inc., March 1991.
7. Personal communication, E. L. Fuller, Electric Power Research Institute, to D. G. Kuhtenia, May 1992.
8. Han, J. T. "2. Natural Circulation in Reactor Coolant System," *Uncertainty Papers On Severe Accident Source Terms*. U.S. Nuclear Regulatory Commission Report NUREG-1265, May 1987.
9. Harper, F. T., et.al. *Evaluation of Severe Accident Risks; Quantification of Major Input Parameters: Expert Opinion Elicitation of In-Vessel Issues*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4551, Vol. 2, Rev. 1, Part 1, December 1990.
10. "Standards for Combustible Gas Control System in Light-Water-Cooled Power Reactors," *Code of Federal Regulations*. Part 10, Section 50.44.
11. Lee, M. and M. S. Kazimi. *Modeling of Corium-Concrete Interaction*. Electric Power Research Institute Report NP-5403, September 1987.
12. *Hydrogen Combustion in Reactor Containment Buildings*. Industry Degraded Core Program Technical Report for Task 12.3, September 1983.
13. Zabetakis, M. G. *Research on the Combustion and Explosion Hazards of Hydrogen-Water Vapor-Air Mixtures*. Bureau of Mines Division of Explosives Technology Report No. 3543, September 1956.
14. Davis-Besse IPE MAAP Analysis MRXYFYXX.
15. Ratzel, A. C. *Data Analysis for Nevada Test Site (NTS) Premixed Combustion Tests*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4138, May 1985.
16. Sherman, M. P., et al. *FLAME Facility—The Effect of Obstacles and Transverse Venting on Flame Acceleration and Transition to Detonation for Hydrogen-Air Mixtures at Large Scale*. U.S. Nuclear Regulatory Commission Report NUREG/CR-5275, April 1989.
17. Sherman, M. P., and M. Berman. *The Possibility of Local Detonations During Degraded-Core Accidents in the Bellefonte Nuclear Power Plant*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4803, January 1987.

18. Greimann, L., et al. *Reliability Analysis of Steel Containment Strength*. U.S. Nuclear Regulatory Commission Report NUREG/CR-2442, June 1982.
19. Wolfgang, R. J. "Containment Pressure Capacity." Davis-Besse Nuclear Power Station Calculation C-NSA-059-01-16, September 25, 1991.
20. "Design of Seismic Class I and Class II Structures," *Davis-Besse Updated Safety Analysis Report*. Toledo Edison Company, Volume 5, Section 3.8, 1992.
21. Salmon, C. G., and J. E. Johnson. *Steel Structures: Design and Behavior*. Second edition, Harper & Rowe, Publishers, New York, copyright 1980.
22. Wolfgang, R. J. "Containment Failure Probability." Davis-Besse Nuclear Power Station Calculation C-NSA-059-01-17, October 23, 1991.
23. Greimann, L., et al. *Containment Analysis Techniques, A State-of-the-Art Summary*. U.S. Nuclear Regulatory Commission Report NUREG/CR-3653, March 1985.
24. "Emergency Escape Lock Analysis for 75 psi Internal Pressure." Chicago Bridge and Iron Company Services, Inc., Revision 1, July 11, 1988.
25. "Certified Stress Report for Davis-Besse Nuclear Power Station, Unit 1." Chicago Bridge and Iron Company, January 17, 1977.
26. *Containment Structural Capability of Light Water Nuclear Power Plants*. Industry Degraded Core Program Technical Report for Task 10.1, July 1983.
27. "Davis-Besse Nuclear Power Station Electrical Adaptor Modules." Letter from CONAX, File Number E-25Q, May 2, 1984.
28. Personal communication, M. Lanz, Pathway Bellows, Incorporated, to R. J. Wolfgang, October 13, 1992.
29. *Report of the Containment Performance Working Group*. U.S. Nuclear Regulatory Commission Report NUREG-1037 (Draft Report for Comment), May 1985.
30. "Class 3 - Design Basis Accidents," *Davis-Besse Updated Safety Analysis Report*. Toledo Edison Company, Volume 12, Section 15.4, 1992.
31. Noxon, D. B., and C. L. Naugle. *IPE Generic Level 2 Analysis*. B&W Owners Group and Duke Engineering & Services, Inc., August 1991.
32. Behr, V. L., et al. *Containment Event Analysis for Postulated Severe Accidents: Sequoyah Power Station, Unit 1*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4700 (Volume 2), February 1987.
33. "RPS, SFAS, SFRCS Trip, or SG Tube Rupture." Davis-Besse Nuclear Power Station Emergency Procedure DB-OP-02000, June 18, 1990.
34. Gregory, J. J., et al. *Evaluation of Severe Accident Risks: Sequoyah, Unit 1*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4551 (Volume 5, Rev. 1, Part 2), December 1990.
35. *MAAP-4.0B Users' Manual*. Fauske & Associates, Inc. (Draft).
36. Harper, F. T., et al. *Evaluation of Severe Accident Risks: Quantification of Major Input Parameters (Expert Opinion Elicitation on In-Vessel Issues)*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4551 (Volume 2, Rev. 1, Part 1), December 1990.
37. Zalosh, R. G., et al. *Hydrogen Combustion in Reactor Containment Buildings*. Industry Degraded Core Program Technical Report 12.3, September 1983.

38. *Oconee Nuclear Station Unit 3 Probabilistic Risk Assessment*. Duke Power Company, December 1990.
39. *Nuclear Power Plant Response to Severe Accidents*. Industry Degraded Core Program Technical Summary Report, November 1984.
40. Harper, F. T., et al. *Evaluation of Severe Accident Risks: Quantification of Major Input Parameters (Expert's Determination of Containment Loads and Molten Core Containment Issues)*. U.S. Nuclear Regulatory Commission Report NUREG/CR-4551 (Volume 2, Rev. 1, Part 2), April 1991.
41. Personal communication, M. G. Plys, Fauske & Associates, Inc, to D. G. Kuhtenia, October 1, 1992.
42. Crutchfield, D. M. "Individual Plant Examination for Severe Accident Vulnerabilities." U.S. Nuclear Regulatory Commission Generic Letter 88-20, Supplement 1, Appendix 1, November 23, 1988.
43. Tarbell, W. W., et al. *Pressurized Melt Ejection into Water Pools*. U.S. Nuclear Regulatory Commission Report NUREG/CR-3916, March 1991.
44. Davis-Besse IPE MAAP analysis ARXYFRYX (AXR1e).
45. Kuhtenia, D. G. "SFAS Setpoint Change Impact On Design Basis Containment Response." Davis-Besse Nuclear Power Station Calculation C-NSA-60.05-002, Rev. 0, June 21, 1991.
46. Davis-Besse IPE MAAP analysis MRXYFRYX (MXR1e).
47. Davis-Besse IPE MAAP analysis SRNYFRYD (SNR1e).
48. Rinckel, M. A., et al. *Small Break Loss of Coolant Accident Analysis for the B&W 177FA Raised Loop in Response to NUREG-0737, Item II.K.3.31*. Babcock & Wilcox Company Report BAW-1981, October 1986.
49. Davis-Besse IPE MAAP analysis TINYNINN.
50. Davis-Besse IPE MAAP analysis RIYVXINN.
51. "Davis-Besse REDBL5 SGTR Analysis." Babcock & Wilcox Company Calculation 32-1150650-00, August 1, 1984.
52. *GTPROB Reference Guide*. Science Applications International Corporation, December 1991.

Part 5
IPE PERFORMANCE AND IMPLEMENTATION

Contents

<u>Section</u>	<u>Page</u>
1 IPE PROGRAM ORGANIZATION.....	1
2 REVIEW ACTIVITIES.....	3
REFERENCES FOR PART 5	5

Section 1 IPE PROGRAM ORGANIZATION

The group responsible for all PRA-related activities at Davis-Besse is the Safety Analysis Unit in the Nuclear Engineering Department. This group is comprised of individuals with expertise in fault-tree modeling and analysis, transient analysis, thermal-hydraulic analysis, systems analysis, the Safety Analysis Report, various plant procedures including abnormal procedures and the emergency procedure, integrated plant operation, simulator operation, and offsite dose assessments. In addition to PRA studies, this group is responsible for providing engineering support in such areas as plant operational problems, procedure changes, writing and reviewing 10CFR50.59 changes, plant design changes, and emergency planning. The group is primarily comprised of engineers, but also includes previously licensed senior reactor operators.

It should be noted that the Nuclear Engineering Department was also the group responsible for performing the draft PRA study (Ref. 1). This study was a joint effort between Toledo Edison and SAIC. The study was motivated by Toledo Edison's desire to achieve a better understanding of the safety characteristics of its nuclear unit, especially in the then-current NRC regulatory environment regarding severe accidents.

The Safety Analysis Unit has the overall responsibility for both the front-end analysis and the back-end analysis. This ensured a smooth interface between the systems analysis portion and the containment analysis portion of the IPE.

The supervisor of the Safety-Analysis Unit was the overall IPE program manager responsible for the overall schedule and the allocation of resources necessary to complete the IPE. This arrangement proved very effective in ensuring the PRA team had access to all relevant plant information.

In-house resources were used as much as possible in performing the IPE. Because of the limited experience the Safety Analysis Unit had in performing certain portions of the PRA, however, assistance was obtained from an outside consultant, Safety and Reliability Optimization Services (SAROS), Inc. This assistance primarily entailed support in such areas as development of an overall project plan, technology transfer in current PRA methods, and technical effort (e.g., for assessment of internal flooding, human reliability analysis, and containment event analysis). The overall project plan identified Safety Analysis personnel as the task leaders. Safety Analysis personnel formed an integrated team with personnel from SAROS, and it was this team that performed all the technical tasks associated with the IPE.

The front-end analysis was primarily performed by two full-time engineers with substantial assistance from other Safety Analysis personnel. Consulting support was utilized as needed. Because of the nature of the PRA, virtually all plant departments provided input into the development of the PRA. Davis-Besse system engineers provided information relative to development of the system fault-tree models; operators and maintenance personnel provided integrated system operation and maintenance-related information; and training

personnel provided information and also supported plant simulator exercises to verify certain aspects of the accident sequences and the human reliability analysis.

The back-end analysis was primarily performed by two full-time engineers with additional assistance provided by other Safety Analysis personnel. Consultant support was provided in coordinating the front-end analysis with the back-end analysis and for probabilistic treatment of key containment phenomena. Safety Analysis personnel developed the capability to use the MAAP code in the back-end analysis. This effort included development of a plant-specific input deck, interaction with the authors of the code to refine it to address features unique to Babcock & Wilcox plants, and performance of all MAAP calculations for the back-end analysis.

This submittal represents a summary of the work performed in each of the technical areas, and was prepared by the Safety Analysis and consulting personnel who performed the analyses. Further detail in each area is available in the project files at Davis-Besse.

Section 2 REVIEW ACTIVITIES

To help ensure the overall quality of the IPE, Davis-Besse conducted two different types of reviews: independent in-house reviews and external reviews. The in-house reviews were conducted in several different stages. First, each analytical task went through a peer review within the project team. This review also included a review by SAROS personnel. Subsequent reviews were performed by individuals within Toledo Edison who had specific technical expertise in applicable areas. Finally, the project manager and other cognizant department managers performed reviews.

An independent, in-house technical review of the documents, analysis, and results for all tasks associated with the IPE was performed. These reviews were performed for the development of initiating events, the event trees and corresponding success criteria, all system fault-trees, the various data bases, the human reliability analysis, and the recovery analysis. In addition to reviews performed by the various engineering departments, licensing engineers, training personnel, operations and maintenance organization personnel, and previously licensed senior reactor operators were available to perform reviews.

During development of the system fault trees, independent review teams were formulated to review the fault trees in detail. Individuals with different types of technical expertise were involved; typically, individuals from Systems Engineering, Maintenance, and Operations were included in the review teams. Other individuals who had performed specialized work on certain systems or in some way could provide valuable input were also included on the review teams as appropriate. Each team was tasked with ensuring that the model provided an accurate representation of the system design and actual operating and maintenance practices. A previously licensed senior reactor operator, who was also familiar with the plant safety analyses, was also responsible for reviewing each individual system fault-tree model.

Development of the reliability data bases was performed by one individual, with review of each element by at least one other individual. The sequence quantification was distributed between and performed by two individuals, each of whom reviewed the work performed by the other. A similar approach was used in reviewing the recovery analysis.

Review of the IPE back-end analysis was handled in a similar fashion. One engineer was responsible for developing the MAAP input deck with subsequent independent reviews of each input parameter by at least one other engineer. Each MAAP analysis was performed by, and separately reviewed by, individuals who had attended training in the use of the MAAP code. Additionally, MAAP runs and the quantification of the containment event tree were reviewed in group work sessions by key IPE team members as well as other individuals in the Safety Analysis Unit.

Comments received as part of the reviews were incorporated as appropriate into the various IPE work packages and final report. As a result of the process outlined above, every

individual technical task that comprised the IPE went through at least one independent in-house review, and in most cases there were multiple stages of review.

In addition to the in-house reviews that were performed, Toledo Edison contracted with Duke Engineering & Services, Inc., and the Duke Power Company to perform an external peer review. Duke personnel were selected because of their previous experience in the overall performance and application of PRA methods and their familiarity with plants designed by Babcock & Wilcox. Their review was conducted in a manner that was consistent with a procedure developed for the Electric Power Research Institute (Ref. 2). The results of this review were documented in a separate report (Ref. 3). The overall results of that review were very positive. Among the high-level comments in the Duke review were the following:

- The technical quality of the completed IPE activities is excellent. Planned activities appear to be well thought out and would be expected to work out with the same quality.
- Documentation is also excellent. The level of documentation makes it easy for someone to reproduce and trace the derivation of the results. At the same time it is being kept to a minimum to eliminate waste caused by excessive documentation.
- The planned report appears to address the NRC submittal guidelines.

All technical comments on the front-end and back-end analyses were evaluated and addressed prior to completion of this submittal.

REFERENCES FOR PART 5

1. Hengge, C. A., et al. *Davis-Besse Nuclear Power Station Level 1 Probabilistic Risk Assessment*. The Toledo Edison Company, November 1988.
2. Burns, E. T., et al. *A Review Process for Evaluating IPE Projects: A Tool for Utility PRA Management and Staff*. Electric Power Research Institute Draft Report for Project RP3000-46, August 1991.
3. Brewer, H. D., and D. B. Noxon. *Toledo Edison Davis Besse IPE Review*. Duke Engineering & Services, Inc., October 1992.

Part 6
PLANT IMPROVEMENTS
AND
UNIQUE SAFETY FEATURES

Contents

<u>Section</u>	<u>Page</u>
1 UNIQUE SAFETY FEATURES	1
2 CONSIDERATION OF VULNERABILITIES	5
3 OTHER POTENTIAL PLANT IMPROVEMENTS	9
3.1 Insights Gained from the Front-End Analysis	9
3.2 Insights Gained from the Back-End Analysis	10
REFERENCES FOR PART 6	12

List of Tables

<u>Table</u>	<u>Page</u>
6-1 Guidelines for Assessing IPE Results for Core-Damage Sequences	6
6-2 Guidelines for Assessing IPE Results for Containment Bypass Sequences.....	7

Section 1 UNIQUE SAFETY FEATURES

Throughout the process of developing the Davis-Besse IPE, plant features were observed to be of importance in preventing core damage and limiting potential releases. The following describes some of the unique safety features for Davis-Besse.

Alternate Injection Capability

Because of the separate high pressure injection (HPI) and makeup systems, the plant essentially has four separate pumps capable of injecting water from the borated water storage tank (BWST) into the RCS at high pressures. The makeup system serves as the normal method of returning purified letdown water back to the RCS and supplies seal injection to RCP seals. It can also be aligned to the BWST to supply injection for LOCAs for which the RCS remains at least moderately pressurized. For licensing-basis calculations, however, operation of the makeup system was not credited.

Operation of the makeup system is of importance in large part because it is capable of injection at full RCS pressure. The HPI pumps have a shutoff head of approximately 1600 psig (it is somewhat higher if the pumps are aligned to draw suction from the DHR pumps in the "piggyback" mode of operation). While HPI is effective in mitigating small break LOCAs in conjunction with operation of the auxiliary feedwater system, makeup pump operation provides additional assurance of being able to replace lost inventory at high pressure conditions. This is necessary, for example, during accidents in which all feedwater is unavailable, such that the RCS pressure would remain very high.

Turbine-Driven Auxiliary Feedwater

The AFW system employs two turbine-driven pumps and a motor-driven pump. The availability of two turbine-driven pumps provides the potential for increased redundancy in the event of a station blackout or similar accident. Furthermore, provisions are in place to support local manual control of the turbine-driven pumps in the event that dc power is lost. The actions that would be required have been performed both in training exercises and in past transients, in which automatic pump control failed (although not due to total loss of power).

Station Blackout Diesel Generator

During the seventh refueling outage (i.e., in late 1991), a third, independent diesel generator (referred to as the station blackout generator) was installed to provide additional assurance of onsite ac power following the loss of offsite power. It can be started locally or from the control room and supply power to either of the two safety-related essential buses.

The station blackout diesel generator is housed in a building separate from the emergency diesel generators. It is equipped with its own battery and does not rely on any other support systems. The station blackout generator is also equipped with its own ventilation system and its own day tank, ensuring a minimum of 4 hours run time at full load.

Cooling Water Redundancy

The component cooling water (CCW) and service water systems are among the most important systems for supporting front-line systems. Although each of these systems is nominally comprised of two trains, additional redundancy is provided.

The CCW system consists of three pumps. One of these is normally operating, and a second is in standby (and would be automatically started in the event of loss of flow from the first pump or a SFAS initiation). A third pump is available as an installed spare. It is isolated mechanically and electrically, but could be put into service quickly if needed. The third pump provides added redundancy and, for some failure modes, additional defense against potential common-cause failures.

The service water system is similar, except that two of its three pumps are normally running, with the third isolated as a spare. In addition, there is a separate backup service water pump which is of a different design and is located in a different part of the water treatment facility. As in the case of the CCW system, these pumps augment the redundancy of the system and provide further protection against common-cause failures. For both systems, abnormal procedures provide clear instructions for compensating for specific system faults by aligning available pumps to provide cooling water flow.

Containment Isolation

In evaluating the potential for a failure of containment isolation, each containment penetration was considered. Penetrations were screened out based on certain criteria, such as if the line was a closed loop inside containment (such that failure of the pressure boundary would be required for an isolation pathway to exist), the penetration was normally closed and would be obvious if it were inadvertently left open (e.g., the refueling canal), the penetration was smaller than approximately 3/4" in diameter (such that it would tend to be plugged by aerosols), etc. Following the screening evaluation, only two types of penetrations were identified that had the potential to result in a failure of containment isolation. The first type included the containment vessel vacuum breakers. Each vacuum breaker is equipped with a check valve in series with a motor-operated valve which receives an SFAS signal to close. The second type of penetration was the containment normal sump line. This penetration has two motor-operated isolation valves in series. These valves are normally open, and in the event of an accident involving station blackout, they would fail open. It should be noted, however, that with only minimal amounts of water in containment, this path would be submerged with only minor leakage of liquid possible. Because of the limited number of penetrations and the high reliability of the penetrations to close, containment isolation failures were found not to be significant in this study.

Large Containment Free Volume

The free volume of the Davis-Besse containment is such that the potential buildup of significant volumetric fractions of hydrogen and other combustible gases is limited. The nominal free volume of the Davis-Besse containment is 2.834 million cubic feet. This is a

sufficiently large volume that hydrogen concentrations resulting from fuel heatup and degradation are relatively low. In addition, transients that could release significant amounts of hydrogen would concurrently release large amounts of steam to the containment atmosphere. This steam would both reduce the hydrogen volumetric fraction and act to inert the containment atmosphere.

Therefore, there were no identified sequences which could result in hydrogen concentrations approaching that required for hydrogen detonation. Additionally, few sequences were identified with sufficient hydrogen concentrations to support "global," or complete hydrogen burns. The majority of potential hydrogen burns were calculated to be incomplete partial burns which resulted in much lower pressure spikes than would be the case for a complete burn with an equivalent amount of available hydrogen.

The large free volume also served to reduce the pressure loadings at vessel breach and additional loadings due to steam generation. In part because of the large volume, the time required to overpressurize the containment in the absence of containment heat removal was typically very long. This could afford time for recovery of heat removal systems.

Reactor Cavity Geometry

There is a high likelihood that overlying water will be present for ex-vessel corium located in the reactor cavity. The Davis-Besse containment geometry is such that the reactor cavity is connected via a 3 ft wide by 7 ft high access tunnel to the normal containment sump area. All containment areas and drains lead to the cavity/normal sump area, including the refueling canal. Accordingly, any water released from the RCS or injected into containment would eventually drain to this region.

As a consequence, corium released to the reactor cavity would always be initially covered with overlying water. This would remain the case unless the available inventory was entirely boiled away by corium decay heat, which at Davis-Besse would only be possible if containment has previously failed from overpressurization by steam.

Lower Containment Geometry

The nominal spread area of corium postulated to relocate to lower containment elevations is likely to be sufficient to prevent significant corium-concrete interactions even without overlying water. A concrete curb exists to protect the containment vessel wall from immediate direct contact with relocated corium.

Plant geometry in the area of the lower containment where corium might relocate if a high pressure melt ejection occurred provides a significant nominal spread area. With this area and the resultant lack of significant corium depth, convective and radiative heat transfer rates are sufficient to maintain corium temperatures below the melting point of containment concrete.

A 1.5 ft thick by 2.5 ft high concrete curb exists along the lower containment (elevation 565) floor outer circumference. Without this curb, corium which may relocate to

the lower containment elevation via the incore tunnel would have the potential to spread out and directly contact the steel wall of the containment vessel. This could lead to a short-term ablative failure of the containment. The presence of the concrete curb, however, removes this potential and eliminates a possible early containment failure mode.

Containment Penetration Thermal Ruggedness

Containment penetration seal materials are not vulnerable to significant degradation from thermal effects. Plant-specific penetration seal materials and geometries are such that significant degradation due to possible long term exposure to elevated temperatures is precluded. This includes major penetrations such as the equipment hatch, personnel hatch, and containment purge lines.

Section 2 CONSIDERATION OF VULNERABILITIES

One of the primary NRC goals for the individual plant examination process is for utilities to "identify plant-specific vulnerabilities to severe accidents that could be fixed with low cost improvements" (Ref. 1). Past experience has often revealed that the benefits associated with adding additional safety systems or trains of equipment are not justified by their high costs. The results of the IPE were analyzed to determine appropriate courses of action to address the principal insights. The general criterion suggested in Generic Letter 88-20 and NUREG/CR-1335 (Ref. 2) that licensees should look for "cost-effective safety improvements that reduce or eliminate the important vulnerabilities" as well as the guidance provided in NUMARC Report 91-04 (Ref. 3) were applied in deciding on actions that might need to be taken to address the results and insights from the IPE.

The basic finding of the extensive evaluations summarized in this report is that there are no fundamental weaknesses or vulnerabilities with regard to severe accidents at the Davis-Besse Nuclear Power Station. The term vulnerability, as used in this report, refers to those components, systems, operator actions, and/or plant design configurations that contribute significantly to an unacceptably high severe accident risk.

Overall, the goal was risk reduction in a cost-effective manner. This could be achieved by modifications, by changes in operating procedures or training practices, or by handling certain issues in future severe accident management guidance. Procedural changes are less costly than modifications, but may unacceptably increase operational staff burdens. Also, some accident sequences may be easily addressed by a single change which results in a significant reduction in core-damage frequency, while other sequences may require multiple changes to achieve a significant reduction. Therefore, application of these criteria necessitates that potential risk reductions be balanced against the capital cost and other impacts on normal plant operation. The considerations that were taken into account in evaluating potential changes included the following:

- (1) The cost-effectiveness and non-cost related impacts of proposed actions to address contributions to core-damage frequency (individually and collectively) should be carefully considered. Non-cost related impacts may include increased operational staff burdens, effects on general plant operations, or changes to outage schedules.
- (2) The guidelines in NUMARC Report 91-04, which are represented in Tables 6-1 and 6-2, should be applied first to individual accident sequences, not classes. This is to be done generally in decreasing order of core-damage frequency.
- (3) If the cumulative core-damage frequency for any accident class (a group of related sequences) falls within the NUMARC guidelines after criterion (2) is applied, additional actions should be considered.

Table 6-1
Guidelines for Assessing IPE Results for Core-Damage Sequences

Mean Core-Damage Frequency Per Sequence Group (per reactor-year)	Proposed Resolution
Greater than 1×10^{-4} or Greater than 50% of total core-damage frequency	<ol style="list-style-type: none"> 1. Find a cost-effective plant administrative, procedural or hardware modification with emphasis on eliminating or reducing the likelihood of the source of the accident sequence initiator. 2. If unable to satisfy above response, treat in emergency operating procedures (EOPs) or other plant procedure with emphasis on prevention of core damage. 3. If unable to satisfy above responses, ensure severe accident management guidance (SAMG) is in place with emphasis on prevention/mitigation of core damage, vessel failure, and/or containment failure.
1×10^{-4} to 1×10^{-5} or 20% to 50% of total core-damage frequency	<ol style="list-style-type: none"> 1. Find a cost-effective treatment in EOPs or other plant procedure or minor hardware change with emphasis on prevention of core damage. 2. If unable to satisfy above response, ensure SAMG is in place with emphasis on prevention/mitigation of core damage, vessel failure, and/or containment failure.
1×10^{-5} to 1×10^{-6}	Ensure SAMG is in place with emphasis on prevention/mitigation of core damage, vessel failure, and/or containment failure.
Less than 1×10^{-6}	No specific action required.

Table 6-2
Guidelines for Assessing IPE Results for Containment Bypass Sequences

Mean Containment Bypass Frequency (per reactor-year)	Proposed Resolution
Greater than 1×10^{-5} or Greater than 20% of total core- damage frequency	<ol style="list-style-type: none"> 1. Find a cost-effective plant administrative, procedural or hardware modification with emphasis on eliminating or reducing the likelihood of the source of the accident sequence initiator. 2. If unable to satisfy above response, treat in emergency operating procedures (EOPs) or other plant procedure with emphasis on prevention of core damage. 3. If unable to satisfy above responses, ensure severe accident management guidance (SAMG) is in place with emphasis on prevention/mitigation of core damage, vessel failure, and/or containment failure.
1×10^{-5} to 1×10^{-6} or 5% to 20% of total core-damage frequency	<ol style="list-style-type: none"> 1. Find a cost-effective treatment in EOPs or other plant procedure or minor hardware change with emphasis on prevention of core damage. 2. If unable to satisfy above response, ensure SAMG is in place with emphasis on prevention/mitigation of core damage, vessel failure, and/or containment failure.
1×10^{-6} to 1×10^{-7}	Ensure SAMG is in place with emphasis on prevention/ mitigation of core damage, vessel failure, and/or containment failure.
Less than 1×10^{-7}	No specific action required.

- (4) If the total core-damage frequency for all accident classes exceeds the target value of 1×10^{-4} per year after the application of criteria (2) and (3), additional actions should be considered.
- (5) If the disposition of a sequence after the application of criteria (1) through (4) entailed reference to future severe accident management guidance (SAMG), no further evaluation was required. These sequences would then be captured to ensure that SAMG, when developed, adequately addresses them.

Application of the considerations noted above to the IPE results led to the following conclusions:

- (1) The overall core-damage frequency was estimated to be 6.6×10^{-5} per year, so that it is below the target value without further action to reduce risk. In addition, the total frequency of containment bypass was calculated to be well below 1×10^{-5} per year.
- (2) Core-damage sequence TB_TU_T constituted approximately 50% of the overall core-damage frequency. As noted previously, this sequence is defined at a functional level. An examination of the system-level sequences and sequence cut sets that make up its frequency, however, indicates that it is not dominated by one or a few initiating events, system faults, or other plant features. Rather, the frequency results from a large number of different features, each contributing a relatively small amount.
- (3) Core-damage sequence TQU_T constitutes approximately 21% of the overall core-damage frequency. The majority of the contribution to this sequence involves postulated RCP seal LOCAs resulting from a loss of all CCW or all service water. Procedures are already in place to respond to guide recovery efforts aimed at restoring CCW or service water flow if either is lost. Appropriate procedures also clearly call for tripping the RCPs to prevent the seal LOCA.
- (4) One interfacing-systems LOCA sequence constituted approximately 40% of the overall frequency of containment bypass, but contributed less than 1% to the total core-damage frequency. This particular sequence hinged on the assessment of a particular error of commission that may not be realistic. Additional training relative to this and other potential interfacing-systems LOCAs has already been implemented, and should further reduce the potential for this type of accident.

For the three sequences summarized above, possible improvements to reduce their frequencies are under consideration. These potential improvements focus on plant administrative and procedural enhancements, rather than major hardware modifications. All other core-damage and containment bypass sequences fall into the categories which suggest either inclusion in severe accident management guidance, or that no specific actions need be considered.

Section 3 OTHER POTENTIAL PLANT IMPROVEMENTS

This section discusses plant enhancements that are being evaluated as a result of insights gained through performance of the IPE. It discusses insights gained through performance of both the front-end analysis (that is, the systems analysis) and the back-end analysis (the containment analysis). It should be clarified that the insights discussed below have not yet been evaluated in detail, nor have any specific resolutions been identified or evaluated. Consequently, the items identified below are a listing of those currently under evaluation; they are not a listing of modifications or improvements that will necessarily be implemented.

3.1 Insights Gained from the Front-End Analysis

During performance of the systems analysis portion of the IPE, several insights were noted, as described below.

Common power supplies for feedwater and makeup/HPI cooling. The systems available to respond to a loss of main feedwater include the turbine-driven pumps of the AFW system, the motor-driven feed pump, and makeup/HPI cooling. Both the motor-driven feed pump and makeup/HPI cooling require dc power from buses that are ultimately supplied by 4 kvac bus D1. The motor-driven feed pump derives breaker control power from dc bus DBN. The PORV, which may be used as the bleed path for makeup/HPI cooling, requires control power from dc bus D2N, and one makeup pump is supplied by dc bus D1P for breaker control power. Loss of power from bus D1 (e.g., due to bus D1 fault) could lead to depletion of the batteries that would supply power to these buses. In addition to affecting the availability of the motor-driven feed pump and makeup/HPI cooling, the flow control valves for the AFW supply to one of the steam generators would fail open upon loss of the dc power supply. Without operator action to control the turbine-driven pump for the affected AFW train, water carryover into the steam supply lines could cause loss of both turbine-driven pumps. Various options for changing procedural guidance or taking other steps to enhance the redundancy of the power supplies as they affect these options for core cooling are being investigated.

Shedding of dc loads. Procedural guidance for load shedding to preserve the dc supply from the batteries is only discussed for the case when ac power is unavailable to both divisions (and the respective chargers). Analysis of the IPE results identified cases in which load shedding in the event of a loss of only one electrical side could be valuable in delaying loss of dc power to provide more time for restoration of ac power.

BWST refill options. For some sequences involving steam generator tube ruptures, the BWST inventory could be depleted by injection before the RCS was depressurized sufficiently to terminate the flow through the broken tube. For most such sequences, the

break flow would be substantially reduced from its initial level, and providing makeup to the BWST could provide ample time for taking measures needed to complete the cooldown and establish shutdown cooling. While means are available to provide water to refill the BWST, there is no explicit procedural guidance for taking that step. Consideration will be given to enhancing procedures or training to cover such long-term contingencies.

Sump recirculation using the makeup system. Emergency procedure guidance currently prohibits using the makeup pumps to perform high pressure recirculation from the containment sump (Ref. 4). Thus, although the makeup system serves as a potential backup to the HPI system for injection from the BWST, it was not considered as an option for long-term recirculation after the BWST was depleted. Modifying or removing this prohibition may reduce the potential for some high pressure core-damage sequences. Consideration will be given to a review of technical issues, including pump capabilities (i.e. NPSH) and the required system lineup, and modification of the procedure.

Isolation of RCP seal return following loss of seal cooling. In developing the success criteria relating to preventing a small LOCA due to failure of the RCP seals, it was noted that available technical information indicated the potential for leakage to be reduced if seal return was isolated after tripping the pumps. This step is not covered in current procedures. The need for adding this step to appropriate procedures will be considered.

Service water room ventilation. The system procedure for service water requires that two fans in both ventilation trains be operable when outside ambient air temperature is above 86F. Under these conditions, one train of service water would be unavailable in the event that one fan fails. Consideration will be given to procedural guidance for establishing an alternate means of room ventilation, including the possibility of opening the door for the service water pump room, and steps that should be taken to preserve essential service water flow if adequate room cooling cannot be established to maintain operation of both trains.

Fuel oil for the station blackout diesel generator. The station blackout diesel generator provides additional redundancy in the event of a loss of offsite power coincident with a loss of one or both emergency diesel generators. Its usefulness is somewhat limited due to the amount of fuel oil available to supply it. The supply is typically equivalent to between 4 and 8 hours of run time for the generator. Provisions to replenish fuel oil should be considered and included in appropriate procedures.

3.2 Insights Gained from the Back-End Analysis

During performance of the containment analysis portion of the IPE, insights relating to both short-term and long-term measures that might be taken were identified. These insights are summarized below.

BWST level at switchover to sump recirculation. Currently, procedures call for initiating the switchover from the BWST to the containment emergency sump as the

suction source for injection to the RCS at a level of 8 ft in the BWST. This would leave roughly 105,000 gallons of unused inventory in the tank. It may be possible (e.g., for scenarios other than those involving large LOCAs) to reduce this level to optimize use of available water. This would also serve to extend the time period to accomplish potential BWST refill actions.

Operator actions for inadequate core cooling. Sequences have been noted when analyzed with MAAP in which different timing of operator inadequate core cooling (ICC) actions, and particularly those related to RCS depressurization and restarting the RCPs, would have delayed the onset of serious core damage. There are also concerns regarding the effect of RCP restarts on creep rupture of the steam generator tubes or RCS piping for high pressure accidents. As such, an overall review of ICC operator actions may be prudent. This may best be conducted in conjunction with B&W Owners Group severe accident management activities.

Emergency plan evaluation criteria. With more realistic accident source terms now available, re-examination of current evaluation criteria should be accomplished to ensure consistency with current source term expectations for severe accidents.

Monitoring of carbon monoxide levels in containment. If core-concrete interactions occur in a severe accident, significant amounts of flammable carbon monoxide would be generated. Consideration of carbon monoxide as well as hydrogen may need to be incorporated into emergency plan evaluation criteria or severe accident management criteria. This may be best handled under ongoing severe accident management work by the B&W Owners Group.

REFERENCES FOR PART 6

1. Crutchfield, D. M. "Individual Plant Examination for Severe Accident Vulnerabilities." U.S. Nuclear Regulatory Commission Generic Letter 88-20, November 23, 1988.
2. *Individual Plant Examination: Submittal Guidance*. U.S. Nuclear Regulatory Commission Report NUREG-1335, August 1989.
3. *Severe Accident Issue Closure Guidelines*. Nuclear Management and Resources Council Report 91-04, January 1992.
4. "RPS, SFAS, SFRCS Trip, or SG Tube Rupture". Davis-Besse Nuclear Power Station Emergency Procedure DB-OP-02000, June 18, 1990.

Part 7
SUMMARY AND CONCLUSIONS

Contents

<u>Section</u>	<u>Page</u>
1 SUMMARY OF RESULTS FROM THE IPE	1
1.1 Results from the Front-End Analysis	1
1.2 Results from the Back-End Analysis	5
2 CONCLUSIONS	11

List of Illustrations

<u>Figure</u>	<u>Page</u>
7-1 Breakdown of Core-Damage Frequency by Category of Initiating Event	2
7-2 Overall Conditional Probabilities for Containment Failure Modes	6
7-3 Overall Conditional Probabilities for Release Categories Given Core Damage	9

Section 1 SUMMARY OF RESULTS FROM THE IPE

The PRA performed to satisfy the intent of the IPE provided a perspective on the types and frequencies of severe accidents that could be important for Davis-Besse. The analysis process and results also yielded insights into features of the plant design and operating practices that may enhance the ability to prevent or respond to severe accidents in the future. This section summarizes the results of the assessment of core-damage sequences (the front-end analysis) and the evaluation of containment response (the back-end analysis). Section 2 outlines conclusions developed through this examination. Sections 4.1 of Part 3 and Sections 6.3 and 7.2 of Part 4 describe the study results in more detail.

1.1 RESULTS FROM THE FRONT-END ANALYSIS

The total core-damage frequency was estimated to be 6.6×10^{-5} per year. As shown in Figure 7-1, most of this frequency was assessed to be due to sequences initiated by transients, with the remainder divided among loss-of-coolant accidents (LOCAs), steam generator tube ruptures (SGTRs), and internal floods.

The frequency of core damage resulting from transients was determined to be due largely to two types of functional sequences. The first sequence involves loss of heat removal via the steam generators and failure of direct core cooling by injection from the makeup system, with decay heat removed through the pressurizer relief valves (a mode of cooling referred to as makeup/HPI cooling). This functional sequence would entail a loss of main feedwater, either as an initiating event or as a consequence of another initiating event. All three of the pumps in the auxiliary feedwater system (two turbine-driven and one motor-driven) would have to be unavailable to supply backup flow to the steam generators. Finally, makeup/HPI cooling, which can be accomplished by various redundant pathways, would have to fail. This sequence contributed about 50% of the total core-damage frequency.

Many different types of minimal cut sets contribute to this functional sequence, and no single or small number of plant features stands out. Many of the cut sets, however, share one of two characteristics that provide a link between the failure of feedwater for heat removal by the steam generators and the failure of makeup/HPI cooling. The first characteristic involves the need for certain operator actions. Among the important causes of failure of auxiliary feedwater are the failure of the operators to start the motor-driven feed pump if the turbine-driven pumps were not available, and the failure to control the turbine-driven pumps manually if automatic control were to fail. Makeup/HPI cooling would also require manual initiation. Although each of these actions was assessed to be reliable individually because of the availability of proper training and procedural guidance, a relatively high level of dependence was assessed between the failures related to the auxiliary feedwater system and the failure to initiate makeup/HPI cooling. This was particularly the case for the failure to start the motor-driven feed pump, since both that action and the need for makeup/HPI cooling would be

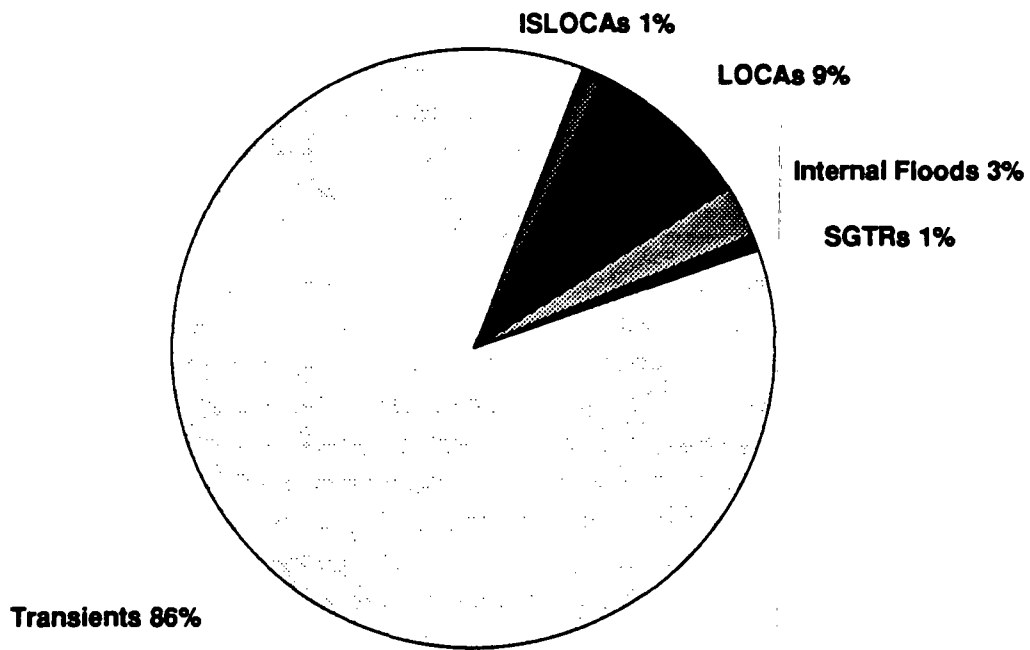


Figure 7-1. Breakdown of Core-Damage Frequency by Category of Initiating Event

direct responses to the loss of feedwater from other sources. Therefore, the cut sets involving combinations of these interactions were among the important contributors to the sequence frequency.

The second characteristic shared by some of the cut sets was a dependence on support systems. In this case, ac and dc power were especially important. In the event of loss of one of the two trains of safety-related dc power, the flow control valve for one train of turbine-driven auxiliary feedwater would fail open. Without operator action, the steam generator being supplied by that train could be overfed and, because of cross-connections in the steam supplies for the turbine-driven pumps, both pumps could be affected by water carryover into the steam lines. Depending on the specific power supply that was affected, the loss of dc power could cause unavailability of the pilot-operated relief valve, which could otherwise provide one of the paths for removing decay heat during makeup/HPI cooling. Makeup/HPI cooling could also be affected if the dc supply that was lost would cause unavailability of the control power needed to start one of the makeup pumps. The action to control the affected train of turbine-driven auxiliary feedwater manually was assessed to be reasonably reliable, since it is thoroughly documented in the emergency procedure, is practiced, and has been used during upsets involving the control system in the past. Nevertheless, the dependence on dc power provided another link between the two possible modes of core cooling following loss of main feedwater. A failure of dc power could result from an initiating bus fault, from other system faults, or due to battery depletion following loss of offsite power and failure of one of the diesel generators. The latter would also reduce the availability of the makeup system as well, since both makeup pumps are motor-driven.

Sensitivity studies were performed to aid in understanding these contributions. For example, the reliability of the human action to start the motor-driven feed pump and of the combinations involving that action and the initiation of makeup/HPI cooling were varied to determine if a change such as automating the starting of the motor-driven pump would be of significant benefit. None of the sensitivity studies that was performed indicated that substantial reductions in core-damage frequency would be obtained by making the implied changes.

The second type of transient-initiated sequence that was a significant contributor to the core-damage frequency was a loss of seal cooling for the reactor coolant pumps (RCPs), leading to a small LOCA due to failure of the seals, followed by failure to maintain adequate RCS inventory (i.e., failure of safety injection). For a seal LOCA to occur, the RCPs would have to continue operating while seal cooling was lost or degraded. Seal cooling is normally supplied by both injection from the makeup system and component cooling water (CCW). Loss of both these sources of cooling, or failure to maintain adequate seal return flow, could lead to degradation of the three stages of the seals. This sequence was responsible for approximately 20% of the total core-damage frequency.

The potential for failures of support systems played a dominant role for this type of sequence. Component cooling water is required for cooling of the pumps in both the makeup and HPI systems. Thus, if the CCW system were to fail, both sources of seal cooling (i.e.,

CCW and seal injection from makeup) would be lost, and there would be no means for safety injection at high pressure. Loss of cooling by the CCW system could also result from loss of the service water system, which serves as the heat sink for the CCW system. Both of these systems have significant redundancy, but they could be subject to common-cause failures. Various failures of the operators to restore cooling flow and to trip the RCPs when required are also important elements of the cut sets for this sequence.

Other types of small LOCAs have been found to be important at some PWRs. The frequency of core damage due to small LOCAs is relatively small for Davis-Besse for a variety of reasons, but partly because both the HPI and makeup systems can provide adequate control of RCS inventory, offering a degree of redundancy and diversity. In the long term, it would generally be possible to cool down to conditions at which core cooling could be provided by the decay heat removal (DHR) system, or high pressure recirculation could be established. For medium and large LOCAs, the dominant contributors were primarily common-cause failures or failures of the operating staff to establish recirculation. No individual failure modes were found to be particularly important.

Core-damage sequences initiated by SGTRs were also assessed to be relatively low in frequency. The primary reason for this was the very long time available for response in most cases. In general, the emergency procedure would lead to early cooldown to the point at which the steam generator containing the broken tube could be isolated, effectively terminating the leakage from the RCS. Even if this could not be accomplished for some reason, the borated water storage tank (BWST), which is the supply source for the injection systems, normally contains nearly 500,000 gallons of water. For most scenarios, the lowering of RCS pressure would cause the leak rate to be reduced to the point at which this volume would last for a period of days. This would afford ample time for response and recovery of affected equipment.

The assessment of interfacing-systems LOCAs drew heavily upon an investigation performed for a generic Babcock & Wilcox plant for the NRC. The frequencies of these LOCAs were assessed to be dominated by scenarios that would involve successful injection until the BWST contents were depleted. Therefore, in most cases there would be significant time for operator action to isolate the breaks. The generic assessment performed for the NRC was dominated by a scenario in which it was postulated that an operator error of commission could lead to premature entry into shutdown cooling while the RCS was still at high pressure. This scenario was reevaluated for applicability to Davis-Besse. There remains significant uncertainty with respect to whether or not it is credible for such an error to be made while RCS pressure is high enough to threaten the integrity of the DHR system. Nevertheless, it was retained and is the largest contributor to the frequency of core damage due to interfacing-systems LOCAs.

Internal flooding was also investigated in detail. Three areas were identified that were susceptible to flooding and that could have been important with respect to core damage: the room containing the service water pumps, the room containing the pumps and heat exchangers for the CCW system, and the rooms housing the HPI and DHR pumps. In the

event of loss of any of these areas, however, there would still be options for maintaining core cooling. Therefore, internal flooding was not found to be as important for Davis-Besse as it has been for some other plants.

Section 4 of Part 3 provides a much more detailed discussion of the important core-damage sequences, the plant features that contribute most to them, and the areas that were investigated with respect to potential plant changes. In summary, while some changes continue to be considered, none was judged to be necessary to address a vulnerability or was found to be clearly desirable from a quantitative or qualitative perspective.

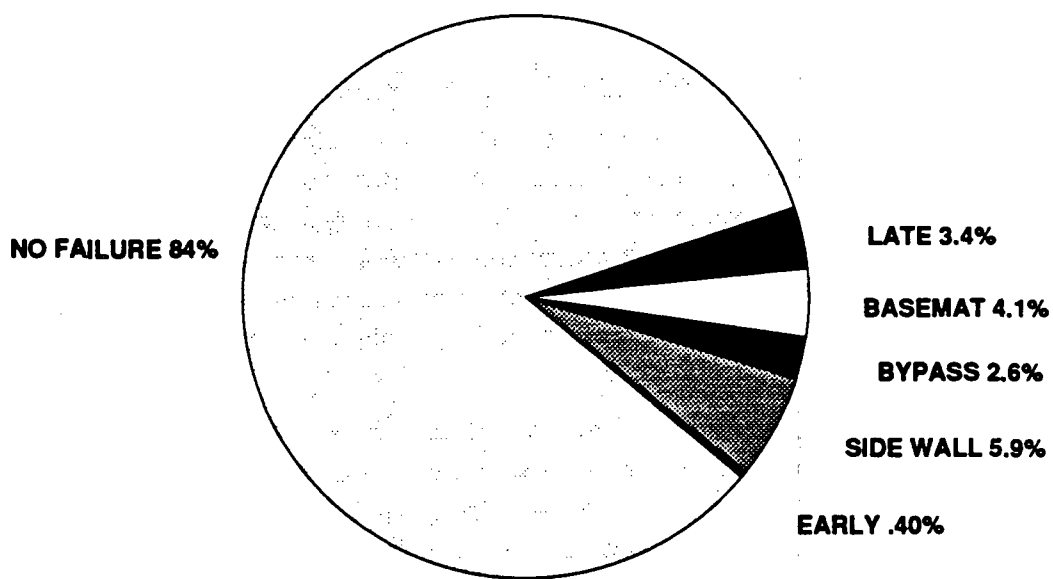
1.2 RESULTS FROM THE BACK-END ANALYSIS

The back-end analysis consisted of both extensive deterministic evaluations of containment response using the MAAP code and investigation of other possible accident progressions using a containment event tree. The calculations made using MAAP indicated that loadings due to severe accidents would remain within the capabilities of the containment for all accidents except those in which containment heat removal was unavailable; in that case, the containment could eventually overpressurize due to the evolution of steam and/or non-condensable gases.

Based on the quantification of the end states for the containment event tree, the conditional probabilities for various containment failure modes given core damage have been calculated. They are summarized in Figure 7-2. This figure indicates general consistency with the MAAP results; no containment failure is predicted for about 84% of the sequences that comprise the core-damage frequency. For those cases in which containment failure would not be expected to occur, the core debris would be in a cooled state and containment heat removal would be functioning to limit the pressure rise inside containment.

As it is used here, early failure is a broad category that includes failures of containment isolation, bypass sequences, and failures due to internal loadings prior to or around the time of failure of the reactor vessel due to the molten core debris. Most of this contribution (2.6% of the total 3%) is from bypass sequences. Nearly 80% of the contribution from bypass sequences is from interfacing-systems LOCAs and initiating SGTRs; the remainder stems from tube ruptures that result from failure of the tubes during core degradation. The remaining small fraction of early failures is spread among several categories of low-probability challenges, including early hydrogen burns, in-vessel and ex-vessel steam explosions, and the loading at vessel breach due to steam generation and direct containment heating. Isolation failures were assessed to contribute a negligible amount to the potential for releases from containment.

Side wall failure refers to the potential for attack of core debris on the containment wall itself. This could occur in the event of transport of a significant portion of the core debris from the reactor cavity up to the basement level of containment at the time of vessel failure. The area to which this dispersion would take place would be adjacent to the containment wall. The steel wall is protected by a concrete curb that is 1.5 ft thick and 2.5 ft high, so that direct



Note: Isolation failure is Negligible

Figure 7-2. Overall Conditional Probabilities for Containment Failure Modes

failure by the debris would not occur. If the core debris were cooled, as it would be expected to be for accidents in which the contents of the BWST were injected, no significant ablation of the concrete curb would be expected. If the debris were not cooled, however, the concrete could be ablated, leading to containment failure several hours after vessel failure.

Late failure would occur most frequently for cases in which no means of removing heat from containment was available. The generation of steam and/or non-condensable gases could eventually lead to overpressurization of the containment. A small contribution to late failure also results from the possibility of late burning of hydrogen and other combustible gases.

All sequences in which the core debris was not cooled but no other failure mode occurred were assigned to the category of basemat meltthrough. For some of these accidents, it is very likely that ablation of the concrete would cease before the basemat was penetrated, as decay heat diminished, cooling water was made available, etc. No attempt was made to discriminate these outcomes further.

The most important findings from the back-end analysis relate to the reasons that the containment was likely to retain its integrity for most types of accidents. Chief among these reasons is the very large free volume available in the containment. At $2.8 \times 10^6 \text{ ft}^3$, there is substantial margin to accommodate severe accident loadings without approaching pressures that would be likely to result in containment failure.

The geometry of the reactor cavity was also important. The cavity area is relatively large, so that even if the core debris were to be retained in the cavity, it is likely that it would form a coolable geometry. In addition, all areas of the containment drain eventually to the containment normal sump, which is located in the cavity region. Therefore, any water that is present in containment would be available for cooling debris in the cavity. If the contents of the BWST had been injected, a depth of water of approximately 25 ft would be present in the cavity. Even if only the original volume of the RCS and the core flood tanks were present, the debris would be covered by water at least 4 ft deep. This water would generally cause the debris to re-freeze, and with containment heat removal available, should allow a relatively stable condition to develop.

The cavity communicates with the containment basement primarily via the incore instrument tunnel. For accidents that would progress at relatively high RCS pressure (500 to 600 psig or greater), it is possible that debris would be dispersed to the basement. At that level, there would be an area over which the debris could spread even larger than the cavity. If the contents of the BWST were injected, there would be several feet of overlying water in that area as well. Therefore, a stable condition could be achieved similar to that in the cavity.

Because of the large volume of the containment, it would be very difficult for sufficient hydrogen to be generated or to accumulate to support a burn that could challenge the containment capacity. Similarly, pressurization due to direct containment heating or steam generation at vessel breach would not be likely to cause the capacity to be exceeded. Direct containment heating could be further limited because there would not be direct pathways for

finely fragmented fuel to be transferred efficiently from the basement to the upper regions of containment.

Failure of containment isolation was found to be a negligible contributor to the potential for releases from the containment. This is due in part to administrative controls, especially those that prevent using the containment purge lines during power operation. Other penetrations are well monitored.

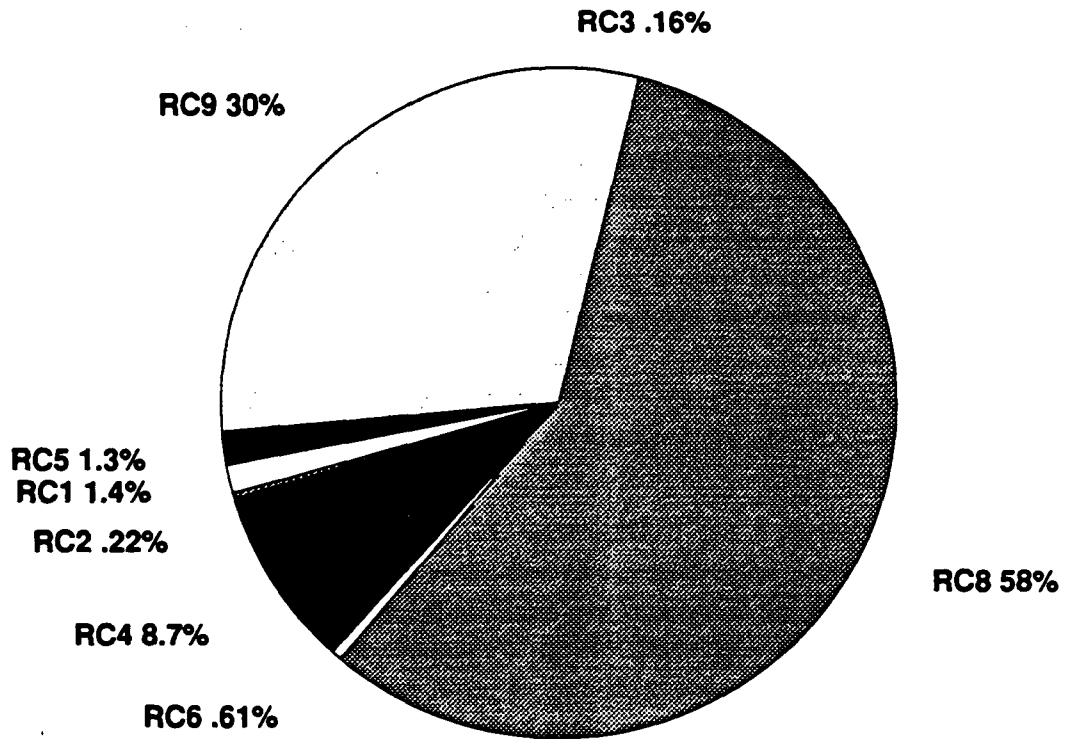
The possibility that core damage could be arrested prior to vessel breach was also considered. Two mechanisms were addressed in the containment event tree: restoration of cooling flow, such as by reducing RCS pressure sufficiently to allow low pressure injection; and cooling of debris, after it had slumped into the bottom head of the reactor vessel, via heat transfer to water surrounding the vessel.

Approximately 8% of the core-damage sequences led to conditions in which cooling was assessed to be restored while the core was still largely intact. Even in these cases, containment failure was still possible (e.g., due to burning of hydrogen generated during the initial degradation, or due to long-term overpressurization in the absence of containment heat removal). Direct containment heating and other loadings associated with vessel breach, as well as core-concrete interactions, would, however, be precluded.

The second possibility cited above refers to the potential for cooling by submergence of the reactor vessel. If the contents of the BWST were injected prior to vessel breach, the vessel would be flooded up to about the level of the nozzles for the hot legs. Because uncertainties remain regarding the manner in which this mode of cooling might work (for example, the debris might still attack the vessel at the bottom-head penetrations), no credit was given to this possibility in the base-case assessment. A sensitivity study was performed in which it was assumed to be very likely that this mode of cooling would succeed if the BWST contents were injected. In this sensitivity study, the fraction of sequences in which vessel failure was prevented increased from 8% to 29%. The overall breakdown of containment failure modes remained largely unchanged, however, since containment failure would not have been predicted for the majority of affected sequences even in the base case. The major impact would be to prevent relatively low-probability failure modes, such as pressurization at vessel breach or ablation of concrete in the cavity or basement in the presence of overlying water.

Each of the outcomes for the containment event tree (CET) was assigned to one of the release categories. The conditional probabilities for the outcomes were also combined according to the assigned release categories. The results, in terms of overall conditional probabilities of the release categories, are presented in Figure 7-3.

The results illustrated by this figure are consistent with those described above with respect to the relative frequencies of various containment failure modes. Release categories 8 and 9, which encompass scenarios in which the containment maintains its integrity (note that these categories also include basemat meltthrough cases), combine for approximately 88% of the overall frequency of core damage.



Note: RC7 is .0032%

Figure 7-3. Overall Conditional Probabilities for Release Categories Given Core Damage

Release category 1 would be used for the most severe releases, and includes bypass sequences in which there would be limited scrubbing of fission products. The contributors to the frequency of this release category are steam generator tube ruptures (either as initiating events or due to creep rupture of tubes during core degradation) and interfacing-systems LOCAs which were not effectively scrubbed. Slightly more than 1% of the total core-damage frequency was assessed to result in releases in this category.

Release categories 2 and 3 would include early containment failures (other than bypass sequences), without and with removal of fission products by containment sprays, respectively. For these release categories, the releases would not include a significant component due to ex-vessel releases associated with core-concrete interactions. These release categories combine to account for only about 0.4% of the total core-damage frequency.

Release category 4 encompasses CET outcomes in which there is a failure of containment in conjunction with an ex-vessel release of fission products due to core-concrete interactions, under conditions in which scrubbing of fission products would not be available. This release category would include accidents that would involve dispersal of core debris to the basement level, followed by ablation of the concrete curb protecting the containment wall due to failure of ex-vessel cooling. Approximately 9% of the core-damage frequency was assigned to this release category. Release category 5 includes the remainder of the interfacing-systems LOCAs, which would be subjected to scrubbing by overlying water in the auxiliary building.

Release categories 6 and 7 correspond to late containment failures with and without fission-product scrubbing, respectively, and without ex-vessel release of fission products. The frequencies of these release categories are small, in large part because the frequency of late failure is relatively small, and much of the frequency of longer-term releases would be associated with conditions in which failure of ex-vessel cooling would lead to additional releases of fission products due to core-concrete interactions (and, consequently, to assignment to release category 4).

The results of the back-end analysis are discussed more fully in Sections 6 and 7 of Part 4 of this submittal. Although a broad range of potential challenges to containment integrity were identified and investigated, the containment was generally found to be capable of accommodating those challenges. No vulnerabilities or serious weaknesses were identified relative to containment response.

Section 2 CONCLUSIONS

The Toledo Edison Company has completed a level 2 probabilistic risk assessment of the Davis-Besse Nuclear Power Station. This report has described the results and demonstrated compliance with the information requested by the Nuclear Regulatory Commission's Generic Letter 88-20. As has been shown, in addition to satisfying the NRC's request for an IPE, the following technical objectives have also been met:

- To apply state-of-the-art PRA techniques to develop a more current understanding of the types of severe accidents that could be important for Davis-Besse,
- To identify any areas in which there might be the need or opportunity to reduce the frequency of core damage or of serious radiological releases in a cost-effective manner, and
- To provide the plant-specific inputs for an accident-management program.

Several additional objectives that affected the manner in which the PRA was structured and implemented to meet these overall objectives were identified and have also been achieved. These additional objectives included the following:

- To develop a model for Davis-Besse that could be readily updated in the future, as changes are made to the plant or as additional insights into severe accident behavior become available, so that the model and results could be applied to address safety and regulatory issues as they arise;
- To continue to develop the expertise within the Toledo Edison Company necessary to perform the analyses for the IPE and to use them in these future applications; and
- To document the analyses in a manner that would both make the future applications tractable and provide the necessary bases for external reviewers to determine that the work had been accomplished in a thorough and competent manner.

The results of the study include the definition and quantification of potential accident sequences that could result in core damage, as well as an evaluation of the accident progression, resultant containment response, and potential radionuclide releases.

Overall, no vulnerabilities were found to be present at Davis-Besse. Neither the core-damage frequency nor the frequency of serious releases is high relative to risk estimates generally obtained for other plants. Although a small number of sequences is responsible for a large fraction of the core-damage frequency, examination of these sequences indicates that there are many individual contributors to their frequencies, and no single or small number of features contributes an inordinate fraction of the total core-damage frequency. Furthermore, although there are, as in any PRA, uncertain aspects of the plant models or data that, if assessed differently, could result in higher (or lower) estimates of core-damage frequency,

none is considered to be both so uncertain and potentially able to produce such a large contribution to core-damage frequency that it should be considered to be a vulnerability.

Efforts are ongoing to evaluate various options to enhance plant operations further based on risk insights gained during development of the IPE. These insights, which are described further in Part 6 of this report, relate to the following areas:

- Improved redundancy in the electrical supplies needed to support the feedwater and makeup/HPI cooling options,
- Procedures for shedding dc loads when only one division is lacking ac power to its charger,
- Options for restoring inventory in the BWST during long-term demands, such as for steam generator tube ruptures,
- Measures to enhance availability of the service water system when there are failures of ventilation for the service water pump room,
- Provisions for ensuring a long-term supply of fuel oil is available for the station blackout diesel generator,
- The possibility of using the makeup system for high pressure recirculation from the containment sump,
- Optimization of the use of BWST inventory prior to switchover to recirculation from the sump,
- Operator actions during conditions of inadequate core cooling that could enhance response to a severe accident,
- The use of more realistic source terms for assessment of actions associated with emergency planning, and
- Monitoring of carbon monoxide in containment, in addition to hydrogen, during post-accident conditions.

Based on the outcome of these evaluations, appropriate changes will be implemented on a timely basis. All insights will also be considered in conjunction with other severe accident management inputs being developed through the Babcock & Wilcox Owners Group.